28.11.2020

Здравствуйте, ув. обучающиеся!

Учебная дисциплина: Основы информационных технологий

Тема урока: «Назначение и структура сети Интернет. Адресация в сети Интернет»

Задание к лекции:

Вам необходимо самостоятельно изучить текст лекции, выполнить задания и письменно ответить на контрольные вопросы.

Выполненную работу оформить письменно в рабочих тетрадях (либо в электронном виде) и отправить отдельным файлом (электронный документ) в личное сообщение через социальную сеть VK или на электронную почту преподавателя (ol.sklyarova2015@gmail.com).

Если такой возможности нет, выполненное задание предоставить в распечатанном (рукописном) виде после возобновления занятий.

1. КРАТКИЕ СВЕДЕНИЯ ИЗ ТЕОРИИ:

Структура и основные принципы работы сети Интернет.

Глобальные сети (Wide Area Network, WAN) – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга. Глобальные сети объединяют пользователей, расположенных по всему миру, используя при этом самые разнообразные каналы связи.

Современный Интернет — весьма сложная и высокотехнологичная система, позволяющая пользователю общаться с людьми, находящимися в любой точке земного шара, быстро и комфортно отыскивать любую необходимую информацию, публиковать для всеобщего сведения данные, которые он хотел бы сообщить всему миру.

В действительности Internet не просто сеть, — это структура, объединяющая обычные сети. **Internet — это «сеть сетей».**

Подсеть связи состоит из каналов передачи информации и коммуникационных узлов, которые предназначены для передачи данных по сети, выбора оптимального маршрута передачи информации, коммутации пакетов и реализации ряда других функций с помощью компьютера (одного или нескольких) и соответствующего программного обеспечения, имеющихся в коммуникационном узле. Компьютеры, за которыми работают пользователи-клиенты, называются ***рабочими станциями,*** а компьютеры, являющиеся источниками ресурсов сети, предоставляемых пользователям, называются ***серверами***. Такая структура сети получила название ***узловой***.

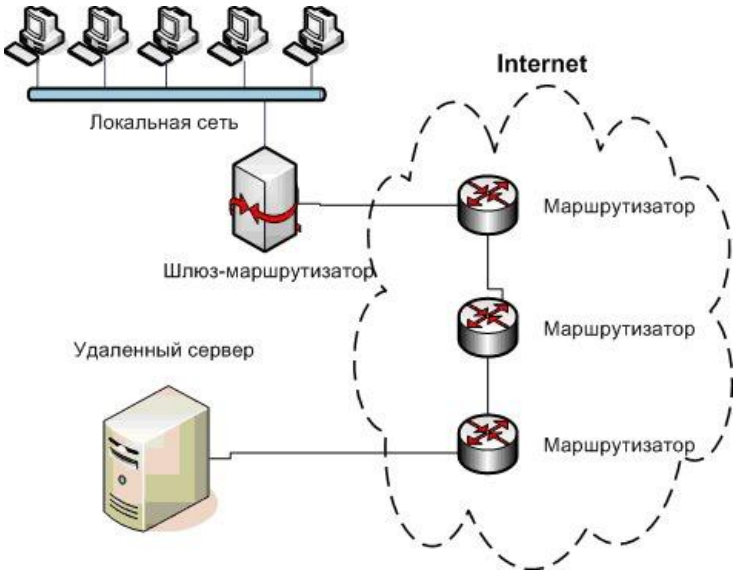


Рис.1 Схема взаимодействия в сети Интернет

Интернет – это глобальная информационная система, которая:

- логически взаимосвязана пространством глобальных уникальных адресов, основанных на Интернет-протоколе (IP);
- способна поддерживать коммуникации с использованием семейства протокола управления передачей - TCP/IP или его последующих расширений/преемников и/или других IP-совместимых протоколов;
- обеспечивает, использует или делает доступными различные услуги.

Инфраструктура Интернет (рис.2):

1. магистральный уровень (система связанных высокоскоростных телекоммуникационных серверов).
2. уровень сетей и точек доступа (крупные телекоммуникационные сети), подключенных к магистрали.
3. уровень региональных и других сетей.
4. ISP – интернет-провайдеры.
5. пользователи.

К техническим ресурсам сети Интернет относятся компьютерные узлы, маршрутизаторы, шлюзы, каналы связи и др.

В основу архитектуры сетей положен ***многоуровневый принцип передачи сообщений***. Формирование сообщения осуществляется на самом верхнем уровне модели ISO/OSI.. Затем (при передаче) оно последовательно проходит все уровни системы до самого нижнего, где и передается по каналу связи адресату. По мере прохождения каждого из уровней системы сообщение трансформируется, разбивается на сравнительно короткие части, которые снабжаются дополнительными заголовками, обеспечивающими информацией аналогичные уровни на узле адресата. В этом узле сообщение проходит от нижнего уровня к верхнему, снимая с себя заголовки. В результате адресат принимает сообщение в первоначальном виде.

Рис.2 Инфраструктура сети Интернет

В территориальных сетях ***управление обменом данных*** осуществляется протоколами верхнего уровня модели ISO/OSI. Независимо от внутренней конструкции каждого конкретного протокола верхнего уровня для них характерно наличие общих функций: инициализация связи, передача и прием данных, завершение обмена. Каждый протокол имеет средства для идентификации любой рабочей станции сети по имени, сетевому адресу или по обоим этим атрибутам. Активизация обмена информацией между взаимодействующими узлами начинается после идентификации узла адресата узлом, инициирующим обмен данными. Инициирующая станция устанавливает один из методов организации обмена данными: ***метод дейтаграмм*** или метод сеансов связи. Протокол предоставляет средства для приема/передачи сообщений адресатом и источником. При этом обычно накладываются ограничения на длину сообщений.

TCP/IP — технология межсетевого взаимодействия

Наиболее распространенным протоколом управления обменом данных является протокол TCP/IP. **Главное отличие сети Internet от других сетей заключается именно в ее протоколах TCP/IP**, охватывающих целое семейство протоколов взаимодействия между компьютерами сети. **TCP/IP** — это технология межсетевого взаимодействия, технология Internet. Поэтому глобальная сеть, объединяющая множество сетей с технологией **TCP/IP**, называется **Internet.**

Протокол TCP/IP — это семейство программно реализованных протоколов старшего уровня, не работающих с аппаратными прерываниями. Технически протокол TCP/IP состоит из двух частей — IP и TCP.

Протокол IP (Internet Protocol — межсетевой протокол) является главным протоколом семейства, он реализует распространение информации в IP-сети и

выполняется на третьем (сетевом) уровне модели ISO/OSI. Протокол IP обеспечивает дейтаграммную доставку пакетов, его основная задача — маршрутизация пакетов. Он не отвечает за надежность доставки информации, за ее целостность, за сохранение порядка потока пакетов. Сети, в которых используется протокол IP, называются IP-сетями. Они работают в основном по аналоговым каналам (т.е. для подключения компьютера к сети требуется IP-модем) и являются сетями с коммутацией пакетов. Пакет здесь называется **дейтаграммой.**

Высокоуровневый протокол TCP (Transmission Control Protocol — протокол управления передачей) работает на транспортном уровне и частично — на сеансовом уровне. Это протокол с установлением логического соединения между отправителем и получателем. Он обеспечивает сеансовую связь между двумя узлами с гарантированной доставкой информации, осуществляет контроль целостности передаваемой информации, сохраняет порядок потока пакетов.

Для компьютеров протокол TCP/IP — это то же, что правила разговора для людей. Он принят в качестве официального стандарта в сети Internet, т.е. сетевая технология TCP/IP де-факто стала технологией всемирной сети Интернет.

Ключевую часть протокола составляет схема маршрутизации пакетов, основанная на уникальных адресах сети Internet. Каждая рабочая станция, входящая в состав локальной или глобальной сети, имеет уникальный адрес, который включает две части, определяющие адрес сети и адрес станции внутри сети. Такая схема позволяет передавать сообщения как внутри данной сети, так и во внешние сети.

Работа сети Internet основана на использовании семейств коммуникационных протоколов **TCP/IP (Transmission Control Protocol/Internet Protocol).** TCP/IP используется для передачи данных как в глобальной сети Internet, так и во многих локальных сетях.

Название TCP/IP определяет семейство протоколов передачи данных сети. **Протокол** — это набор правил, которых должны придерживаться все компании, чтобы обеспечить совместимость производимого аппаратного и программного обеспечения. Эти правила гарантируют совместимость производимого аппаратного и программного обеспечения. Кроме того, TCP/IP – это гарантия того, что ваш персональный компьютер сможет связаться по сети Internet с любым компьютером в мире, также работающим с TCP/IP. При соблюдении определенных стандартов для функционирования всей системы не имеет значения, кто является производителем программного обеспечения или аппаратных средств. Идеология открытых систем предполагает использование стандартных аппаратных средств и программного обеспечения. **TCP/IP — открытый протокол и вся специальная информация издана и может быть свободно использована.**

Различный сервис, включаемый в TCP/IP, и функции этого семейства протоколов могут быть классифицированы по типу выполняемых задач. Упомянем лишь основные протоколы, так как общее их число насчитывает не один десяток:

транспортные протоколы — управляют передачей данных между двумя машинами**:**

- **TCP/IP** (Transmission Control Protocol),
- **UDP** (User Datagram Protocol);

протоколы маршрутизации — обрабатывают адресацию данных, обеспечивают фактическую передачу данных и определяют наилучшие пути передвижения пакета**:**

- **IP** (Internet Protocol),
- **ICMP** (Internet Control Message Protocol),
- **RIP** (Routing Information Protocol)

и другие;

протоколы поддержки сетевого адреса — обрабатывают адресацию данных, обеспечивают идентификацию машины с уникальным номером и именем**:**

- **DNS** (Domain Name System),
- **ARP** (Address Resolution Protocol)

и другие;

протоколы прикладных сервисов — это программы, которые пользователь (или компьютер) использует для получения доступа к различным услугам**:**

- **FTP** (File Transfer Protocol),
- **TELNET**,
- **HTTP** (HyperText Transfer Protocol)
- **NNTP** (NetNewsTransfer Protocol)

и другие

Сюда включается передача файлов между компьютерами, удаленный терминальный доступ к системе, передача гипермедийной информации и т.д.;

шлюзовые протоколы помогают передавать по сети сообщения о маршругазации и информацию о состоянии сети, а так же обрабатывать данные для локальных сетей**:**

- **EGP** (Exterior Gateway Protocol),
- **GGP** (Gateway-to-Gateway Protocol),
- **IGP** (Interior Gateway Protocol);

другие протоколы – используются для передачи сообщений электронной почты, при работе с каталогами и файлами удаленного компьютера и так далее**:**

- **SMTP** (Simple Mail Transfer Protocol),
- **NFS** (Network File System).

Доменные имена

Кроме IP-адресов, для идентификации конкретных хостов в Сети используется так называемое ***доменное имя хоста (Domain host name)***. Так же, как и IP-адрес, это имя ***является уникальным для каждого компьютера (хоста)***, подключенного к Internet, — только здесь вместо цифровых значений адреса применяются слова.

В данном случае понятие ***домена*** означает ***совокупность хостов Internet, объединенных по какому-то признаку*** (например, по территориальному, когда речь идет о домене государства).

Разумеется, использование доменного имени хоста было введено только для того, чтобы облегчить пользователям задачу запоминания имен нужных им компьютеров. Сами компьютеры, по понятным причинам, в таком сервисе не нуждаются и вполне обходятся IP-адресами. Но вы только представьте, что вместо таких звучных имен как, *www.microsoft.com* или *www.ibm.com* вам пришлось бы запоминать наборы цифр, — 207.46.19.190 или 129.42.60.216 соответственно.

Чаще всего доменное имя компании состоит из трех составляющих, первая часть — имя хоста, вторая — имя домена компании, и последняя — имя домена страны или имя одного из семи специальных доменов, обозначающих принадлежность хоста, организации определенного профиля деятельности (см. табл. 1). Так, если ваша компания называется «KomLinc», то чаще всего Web-сервер компании будет назван www.komlinc.ru (если это российская компания), или, к примеру, www.komlinc.com, если вы попросили провайдера зарегистрировать вас в основном международном домене коммерческих организаций.

Последняя часть доменного имени называется идентификатором домена верхнего уровня (например, *.ru* или *.com*). Существует семь доменов верхнего уровня, установленных InterNIC.

Таблица 1. Международные домены верхнего уровня

Имя домена	Принадлежность хостов домена
ARPA	Пра-пра... бабушка Internet, сеть ARPANet (выходит из употребления)
COM	Коммерческие организации (фирмы, компании, банки и так далее)
GOV	Правительственные учреждения и организации
EDU	Образовательные учреждения
MIL	Военные учреждения
NET	«Сетевые» организации, управляющие Internet или входящие в его структуру
ORG	Организации, которые не относятся ни к одной из перечисленных категорий

Исторически сложилось так, что эти семь доменов верхнего уровня по умолчанию обозначают факт географического расположения (принадлежащего к ним) хоста на территории США. Поэтому международный комитет InterNIC

наряду с вышеперечисленными доменами верхнего уровня допускает применение доменов (специальных сочетаний символов) для идентификации иных стран, в которой находится организация-владелец данного хоста.

Итак, домены верхнего уровня подразделяются на **организационные** (см. табл.1) и **территориальные.** Имеются двухбуквенные обозначения для всех стран мира: *.ru* — для России (пока в ходу и домен *.su,* объединяющий хосты на территории республик бывшего СССР), *.ca* — для Канады, *.uk* — для Великобритании и т.д. Они обычно используются вместо одного из семи идентификаторов, перечисленных выше в таблице 1.

Территориальные домены верхнего уровня:

.ru (Russia)— Россия;
.su (Soviet Union) — страны бывшего СССР, ныне ряд государств СНГ;
.uk (United Kingdom) — Великобритания;
.ua (Ukraine) — Украина;
.bg (Bulgaria) — Болгария;
.hu (Hungary) — Венгрия;
.de (Deutchland) — Германия, и др.

С полным списком всех доменных имен государств можно познакомиться на различных серверах в Internet.

Не все компании за пределами США имеют идентификаторы страны. В какой-то мере использование идентификатора страны или одного из семи идентификаторов, принятых в США, зависит от того, когда проводилась регистрация доменного имени компании. Так, компаниям, которые достаточно давно подключились к Internet (когда число зарегистрированных организаций было сравнительно невелико), был дан трехбуквенный идентификатор. Некоторые корпорации, работающие за пределами США, но регистрирующие доменное имя через американскую компанию, сами выбирают, использовать ли им идентификатор страны пребывания. Сегодня в России можно получить доменный идентификатор *.com,* для чего следует оговорить этот вопрос со своим провайдером Internet.

Как работают серверы DNS

Теперь поговорим о том, каким образом доменные имена преобразуются в понятные для компьютера IP-адреса.

Занимается этим **Domain Name System (DNS, Доменная система имен)** сервис, обеспечиваемый TCP/IP, который помогает в адресации сообщений. Именно благодаря работе DNS вы можете не запоминать IP-адрес, а использовать намного более простой доменный адрес. Система DNS транслирует символическое доменное имя компьютера в IP-адрес, находя запись в распределенной базе

данных (хранящейся на тысячах компьютерах), соответствующую этому доменному имени. Стоит также отметить, что серверы DNS в русскоязычной компьютерной литературе часто называют **«серверами имен».**

Основы IP-адресации

Первым обязательным параметром в свойствах протокола TCP/IP любого компьютера является его IP-адрес.

IP-адрес — это уникальная 32-разрядная последовательность двоичных цифр, с помощью которой компьютер однозначно идентифицируется в IP-сети. (Напомним, что на канальном уровне в роли таких же уникальных адресов компьютеров выступают MAC-адреса сетевых адаптеров, невозможность совпадения которых контролируется изготовителями на стадии производства.)

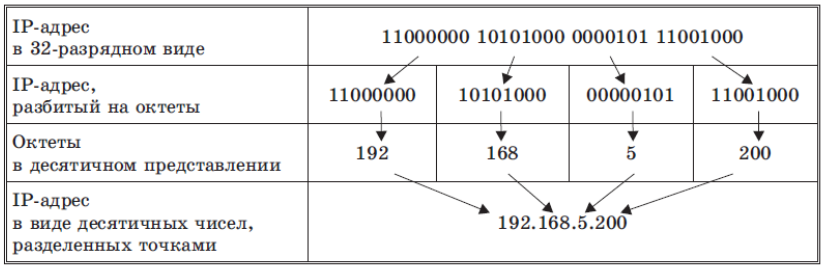
Мы будем обсуждать наиболее распространенная версию 4 протокола IP, или IPv4. Однако уже создана следующая версия протокола IP версии 6 (IPv6), в которой IP-адрес представляется в виде 128-битной последовательности двоичных цифр. Эта версия протокола IP пока еще не получила широкого распространения, хотя и поддерживается многими современными маршрутизаторами и операционными системами (например, Windows XP или Windows Server 2003).

IP v6	**Протокол IP v6 — в Windows XP**
Многие активно развивающиеся в техническом отношении страны (Китай, Япония, Корея и др.) начинают испытывать дефицит IP-адресов, идентифицирующих не только компьютеры, но и другие устройства с функциями доступа в Интернет. Принятый сейчас 32-битовый стандарт обеспечивает количество IP-адресов, равное почти 4,3 млрд., но их большая часть закреплена за США (около 70%), Канадой и европейскими странами, а вот, например, КНР получила их всего 22 млн. Новая, 128-разрядная версия протокола IP v.6 позволит увеличить количество IP-адресов до огромной величины — 3.4*10^38	Для использования протокола IPv6 в Windows XP имеется необходимое программное обеспечение, которое, однако, по умолчанию не активизировано. Чтобы задействовать новый протокол, достаточно в командной строке (меню **Пуск, Выполнить**) ввести и запустить на исполнение команду ipv6 install. Получить необходимые справки по работе с протоколом IPv6 можно (после его инсталляции) командой ipv6 /? .

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 битов (на октеты), каждый октет переводят в десятичное число и при записи разделяют эти числа точками. В таком виде (это представление называется «десятичные числа с точками», или, по-английски,

«dotted-decimal notation») IP-адреса занимают гораздо меньше места и намного легче запоминаются.

Различные представления IP-адреса



Чтобы быстро осуществлять подобное преобразование в уме (что сетевым администраторам требуется нередко, а калькулятор не всегда под рукой), полезно запомнить следующую таблицу. В ней приведены десятичные значения степеней числа 2 с показателем, равным порядковому номеру бита в октете (напомним нумерация битов производится справа налево и начинается с нуля):

Порядковый номер бита в октете	7	6	5	4	3	2	1	0
2 в степени, соответствующей номеру бита	128	64	32	16	8	4	2	1

Запомнив такую таблицу, несложно в уме преобразовывать октеты в десятичные числа и обратно. Десятичное число легко вычисляется как сумма цифр, соответствующих ненулевым битам в октете, например:

10101101 □□128 · 1 + 64 · 0 + 32 · 1 + 16 · 0 + 8 · 1 + 4 · 1 + 2 · 0 + 1 · 1 = 173.

Несколько сложнее перевести десятичное представление в двоичное, но при некоторой тренировке это также не представляет проблем. Например:

201_{10} =128 · 1 + 64 · 1 + 32 · 0 + 16 · 0 + 8 · 1 + 4 · 0 + 2 · 0 + 1 · 1 = 11001001_2.

Однако одного только IP-адреса компьютеру для работы в сети TCP/IP недостаточно. Вторым обязательным параметром, без которого протокол TCP/IP работать не будет, является маска подсети.

Маска подсети — это 32-разрядное число, состоящее из идущих вначале единиц, а затем — нулей, например (в десятичном представлении) 255.255.255.0 или 255.255.240.0.

Маска подсети играет исключительно важную роль в IP-адресации и маршрутизации. Чтобы понять значение этого параметра, вспомним, что сеть ARPANet строилась как набор соединенных друг с другом гетерогенных сетей. Для правильного взаимодействия в такой сложной сети каждый участник должен уметь определять, какие IP-адреса принадлежат его локальной сети, а какие удаленным сетям.

Здесь и используется маска подсети, с помощью которой производится *разделение любого IP-адреса на две части: идентификатор сети (Net ID) и идентификатор узла (Host ID).* Такое разделение делается очень просто: там, где в

маске подсети стоят единицы, находится идентификатор сети, а где стоят нули идентификатор узла.

Например, в IP-адресе 192.168.5.200 при использовании маски подсети 255.255.255.0 идентификатором сети будет число 192.168.5.0, а идентификатором узла число 200. Стоит нам поменять маску подсети, скажем, на число 255.255.0.0, как и идентификатор узла, и идентификатор сети изменятся на 192.168.0.0 и 5.200, соответственно, и от этого, как мы дальше увидим, иначе будет вести себя компьютер при посылке IP-пакетов.

Правила назначения IP-адресов сетей и узлов

Теперь, когда мы знаем, что такое IP-адрес, маска подсети, идентификаторы сети и узла, полезно запомнить правила, которые следует применять при назначении этих параметров:

1) идентификатор сети не может содержать только двоичные нули или только единицы. Например, адрес 0.0.0.0 не может являться идентификатором сети;
2) идентификатор узла также не может содержать только двоичные нули или только единицы такие адреса зарезервированы для специальных целей:
    - все нули в идентификаторе узла означают, что этот адрес является адресом сети. Например, 192.168.5.0 является правильным адресом сети при использовании маски 255.255.255.0 и его нельзя использовать для адресации компьютеров;
    - все единицы в идентификаторе узла означают, что этот адрес является адресом широковещания для данной сети. Например, 192.168.5.255 является адресом широковещания в сети 192.168.5.0 при использовании маски 255.255.255.0 и его нельзя использовать для адресации компьютеров;
3) идентификатор узла в пределах одной и той же подсети должен быть уникальным;
4) диапазон адресов от 127.0.0.1 до 127.255.255.254 нельзя использовать в качестве IP-адресов компьютеров. Вся сеть 127.0.0.0 по маске 255.0.0.0 зарезервирована под так называемый «адрес заглушки» (loopback), используемый в IP для обращения компьютера к самому себе. Это легко проверить: достаточно на любом компьютере с установленным протоколом TCP/IP выполнить команду PING 127.12.34.56 и, если протокол TCP/IP работает, вы увидите, как ваш компьютер будет отвечать на собственные запросы.

Классовая и бесклассовая IP-адресация

Первоначальная система IP-адресации в Интернете выглядела следующим образом. Все пространство возможных IP-адресов (а это более четырех миллиардов, точнее 4 294 967 296 адресов) было разбито на пять классов, причем принадлежность IP-адреса к определенному классу определялась по нескольким битам первого октета (см. табл.). Заметим, что для адресации сетей и узлов использовались только классы A, B и C. Кроме того, для этих сетей были определены фиксированные маски подсети по умолчанию, равные, соответственно, 255.0.0.0, 255.255.0.0 и 255.255.255.0, которые не только жестко определяли диапазон возможных IP-адресов узлов в таких сетях, но и механизм маршрутизации.

Классы адресов в первоначальной схеме IP-адресации

Класс	Первые биты в октете	Возможные значения первого октета	Возможное число сетей	Возможное число узлов в сети
A	0	1–126	126	16777214
B	10	128–191	16384	65534
C	110	192–223	2097152	254
D	1110	224–239	Используется для многоадресной рассылки (multicast)	
E	1111	240–254	Зарезервирован как экспериментальный	

Чтобы рассчитать максимально возможное количество узлов в любой IP-сети, достаточно знать, сколько битов содержится в идентификаторе узла, или, иначе, сколько нулей имеется в маске подсети. Это число используется в качестве показателя степени двойки, а затем из результата вычитается два зарезервированных адреса (сети и широковещания). Аналогичным способом легко вычислить и возможное количество сетей классов A, B или C, если учесть, что первые биты в октете уже зарезервированы, а в классе A нельзя использовать IP-адреса 0.0.0.0 и 127.0.0.0 для адресации сети.

Для получения нужного диапазона IP-адресов организациям предлагалось заполнить регистрационную форму, в которой следовало указать текущее число компьютеров и планируемый рост компьютерного парка в течение двух лет. Первоначально данная схема хорошо работала, поскольку количество сетей было небольшим. Однако с развитием Интернета такой подход к распределению IP-адресов стал вызывать проблемы, особенно острые для сетей класса B. Действительно, организациям, в которых число компьютеров не превышало нескольких сотен (скажем, 500), приходилось регистрировать для себя целую сеть класса B. Поэтому количество доступных сетей класса B стало на глазах «таять», но при этом громадные диапазоны IP-адресов (в нашем примере более 65000) пропадали зря.

Чтобы решить проблему, была разработана бесклассовая схема IP-адресации (Classless InterDomain Routing, CIDR), в которой не только отсутствует привязка IP-адреса к классу сети и маске подсети по умолчанию, но и допускается применение так называемых масок подсети с переменной длиной (Variable Length

Subnet Mask, VLSM). Например, если при выделении сети для вышеуказанной организации с 500 компьютерами вместо фиксированной маски 255.255.0.0 использовать маску 255.255.254.0, то получившегося диапазона из 512 возможных IP-адресов будет вполне достаточно. Оставшиеся 65 тысяч адресов можно зарезервировать на будущее или раздать другим желающим подключиться к Интернету.

Этот подход позволил гораздо более эффективно выделять организациям нужные им диапазоны IP-адресов, и проблема с нехваткой IP-сетей и адресов стала менее острой.

IP-адреса для локальных сетей

Все используемые в Интернете адреса, как мы уже говорили, должны регистрироваться в IANA, что гарантирует их уникальность в масштабе всей планеты. Такие адреса называют реальными, или публичными (public) IP-адресами.

Для локальных сетей, не подключенных к Интернету, регистрация IP-адресов, естественно, не требуется, так что, в принципе, здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к Интернету, RFC 1918 рекомендует применять в локальных сетях только следующие диапазоны так называемых частных (private) IP-адресов (в Интернете эти адреса не существуют и использовать их там нет возможности):

- 10.0.0.0 - 10.255.255.255;
- 172.16.0.0 - 172.31.255.255;
- 192.168.0.0 - 192.168.255.255.

1 Определение адреса сети и номера компьютера в сети

Определение адреса сети и номер компьютера в сети, если IP-адрес компьютера 192.168.1.2 , а маска подсети 255.255.254.0.

Алгоритм:

1. Перевести числа в двоичный код.

IP-адрес: 11000000 10101000 00000001 00000010 (192.168.1.2)

Маска подсети: 11111111 11111111 11111110 00000000 (255.255.254.0)

Адрес сети: 11000000 10101000 00000000 00000000 (192.168.0.0)

2. Применить к ним операцию поразрядной конъюнкции (побитовое И)

```
IP-адрес:       11000000 10101000 00000001 00000010 (192.168.1.2)
Маска подсети:  11111111 11111111 11111110 00000000 (255.255.254.0)
Адрес сети:     11000000 10101000 00000000 00000000 (192.168.0.0)
```

Легенда:

- часть маски, определяющая адрес сети и состоящая из единиц;
- адрес сети, который определяется маской подсети;
- диапазон адресов устройств в этой сети.

3. Записать адрес сети и номер компьютера в сети

Адрес сети: 11000000 10101000 00000000 00000000 (192.168.0.0)

Номер компьютера в сети: 00000000 00000000 00000001 00000010 (0.0.1.2)

САМОСТОЯТЕЛЬНО

По заданным IP-адресу и маске сети определите адрес сети:

IP-адрес: 224.23.252.131

Маска: 255.255.240.0

2 Определение возможного количества компьютеров в сети по маске подсети

Маска сети: 255.255.254.0

Алгоритм:

Представим число в двоичном виде
11111111.11111111.11111110.00000000
Общее количество нулевых бит - 9
Число компьютеров в сети: 2^9 -2= 510
Ответ: возможно 510 компьютеров в сети

САМОСТОЯТЕЛЬНО

Определить возможное количество компьютеров в сети по маске подсети

255.255.240.0

3 Определение порядкового номера в сети

САМОСТОЯТЕЛЬНО

1. **Решить самостоятельно**

*Если маска подсети **255.255.255.248** и IP-адрес компьютера в сети **156.128.0.227**, то номер компьютера в сети равен _____.*

2. ЗАДАНИЯ К ЛЕКЦИИ

1. Ознакомиться с теоретическим материалом лекции.
2. Законспектировать в тетради материал.
3. Изучить конспект.
4. По заданным IP-адресу и маске сети определите адрес сети: **IP-адрес:** 224.23.252.131 **Маска:** 255.255.240.0.
5. Определить возможное количество компьютеров в сети по маске подсети 255.255.240.0
6. Устно ответить на контрольные вопросы.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем заключается структура и принцип функционирования сети Интернет?
2. Что такое протоколы. Назовите наиболее инзвестные протоколы Интернет.
3. Какие бывают виды адресов компьютеров в сети?
4. Что такое DNS?
5. К какому классу сетей относится Ваш компьютер?
6. Для чего нужна маска подсети?
7. Как определить количество компьютеров в сети по маске?