ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Пример тестовых заданий по вступительному испытанию **КОМПЬЮТЕРНЫЕ СЕТИ**

Раздел 1.

1. Общие принципы построения компьютерных сетей
2. Архитектура и стандартизация сетей
3. Сетевые услуги и службы
4. Безопасность в компьютерных сетях
5. Методы передачи данных в компьютерных сетях
6. Технологии обмена данными в компьютерных сетях (стеки протоколов)
7. Основные компоненты структурированной кабельной системы
8. Адресация IPv4 в компьютерных сетях

Общие принципы построения компьютерных сетей

По типу функционального взаимодействия компьютерные сети бывают:

- с выделенным сервером (клиент-серверные);
- Одноранговые

Сервер — специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам свои ресурсы (файлы данных, накопители, процессорное время и т.д.).

Сети типа «клиент-сервер» (client-server) создаются в учреждениях или крупных предприятия с большим количеством пользователей.

В таких сетях выделяется один или несколько компьютеров, называемых серверами. Их задача состоит в быстрой и эффективной обработке большого числа запросов других компьютеров — клиентов.

В одноранговой сети (peer-to-peer) все компьютеры равноправны. Каждый компьютер может выступать как в роли сервера, предоставляя файлы и аппаратные ресурсы (принтеры, жесткие диски, программы и т.д.) другим компьютерам, так и в роли клиента, пользующегося ресурсами других компьютеров.

Одноранговые сети

Преимущества

- простота настройки
- низкая стоимость создания и поддержки (не требуется постоянное присутствие системного администратора)
- независимость компьютеров и их ресурсов друг от друга
- отсутствие необходимости в дополнительном программном обеспечении

Недостатки

- отсутствие возможности централизованного (из одного места) управления сетью и доступа к данным
- их низкая защищенность

Сети типа «клиент-сервер»

Преимущества

- масштабируемость (добавление новых устройств)
- безопасность
- централизованное управление

Недостатки

- высокая стоимость оборудования
- сложность в развертывании и поддержке (требуется постоянное присутствие квалифицированного системного администратора)
- наличие единой точки отказа (неисправность сервера может сделать всю сеть практически неработоспособной, а ресурсы недоступными)

Архитектура и стандартизация сетей

Для упрощения структуры, большинство сетей организуется в наборы уровней или слоев, каждый последующий из которых возводится над предыдущим. Во всех сетях целью каждого уровня является предоставление служб для верхних уровней. Уровень n одной машины поддерживает связь с уровнем n другой машины. Правила и соглашения, используемые в данном общении, называются протоколом уровня n. Протокол является договоренностью общающихся сторон о том, как должно происходить общение.

Данные не пересылаются с уровня n одной машины на уровень n другой машины. Вместо этого каждый уровень передает данные и управление уровню, лежащему ниже, пока не достигается самый нижний уровень. Ниже первого уровня располагается физический носитель, по которому и производится обмен информацией. Набор уровней и протоколов называется архитектурой сети. Список (совокупность, набор) протоколов, достаточный для организации взаимодействия узлов в сети называется стеком протоколов. Между каждой парой смежных уровней находится интерфейс, определяющий набор примитивных операций, предоставляемых нижним уровнем верхнему.

Модель OSI

Эталонная модель взаимодействи открытых систем (Open System Interconnection Reference Model) ил модель OSI (OSI Model) считаетс основной архитектурной модель передачи данных межд компьютерами.

Эталонная модель взаимодействи открытых систем или модель OS определяет уровни взаимодействи систем, их стандартные названия функции, которые должен выполнят каждый уровень.

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Уровни модели OSI.

Уровень 7. Уровень приложений (Application layer). Обслуживает сетевые приложения, с помощью которых пользователь получает доступ к сетевым услугам. Например, браузеры или почтовые клиенты.

Уровень 6. Уровень представлений (Presentation layer). Отвечает за то, чтобы информация, посылаемая уровнем приложений одного компьютера, могла быть прочитана уровнем приложений другого компьютера, т.е. определяет форматы передаваемой информации. Задачей данного уровня является перекодировка, сжатие и распаковка данных, их шифрование и дешифрование.

Уровень 5. Сеансовый уровень (Session layer). Позволяет двум приложениям устанавливать, управлять и завершать сеансы связи (сессии) друг с другом. Сеансовый уровень синхронизирует диалог между приложениями и отвечает за восстановление аварийно прерванных сеансов связи.

Уровень 4. Транспортный уровень (Transport layer). Отвечает за надежную передачу данных между взаимодействующими приложениями разных компьютеров. На стороне отправителя транспортный уровень разбивает данные на блоки небольшого размера, называемые сегментами, и доставляет их получателю в нужной последовательности. Этот процесс называется сегментацией. На транспортном уровне получателя эти сегменты собираются в исходный поток данных.

Уровень 3. Сетевой уровень (Network layer). Отвечает за соединение узлов, расположенных в разных сетях. Он выполняет две основные функции — логическую адресацию и маршрутизацию. Каждому устройству, подключенному к сети, назначается логический адрес, который также называют адресом 3 уровня. Он используется для маршрутизации пакетов. Маршрутизация — это процесс определения наилучшего маршрута передачи информации от отправителя к получателю, когда отправитель и получатель находятся в разных сетях, соединенных произвольным образом. Также на сетевом уровне решаются задачи управления потоком данных и диагностики ошибок передачи. Помещает сегменты, полученные от транспортного уровня, в пакеты (также называемые дейтаграммами).

Уровень 2. Канальный уровень (Data link layer). Обеспечивает сетевым узлам доступ к среде передачи и решает вопросы физической адресации, обнаружения и коррекции ошибок, упорядоченной доставки кадров, логической топологии. Канальный уровень помещает пакеты (дейтаграммы), полученные с сетевого уровня в кадры.

Уровень 1. Физический уровень (Physical layer). Выполняет передачу потока битов, полученных от канального уровня, через физическую среду в виде электрических, оптических или радиосигналов. Физический уровень отвечает за активацию, поддержание и деактивизацию физического канала между устройствами. Спецификации физического уровня определяют уровни напряжений, скорости физической передачи данных, максимальные расстояния передачи информации, физические разъемы, и другие подобные характеристики.

Сетевые услуги и службы

Служба — это сетевой компонент, реализующий некоторый набор услуг. *Сетевой сервис* — это интерфейс между потребителем услуг (например, пользователем) и поставщиком услуг (службой). Серверная часть может предоставлять сетевые услуги клиентской части по инициативе этой клиентской части. *Серверное программное обеспечение* — программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента, предоставляя ему доступ к определенным ресурсам или услугам.

К сетевыми услугам относятся хранение данных, поиск информации, почтовые услуги (электронная почта), передача данных между узлами в сети, организация сеансов взаимодействия между прикладными процессами.

Потребителями сетевых услуг являются пользователи, программы, операционные системы, функциональные блоки, вычислительные процессы и т.д. Поставщик сетевых услуг — это сетевая служба, реализующая услуги или набор услуг. Так, поставщиками услуг являются средства обеспечения общего доступа и использования локальных и удаленных ресурсов и услуг.

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

Безопасность в компьютерных сетях

Безопасность сети — это только часть информационной безопасности, она обычно ассоциируется с устройствами, которые защищают саму сеть. Межсетевой экран может быть как автономным устройством, которое находится рядом с сетевым оборудованием, таким как маршрутизаторы или коммутаторы, так и программным обеспечением, развернутым в том же физическом блоке, который выполняет функции маршрутизатора и коммутатора. Для защиты сети могут использоваться межсетевые экраны, системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), устройства VPN, системы предотвращения утечки данных (DLP) и др.

Выделяют 4 основных принципа проектирования сетевой безопасности на объекте информатизации:

- Защита оборудования, подключенного к сетевой инфраструктуре. В качестве защитных мер используют антивирусные решения с регулярным обновлением баз, межсетевые экраны с фильтрацией трафика и блокировкой нежелательных абонентов и т. д.
- Оборудование должны быть отказоустойчивым и предусматривать возможность быстрого восстановления. Подразумевается наличие дублирующих компонентов в критически важных узлах.
- Систематический мониторинг всей инфраструктуры компании для обнаружения уязвимых точек. Также система должна предоставлять подробную информацию о любом программном или аппаратном компоненте оборудования.
- Постоянный мониторинг пропускной способности сетевого канала. Это гарантирует своевременную блокировку нежелательного трафику, а также позволяет осуществить балансировку нагрузки в ручном режиме.
- Критически важные узлы инфраструктуры организации должны обеспечивать высокую доступность при любой угрозе либо атаке на компанию. Это достигается за счет создания второй независимой площадки (ЦОДа), которая реплицирует данные с первой в синхронном режиме.

Основы передачи данных

Полудуплексная передача (half-duplex): устройства передают данные через физическую среду поочередно. Для решения проблемы, когда несколько отправителей хотят передавать одновременно, применяются методы множественного доступа (multiple access), реализуемые на канальном уровне. Методы множественного доступа определяют очередность доступа к общей среде передачи. Примером сети с полудуплексной передачей является сеть Wi-Fi с методом доступа CSMA/CA.

Дуплексная или полнодуплексная передача (duplex или full duplex): передача ведется одновременно в двух направлениях — прямом и обратном. Взаимодействующие устройства могут одновременно передавать и получать данные. Специальных методов доступа к среде на канальном уровне не требуется. Примером сети с дуплексной передачей является коммутируемая сеть Ethernet.

Определение направления передачи данных называется коммутацией (switching). Одним из методов коммутации является коммутация пакетов (packet switching), которая основана на использовании мультиплексирования с разделением по времени.

Передаваемые по сети сообщения разбиваются на небольшие блоки, называемые пакетами (packet). Пакеты передаются по одному и тому же каналу связи по мере их поступления независимо от их источников и адресатов. Взаимодействующие устройства занимают канал только на время передачи пакета.

Каждый пакет состоит из двух частей:

заголовок — содержит служебные данные, необходимые для управления доставкой пакета (адресную информацию, порядковый номер и т.д.);

данные — сообщение, которое подлежит передаче.

Порядок обмена пакетами, их размер, а также конкретный состав их заголовка определяется соответствующим сетевым протоколом.

Сети с коммутацией каналов обладают фиксированной полосой пропускания и очень малым временем задержки сигналов. Исходная технология передачи для них была связана с голосовой телефонией, видеотелефонией и видеоконференциями. Эта технология оказалась недостаточно гибкой для передачи данных, где требования к скорости передачи сильно варьируются в коротких интервалах времени. Однако некоторые старые поколения сети передачи данных до сих пор используют принцип коммутации каналов.

В основу коммутаций каналов залажен набор номера источником данных. Маршрутизация сообщения базируется на указании номера адресата, когда канал установлен. Соединение разрывают, когда сообщение состоялось. Во время обмена сообщениями объем данных, прошедших через коммутатор фиксируется не взирая на то, что данные могли быть и не использованы. В конце сообщения соединение разрывают. Телефонные сети, как и цифровые системы интегрального обслуживания (ЦСИО) используют в работе принцип коммутации каналов.

Модель и стек протоколов TCP/IP

Стек протоколов TCP/IP был создан раньше модели OSI, поэтому его разработчики не использовали модель OSI для описания архитектуры стека. Они разработали собственную модель TCP/IP (Transmission Control Protocol/Internet Protocol).

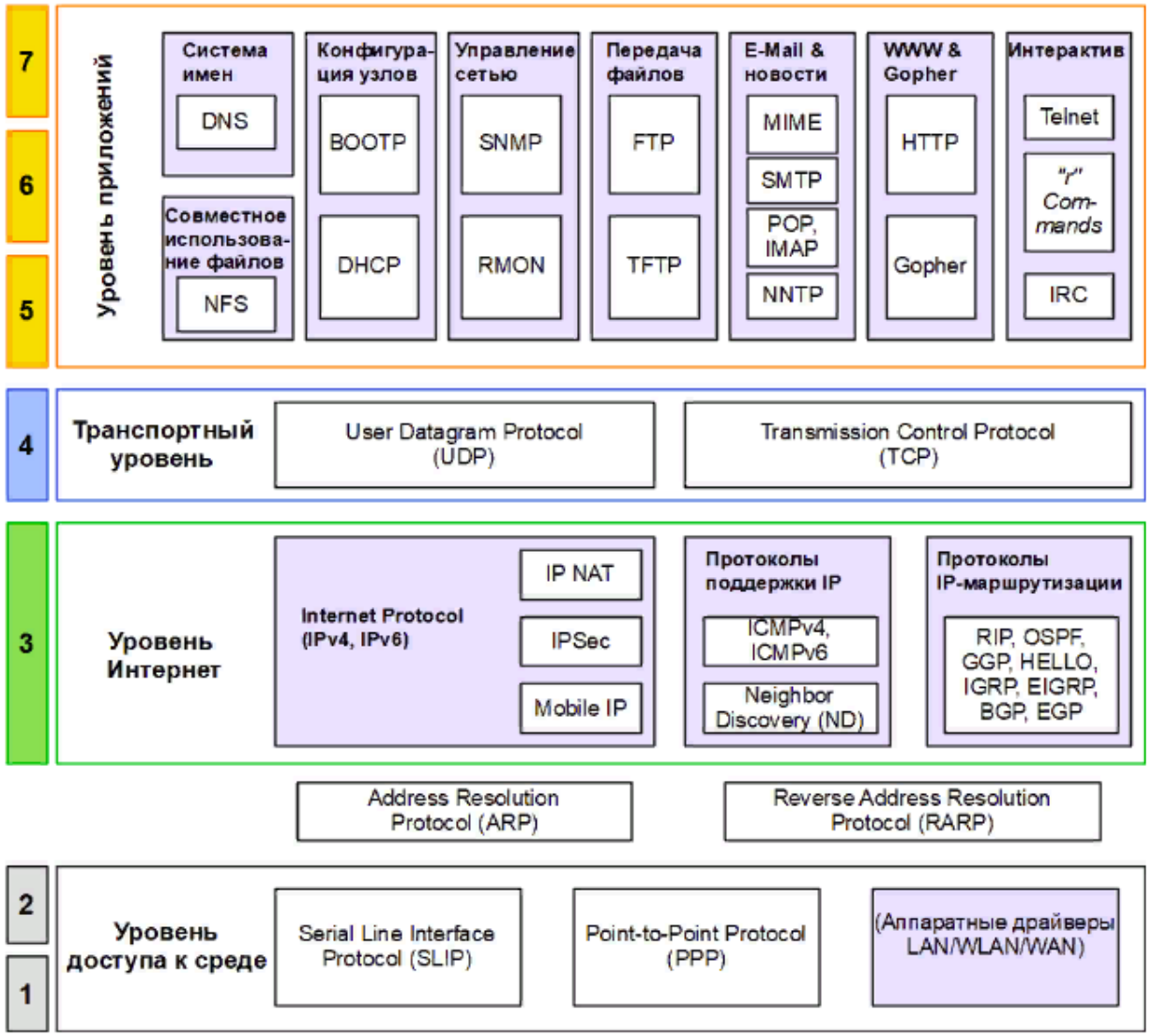
Тверхним уровням модели OSI соответствует уровень приложений (Application layer) в модели TCP/IP, который включается в себя функции представления, кодирования и контроля над установлением соединения. На этом уровне работают протоколы FTP, TFTP, HTTP/HTTPs, DHCP, DNS, Telnet, SMTP, POP3, IMAP и др.

Транспортный уровень (Transport layer) модели TCP/IP выполняет те же функции, что и одноименный уровень в модели OSI. На этом уровне работают два протокола — TCP и UDP. Протокол TCP (Transmission Control Protocol) обеспечивает надежную доставку сегментов по сети за счет установления логического соединения между отправителем и получателем данных. Протокол UDP (User Datagram Protocol) не устанавливает соединение между отправителем и получателем сообщения и не гарантирует надежную доставку данных.

Уровень Интернет (Internet layer) аналогичен по функциям сетевому уровню модели OSI и обеспечивает организацию связи между различными сетями и подсетями. Основным протоколом уровня Интернет является IP, который выполняет две функции — логическую адресацию узлов и выбор наилучшего маршрута до сети назначения (маршрутизацию). Также на этом уровня работают протоколы ICMP, IGMP, протоколы маршрутизации RIP, OSPF, BGP.

Уровень доступа к среде (Network access layer) объединяет функции канального и физического уровня модели OSI, обеспечивая физическую передачу данных в сети. Существует множество различных протоколов уровня доступа к сети, из которых самыми распространенными являются Ethernet, PPP, IEEE 802.11 (Wi-Fi), ATM и др.

Модель и стек TCP/IP



Протоколы TCP/IP

Internet Protocol (IP). Протокол IP является основным протоколом стека TCP/IP. Он обеспечивает обмен данными между сетевыми устройствами с помощью блоков, называемых пакетами или дейтаграммами. Каждый пакет снабжается адресной информацией, которая позволяет выбрать лучший маршрут для его доставки. Протокол IP передает сетевые пакеты без установления соединения, без обеспечения надежности и без подтверждения доставки. Эта функция выполняется протоколами более высокого уровня. Поэтому его иногда называют best-effort protocol. Существует две версии протокола IP: IPv4 и IPv6.

Transmission Control Protocol (TCP). Протокол TCP является протоколом транспортного уровня стека TCP/IP. Он обеспечивает установку соединения между отправителем и получателем, разбиение крупных информационных блоков на сегменты ограниченной длины, а также их гарантированную доставку получателю в заданном порядке и без ошибок. Функционирование протокола TCP предполагает его взаимодействие с протоколами уровня приложений. Для этого чтобы обеспечить прием/передачу данных несколькими сетевыми приложениями, одновременно работающими на одном IP-интерфейсе, используется адрес транспортного уровня, называемый порт (port). Порт служит для идентификации приложения, которому должны быть доставлены данные.

User Datagram Protocol (UDP). Протокол UDP второй важный протокол транспортного уровня. В отличие от TCP, он не устанавливает соединение перед передачей данных и не требует от получателя подтверждений о доставке, но за счет именно этих особенностей он работает быстрее, чем TCP. Протокол UDP используют в тех задачах, где в первую очередь необходимо обеспечить хорошую скорость передачи данных, а гарантия доставки и надежность имеют второстепенное значение. Примером такой задачи является передача потокового видео по технологии IPTV.

Протоколы для получения информации с Web-сайтов и передачи файлов:

Hypertext Transfer Protocol (HTTP). Протокол HTTP является протоколом уровня приложений стека TCP/IP. Это протокол запроса и ответа, используемый Web-браузерами для передачи файлов, текста и графики между клиентами и серверами. Клиент (Web-браузер) инициирует запрос на установку соединения и получает ответ от удаленного сервера, на котором размещен Web-сайт. Соединение устанавливается через TCP-порт 80. Адрес HTTP или Web-сайта начинается с префикс http: //.

File Transfer Protocol (FTP). Протокол уровня приложений стека TCP/IP для передачи файлов между сетевыми узлами. Это клиент-серверный протокол, использующий транспортные услуги протокола TCP. Для успешной передачи файлов FTP требует 2 соединения: с использованием TCP-порта 21 для управления и TCP-порта 20 для данных. Чаще всего FTP используется для загрузки файлов из Интернета. Существуют тысячи общедоступных и частных FTP-сайтов, обеспечивающих ограниченный или анонимный доступ к неограниченным объемам данных. Синтаксис адреса FTP аналогичен протоколу HTTP, но в качестве префикса используется ftp: //.

Trivial File Transfer Protocol (TFTP). Простой протокол передачи файлов между клиентом и сервером. В отличие от FTP, протокол TFTP не содержит возможностей аутентификации и основан на транспортном протоколе UDP. Основное назначение TFTP — обеспечение простоты реализации клиента. Поэтому он часто используется для загрузки нового программного обеспечения или конфигурации в коммутаторы или маршрутизаторы.

Протоколы электронной почты:

Post Office Protocol 3 (POP3). Стандартный протокол уровня приложений стека TCP/IP для получения электронной почты с удаленного сервера, работающий на TCP-порту 110. На сервере электронной почты хранятся сообщения, которые могут быть сразу получены удаленными системами с помощью программного обеспечения почтового клиента. Клиент устанавливает соединение, чтобы загрузить электронную почту пользователя, а пока полученная электронная почта удаляется с сервера, разрывает соединение.

Internet Message Access Protocol (IMAP). Еще один протокол, используемый для получения электронной почты удаленными клиентами, которые поддерживают как автономный, так и онлайн-режимы работы. Для установки соединения используется TCP-порт 143. В отличие от POP3, IMAP предоставляет пользователю широкие возможности для работы с почтовыми ящиками, находящимися на почтовом сервере, а также одновременный доступ нескольких клиентов к одному почтовому ящику. Программное обеспечение почтового клиента получает доступ к сообщениям электронной почты на сервере так, как будто они расположены на компьютере получателя. Сообщениями электронной почты можно манипулировать с компьютера пользователя (клиента) без их постоянной пересылки с сервера и обратно.

Simple Mail Transfer Protocol (SMTP). Протокол для надежной и эффективной отправки почтовых сообщений в сетях TCP/IP. POP3 и IMAP обычно считаются протоколами приема электронной почты, в то время как SMTP обычно предоставляет услуги для отправки сообщений электронной почты на почтовые серверы. Небольшие текстовые команды используются для согласования и управления передачей через TCP-соединение. Для исходящих почтовых сообщений используется TCP-порт 25.

Доменное имя (от англ. domain name — «название области», «домен») — это уникальный буквенно-цифровой идентификатор определенного узла (устройства или сетевого соединения), являющегося частью Интернета; название, имя сайта. Все имеющиеся доменные имена функционируют благодаря системе доменных имен DNS (Domain Name System).

Domain Name System (DNS). Протокол именования в Интернете, используемый для адресации и именования удаленных компьютерных систем. Процесс поиска DNS преобразует доменные имена в числовые IP-адреса, которые хранятся на DNS-серверах. Эта функция предотвращает необходимость запоминания пользователем IP-адреса Web-сайта, например 192.168.176.56. Вместо этого DNS позволяет пользователю вводить доменное имя сайта (например, www.dlink.ru) и получать IP-адрес.

Протоколы уровня приложения для конфигурации, получения удаленного доступа и синхронизации времени:

- Telnet. Клиент-серверый протокол эмуляции терминала, использующий протокол TCP для установления соединения. Telnet устанавливает незашифрованный обмен данными между клиентом и сервером через TCP-порт 23 и позволяет локальным клиентским машинам получать доступ к удаленным узлам, как если бы пользователь непосредственно работал на удаленном устройстве. Telnet можно использовать для разных задач, в том числе для доступа к электронной почте, базам данных, файлам, интерфейсам командной строки удаленных коммутаторов и маршрутизаторов. Этот метод доступа уязвим с точки зрения безопасности. Данные не шифруются и могут быть перехвачены злоумышленниками; также не поддерживается безопасная аутентификация. Протокол Secure Shell (SSH) заменил Telnet в большинстве сред удаленного доступа и обеспечивает более надежные функции безопасности и аутентификации.
- Dynamic Host Configuration Protocol (DHCP). Протокол, используемый для динамического назначения IP-адресов и сетевой конфигурации клиентов, которые отправляются с центрального сервера. Это значительно упрощает администрирование и позволяет автоматически настраивать сеть для DHCP-клиентов. Клиенты отправляют сообщение на DHCP-сервер, запрашивая сетевой IP-адрес, маску подсети, адрес DNS-сервера, IP-адрес шлюза по умолчанию и другие необходимые данные.

Internet Control Message Protocol (ICMP). Протокол ICMP является неотъемлемой частью протокола IP и определяет различные типы сообщений, которые позволяют устройствам обмениваться информацией. Сообщения об ошибках используются для оповещения устройства-отправителя о проблемах, возникших при передаче пакета. Обычно генерируются в ответ на какое-либо событие, возникшее при передаче пакета, например, когда пакет не может достичь места назначения. Информационные сообщения используются для диагностики, тестирования, обмена информацией и других целей. Они не содержат описания ошибок и обычно не отправляются при возникновении какого-либо события. Примером является утилита ping, которая используется для проверки доступности другого узла в IP-сети. Это выполняется путем отправки пакета ICMP «эхо-запрос» на IP-адрес требуемого интерфейса и ожидания ответа. Данная утилита используется системными администраторами, которые хотят проверить подключение по локальной сети. Существует две версии протокола ICMP: ICMP v4 и ICMP v6.

Основные компоненты структурированной кабельной системы

СКС представляет собой иерархическую кабельную систему, смонтированную в здании или в группе зданий, состоящую из структурных подсистем. В состав СКС входят следующие элементы:

- главный кросс (MC);
- кабель магистральной подсистемы первого и второго уровня;
- промежуточные кроссы (IC);
- горизонтальные кроссы (HC) и кабели горизонтальной подсистемы;
- консолидационные точки (CP);
- многопользовательские телекоммуникационные розетки (MuTOA или MuTO);
- телекоммуникационные розетки (TO) и др.

Основная задача структурированной кабельной системы — создание надежной и функциональной информационно-телекоммуникационной инфраструктуры, которая позволяет подключать стационарные и мобильные устройства к локальной сети и к Интернету. Данная функция реализуется соответствующим расположением слотов доступа, терминалов и физических точек.

Построенная в соответствии со стандартами сеть позволяет подключать устройства, расположенные в любой точке объекта или группы объектов. Структурированная кабельная система обеспечивает бесперебойную передачу сигналов всех типов и является основой локальной компьютерной сети. Каждая точка подключения к СКС способна обеспечить доступ ко всем ресурсам сети. Грамотно построенные СКС позволяют получить стабильное соединение для высокоскоростной передачи цифровых сигналов и данных между серверами, персональными компьютерами, сетевыми устройствами.

Среди преимуществ СКС перед компьютерными и телефонными линиями можно выделить следующее:

- Высокая скорость передачи данных;
- Автоматизация процессов контроля и управления коммуникационными системами;
- Надежность системы. В случае аварийной ситуации неисправный участок быстро локализуется, выполняется переход на резервную линию для проведения ремонтных работ;
- Функциональные возможности системы позволяют настроить систему под индивидуальные потребности конкретного пользователя;
- Внедрение структурированной кабельной системы повышает эффективность работы организации, снижает эксплуатационные расходы, улучшает взаимодействие сотрудников внутри компании, способствует повышению качества обслуживания клиентов;
- СКС обеспечивает работу компьютерного оборудования разных поколений — интерфейсы системы позволяют подключать любое оборудование локальных сетей и речевых приложений. Возможно одновременное использование разнотипных сетевых протоколов;
- Возможности администрирования сокращают трудозатраты на обслуживание локальной сети и повышают удобство эксплуатации;
- Современные технологии связи позволяют пользователям менять рабочие места без изменения данных для доступа к сети;
- Универсальность системы. СКС строится по принципам открытой архитектуры с техническими характеристиками, определенными в стандартах;
- Возможность масштабирования. Оборудование СКС выбирается с резервом по производительности, к тому же остается возможность расширения системы.

Сетевое оборудование

Для подключения компьютера или любого устройства пользователя к сети требуется ряд компонентов:

- сетевая интерфейсная карта (сетевой адаптер);
- сетевое или телекоммуникационное оборудование: коммутатор, маршрутизатор или точка доступа;
- проводная или беспроводная среда передачи.

Сетевой адаптер — специальная печатная плата, установленная в компьютер, которая позволяет подключить его к сети.

Повторитель (repeater) является самым простым из сетевых устройств. Он работает на физическом (первом) уровне модели OSI и используется для соединения сегментов среды передачи для увеличения общей длины сети.

Концентратор — это повторитель, который имел несколько портов и соединял несколько физических сегментов сети (отрезков кабеля). Устройства, которым требовалось подключение к локальной сети, соединялись с концентратором отдельным кабелем. Он работал на физическом (первом) уровне модели OSI. Основной его задачей было повторение сигнала, поступившего с одного из портов на все остальные активные порты, предварительно восстанавливая их. Концентратор также не был наделен функциями обработки трафика.

Коллизия (collision) — наложение или столкновение сигналов, которое возникает во время одновременной передачи данных двумя или более узлами и приводит к повреждению данных.

Домен коллизий (collision domain) — часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети она возникла.

Мост (bridge) был разработан компанией Digital Equipment Corporation (DEC) в начале 1980-х годов и представлял собой устройство физического (первого) и канального (второго) уровней модели OSI, предназначенное для объединения двух локальных сетей или двух сегментов одной сети.

В настоящее время коммутаторы (switch) являются основным строительным блоком для создания локальных сетей.

Коммутатор представляет собой многопортовый мост и по принципу обработки данных ничем не отличается от него, однако в отличие от моста поддерживает множество дополнительных функций. Различают коммутаторы, работающие на канальном (втором) и сетевом (третьем) уровне модели OSI. Традиционный коммутатор работает на втором уровне. Маршрутизирующий коммутатор работает на канальном и сетевом уровнях.

Точка доступа (Access Point) функционирует на канальном уровне модели OSI. Она представляет собой беспроводную станцию, которая обеспечивает доступ ассоциированных с ней беспроводных клиентских устройств к проводной и/или беспроводной сети через беспроводную среду передачи.

Маршрутизатор (router) — это устройство сетевого (третьего) уровня модели OSI. Его основной задачей является анализ логических (сетевых) адресов (чаще всего IP-адресов) и определение наилучшего маршрута передачи пакета от источника к получателю.

Топологии компьютерных сетей

Топология сети — это способ описания конфигурации сети, схемы расположения и соединения сетевых устройств.

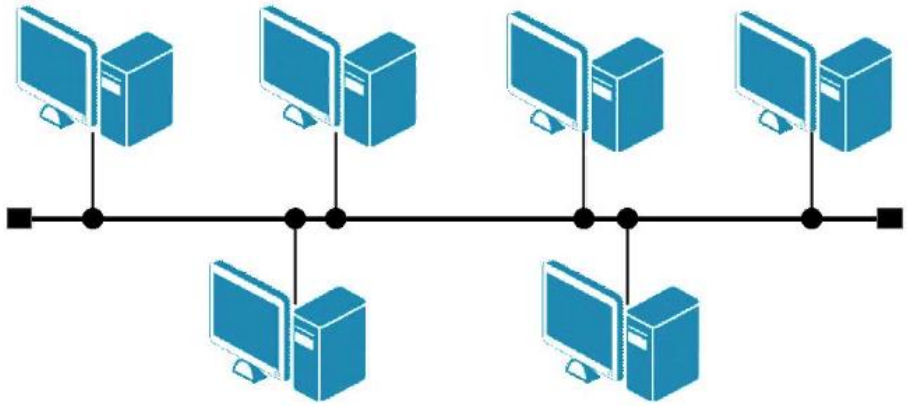
Существуют следующие базовые топологии, на основе которых строятся компьютерные сети:

- «шина» (bus);
- «кольцо» (ring);
- «звезда» (star).
- «дерево» (tree);
- ячеистая полносвязная топология (fully connected mesh);
- ячеистая топология частичной (неполной) связности (partially connected mesh).

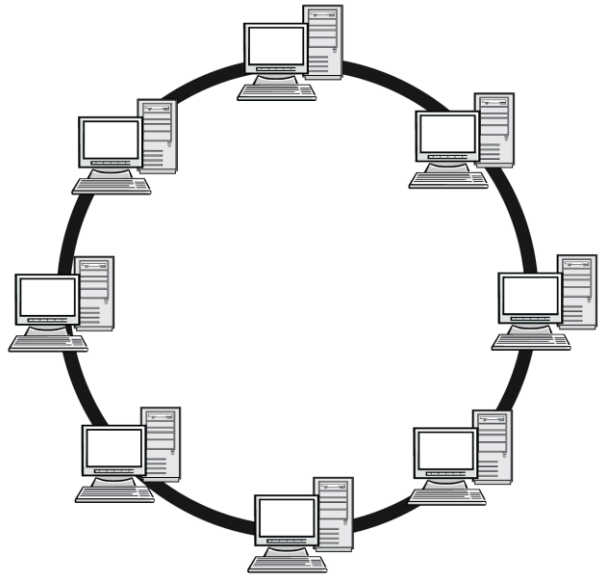
Топология «шина» (bus) является самым простейшим вариантом организации локальной сети. В сети с физической топологией «шина» все узлы равноправно подключаются к общей среде передачи и поэтому каждый узел «слышит» то, что передают другие узлы.

Несмотря на то, что топология «шина» характеризуется простотой реализации и дешевизной, она имеет ряд существенных недостатков:

- Существует ограничение на расстояние между узлами сети. Расстояние между самыми дальними узлами должно быть меньше, чем расстояние затухания сигнала при его передаче через данную физическую среду.
- Существует ограничение на количество устройств, подключаемых к сети. Поскольку сеть используется совместно, при увеличении в ней количества узлов, увеличивается число коллизий. Это уменьшает общую производительность сети и замедляет ее работу.
- При использовании в качестве среды передачи кабеля, он является «единой точкой отказа». В случае обрыва любого участка кабеля нарушается работа всей сети.



Физическая топология «кольцо» предполагает такую организацию сети, в которой каждый из узлов соединен с двумя другими так, чтобы от одного он получал информацию, а второму передавал ее до тех пор, пока данные не будут получены узлом-приемником. Последний узел подключается к первому, замыкая кольцо. Передача данных по кольцу осуществляется лишь в одном направлении, последовательно от узла к узлу.



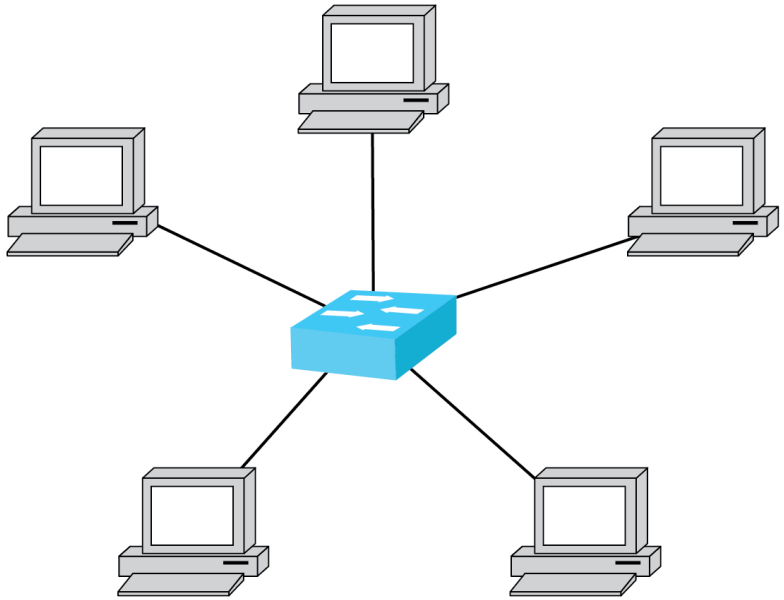
Достоинства топологии:

- Равные возможности доступа узлов к среде передачи, благодаря чему ни один из них не может ее монопольно захватить.
- Не возникают коллизии.
- Можно строить сети большой протяженности.

Недостатки топологии:

- Низкая производительность сети. В зависимости от количества узлов в сети, время передачи данных может быть достаточно большим, поскольку сигнал должен пройти последовательно через все узлы, каждый из которых проверяет, не ему ли адресована информация.
- Невысокая надежность сети. Выход из строя хотя бы одного из узлов и/или обрыв кабеля приводит к полной неработоспособности сети. Чтобы избежать остановки работы сети при выходе из строя узла или обрыве кабеля, обычно используют двойное кольцо, что приводит к существенным финансовым затратам.
- Сложность расширения сети. Добавление в сеть нового узла часто требует ее остановки, что нарушает работу всех других узлов.

Топология «звезда» (star) — одна из самых распространенных топологий компьютерных сетей. Чаще всего она используется в локальных сетях небольших офисов или домашних сетях. В этой топологии все узлы подключаются линией связи «точка-точка» к центральному устройству, в качестве которого в современных сетях может использоваться коммутатор, маршрутизатор или точка доступа. Обмен данными между узлами осуществляется через центральное устройство, которое выполняет и контролирует функции, реализованные в сети, а также усиливает проходящие через него сигналы.



Преимущества топологии:

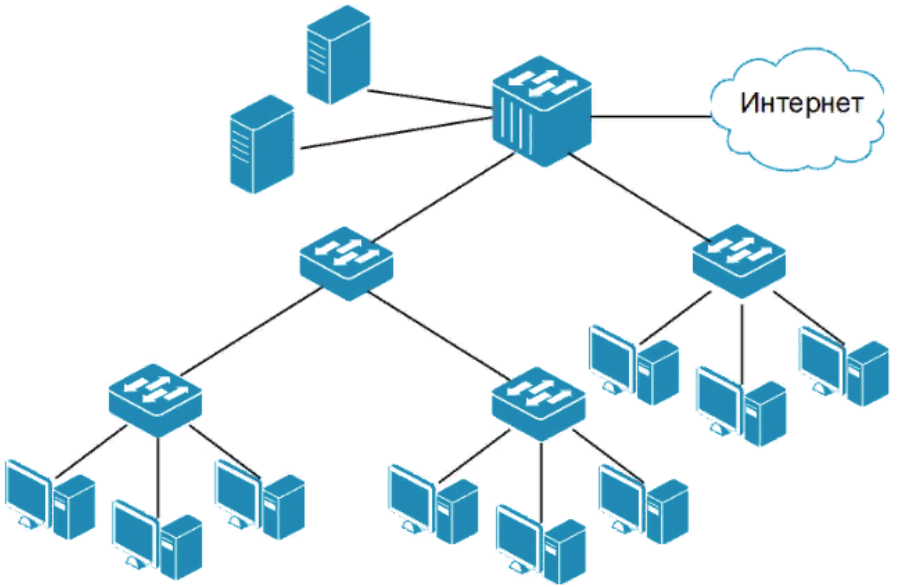
- Простота обслуживания и устранения неисправностей в сети, а также простота подключения новых устройств.
- Защищенность сети. В качестве центрального устройства может использоваться сетевое оборудование с развитыми функциями безопасности, которое обеспечивает контроль потоков проходящего через него трафика. Помимо этого можно физически ограничить доступ к центральному устройству, поместив его в безопасное место.
- Возможность использования кабелей различных типов для подключения узлов проводной сети к центральному устройству, если оно оборудовано портами различных типов (оптическими, медными).
- Возможность использования недорого оборудования.

Недостатки топологии:

- Наличие единой точки отказа. Выход центрального устройства из строя приведет к неработоспособности всей сети.
- Для подключения устройств проводной сети требуется большое количество кабеля.
- Количество устройств, которые могут быть объединены в сеть, ограничено количеством портов центрального устройства (для проводной сети) или производительностью точки доступа.

Топология «дерево» (tree) или как ее еще называют «расширенная звезда» (extended star) создается на основе комбинации топологий «звезда» и линейного подключения. Эта топология реализует иерархию узлов. На самом верхнем уровне иерархии находится центральное устройство, которое объединяет между собой центральные устройства отдельных «звезд» линиями связи «точка-точка». Уровней иерархии может быть несколько.

Топология «дерево» является самой распространенной топологией современных компьютерных сетей. Наиболее часто она используется в сетях средних и крупных предприятий, сет[illegible] провайдеров услуг.



Преимущества топологии:

- Возможность расширяемости сети.
- Возможность деления большой сети на сегменты (отдельны «звезды»), что упрощает обслуживание и управление сетью.
- Неисправности в одном сегменте не влияют [illegible] работоспособность остальных сегментов.

Недостатки топологии:

- При увеличении количества сегментов сети усложняется [illegible] обслуживание, и управление, а также поиск и устранени неисправностей.
- Высокая стоимость оборудования.
- Необходимость большого количества кабеля (в случае проводных сетей).
- Требуется высококвалифицированный персонал.

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Адресация IPv4 в компьютерных сетях

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

- Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.
- IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

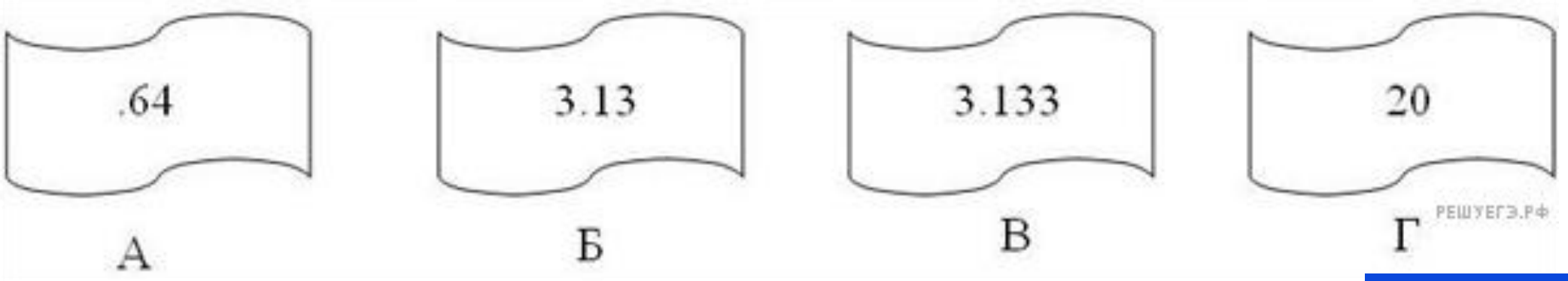
Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

- Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

Примеры решения задач

1 задание.

Петя записал IP—адрес школьного сервера на листке бумаги и положил его в карман куртки. Петина мама случайно постирала куртку вместе с запиской. После стирки Петя обнаружил в кармане четыре обрывка с фрагментами IP—адреса. Эти фрагменты обозначены буквами А, Б, В и Г. Восстановите IP—адрес. В ответе укажите последовательность букв, обозначающих фрагменты, в порядке, соответствующем IP—адресу.



Решение.

IP-адрес представляет собой числа, разъединенные точками, причем числа эти не больше 255.

Посмотрим внимательнее на данные фрагменты: под буквой А мы видим «.64». Число, на которое указывает этот фрагмент, начинается с 64. Так как числа в IP-адресе не могут быть больше 255, мы не можем добавить в конце этого числа еще один разряд, а фрагментов, начинающихся с точки, больше нет, следовательно, этот фрагмент – последний.

Посмотрим на фрагмент под буквой Г. В нем стоит число без точек, значит, это либо последний фрагмент, либо первый. Место последнего фрагмента уже занято, значит, фрагмент Г на первом месте.

В конце фрагмента В - число 133, отделенное точкой. Так как в IP-адресе не может быть числа, большего 255, то за фрагментом В должен следовать фрагмент, начинающийся с точки. Значит, фрагмент В идет перед фрагментом А.

Итого получаем ГБВА.

Ответ: ГБВА

2 задание.

Доступ к файлу ftp.net , находящемуся на сервере txt.org, осуществляется по протоколу http. В таблице фрагменты адреса файла закодированы буквами от А до Ж. Запишите последовательность этих букв, кодирующую адрес указанного файла в сети Интернет.

А	.net
Б	ftp
В	://
Г	http
Д	/
Е	.org
Ж	txt

Решение:

Адрес файла начинается с протокола, после этого ставятся знаки «://», имя сервера, каталог и имя файла. Здесь протокол – под буквой Г, «://» - под буквой В, имя сервера – под буквами ЖЕ, далее идет разделитель «/» (Д), затем – имя файла БА.

Ответ: ГВЖЕДБА

3 задание.

Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес компьютера в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1; младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Если маска подсети 255.255.255.224 и IP-адрес компьютера в сети 162.198.0.157, то порядковый номер компьютера в сети равен_____

Решение:

1. Так как первые три октета (октет - число маски, содержит 8 бит) все равны 255, то в двоичном виде они записываются как 24 единицы, а значит, первые три октета определяют адрес сети.

2. Запишем число 224 в двоичном виде.

$224_{10} = 11100000_2$

3. Запишем последний октет IP-адреса компьютера в сети:

$157_{10} = 10011101_2$

4. Сопоставим последний октет маски и адреса компьютера в сети:

111**00000**

100**11101**

Жирным выделена нужная нам часть, отвечающая (по условию) за адрес компьютера в подсети. Переведем её в десятичную систему счисления:

$11101_2 = 29_{10}$

Ответ: 29

4 задание.

В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно разряды IP-адреса компьютера являются общими для всей подсети – в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел - по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.254.0. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

Решение:

1. Так как первые два октета (октет - число маски, содержит 8 бит)оба равны 255, то в двоичном виде они записываются как 16 единиц, а значит, первые два октета определяют адрес сети.

2. Запишем число 254 в двоичном виде.

$254 = 11111110_2$

В конце этого числа стоит 1 ноль, еще 8 нолей мы получаем из последнего октета маски. Итого у нас есть 9 двоичных разрядов для того, чтобы записать адрес компьютера.

3. $2^9 = 512$, но, так как два адреса не используются, получаем $512 – 2 = 510$.

Ответ: 510

5 задание.

В терминологии сетей TCP/IP маской сети называется двоичное число, определяющее, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. При этом в маске сначала (в старших разрядах) стоят единицы, а затем с некоторого места — нули. Обычно маска записывается по тем же правилам, что и IP-адрес, — в виде четырёх байтов, причём каждый байт записывается в виде десятичного числа. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 98.162.71.94 адрес сети равен 98.162.71.64. Чему равно наибольшее количество возможных адресов в этой сети?

Решение:

Запишем четвёртый байт IP-адреса и адреса сети в двоичной системе счисления:

$9410 = 01011110_2$

$6410 = 01000000_2$

Заметим, что 3 первых слева бита адреса сети совпадают с IP-адресом, а затем идут нули. Чтобы найти, чему равно наибольшее количество возможных адресов в сети, нужно найти количество нулевых бит в последнем байте маски. Значит, поскольку необходимо найти наибольшее количество возможных адресов в этой сети, значение последнего байта маски равняется $11000000_2 = 192_{10}$. Количество нулей в последнем байте маски равняется 6.

Следовательно, наибольшее количество возможных адресов в этой сети равняется $2^6 = 64$.

Ответ: 64

7 задание.

В терминологии сетей TCP/IP маской сети называют двоичное число, которое показывает, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу узла в этой сети. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и его маске. По заданным IP-адресу узла и маске определите адрес сети:

IP-адрес: 145.92.137.88 Маска: 255.255.240.0

При записи ответа выберите из приведенных в таблице чисел 4 фрагмента четыре элемента IP-адреса и запишите в нужном порядке соответствующие им буквы без точек.

A	B	C	D	E	F	G	H
0	145	255	137	128	240	88	92

Решение:

1. Запишем числа маски сети в двоичной системе счисления.

$255_{10} = 11111111_2$

$240_{10} = 11110000_2$

$0_{10} = 00000000_2$

2. Адрес сети получается в результате поразрядной конъюнкции чисел маски и чисел адреса узла (в двоичном коде). Так как конъюнкция 0 с чем-либо всегда равна 0, то на тех местах, где числа маски равны 0, в адресе узла стоит 0. Аналогично, там, где числа маски равны 255, стоит само число, так как конъюнкция 1 с любым числом всегда равна этому числу.

3. Рассмотрим конъюнкцию числа 240 с числом 137.

$240_{10} = 11110000_2$

$137_{10} = 10001001_2$

Результатом конъюнкции является число $10000000_2 = 128$.

4. Сопоставим варианты ответа получившимся числам: 145, 92, 128, 0.

Ответ: ВНЕА

8 задание.

В терминологии сетей TCP/IP маска сети — это двоичное число, меньшее 232; в маске сначала (в старших разрядах) стоят единицы, а затем с некоторого места нули. Маска определяет, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. Обычно маска записывается по тем же правилам, что и IP-адрес — в виде четырёх байт, причём каждый байт записывается в виде десятичного числа. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 84.77.95.123 третий слева байт маски равен 224. Чему равен третий байт адреса сети для этого узла?

Решение:

Рассмотрим третий байт IP-адреса и маски в двоичной системе счисления:

$95_{10} = 01011111_2$

$224_{10} = 1110\ 0000_2$

Следовательно, поскольку три первых слева бита третьего байта маски — единицы, третий байт адреса сети для этого узла равен $01000000_2 = 64_{10}$.

Ответ: 64

9 задание.

В терминологии сетей TCP/IP маской сети называется двоичное число, определяющее, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. При этом в маске сначала (в старших разрядах) стоят единицы, а затем с некоторого места — нули. Обычно маска записывается по тем же правилам, что и IP-адрес, — в виде четырёх байтов, причём каждый байт записывается в виде десятичного числа. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 132.214.141.28 адрес сети равен 132.214.141.0. Укажите наибольшее возможное значение последнего (самого правого) байта маски этой сети. Ответ запишите в виде десятичного числа.

Решение:

Рассмотрим последний байт IP-адреса и адреса сети в двоичной системе счисления:

$28_{10} = 00011100_2$

$0_{10} = 00000000_2$

Видим, что первые 3 бита четвёртого байта маски могут быть единицами и нулями, а четвёртый бит обязательно равен 0. Значит, максимальный четвёртый байт маски имеет вид $11100000_2 = 224_{10}$.

Ответ: 224

10 задание.

В терминологии сетей TCP/IP маска сети — это двоичное число, меньшее 232; в маске сначала (в старших разрядах) стоят единицы, а затем с некоторого места нули. Маска определяет, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети. Обычно маска записывается по тем же правилам, что и IP-адрес — в виде четырёх байт, причём каждый байт записывается в виде десятичного числа. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 224.128.112.142 адрес сети равен 224.128.64.0. Чему равен третий слева байт маски? Ответ запишите в виде десятичного числа.

Решение:

Рассмотрим третий слева байт в IP-адресе узла и адресе сети, представим их в двоичном виде:

$112_{10} = 01110000_2$; $64_{10} = 01000000_2$.

Маской сети является такое двоичное число, которое при поразрядной конъюнкции с IP-адресом узла даст адрес сети, при этом первая часть числа состоит из единиц, а всё остальное – нули. Таким числом является $11000000_2 = 192_{10}$.

Ответ: 192

11 задание.

Для узла с IP-адресом 203.155.196.98 адрес сети равен 203.155.192.0. Найдите наибольшее возможное количество единиц в двоичной записи маски подсети.

Решение:

Заметим, что первый и второй байты IP-адреса и адреса сети равны, следовательно, первый и второй байты маски IP адреса состоят только из единиц.

Запишем третий байт IP-адреса и адреса сети в двоичной системе счисления:

$196_{10} = 11000100_2$

$192_{10} = 11000000_2$

Видим, что два первых слева бита маски − единицы, а биты с третьего по пятый могут быть как нулями, так и единицами. Для того, чтобы значение было наибольшим, эти биты должен быть равны единице. Получаем, что третий слева байт маски равен $11111000_2 = 248_{10}$. В маске сети сначала идут единицы, а затем нули, следовательно, четвёртый байт маски состоит из нулей.

Таким образом, наибольшее количество единиц в двоичной записи маски подсети: 8 + 8 + 5 =21.

Ответ: 21

Рекомендованная литература

Подойдет любая литература адекватного года.

1. «IP-АДРЕСАЦИЯ» Н. В. Ломовцева, Л. В. Волкова
2. «Сети и телекоммуникации: учебник и практикум для СПО» / под ред. К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова