3) Место протокола IP в модели OSI и стеке TCP/IP

Согласно модели OSI (Open Systems Interconnection) все программное обеспечение системы, делится на 7 уровней, для каждого из которых в рамках модели определены выполняемые функции и интерфейсы. Итак УРОВЕНЬ - это набор правил, соглашений, направленных на решение определенной группы задач.
В модели OSI протокол IP находится на сетевом уровне, а в стеке TCP/IP – на уровне сети Интернет
Уровень N оказывает услуги уровню N плюс 1 и получает услуги, от уровня N минус 1.

4) Назначение

- Протокол IP обеспечивает передачу блоков данных, называемых дейтаграммами, от отправителя к получателям, где отправители и получатели являются компьютерами, идентифицируемыми адресами фиксированной длины (*IP-адресами*).
- Протокол IP поддерживает сервис сетевого уровня без установления соединения, и поэтому доставка им сообщений по сети рассматривается как ненадежная. После того, как дейтаграмма отправляется в сеть, ее дальнейшая судьба никак не контролируется отправителем (на уровне протокола IP). Если дейтаграмма не может быть доставлена, она уничтожается. Узел, уничтоживший дейтаграмму, может оправить по обратному адресу ICMP-сообщение о причине сбоя.

- Протокол IP обеспечивает при необходимости также фрагментацию и сборку дейтаграмм для передачи данных через сети с малым размером пакетов.

5) При прохождении данных через уровни OSI используется концепция инкапсуляции: уровень получает данные от вышележащего уровня, помещает их в оболочку, которая представляет собой некоторую информацию, которая предназначена одноименному уровню в другой системе. Оболочка не изменяется нижележащими уровнями, через которые эти данные передаются.
Для сети ARPANet кроме протокола IP, не обеспечивающего гарантированное качество обслуживания, был разработан протокол верхнего уровня – TCP (Transmission Control Protocol) -протокол управления передачей, который гарантировал определенное качество обслуживания, а так же целостность сообщений.
Набор протоколов TCP/IP, а позднее и UDP получили название стека протоколов IP.
В стеке протоколов TCP/UDP/IP три верхних уровня модели OSI не разделяются и рассматриваются как единый прикладной уровень, на котором находятся такие прикладные сервисы, как служба имен доменов DNS, протокол передачи файлов FTP, электронная почта e-mail, протокол инициирования сессий SIP, протокол передачи в реальном времени RTP и др. .

Протоколы TCP, UDP, SCTP являются протоколами транспортного уровня стека протоколов IP.
Протокол IP поддерживает сервис сетевого уровня без установления соединения, и поэтому доставка им сообщений по сети рассматривается как ненадежная.

6) В транзитных узлах (маршрутизаторах) прикладной и транспортный уровни отсутствуют. Сегменты, сформированные на транспортном уровне передаются на сетевой. Основная задача протокола – обеспечить доставку данных по сети на основании IP адреса. То есть нет гарантии доставки, гарантии последовательной доставки, нет подтверждений, нет контроля ошибок. Решением всех этих проблем занимается верхний уровень.

IP-адрес позволяет определить компьютер, производящий обмен данными, и подразумевать конкретного человека, которые имеет доступ к данному компьютеру. IP-адрес называется динамическим, когда пользователю провайдер временно (на время непрерывного обмена данными) предоставляет один из списка публичных адресов. Благодаря раздаче IP-адресов регистраторами, известны физические адреса провайдеров и их сетей, на основе которых можно определить приблизительное местоположение компьютера по IP-адресу.

7) Выделением и регистрацией IP-адресов в Интернете занимаются организации, именуемые регистраторами IP-адресов (IP Registry). Это организации, являющиеся органами самоуправления Интернета.
IANA выделяет самые крупные блоки IP-адресов региональным регистраторам и большим организациям
RIR выделяют крупные и средние блоки адресов местным регистраторам (LIR), а также ведут базу данных выделенных IP-адресов и предоставляют доступ к ней.
LIR выделяют мелкие блоки IP-адресов операторам связи и потребителям и регистрируют их в базе данных своего регионального регистратора. Как правило, роль местного регистратора исполняет оператор связи (интернет-провайдер). Таких регистраторов несколько тысяч. Все выделенные IP-адреса регистрируются в специальной базе данных, которую поддерживает региональный регистратор (RIR). Сведения из этой базы данных (за исключением некоторых полей) доступны любому лицу по протоколу whois.

8) Для того чтобы пользователям не приходилось держать в памяти IP-адреса применяет служба доменных имен (DNS). Однако не всегда доменное имя равнозначно соответствует определенному IP-адресу.
Для крупных интернет-ресурсов типична ситуация когда по одному доменному имени, например, социальной сети вконтакте (или поисковика яндекса) - выдается несколько IP-адресов - распределяющих нагрузку серверов ("зеркал").
Для небольших интернет страниц встречается обратная ситуация, когда на одном сервере компании хостинга (например, sprinthost) располагается несколько ресурсов по одному IP-адресу, но с различными доменными именами: videodiscovery, topshef,

fitdeal, carhappy, business100-idei. В последнее время, данных подход сталкивается с проблемой, когда Россвязьнадозор вносит один из сайтов в черный список по доменному имени, а провайдеры блокируют его по IP-адресу. Что в свою очередь вызывает блокировку все интернет страниц расположенных по данному IP-адресу.

Несмотря на то, что публичные IP-адреса раздаются регистраторами, в само устройство IP-адрес назначается вручную при его настройке, либо при использовании специальных протоколов раздачи IP-адресов. Однако, диапазон раздаваемых IP-адресов, все так же настраивается вручную, но уже не пользователем, а администратором сети.

В начале XXI века наибольшее распространение получили протоколы автоматической раздачи адресов DHCP и загрузки по сети BOOTP.

9) Протокол нижележащего и вышележащего уровня OSI

Транспортный уровень (вышележащий) пользуется следующими услугами IP

- Определения пути передачи данных (маршрутизации).
- Передачу данных сегмента по сети от отправителя к получателю.
- Осуществление фрагментации при необходимости.
- Отслеживание неполадок.

Примеры протоколов:TCP, UDP, SCTP и т.д.

Канальный уровень (нижележащий) предоставляет IP следующий функционал

- Организации локальных и магистральных сетей передачи данных.
- Управление логическим каналом.
- Обеспечивает проверку и правильность передачи информации по соединению.

Примеры протоколов: Ethernet (IEEE 802.2), Fiber Distributed Data Interface, ARP и т.д.

10) Стандартизирующие документы

Протокол IP (Internet Protocol) - протокол интернет: Определен в RFC-791 - 1981 год, Университет Южной Калифорнии, его автор Jon Postel.
Формат заголовка протокола IPv4 используется до сих пор. Еще в 1981г. были описаны основные классы IP-адресации. В протоколе изначально заложен механизм дифференциального обслуживания(ToS). IP поддерживает возможную фрагментацию пакетов и ограничивает время жизни пакетов.
В 1981г. IP стандартизирован RFC-791, автор которого Jon Postel, из Университета Южной Калифорнии, США. (обновлен в 1349, 2474, 6864)
В 1992г. выходит обновление механизма ToS в RFC-1349. Затем 1998г. в RFC-2474 для IPv4 и IPv6 (DCSP).

11) В 1994г. определяются диапазоны адресации для частных адресов компаниями IBM, Chrysler и координационным центром Интернет RIPE в RFC-1597. Документ был обновлен в 1996г. в RFC-1918, и в 2013г. с учетом доменных имен компанией Apple в RFC-6761.
В 2002г. компания Motorola вводит замену ToS на DiffServ(другая классификация трафика) в RFC-3260.
В 2002г. IANA выделяет специальные IP-адреса в RFC-3330, который был обновлен в 2010г. в RFC-5735, 2012г. в RFC-6598 и 2013г. в RFC-6890.
В 2005г. компания BBC Technologies описывает архитектуру безопасности (IPSec) для протокола IP в RFC-4301.
В 2013г. Университетом Южной Калифорнии обновляется документация по применению поля идентификации фрагмента пакета (ID) в RFC-6864.

12) Адресация

Для адресации устройств в IP сети каждому устройству присвоен свой уникальный адрес. В протоколе IPv4 для записи адреса используется 32 бита (4 байта), в IPv6 – 128 бит. IP адрес обычно представляется в виде четырех десятичных чисел, разделенных точками. Каждое число может принимать значение от 0 до 255.
IP адресация так же как и сеть имеет иерархическую структуру. И состоит из идентификатора сети (NETID), к которой подключен хост, и идентификатора хоста внутри сети (HOSTID).
Каждый IP-адрес включает идентификатор сети (NETID) и идентификатор сетевого узла (HOSTID). Идентификатор сети (также называется сетевым адресом) определяет системы, расположенные в одной физической сети, ограниченной IP-маршрутизаторами. Все системы в одной физической сети должны иметь одинаковый сетевой идентификатор, уникальный для всей сети.
Каждый IP-адрес имеет длину 32 бита и состоит из четырёх 8-битных полей, называемых октетами (octets), которые отделяются друг от друга точками. Каждый октет представляет десятичное число в диапазоне от 0 до 255.

Например, имеется адрес 192.168.10.1 - или 11000000 10101000 00001010 00000001 - всего 32 бита или 4 октета.
Например, если сетевая часть состоит из первых 3х октетов: 192.168.10 - или 11000000 10101000 00001010 - всего 24 бита, то считается что компьютер находится в IP-сети с адресом 192.168.10.0.

13) Существует пять классов адресов от A до E.
Класс A используется в очень больших сетях, класс B в среднего размера сетях, класс C в небольших подсетях.

IPv4-адресс составляет 32 бита (4 байта).
В классе A - зарезервирован под класс 1 бит - NETID - 8 бит (126 сетей), HOSTID - 24 бита (16 000 000 узлов).

В классе B - зарезервированы 2 бита под класс - NETID - 16 бит (16 000 сетей), HOSTID - 16 бит (65 000 узлов).
В классе C - зарезервированы 3 бита под класс - NETID - 24 бита (2 000 000 сетей), HOSTID - 8 бит (254 узлов).
В классе D - зарезервированы 4 бита под класс, сам адрес мультикаст рассылки из 28 бит.
В классе E - зарезервированы 5 бит под класс, 27 бит зарезервировано.
Мультикаст рассылка (или отправка пакетов группе пользователей) активно используется провайдерами для экономии пропускной способности при вещании телеканалов (IPTV).

К специальным адресам можно отнести: 0.0.0.0 - адрес шлюза по умолчанию, 255.255.255.255 – широковещательный адрес для всех узлов локальной сети отправителя, но в другие локальные сети пакет не отправляется
Существуют определенные адреса, которые не могут быть присвоены узлам по различным причинам. Имеются также специальные ip адреса, которые могут быть присвоены узлам, но с ограничениями на то, как те узлы могут взаимодействовать в пределах сети.

14) Существуют несколько типов адресов IPv4: индивидуальный, групповой и широковещательный. Индивидуальный назначается одному сетевому интерфейсу, расположенному в определенной подсети данной сети, и используется для подключений типа «точка-точка».
Групповой назначается одному или нескольким сетевым интерфейсам в различных подсетях данной сети, и используется для подключений типа «точка - многие точки».
Широковещательный назначается всем сетевым интерфейсам, расположенным в подсети данной сети, и используется для подключений типа «точка - все точки подсети».

Имеется сеть 10.0.0.0, в которой NETID - 10.0.0, а HOSTID - 0. Широковещательный адрес в такой сети имеет HOSTID - 255, т.е. имеет значение 10.0.0.255. Адрес хоста сети 10.0.0.0 должен иметь HOSTID от 1 до 254, т.к. значения 0 и 255 уже заняты под адрес сети и широковещательный адрес.

15) Специальные адреса IPv4
Когда NETID - 127. , а HOSTID - любой: адрес сетевой петли (loopback), применяемый как локальный адрес внутри устройства или для тестирования сетевых устройств.
127.0.0.1 - адрес тестирования в пределах одной машины, данные не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые.
Существуют еще блоки адресов, зарезервированные для использования исключительно для примеров в документациях.
В руководстве RFC5737 дается указание не использовать их при адресации интернет и локальных сетей.

- 192.0.2.0/24 TEST-NET-1
- 198.51.100.0/24 TEST-NET-2

- 203.0.113.0/24 TEST-NET-3

Первый из указанных блоков был исключен из списка запрещенных при адресации, но его использование нежелательно.
Для того, чтобы не допускать возможность конфликтов при последующем подключении сети к интернету, рекомендуется применять в локальных сетях только следующие диапазоны так **называемых частных IP-адресов** (в интернете эти адреса не существуют и
использовать их там нет возможности). К частным IP-адресам (внутренним, виртуальным, плюшевым) относят следующие диапазоны:

- 10.0.0.0 - 10.255.255.255,
- 172.16.0.0 - 172.31.255.255,
- 192.168.0.0 - 192.168.255.255

16) Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Маска подсети показывает, где в IP-адресе номер подсети, а где номер хоста.
Структура маски:

- Единицы в позициях, задающих номер сети.
- Нули в позициях задающих номер хоста.

Способ получения номера сети: побитовое сложение IP-адреса и маски подсети
Например, если адрес 213.180.193.3 ассоциировать с маской 255.255.255.0, то номером сети будет 213.180.193.0, как это и определено системой классов. В масках количество единиц в последовательности, определяющей границу номера сети (NETID), не обязательно должно быть кратным 8, чтобы повторять деление адреса на октеты/байты. Маски кратные 8 битам назваются фиксированными, а не кратные - масками переменной длинны (VLSM, variable lenght subnet mask). У сетевой маски имеется упрощенный формат записи по числу единиц, входящих в маску. Например, маску 255.255.255.0 можно записать как /24, т.к. маска состоит из 24 единиц.

17) При классовой адресации сетей, маска сети определяется на основе адреса (его класса).
Например, в сети класса B(NETID=16 бит) адрес узла - 172.16.30.10, а маска должна иметь 16 единиц.
Эта маска в десятичной форме будет выглядеть как: 255.255.0.0.
Таким образом получаем: NETID = 172.16.0.0, HOSTID = 0.0.30.10 .
Все это означает, что сетевые узлы в IP-адресе которых значится 172.16. ... смогут обмениваться пакетами без применения маршрутизатора, независимо от 3й десятичной цифры адреса (чего не может быть при маске в 24 единице, классе C). Для приведенного рисунка это все 3 компьютера и маршрутизатор.

Рассмотрим как передаются пакеты между сетями с различными NETID. Для этого на компьютерах прописаны маршруты по-умолчанию (или другие маршруты) ведущие к шлюзу выхода из их подсети (к маршрутизатору). Маршрутизатор на основе таблицы

маршрутизации перенаправляет пакеты в следующую сеть с своего IP-адреса который ей принадлежит, в соотвествии с маршрутом, чтобы пакет попал в пункт назначения. Однако, если необходимо разбить такую сеть на подсети, нужно задать маску с большим количеством единиц. Например, для адреса 172.16.30.20 маску 24 единицы (255.255.255.0). Тогда, NETID = 172.16.30.0 (HOSTID = 0.0.0.20), что означает что обмен пакетами без помощи маршрутизатора будет осуществляться только в этой сети.

18) Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации.
При разбиении на подсети, осуществляется планирование подсетей.
Задача администратора сети разбить сеть 201.222.5.0 на 1 магистральную подсеть, и 2 подсети пользователей, таким образом, чтобы в пользовательских подсетях было 5 узлов. Подсети объединены 2 маршрутизаторами, и имеют 1 маршрутизатор верхнего уровня для выхода в вышележащие сети.
Администратор применяет маску = 29 (255.255.255.248), таким образом производит разбиение на подсети с адресами: 201.222.5.0, 201.222.5.8(обратите внимание, что это адрес сети - HOSTID), 201.222.5.16 и так далее.
В таких сетях на HOSTID остается 3 бита: - 7 адресов, из которых 1 адрес сети, 5 адресов узлов и 1 адрес широковещательный в данной сети. Например, адрес сети - 201.222.5.8, широковещательный адрес этой сети 201.222.5.15, адрес одного из узлов сети - 201.222.5.14, при этом HOSTID = 0.0.0.6.
В масках переменной длинны (VLSM) количество единиц в последовательности, определяющей границу номера сети (NETID), не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

19) Зная IP-адрес и маску можно определить не только адрес подсети, в которой расположен узел, но и широковещательный адрес (broadcast), а так же адреса первого и последнего узла в подсети. Широковещательный адрес рассылает пакеты всей подсети и не может быть назначен узлу, так же как и адрес сети.
Например, имеется IP-адрес 201.222.5.10/29 , с указанием маски в 29 единиц. Сетевая маска /29 - соответствует 11111111.11111111.11111111.11111000, или 255.255.255.248, что означает что 3 последние бита адреса определяют HOSTID. После логического умножения IP-адреса с маской, получаем 11001001.11011110.00000101.00001000
Число бит относящееся к NETID определяется классом адреса или сетевой маской. В свою очередь размер HOSTID задает максимальное количество узлов в подсети с таким идентификатором согласно формуле (2 в степени n) - 2. Чем больше бит в NETID, тем меньше остается бит для HOSTID.
Например: маска 255.255.255.248 (/29), тогда к HOSTID относится 32-29 = 3 бита. Согласно формуле 2 в 3 степени дает 8 значений адресов. Но возможных узлов подсети меньше количества адресов на 2. Т.к. следует вычесть одно значение определяющее адрес подсети и одно значение для широковещательного адреса в подсети - получается 8 - 2 = 6 - максимальное количество хостов в подсети. Из такого правила имеется исключение, когда применяются маски в 31 или 32 единицы.

20) Большинство современных маршрутизаторов отлично работают и с масками /31, используя адрес подсети и broadcast в качестве адресов интерфейсов. Например, на Juniper и Cisco вы можете смело использовать маску /31, хотя Cisco при этом выдает предупреждение, а вот ZyXEL уже не дает выбрать маску /31.
Также достаточно часто используется маска /32. Во-первых, для всяких служебных нужд при адресации, т. н. loopback-интерфейсов, во-вторых, /32 — это подсеть, состоящая из одного хоста, то есть никакая и не сеть, в сущности. Чем чаще администратор сети оперирует не с группами хостов, а с индивидуальными машинами, тем менее сеть масштабируема. С пользователями лучше обращаться не индивидуально, а целыми подсетями, иначе сеть быстро станет неуправляемой.

21) Формат заголовка IPv4
V – Версия. 4 бита
IHL – Длина заголовка. 4 бита
ToS – Тип обслуживания. 8 бит (Указывает предпочтительные для данного пакета тип приоритета, задержку, пропускную способность и надежность)
TL – Длина пакета IP. 16 бит
ID – Идентификатор фрагмента. 16 бит
FL – Флаги. 3 бита
FO – Смещение фрагмента. 3 бита
ID, FL и FO Обеспечивают фрагментацию и сборку пакетов. Теоретически длина пакета может достигать 65535 байт. На практике все рабочие станции и маршрутизаторы работают с длиной, не превышающей 576 байт
TTL– Счетчик допустимого времени пребывания пакета в сети. 8 бит (Определяет время жизни пакета в сети, каждый маршрутизатор уменьшает значение поля на единицу и отбрасывает пакет, когда оно принимает значение 0
)
P – Протокол. 8 бит (Идентифицирует протокол верхнего уровня (TCP или UDP)
)
HC – Контрольная сумма заголовка. 16 бит
IP-address S – Адрес источника пакета. 32 бита
IP-address D – Адрес получателя пакета. 32 бита
IP-address S и IP-address D содержат адрес источника пакета и адрес получателя, на основании которых осуществляется маршрутизация пакета в соответствующее цифровое устройство
DATA– Данные

22) Заголовок пакета IPv4 содержит 20 байт, которые занимают служебные поля. Рассмотрим первые 2 байта.
Первое поле версия протокола(V) - 4 бита, указывает 4ю версию протокола IP. Поле IHL - 4 бита - длина заголовка.
Поле тип обслуживания(ToS) - 8 бит. Изначально был определен в RFC-791. Первые 3 бита определяют приоритет трафика (обычный, приоритетный, срочный, видео и

голос, видео, экстренные службы и прочее). Далее следует 3 флага: задержка, пропускная способность, надежность. Последние 2 бита зарезервированы.

23) Поле ToS всегда содержит 8 бит, однако с течением времени значения этих бит понимаются по-разному. Ранее было описано изначальное их назначение согласно RFC-791. Спустя 11 лет в RFC-1349 был добавлен еще один флаг - стоимость. В 1998г. в RFC-2474 введено понятие дифференцированного обслуживание, и значение бит в поле ToS подразумевает Differentiated Services Codepoint(DSCP) использующий 6 бит. Спустя 3 года в RFC-3168 задействуют оставшиеся 2 бит под уведомление о перегрузке (Explicit Congestion Notification, ECN).
Значения EC бывают: поток не поддерживает уведомления о перегрузке, подтвержденная перегрузка, поток поддерживает уведомления (причем последнее имеет два значения оставленные на усмотрение протоколов верхнего уровня, например, TCP)

24) После поля ToS в заголовке пакета IPv4 следует поле длинны пакета IP (TL) в 16 бит. Далее три поля определяют наличие фрагментации пакета, в случае если он был слишком велик для передачи:
ID - идентификатор фрагмента - 16 бит;
FL - флаги фрагментации - 3 бита(Flag1 - зарезервирован = 0, Flag2 - не фрагментировать, Flag3 - у пакета есть еще фрагменты);
FO - смещение фрагмента данных относительно данных первого пакета - 13 бит.

25) После полей фрагментации следует поле время жизни пакета (TTL) длинной в 8 бит. Данное поле предназначено для борьбы с последствиями возникновения сетевых петель. В случае возникновения сетевой петли, пакет начинает циркулировать по сети создавая паразитный трафик, которые в случае замкнутой петли может привести к перегрузке сети и оборудования. Обычно TTL устанавливается в значение 64 или 255. Время жизни пакета измеряется в количестве переходов через маршрутизаторы.
В представленном примере при изначальном времени жизни пакета = 10, пакет может пройти петлю из 3х маршрутизаторов 3 раза, после чего будет отброшен. Для 11 мегабитного потока это приведет к возникновению помимо 11 Мбит/с изначального потока еще 22 Мбит/с паразитного потока трафика. Но благодаря TTL сеть будет продолжать функционировать.
При отбросе пакетов с истекшим временем жизни маршрутизатор может отправить ICMP пакет отправителю, указав причину уничтожения пакета. На основании данной информации сетевой администратор может выяснить причину, по которой пакеты сбились с верного маршрута и совместно с другими администраторами устранить ее. Особую сложность представляет устранение сетевых петель большой протяженности.
За полем TTL следует поле протокола вышележащего уровня P - 8 бит. Обычно оно указывает на применение UDP(17) или TCP(6) протокола, OSPF(89) или других протоколов.

26) После поля протокола вышележащего уровня идет поле контрольной суммы заголовка IP - 16 бит, ее расчет будет показан далее.

Самые важные поля в заголовке IP это IP адреса - источника(source) и пункта назначения (destination) - каждый из 32 бит для IPv4. После этого уже следуют сами данные пакета.

Поле контрольной суммы (HC) учитывает значения всех полей заголовка IP: V, IHL, ToS, TL, ID, FL, FO, TTL, P, HC=0000 (hex), S-IPaddr, D-IPaddr. Для расчета контрольной суммы значения заголовков можно предствить группами hex кода по 16 бит. Эти группы подвергаются Hex-сложению, с переносом цифр в старший разряд. Однако в случае появления нового разряда, - двоичную единицу следует проссумировать с самым младшим разрядом (перенос старшего бита). Полученная сумма (в примере это 2544 (hex)) должна быть инвертирована в двоичном виде (дополнение до 1). В результате значение поля контрльной суммы будет равно DABB.

27) Принцип работы

Когда приложение решает отправить пакет по сети, то формируются служебные заголовки на 5-7 уровнях модели OSI, далее формирует заголовок транспортного протокола с указанием его логического порта отправителя и получателя. Логический порт получателя будет применяться для того чтобы потом можно было определить для какого приложения на удаленной стороне предназначена информация. Далее добавляется заголовок IP и IP-адреса, формируется заголовок Ethernet с MAC-адресами, и сетевая карта начинает генерировать синхропоследовательность и далее сам пакет со всеми заголовками.

Адаптивная маршрутизация основана на том, что маршрутизаторы периодически обмениваются специальной топологической информацией доступных сетях, а также о связях между маршрутизаторами. Недостатком таких алгоритмов является необходимость постоянной перезаписи таблиц маршрутизации.

Неадаптивная маршрутизация не принимает во внимание текущее состояние сети. Все маршруты рассчитываются до начала использования сети. Недостатком таких алгоритмов является невозможность реагирования на изменения топологии сети. Отказоустойчивость сводится к переходу на резервные маршруты в случае аварии или перегрузки, а после восстановления - возврату на основные маршруты.

Пакеты доставляются от отправителя к получателю через сетевые узлы (маршрутизаторы, router), которые на основании таблиц маршрутизации определяют путь до следующего узла. Пакеты хранятся в памяти, в очереде на обслуживание, или в случае ожидания подтверждения, или в ожидании восстановления канала передачи данных. При перегрузке очередей или сети, пакеты могут быть отброшены (удалены), что приведет к потере этих пакетов. Если трафик, поступающий в сетевой узел, превышает тот, который может быть обслужен, то в качестве технологии управления загрузкой сети может использоваться отбрасывание пакетов.

В сетях с коммутацией пакетов существует две технологии.

Первая технология - передача пакетов с установлением соединения. Перед транспортировкой пакетов, принадлежащих одному сообщению, осуществляется процедура установления соединения. После этого все пакеты к узлу назначения доставляются по одному и тому же виртуальному каналу.

Вторая технология - передача пакетов без установления соединения - метод дейтаграмм. Пакеты, принадлежащие одному сообщению, доставляются к узлу назначения по произвольным маршрутам. Примером такой сети является сеть на базе протокола IP

28) Алгоритм работы протокола IP

Маршрутизатор получает пакет, разбирает заголовок Ethernet, чтобы определить, что данный пакет адресован к маршрутизатору, разбирает заголовок IP чтобы посмотреть IP-адрес получателя, и на его основе с помощью таблицы маршрутизации выбирает верный маршрут следования пакета. Далее генерирует этот пакет с нового интерфейса, в соответствии с маршрутом, при этом формируя свой заголовок Ethernet с указанием своего MAC-адреса. Аналогично действует следующий маршрутизатор.
Когда пакет поступает на устройство назначения, то проверяется MAC и IP адреса, что этот пакет адресован данному устройству, после чего последовательно разбираются все заголовке вышележащих уровней и пользовательские данные - приложением, которое прослушивает указанный в пакете логический порт назначения.
Проверка пакета осуществляется по контрольной сумме, указанной в заголовке пакета
Для оповещения отправителя об удалении пакета используется протокол ICMP.
Таблица маршрутизации содержит четкие инструкции по маршрутизации пакетов, и формируется на основе таблиц составленных вручную сетевыми администраторами и таблиц формируемыми протоколами маршрутизации. В итоговую таблицу попадают только самые оптимальные маршруты с учетом приоритета того источника из которого они были получены.

29) Обеспечение QoS (Quality of services)

В настоящее время вместе с планомерным увеличением скоростей передачи данных в телекоммуникациях увеличивается доля интерактивного трафика, крайне чувствительного к параметрам среды транспортировки. Поэтому задача обеспечения качества обслуживания (**Quality of Service - QoS**) становится все более актуальной.
Сервисные модели QoS :

- Best Effort Service
- Integrate Service (IntServ)
- Differentiated Service (DiffServ)

30) Best Effort Service (Негарантированная доставка)

- Абсолютное отсутствие механизмов QoS.
- Используются все доступные ресурсы сети без какого-либо выделения отдельных классов трафика и регулирования.

- Считается, что лучшим механизмом обеспечения QoS является увеличение пропускной способности . Это в принципе правильно, однако некоторые виды трафика (например, голосовой) очень чувствительны к задержкам пакетов и вариации скорости их прохождения. Модель Best Effort Service даже при наличии больших резервов допускает возникновение перегрузок в случае резких всплесков трафика. Поэтому были разработаны и другие подходы к обеспечению QoS.

31) Integrate Service (IntServ)
Integrated Service (IntServ, RFC 1633) - модель интегрированного обслуживания. Может обеспечить сквозное (End-to-End) качество обслуживания, гарантируя необходимую пропускную способность. IntServ использует для своих целей протокол сигнализации RSVP. Позволяет приложениям выражать сквозные требования к ресурсам и содержит механизмы обеспечения данных требований. IntServ можно кратко охарактеризовать как резервирование ресурсов (Resource reservation).

32) Differentiated Service (DiffServ)
Архитектура DiffServ подразумевает определение поля DiffServ (DS), которое заменяет поле типа обслуживания в протоколе IPv4, используемое при принятии решений о пересылке данных через каждый узел (PHB) для классификации пакетов и функций согласования трафика, например таких, как измерение, маркирование, формирование и контроль.
DSCP(Differentiated Services Codepoint) — шесть битов (DS5-DS0)
ECN(Explicit Congestion Notification) — два бита
Биты DS5, DS4 и DS3 определяют класс, биты DS2 и DS1 определяют вероятность сброса, а бит DS0 всегда устанавливается равным нулю.

33) Существует четыре AF-класса — обозначаемых как AF1x – AF4x. В каждом классе есть три возможности сброса. В зависимости от имеющейся сетевой политики, пакеты могут выбираться для пересылки на основе необходимой пропускной способности, задержки, джиттера (изменений времени задержки), потерь или в соответствии с приоритетом доступа к службам сети.
С этой системой устройство располагает по приоритетам трафик по классам сначала. Затем сетевое устройство дифференцирует и устанавливает приоритет пакетов, принадлежащих к трафику одного и того же класса, принимая во внимание вероятность сброса пакетов.

34) Применение протокола IPv4
В современной сети Интернет используется IP четвёртой версии, также известный как IPv4. Сейчас проблемой стал процесс исчерпания IPv4-адресов, который можно определить исходя из того, что IANA раздала последние адресные блоки в феврале 2014г. А региональный регистратор APNIC прекратил выделение адресов в апреле 2011г.

Причины исчерпания адресов:

- Мобильные устройства – мобильные телефоны стали полноценными интернет-хостами.
- Неэффективное использование адресов - Организации, которые получили IP-адреса в 1980-х годах, часто имеют большее количество IP-адресов, чем им реально требуется
- Расширение Интернета
- Постоянные соединения – современные маршрутизаторы, широкополосные модемы редко выключаются, в отличии от первых телефонных модемов

Существует большое число технологий, решающих эту проблему, одной из которых является протокол IPv6, но его внедрение тормозиться из-за невозможности перестройки всей сети.

35) Уязвимости протокола IP. Основные типы угроз безопасности, связанные с протоколом IP

Smurf (атака, направленная на ошибки реализации TCP-IP протокола)

- Сейчас этот вид атаки считается экзотикой, однако раньше, когда TCP-IP протокол был достаточно новым, в нём содержалось некоторое количество ошибок, которые позволяли, например, подменять IP адреса. Однако, этот тип атаки применяется до сих пор. Некоторые специалисты выделяют TCP Smurf, UDP Smurf, ICMP Smurf. Конечно, такое деление основано на типе пакетов.
- Рекомендации: коммутаторы CISCO предоставляют хорошую защиту, как и многие другие, а также свежее ПО и межсетевые экраны; необходимо блокировать широковещательные запросы.

36) Dummy ARP (Ложный ARP)

- ARP сервер, маршрутизатор или коммутатор знают какие IP принадлежат MAC адресам (т.е. сетевым картам). При возможности физического доступа к сети, взломщик может подделать ARP ответ и выдать себя за другой компьютер в сети, получив его IP. Тем самым все пакеты, предназначенные тому компьютеру, будет получать он. Это возможно, если тот компьютер выключен, иначе это действие вызовет конфликт IP адресов (в одной сети не могут быть 2 компьютера с одним и тем же IP адресом).
- Рекомендации: используйте ПО, которое информирует об изменении MAC адресов у IP, следите за лог-файлами ARP сервера.

37) IP-Spoofing (Спуфинг или Подмена IP адреса)

- Атакующий подменяет свой реальный IP фиктивным. Это необходимо, если доступ к ресурсу имеют только определённые IP адреса. Взломщику нужно изменить свой реальный IP на «привилегированный» или «доверенный», чтобы получить доступ. Этот способ может быть использован по-другому. После того, как два компьютера установили между собой соединение, проверив пароли,

взломщик может вызвать на жертве перегрузку сетевых ресурсов специально сгенерированными пакетами. Тем самым он может перенаправить трафик на себя и таким образом обойти процедуру аутентификации.

- Рекомендации: их может быть много, по той причине, что приёмов достаточно много. Но стоит упомянуть, что угрозу снизит (но возможно затруднит легимитивные соединения) уменьшение времени ответного пакета с установленными флагами SYN и ACK, а также увеличить максимальное количество SYN-запросов на установление соединения в очереди. Так же можно использовать SYN-Cookies.