**1. Перечислить все сетевые утилиты.**

* ping
* tracert
* route
* netstat
* arp
* nslookup
* host-name
* ipconfig
* nbtstat
* net

**2. Перечислить все уровни модели OSI/ISO. Описать назначение каждого уровня.**

* ***Физический***
  + Физический уровень определяет свойства среды передачи данных (коаксиальный кабель, витая пара, оптоволоконный канал и т.п.) и способы ее соединения с сетевыми адаптерами: технические характеристики кабелей (сопротивление, емкость, изоляция и т.д.), перечень допустимых разъемов, способы обработки сигнала и т.п.
* ***Канальный уровень***
  + Канальный уровень отвечает за доставку кадров (frame) между устройствами, подключенными к одному сетевому сегменту. Кадры канального уровня не пересекают границ сетевого сегмента.
  + На канальном уровне модели рассматривается два подуровня: подуровень управления доступом к среде передачи данных - определяет методы совместного использования сетевыми адаптерами среды передачи данных. подуровень управления логическим каналом - определяет понятия канала между двумя сетевыми адаптерами, а также способы обнаружения и исправления ошибок передачи данных. Основное назначение процедур канального уровня подготовить блок данных (обычно называемый кадром) для следующего сетевого уровня.
* ***Сетевой уровень***
  + Сетевой уровень определяет методы адресации и маршрутизации пакетов в сети. В отличие от канального уровня сетевой уровень определяет единый метод адресации для всех компьютеров в сети не зависимого от способа передачи данных. На этом уровне определяются способы соединения компьютерных сетей.
* ***Транспортный уровень***
  + Основным назначением процедур транспортного уровня является подготовка и доставка пакетов данных между конечными точками без ошибок и в правильной последовательности.
* ***Сеансовый уровень***
  + Сеансовый уровень определяет способы установки и разрыва соединений (называемых сеансами) двух приложений, работающих в сети. Следует отметить, что сеансовый уровень - это точка взаимодействия программ и компьютерной сети.
* ***Представительский уровень***
  + На представительский уровне определяется формат данных, используемых приложениями. Процедуры этого уровня описывают способы шифрования, сжатия и преобразования наборов символов данных.
* ***Прикладной уровень***
  + Основное назначения уровня: определить способы взаимодействия пользователей с системой (определить интерфейс).

**3. Поясните понятие сетевой протокол.**

Сетевой протокол — набор правил и действий между соседними уровнями модели OSI.

**4. Указать где в OSI/ISO проходит граница между аппаратным и программным обеспечением.**

Между LLC и MAC

**5. Определить понятие CSMA/CD.**

CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с прослушиванием несущей и обнаружением коллизий) — технология множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий.

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

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

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

**6. Как называется программное обеспечение реализующий подуровень LLC канального уровня.**

Драйвер

**7. Что определяет спецификация NDIS?**

NDIS - спецификация интерфейса сетевого драйвера для сопряжения драйверов сетевых адаптеров с операционной системой.

**8. Свойства ненадежных протоколов. Примеры ненадежных и надежных протоколов**

* отсутствие механизмов обеспечения надежности: пакеты не упорядочиваются, и их прием не подтверждается;
* отсутствие гарантий доставки: пакеты отправляются без гарантии доставки, поэтому процесс Прикладного уровня (программа пользователя) должен сам отслеживать и обеспечивать (если это необходимо повторную передачу);
* отсутствие обработки соединений: каждый отправляемый или получаемый пакет является независимой единицей работы; UDP не имеет методов установления, управления и завершения соединения между отправителем и получателем данных;
* UDP может по требованию вычислять контрольную сумму для пакета данных, но проверка соответствия контрольной суммы ложится на процесс Прикладного уровня;
* отсутствие буферизации: UDP оперирует только одним пакетом, и вся работа по буферизации ложится на процесс Прикладного уровня;
* UDP не содержит средств, позволяющих разбивать сообщение на несколько пакетов (фрагментировать) – вся эта работа возложена на процесс Прикладного уровня.

Ненадежные: UDP

Надежные: TCP

**9. Перечислить все уровни модели TCP/IP. Описать назначение каждого уровня. Привести примеры протоколов каждого уровня.**

Структура TCP/IP является более простой: в ней выделяются Прикладной, Транспортный, Межсетевой и уровень доступа к сети.

Транспортный уровень – TCP (Transmission Control Protocol), чье имя присутствует в названии всего стека; UDP (User Datagram Protocol) – протокол передачи дейтаграмм пользователя.

Межсетевой уровень - IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse ARP).

Уровень доступа к сети - Ethernet, SLIP (Serial Line IP), PPP (Point-to-Point Protocol).

**10. Поясните понятия хост, адрес хоста, имя хоста.**

Хост – устройство, имеющее сетевой адаптер

Адрес хоста – IP-адрес устройства

Имя хоста – символьное имя устройства

**11. Какая организация поддерживает сетевые протоколы Internet. Как называются документы, описывающие эти протоколы.**

IETF – группа по проектированию Internet, поскольку именно она занимается поддержкой документов, именуемых RFC (Request for Comments), в которых описаны все правила и форматы всех протоколов и служб TCP/IP в сети Internet.

**12. Что такое МАС-адрес? Структура Ethernet МАС-адреса.**

Физический или локальный адрес узла, определяемый технологией, с помощью которой построена сеть, в которую входит узел. В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов.

Младшие 24 разряда кода адреса называются OUA– уникальный адрес. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров.

Следующие 22 разряда кода называются OUI – уникальный идентификатор. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть.

**13. Как посмотреть MAC-адрес сетевой карты на компьютере?**

ipconfig /all

**14. Основное назначение межсетевого уровня.**

Доставка дейтаграмм

**15. Структура IP-адреса.**

Адрес IP представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых октетами. Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками.

**16. Типы IP-адресации. Классы адресов Internet.**

Существует две модели адресации: классовая и бесклассовая. В классовой модели адресации все адреса подразделяются на пять классов: A, B, C, D, E.

Классы D и E имеют специальное назначение: D – предназначен для использования групповых адресов, позволяющих отправлять сообщения группе хостов; E – исключительно для экспериментального применения.

Бесклассовая позволяет произвольным образом назначать границу сетевой и хостовой части IP-адреса. Для этого каждому IP-адресу прилагается 32-битовая маска, которую часто называют маской сети (netmask) или маской подсети (subnetmask).

**17. Поясните понятия публичный IP-адрес и частный IP-адрес.**

Публичный(белый) IP адрес – уникальный адрес в глобальной сети Интернет. Частный(серый) адрес – уникальный адрес в локальной сети, но в другой локальной сети может быть такой же уникальный адрес.

**18. Как посмотреть IP-адрес компьютера.**

ipconfig

**19. Как протестировать IP-соединение в локальной сети?**

ping

**20. Как получить перечень сетевых узлов между двумя хостами?**

route

**21. Перечислите параметры настройки TCP/IP.**

IP, маска, шлюз, DNS

**22. Поясните понятие маска подсети.**

Маска подсети (subnetmask) – это число, которое используется в паре с IP-адресом, состоит из непрерывной последовательности единиц, после которых следует непрерывная последовательность нулей. Двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

**23. Основные отличия между IPv4 и IPv6.**

Протокол IPv6 имеет следующие основные особенности:

-длина адреса 128 бит – такая длина обеспечивает примерно 3.4×1038адресов;

-автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;

-встроенная безопасность – для передачи данных является обязательным использование протокола защищенной передачи IPsec (протокол IPv4 также может использовать IPsec, но не обязан этого делать).

В реализации, про которую говорил Шиман, так: адрес пополам делится по 64 бита, старшие 64 бита ip адрес, младшие – 48 бит MAC адрес и 16 нулей.

То есть: 128 бит: первые 64 ip адрес, потом 16 нулей, потом MAC адрес.

**24. Поясните понятие сетевой порт. На каком уровне модели TCP/IP это понятие определено.**

Процесс, получающий или отправляющий данные с помощью Транспортного уровня, идентифицируется номером, который называется номером порта.

**25. Как классифицируются сетевые порты.**

хорошо известные номера портов (well-known port number), зарегистрированные номера портов (registered partnumber), динамически номера портов (dynamic port number).

**26. Как посмотреть какими программами заняты сетевые порты на компьютере?**

netstat

**27. Поясните понятие архитектура клиент/сервер.**

Будем говорить, что распределенное приложение имеет архитектуру клиент-сервер, если все процессы распределенного приложения можно условно разбить на две группы. Одна группа процессов называется серверами другая – клиентами. Обмен данными осуществляется только между процессами-клиентами и процессами-серверами. Основное отличие процесса-клиента от процесса-сервера в том, что инициатором обмена данными всегда является процесс-клиент. Другими словами, процесс-клиент обращается за услугой (сервисом) к процессу-серверу.

**28. Что такое сетевая служба. Приведите примеры сетевых служб.**

Программная реализация протокола сетевого уровня.

Сетевые службы предназначены для выполнения определенных функций, в рамках действующего протокола, например, служба разрешения имен(DNS), служба автоматического выделения адресов(DHCP) и т.д.

**29. Поясните понятие интерфейс внутренней петли.**

Большинство реализаций TCP/IP поддерживает интерфейс внутренней петли (loopback interface), который позволяет двум прикладным процессам, находящимся на одном хосте, обмениваться данными посредством протокола TCP/IP. При этом, как обычно, формируются дейтаграммы, но они не покидают пределы одного хоста. Для интерфейса внутренней петли, зарезервирована сеть 127.0.0.0. В соответствии с общепринятыми соглашениями, большинство операционных систем назначают для интерфейса внутренней петли адрес 127.0.0.1 и присваивают символическое имя localhost.

**30. Назначение сетевых служб DNS и DHCP.**

 Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла.

Службу DNS можно рассматривать, как распределенную иерархическую базу данных, основное назначение которой ответить на два вида запросов: выдать IP-адрес по символическому имени хоста и наоборот – выдать символическое имя хоста по его IP-адресу.

DHCP (Dynamic Host Configuration Protocol) – это сетевая служба (и протокол) Прикладного уровня TCP/IP, обеспечивающая выделение и доставку IP-адресов и сопутствующей конфигурационной информации (маска сети, адрес локального шлюза, адреса серверов DNS и т.п.) хостам.

**31. Организация, ведающая распределением IP-адресов, поддержкой сетевых доменов Internet верхнего уровня, регистрацией портов.**

ICANN - « Корпорация по управлению доменными именами и IP-адресами» (Internet Corporation for Assigned Names and Numbers)

**32. Поясните понятие сетевой сокет.**

Совокупность IP-адреса и номера порта называется сокетом. Сокет однозначно идентифицирует прикладной процесс в сети TCP/IP. Следует помнить, что одни и те же номера портов могут быть использованы как для протокола UDP, так и для протокола TCP

**33. Назначение стандарта POSIX.**

Стандарт POSIX – это набор документов, описывающих интерфейсы между прикладной программой и операционной системой. Стандарт создан для обеспечения совместимости различных Unix-подобных операционных систем и переносимости исходных программ на уровне исходного кода.

**34. Структура TCP/IP TCP-сервера. Все функции и все параметры функций.**

Первые блоки обеих программ идентичны и предназначены для инициализации библиотеки WS2\_32.DLL.

Второй блок программы сервера создает сокет (функция soсket) и устанавливает параметры этого сокета. Следует обратить внимание на параметр SOCK\_STREEM функции socket, указывающий, что сокет будет использоваться для соединения (сокет ориентированный на поток). Для установки параметров сокета, используется функция bind. При этом говорят, что сокет связывают с параметрами. Для хранения параметров сокета в Winsock2 предусмотрена специальная структура SOCKADDR\_IN (она тоже присутствует на рисунке). Перед выполнением функции bind, которая использует эту структуру в качестве параметра, необходимо ее заполнить данными. Пока скажем только, что в SOCKADDR\_IN хранится IP-адрес и номер порта сервера.

В третьем блоке программы сервера выполняются две функции Winsock2: listen и accept. Функция listen переводит сокет, ориентированный на поток, в состояния прослушивания (открывает доступ к сокету) и задает некоторые параметры очереди соединений. Функция accept переводит процесс сервера в состояние ожидания, до момента пока программа клиента не выполнит функцию connect (подключится к сокету). Если на стороне клиента корректно выполнена функция connect, то функция accept возвращает новый сокет (с эфемерным портом), который предназначен для обмена данными с подключившимся клиентом. Кроме того, автоматически заполняется структура SOCKADDR\_IN параметрами сокета клиента.

Четвертый и пятый блоки программы сервера предназначены для обмена данными по созданному соединению. Следует обратить внимание, что, во-первых, используются функции send и recv, а во-вторых, в качестве параметра эти функции используют сокет, созданный командой accept.

**35. Структура TCP/IP TCP-клиента. Все функции и все параметры функций.**

В программе клиента осталось пояснить, только работу третьего блока. В этом блоке выполняется функция connect, предназначенная для установки соединения с сокетом сервера. Функция в качестве параметров имеет, созданный в предыдущем блоке, дескриптор сокета (ориентированного на поток) и структуру SOCKADDR\_IN с параметрами сокета сервера.