Лабораторная работа № 9
Изучение адресации сетевого уровня IPv4

Цель работы: Изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных.

Оборудование: персональный компьютер, включенный в сеть IP, Microsoft Windows.

1. Основные сведения

Сетевой уровень (network layer) служит для образования единой транспортной системы, объединяющей несколько сетей LAN разных технологий (Ethernet, Token Ring, FDDI), PAN, MAN, Wi-Fi, просто отдельных компьютеров (host) в единую сеть - называемой составной сетью, ярким примером такой сети является Интернет. Сетевой уровень широко используются в глобальных сетях WAN.

Сетевой уровень отвечает за возможность доставки **ПАКЕТОВ** по составной сети передачи данных – совокупности сегментов LAN - сетей, PAN, MAN, Wi-Fi, Token Ring, FDDI объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Технология, позволяющая соединить в единую сеть множество разнотипных сетей, в общем случае построенных на основе разных технологий, называется **технологией межсетевого взаимодействия.**

Чтобы связать между собой сети, построенные на основе столь отличающихся технологий, нужны ***дополнительные средства***, и такие средства предоставляет сетевой уровень.

Функции сетевого уровня реализуются:

- группой протоколов;
- специальными устройствами — маршрутизаторами.

Одной из функций маршрутизатора является ***физическое соединение сетей***. Маршрутизатор имеет несколько сетевых интерфейсов, подобных интерфейсам компьютера, к каждому из которых может быть подключена одна сеть. Таким образом, все интерфейсы маршрутизатора можно считать узлами разных сетей. Маршрутизатор может быть реализован программно, на базе универсального компьютера (например, типовая конфигурация Unix или Windows включает программный модуль маршрутизатора). Однако чаще маршрутизаторы реализуются на базе специализированных аппаратных платформ. В состав программного обеспечения маршрутизатора входят протокольные модули сетевого уровня.

Таким образом, чтобы связать разнородные сети, необходимо соединить все эти сети маршрутизаторами и установить протокольные модули сетевого уровня на все конечные узлы пользователей, которые хотели бы связываться через составную сеть

Для того чтобы протоколы сетевого уровня могли доставлять пакеты любому узлу составной сети, эти узлы должны иметь адреса, уникальные в пределах данной составной сети. Такие адреса называются **сетевыми, или глобальными.** *Каждый узел составной сети, который намерен обмениваться данными с другими узлами*

составной сети, должен иметь ***сетевой адрес наряду с адресом, назначенным ему на канальном уровне.***

На сетевом уровне применяются два вида стеков протоколов. Первый вид — ***маршрутизируемые протоколы*** — реализуют продвижение пакетов через сеть. Второй вид протоколов, называется ***маршрутизирующими протоколами***, или протоколами маршрутизации. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений, на основании которой осуществляется выбор маршрута продвижения пакетов.

Сетевой уровень, также решает задачу создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

В настоящее время самым распространенным, достаточным является сетевой протокол TCP/IP

В связи с необходимостью пере направлять пакеты из одной подсети сети в другую, сетевые адреса должны удовлетворять следующим требованиям:

1. Адреса должны быть уникальны. В сети не может быть нескольких участников с одинаковыми адресами во избежание неоднозначности.
2. Сетевой адрес должен содержать информацию о том, как достичь получателя по сети, т.е. он должен иметь адрес подсети и адрес получателя.

Это приводит к **СТРУКТУРНОСТИ АДРЕСА** – адрес разбивается на части, позволяющие определить местоположение участника внутри сети.

Адрес в составной сети может быть цифровым, так и символьным. Структура символьного адреса может быть сложной многоуровневой, например адрес содержит информацию о стране, области, населенном пункте, предприятии, здании, отделе и т.д. Цифровой адрес простой: содержащей номер сети и номер компьютера в сети.

Примером такой адресации может служить доменная адресация в Интернет, по адресу asu.bru.mogilev.by нетрудно понять, где находится данный участник сети и как до него добраться. В цифровой форме 10.203.0.120. Цифровая структура адреса позволяет значительно сократить размер адреса и сохраняет возможность работы в сети любой структуры, но для этого могут потребоваться сложные и, часто, не столь очевидные алгоритмы, как в предыдущем случае.

2. ПРОТОКОЛ IP (INTERNET PROTOCOL)

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов **TCP/IP**» означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC описывают внутреннюю работу сети Internet. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию. Стандарты TCP/IP всегда публикуются в виде документов RFC, но не все RFC определяют стандарты.

2.1 НАЗНАЧЕНИЕ IP

IP-протокол создан для использования в объединенных системах компьютерных коммуникационных сетей с коммутацией пакетов. Протокол IP-обеспечивает передачу блоков данных, называемых датаграммами (дейтаграммами), от отправителя к получателям, где отправители и получатели являются узлами, идентифицируемыми адресами фиксированной длины. IP-протокол обеспечивает, при необходимости также фрагментацию и сборку датаграмм для передачи данных через сети с малым размером пакетов.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом **маршрутизаторами (шлюзами)** отдельных разнородных пакетных **подсетей**, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

В Интернет используется много различных типов пакетов, но один из основных - IP-пакет (RFC-791), именно он вкладывается в кадр Ethernet и именно в него вкладываются пакеты UDP, TCP. **IP-протокол предлагает ненадежную** транспортную среду. Ненадежную, в том смысле, что не существует гарантии благополучной доставки IP-дейтограммы. **Не требуется**, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Алгоритм доставки в рамках данного протокола предельно прост: при ошибке дейтограмма выбрасывается, а отправителю посылается соответствующее ICMP-сообщение (или не посылается ничего). Обеспечение же надежности возлагается на более высокий уровень (UDP или TCP).

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (**маршрутизатор**), который подключен к подсети как обычный узел. Оттуда пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той подсети, что и машина-получатель, там пакет направляется к получателю.

2.2 Функциональность IP

IP-протокол выполняет две главные функции: адресацию и фрагментацию.

Протокол IP используют адреса, помещенные в заголовок IP-пакета. Для передачи используются датаграммы[1]. Выбор пути передачи называется маршрутизацией.

Программные модули IP маршрутизаторов (шлюзов) используют поля в заголовке IP-пакета для фрагментации и восстановления IP-датаграмм, когда это необходимо для их передачи через сети с малым размером пакетов, а также имеют процедуры для принятия решений о маршрутизации, и другие функции.

Протокол IP обрабатывает каждую IP-датаграмму как независимую единицу, не имеющую связи ни с какими другими датаграммами. Протокол не имеет дело ни

с соединениями, ни с логическими цепочками (виртуальными или какими-либо другими).

IP-протокол использует четыре ключевых механизма для формирования своих услуг: *задание типа сервиса, времени жизни, опций и контрольной суммы заголовка.*

Тип обслуживания используется для обозначения требуемой услуги. Тип обслуживания — это абстрактный или обобщенный набор параметров, который характеризует набор услуг, предоставляемых сетями, и составляющих собственно протокол IP. Этот способ обозначения услуг должен использоваться шлюзами для выбора рабочих параметров передачи в конкретной сети, для выбора сети, используемой при следующем переходе датаграммы, для выбора следующего шлюза при маршрутизации сетевой IP-датаграммы.

Механизм ***времени жизни*** служит для указания верхнего предела времени жизни IP-датаграммы. Этот параметр устанавливается отправителем датаграммы и уменьшается в каждой точке на проходимом датаграммой маршруте. Если параметр времени жизни станет нулевым до того, как IP-датаграмма достигнет получателя, эта датаграмма будет уничтожена. Время жизни можно рассматривать как часовой механизм самоуничтожения.

Механизм опций предоставляет функции управления, которые являются необходимыми или просто полезными при определенных ситуациях, однако он не нужен при обычных коммуникациях. Механизм опций предоставляет такие возможности, как временные штампы, безопасность, специальная маршрутизация.

Контрольная сумма заголовка обеспечивает проверку того, что информация, используемая для обработки IP-датаграмм, передана правильно. Данные могут содержать ошибки. Если контрольная сумма неверна, то IP-датаграмма будет разрушена, как только ошибка будет обнаружена.

Протокол IP не обеспечивает надежности коммуникации. Не имеется механизма подтверждений ни между отправителем и получателем, ни между узлами. Не имеется контроля ошибок для поля данных, только контрольная сумма для заголовка. Не поддерживается повторная передача, нет управления потоком.

Обнаруженные ошибки могут быть оглашены посредством протокола ICMP (Internet Control Message Protocol), который поддерживается модулем IP протокола

3. Сетевые IP-адреса

В технологии TCP/IP сетевой адрес называют **IP-адрес**.

Адреса получателя и отправителя должны содержать в себе:

1. номер (адрес) подсети;
2. номер (адрес) участника (хоста) внутри подсети.

IP адреса представляют собой **32-х разрядные двоичные числа**. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса

192.168.200.47

является десятичным эквивалентом двоичного адреса

11000000.10101000.11001000.00101111 *(точки оставлены для удобства)*.

Иногда применяют десятичное значение IP-адреса. Его легко вычислить

$192*256^3+168*256^2+200*256^1+47**256^0 = 3232286767$

или с помощью метода Горнера :

$(((192*256)+168)*256+200)*256+47=3232286767$

Таблица 9.1. Перевод некоторых чисел из двоичной системы счисления в десятичную и обратно.

Двоичное	Десятичное
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

IP-адрес содержит информацию адреса подсети и адреса узла в ней.

Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла, но необходимость в этом несомненно есть. Для решения этой проблемы используются несколько вариантов:

- Первоначально использовался простой способ, а именно: адрес фиксировано, жестко разбивался на две части (RFC 760). Очевидно, что такой жесткий подход не позволяет дифференцированно удовлетворять потребности отдельных предприятий и организаций. Он не нашел широкого применения.
- Второй подход, распространенный до недавнего времени заключается в использовании классов адресов (RFC 791). Вводится пять классов адресов: A, B, C, D, E. Три: из них- A, B и C- используются для адресации сетей, а два- D и E- имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером узла.
- И наконец, третий способ (RFC 950, RFC 1518) основан на использовании маски, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла. При таком подходе адресное пространство можно использовать для создания множества сетей разного размера. Для этих целей наряду с IP адресом введено такое понятие как маска.

  Практический интерес представляют два последних способа построения адреса IP.

3.1 Классы IP-адресов.

Признаком, на **основании** которого IP-адрес относится к тому или иному классу, являются значения нескольких первых битов адреса - таблица. 9.2.

ТАБЛИЦА 9. 2. КЛАССЫ НОМЕРОВ IP

Класс	**Первые биты**	**Наименьший номер сети**	**Наибольший номер сети**	**Максимальное числю узлов в сети**
A	0	1.0.0.0 (0 - не используется)	126.0.0.0 **(127** — зарезервирован)	2^{24} поле 3 байта
B	10	128.0.0.0	191.255.0.0	2^{16}, поле 2 байта
C	110	192.0.0.0	223.255.255.0	2^{8}, поле 1 байт
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано

- **Адреса класса А** назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Это позволяет иметь 2^7-2=126 сетей с числом узлов до 2^{24} =16 777 216 в каждой. Адреса сетей могут принимать значения от 1 (00000001) до 126 (01111110). Из-за ограничений, о которых будет говорится ниже, значение 0 (00000000) первого байта не используется, а значение 127 (01111111) зарезервировано для "внутренней петли».
- **К классу В** относятся все адреса, старшие два бита которых имеют значение 10. В адресах класса **В** ***под номер сети*** и **под номер узла** отводится по два байта. Сети, значения первых двух байтов адресов которых находятся в диапазоне от 128.0. (10000000 00000000) до 191.255 (10111111 11111111), называются сетями класса В. Ясно, что сетей класса В больше, чем сетей класса А, а размеры их меньше.. Максимальное количество узлов в сетях класса В составляет 2^{16} = (65 536).
- **К классу С** относятся все адреса, старшие три бита которых имеют значение 110. **В адресах класса С под номер сети отводится 3 байта, а под номер узла 1 байт**. Сети, старшие три байта которых находятся в диапазоне от 192.0.0 (11000000 00000000 00000000) до 223.255 (11011111 11111111 11111111), называются сетями: класса С. Сети класса С наиболее распространены и имеют наименьшее максимальное число узлов-2^8 степени (256).
- **Если адрес** начинается с последовательности **1110**, то он является адресом **класса D** и обозначает особый, групповой адрес (multicast address). В то время как адреса классов А, В и С используются для идентификации отдельных сетевых интерфейсов, то есть являются **индивидуальными адресами** (unicast address), **групповой адрес идентифицирует группу сетевых интерфейсов, которые в общем случае могут принадлежать разным сетям.** Интерфейс, входящий в группу, получает наряду с обычным индивидуальным IP-адресом еще один групповой адрес. Если при отправке

пакета в качестве адреса назначения указан адрес класса D, то такой пакет должен быть доставлен всем узлам, которые входят в группу.

- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к **<u>классу E</u>**. Адреса этого класса зарезервированы для будущих применений.

На Рис 9.1 Показана двоичная схема классов IP-адресов.

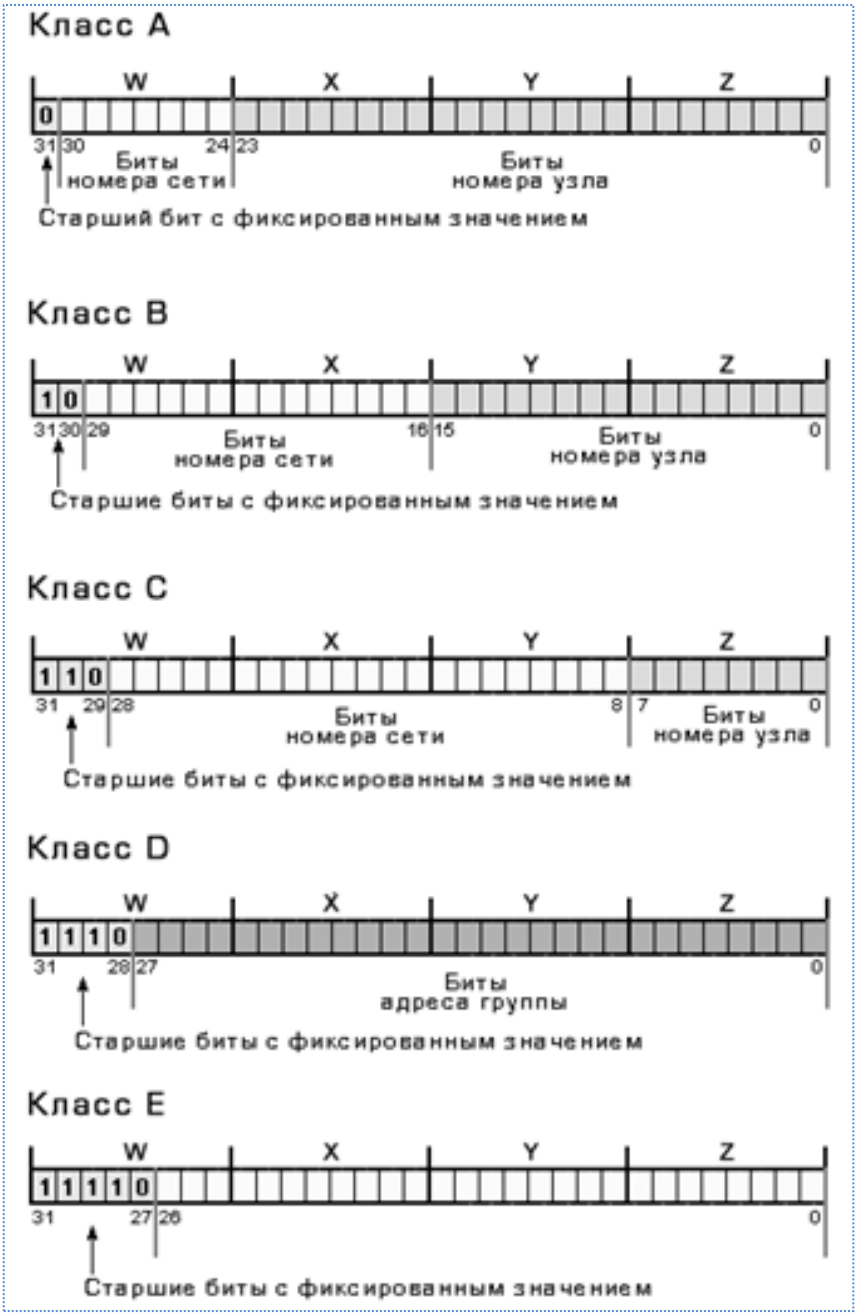

Рис 9.1. Двоичные схемы IP-адресов классов A, B, C, D и E

Чтобы получить из IP-адреса номер сети и номер узла, требуется не только разделить адрес на две соответствующие части, но и дополнить каждую из них нулями до полных 4 байт. Например, адрес класса **B** 129.64.134.5. Первые два байта идентифицируют сеть, а последующие два- узел. Таким образом, номером сети является адрес 129.64.0.0, а номером узла - адрес 0.0.134.5.

3.2 Особые IP-адреса (Ограничения при назначении IP адресов)

Существуют ограничения при назначении IP-адресов ***интерфейсам сети.***

Следующие адреса не назначаются сетевым интерфейсам (но используются для других целей):

1. Содержащие 0 во всех двоичных разрядах поля номера узла; такие IP-адреса используются для записи адресов сетей в целом;
2. Содержащие 1 во всех двоичных разрядах поля номера узла; такие IP-адреса являются широковещательными адресами для сетей, номера которых определяются этими адресами, а именно номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц. Отсюда следует, что максимальное количество узлов, приведенное в табл. 9.2 для сетей каждого класса, должно быть уменьшено на 2. Например, в адресах класса С под номер узла отводится 8 бит, которые позволяют задавать 256 номеров: от 0 до 255. Однако в действительности максимальное число узлов в сети класса С не может превышать 254, так как адреса 0 и 255 запрещены для адресации сетевых интерфейсов.
3. ***Все поля IP-адреса*** состоят из двоичных нулей (0.0.0.0). Такой адрес называется неопределенным адресом и обозначает адрес того узла, который сгенерировал этот пакет. Адрес такого вида в особых случаях помещается в заголовок IP-пакета в поле адреса отправителя.
4. Содержащие в поле ***номера сети*** только нули (0.0.X.X). Такой адрес обозначает адрес назначения узла сети, в которой находится узел, отправивший данный пакет. Такой адрес также может быть использован только в качестве адреса отправителя.
5. ***Все поля IP-адреса*** состоят из двоичных **1** (255.255.255.255), то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такой адрес называется ограниченным широковещательным (limited broadcast). Ограниченность в данном случае означает, что пакет не выйдет за границы данной сети ни при каких условиях. (маршрутизаторы этого не допустят).
6. ***Поле адреса назначения в разрядах, соответствующих номеру узла,*** стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети, номер которой указан в адресе назначения. Например, пакет с адресом 192.190.21.255 будет направлен всем узлам сети 192.190.21.0. Такой тип адреса называется широковещательным (broadcast)

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес является внутренним адресом стека протоколов компьютера (или маршрутизатора). *Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере.* Обе программные части данного приложения спроектированы в расчете на то, что они будут обмениваться сообщениями по сети. Для того чтобы серверная часть приложения могла обмениваться с клиентской было принято решение применение

внутреннего адреса 127.0.0.0. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со 127.

Групповые адреса (multicast), относящиеся к классу D, предназначены для экономичного распространения в Интернете или большой корпоративной сети аудио- или видеопрограмм, адресованных сразу большой аудитории слушателей или зрителей. Если групповой адрес помещен в поле адреса назначения IP-пакета, то данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Один и тот же узел может входить в несколько групп. В общем случае члены группы могут распределяться по различным сетям, находящимся друг от друга на произвольно большом расстоянии.

4. Использование масок для IP-адресации

Схема разделения IP-адреса на номер сети и номер узла, основанная на понятии класса адреса, не является эффективной, поскольку предполагает всего 3 варианта (классы A, B и C) распределения разрядов адреса под соответствующие номера. Рассмотрим для примера следующую ситуацию. Допустим, что некоторая компания, подключающаяся к Интернет, располагает всего 10-ю компьютерами. Поскольку минимальными по возможному числу узлов являются сети класса C, то эта компания должна была бы получить от организации, занимающейся распределением IP-адресов, диапазон в 254 адреса (одну сеть класса C). Неудобство такого подхода очевидно: 244 адреса останутся неиспользованными, поскольку не могут быть распределены компьютерам других организаций, расположенных в других физических сетях. В случае же, если рассматриваемая организация имела бы 20 компьютеров, распределенных по двум физическим сетям, то ей должен был бы выделяться диапазон двух сетей класса C (по одному для каждой физической сети). При этом число "мертвых" адресов удвоится.

Для более гибкого определения границ между разрядами номеров сети и узла внутри IP-адреса используются так называемые маски подсети. Маска подсети – это 4-байтовое число специального вида, которое используется совместно с IP-адресом. "Специальный вид" маски подсети заключается в следующем: двоичные разряды маски, соответствующие разрядам IP-адреса, **отведенным под номер сети, содержат единицы**, а в разрядах, соответствующих разрядам номера узла – нули. Количество разрядов адреса подсети может быть различным и определяется ***маской сети***.

Таким образом, маска сети также является 32-х разрядным двоичным числом. Разряды маски имеют следующий смысл:

1. если разряд маски равен 1, то соответствующий разряд адреса является разрядом адреса подсети;
2. если разряд маски равен 0, то соответствующий разряд адреса является разрядом хоста внутри подсети.

Все единичные разряды маски (если они есть) находятся в старшей (левой) части маски, а нулевые (если они есть) – в правой (младшей).

Для определения адреса сети на 32-х разрядный двоичный IP-адрес накладывается 32-х разрядная двоичная маска и выполняется по битно логическая операция & (И).

В компьютере каждая маска адреса хранится в виде 32-битового значения. Однако для записи префикса и маски адреса неудобно пользоваться двоичным представлением. Вместо этого применяется формат в виде десятичных чисел, разделенных точками, или новая синтаксическая форма, которая была разработана для адресации CIDR. (*Технология бесклассовой междоменной маршрутизации-Classless Inter-Domain Routing, CIDR*). Эта новая форма, получившая название системы обозначений CIDR, определяет, что маска, связанная с адресом, добавляется через косую черту; размер маски указывается в виде десятичного числа. Например, в первоначальной схеме на основе классов адрес 128.10.0.17 состоит из 16-битового префикса сети и 16-битового суффикса хоста. Маска сети в этом случае 255.255.0.0. С использованием адресации CIDR IP-адрес в месте с маской запишется более компактно: 128.10.0.17/16.

Исходя из вышесказанного, маску часто записывают в виде числа единиц в ней содержащихся.

255.255.248.0 (11111111.11111111.11111000.00000000) – является правильной маской подсети (/21),

а 255.255.250.0 (11111111.11111111.11111010.00000000) – является неправильной, недопустимой.

Нетрудно увидеть, что максимальный размер подсети может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

При передаче пакетов используются правила маршрутизации, главное из которых звучит так:

«Пакеты участникам своей подсети доставляются напрямую, а остальным – по другим правилам маршрутизации».

Таким образом, прежде чем отправлять пакет, требуется определить, является ли получатель членом нашей подсети или нет.

5. Определение диапазона адресов подсети.

Определение диапазона адресов подсети можно произвести из определения понятия маски:

1. те разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть одинаковы;
2. адреса хостов в подсети могут быть любыми.

То есть, если наш адрес 192.168.200.47 и маска равна /20, то диапазон можно посчитать:

11000000.10101000.11001000.00101111 – адрес

11111111.11111111.11110000.00000000 – маска

11000000.10101000.1100XXXX.XXXXXXXX – диапазон адресов

где 0,1 – определенные значения разрядов,

X – любое значение,

Что приводит к диапазону адресов:

от

11000000.10101000.11000000.00000000 (192.168.192.0)

до

11000000.10101000.11001111.11111111 (192.168.207.255)

Следует учитывать, что некоторые адреса являются ***ЗАПРЕЩЕННЫМИ*** или ***СЛУЖЕБНЫМИ*** и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие:

0 в первом или последнем байте, (все биты байта равны 0)

255 в любом байте (это широковещательные адреса),

127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня).

А ТАКЖЕ IP-АДРЕСА, СОДЕРЖАЩИЕ 1 ВО ВСЕХ ДВОИЧНЫХ РАЗРЯДАХ ПОЛЯ НОМЕРА УЗЛА; такие IP-адреса являются широковещательными адресами для сетей, номера которых определяются этими адресами.

Поэтому доступный диапазон адресов будет несколько меньше.

Есть специальные диапазоны адресов, которые не применяются в сети Интернет, эти диапазоны адресов предназначены для применения в изолированных локальных сетях.

Диапазоны адресов локальных сетей:

10.X.X.X – для больших локальных сетей;

172.16.X.X – для больших локальных сетей, но применяется реже,

192.168.X.X – для маленьких (небольших) локальных сетей,

не может быть использован в сети ***INTERNET***, т.к. отданы для использования в сетях непосредственно не подключенных к глобальной сети, т.е. он отдан специально для LAN.

6. РАСПРЕДЕЛЕНИЕ IP-АДРЕСОВ

Поскольку каждый узел сети Интернет должен обладать уникальным IP-адресом, то, безусловно, важной является задача координации распределения адресов отдельным сетям и узлам. Такую координирующую роль выполняет Интернет Корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers, ICANN).

Естественно, что ICANN не решает задач выделения IP-адресов конечным пользователям и организациям, а занимается распределением диапазонов адресов между крупными организациями-поставщиками услуг по доступу к Интернет (Internet Service Provider-ISP), которые, в свою очередь, могут взаимодействовать как с более мелкими поставщиками, так и с конечными пользователями. Так, например функции по распределению IP-адресов в Европе ICANN делегировал Координационному Центру RIPE (RIPE NCC, The RIPE Network Coordination Centre). В свою очередь, этот центр делегирует часть своих функций региональным организациям. В частности, российских пользователей обслуживает Региональный сетевой информационный центр "RU-CENTER".

Назначение адресов автономной сети

В небольшой же автономной IP-сети условие уникальности номеров сетей и узлов может быть выполнено силами сетевого администратора.

В этом случае в распоряжении администратора имеются все адресное пространство, так как совпадение IP-адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий, Администратор может выбирать адреса произвольным образом, соблюдая лишь синтаксические правила и учитывая ограничения на особые адреса.

Для того чтобы избежать совпадений с внешними адресами глобальной сети Интернет в стандартах Интернета определено несколько так называемых частных адресов, рекомендуемых для автономного использования в частных (корпоративных) LAN :

- в классе A — сеть **10.0.0.0**;
- в классе B — диапазон из 16 номеров сетей **172.16.0.0-172.31.0.0;**
- в классе C - диапазон из 255 сетей - **192.168.0.0-192.168.255.0.**

Эти адреса, исключенные из множества централизованно распределяемых, составляют огромное адресное пространство, достаточное для нумерации узлов автономных сетей практически любых размеров. Заметим также, что частные адреса, как и при произвольном выборе адресов, в разных автономных сетях могут совпадать. В то же время использование частных адресов для адресации автономных сетей делает возможным корректное подключение их к Интернету. Применяемые при этом специальные технологии подключения (NAT) исключают коллизии адресов.

7. Команда ipconfig

Команда ipconfig отображает краткую информацию, т.е. только IP-адрес, маску подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

8. Задания для выполнения

1. Какие адреса из приведенного ниже списка являются допустимыми адресами хостов и почему:

```
0.10.10.10
10.0.10.10
10.10.0.10
10.10.10.10
127.0.127.127
127.0.127.0
255.0.200.1
1.255.0.0
```

2. Перечислите все допустимые маски, по какому принципу они получаются.

3. Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети):

```
10.212.157.12/24
27.31.12.254/31
192.168.0.217/28
10.7.14.14/16
```

4. Какие из адресов

241.253.169.212
243.253.169.212
242.252.169.212
242.254.169.212
242.253.168.212
242.253.170.212
242.253.169.211
242.253.169.213

будут достигнуты напрямую с хоста 242.254.169.212/21.

Определите диапазон адресов в его подсети.

5. Посмотрите параметры IP на своем компьютере с помощью команды ipconfig. Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры и какие сетевые параметры выбрали бы Вы.

6. Выполнить упражнения – «тест по IP – адресации». (см. ниже).
Или выполнить п. 7.

7. Напишите компьютерную программу со следующими функциями:
   1. Прямое и обратное преобразования 32-битовых чисел в точечное десятичное представление;
   2. Определение к какому классу A, B, C, D, E относится введенный IP-адрес;
   3. Определение и отдельное отображение адреса сети, адреса хоста и маски сети по введенному IP-адресу. (автоматическое определение корректности введенных значений);
   4. Прямое и обратное преобразование из системы обозначений CIDR с косой чертой в эквивалентное точечное десятичное представление.
   5. Определение ограниченного и направленного широковещательных адресов для введенных IP-адреса и маски подсети в данной подсети; (использовать адреса для «частного применения – частных LAN»)

Контрольные вопросы:

1. Для чего нужен сетевой уровень, за что отвечает, как обобщённо называются технологии, обеспечивающие сетевой уровень?
2. Какие устройства необходимы, чтобы связать разнородные сети?
3. Маршрутизаторы – назначение, функции, физические интерфейсы?
4. Какие стеки протоколов применяются совместно с маршрутизаторами, их назначение?
5. Какие требования предъявляются к сетевой адресации, как обобщённо называются сетевые адреса, кому назначаются?
6. Можно ли использовать в качестве сетевого MAC-адрес?
7. Сетевой адрес должен быть цифровым или символьным?

8. Протокол IP, что означает термин «стек протоколов TCP/IP», в каких документах опубликованы стандарты TCP/IP?
9. Как называются блоки данных IP-протокола, и гарантируют протокол IP «надёжную» доставку?
10. Что такое маска подсети,?
11. Какова структура IP-адреса?
12. Чем определяется размер подсети?
13. Как определить диапазон адресов в подсети?
14. Как определить размер подсети?
15.

Дополнительные материалы:

1) В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г. Стр.565
2) Тема № 23. Структура и назначение сетевого уровня. Понятие системы передачи данных. Требования к сетевой адресации. Классовая модель IP. Маршрутизация. Методы получения правил маршрутизации.

Тест IP к Лабораторной работе «Изучение IP-адреса» -

Тест **IP** выполняется в письменном виде.

Полностью записывать последовательности операций логического **И** и **ИЛИ** в двоичном виде! Необходимо сокращать до десятичного вида оба байта, участвующих в операции, если один из байтов равен 0 или 255. Т.е. если в операции логического **И** участвуют 123 и 255, то результат очевидно равен 123 и поэтому расписывать 123 и 255 в двоичном представлении не обязательно. Лабораторные работы, выполненные с нарушением вышеуказанных требований, к рассмотрению не принимаются! Пример выполнения смотрите в «Тест IP- adress (пример выполнения)».

Тест задание: (вариант должен соответствовать порядковому номеру группы по списку)

1) По данным IP-адресам определить, к сети какого класса они принадлежат, получить IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети:

Вариант				
1	36.24.212.27	151.204.234.208	167.143.166.151	81.207.5.124
2	187.196.89.86	37.38.56.94	194.3.50.241	35.42.64.114
3	42.160.157.215	75.59.233.215	163.143.246.230	218.161.0.172
4	45.45.183.158	10.128.217.44	56.86.29.157	186.113.68.173
5	65.72.172.57	191.194.186.67	117.39.255.239	203.80.81.87
6	98.152.43.182	19.160.138.248	78.123.49.191	205.44.61.253
7	182.76.142.213	80.117.227.93	137.225.232.195	160.22.40.236
8	168.173.44.192	37.73.200.123	213.180.159.172	20.55.186.108
9	56.99.61.195	49.229.236.82	55.23.59.226	4.6.214.143
10	110.157.233.184	159.57.141.205	195.137.48.42	190.30.134.79

11	209.91.67.50	158.133.84.236	168.168.105.250	37.108.141.213
12	7.138.74.144	59.27.242.99	132.219.211.86	54.157.52.232
13	136.203.39.139	3.155.81.90	213.255.238.108	105.243.46.212
14	103.250.75.224	83.252.152.35	208.90.192.85	18.245.178.92
15	167.212.40.42	116.199.97.6	144.104.247.170	1.160.40.122
16	23.98.154.27	184.88.219.125	181.64.49.214	179.9.247.251
17	164.238.74.151	99.18.173.124	24.179.162.91	211.153.106.68
18	180.188.147.97	33.186.227.159	13.90.160.97	191.82.177.209
19	189.199.185.101	164.150.57.99	158.46.195.89	116.195.98.49
20	24.48.130.213	100.225.123.180	62.110.158.124	141.162.24.144
21	3.52.113.141	78.177.231.132	123.231.71.121	103.40.12.25
22	32.201.59.140	125.126.183.49	174.224.51.153	223.177.188.195
23	96.51.61.102	173.196.70.227	133.182.215.218	15.49.14.69
24	98.64.253.7	113.130.115.57	44.66.25.36	84.132.112.84
25	221.244.6.39	204.140.56.227	99.223.163.193	180.177.238.93
26	101.208.168.64	58.245.154.7	119.225.239.162	79.154.67.97

2) Используйте IP-адреса из задания 1 и ниже указанную длину маски сети, необходимо получить IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети:

Вариант				
1	/30	/18	/20	/28
2	/6	/21	/26	/10
3	/12	/7	/17	/15
4	/24	/3	/23	/8
5	/26	/13	/20	/27
6	/4	/10	/25	/28
7	/28	/24	/18	/3
8	/10	/14	/20	/9
9	/11	/4	/23	/14
10	/17	/25	/26	/20
11	/10	/27	/29	/11
12	/27	/14	/21	/15
13	/15	/29	/14	/19
14	/17	/10	/21	/13
15	/13	/30	/27	/7
16	/21	/21	/19	/12
17	/27	/27	/18	/23
18	/23	/16	/26	/25
19	/5	/22	/13	/17
20	/8	/11	/20	/20
21	/4	/18	/22	/8
22	/18	/10	/23	/11
23	/26	/20	/13	/18
24	/9	/23	/12	/19
25	/11	/30	/18	/21

26	/14	/28	/21	/6

3) Является ли данная маска сети правильной и какова ее длина в битах:
(По определению маска сети является непрерывной последовательностью битов 1 от старшего разряда после которых идут только биты 0. Поэтому необходимо перевести в двоичное представление указанные маски и проверить этот факт).

Вариант				
1	255.254.0.0	255.255.255.214	255.255.255.248	255.255.248.0
2	255.255.255.0	255.255.255.240	255.253.0.0	255.255.252.0
3	255.255.252.0	255.255.255.192	255.7.0.0	248.0.0.0
4	255.254.0.0	255.255.248.0	240.0.3.0	255.255.255.248
5	248.0.0.0	255.249.0.0	255.255.255.240	224.0.0.0
6	255.255.0.0	252.253.0.0	255.124.0.0	65.255.0.0
7	255.248.0.0	255.255.240.0	255.255.254.0	255.255.255.254
8	255.224.0.0	252.2.0.0	255.240.0.0	255.255.255.240
9	255.255.255.248	255.255.255.252	255.255.248.0	192.0.0.0
10	255.248.9.0	255.255.255.0	255.248.0.0	254.0.0.0
11	255.255.225.255	255.255.193.0	255.255.0.0	255.255.255.128
12	255.255.255.252	255.255.255.128	255.255.255.248	255.192.0.0
13	255.224.0.0	250.0.0.0	255.255.254.0	192.0.0.0
14	255.240.0.0	255.255.192.0	255.255.255.252	255.240.0.0
15	255.255.255.128	255.240.0.0	224.0.0.0	255.224.224.0
16	224.0.0.255	255.192.0.0	255.255.255.240	255.252.0.0
17	255.129.0.0	255.255.248.0	255.255.192.0	254.0.0.0
18	248.0.0.0	255.128.8.0	192.0.0.0	255.128.0.0
19	255.255.255.128	255.255.250.254	255.255.255.192	248.0.0.0
20	255.192.254.0	255.255.255.192	255.128.0.0	255.255.252.0
21	255.0.0.0	255.224.10.0	252.0.0.0	255.255.224.0
22	255.252.11.0	248.0.0.0	255.255.248.0	255.255.255.240
23	255.155.255.255	240.0.0.0	254.0.0.0	255.252.0.0
24	255.255.248.0	255.255.254.0	255.255.224.0	255.125.128.0
25	255.205.255.0	255.255.255.252	255.255.255.0	255.224.0.0
26	224.0.0.0	255.255.255.0	240.255.0.0	224.0.0.0

4) Является ли данный IP-адрес адресом сети с указанной длиной маски сети: *(необходимо вычислить по данному IP-адресу адрес сети и сравнить с исходным адресом, указанным в задании)*

Вариант				
1	185.129.0.0/9	80.0.0.0/5	100.241.96.0/22	129.199.93.82/31
2	185.214.114.0/22	85.0.0.0/7	157.143.151.177/29	58.189.128.0/17
3	128.0.0.0/2	1.193.76.0/24	127.12.0.0/14	134.0.0.0/6
4	120.118.0.0/12	195.165.102.0/18	184.98.36.0/24	200.0.0.0/5
5	32.0.0.0/3	15.53.210.202/30	240.97.66.0/18	189.66.194.64/26
6	152.228.0.0/14	229.0.0.0/3	126.17.238.0/23	66.37.0.0/16
7	146.0.0.0/11	88.142.0.0/14	107.212.0.0/14	202.58.239.204/31
8	65.0.0.0/7	73.100.0.0/17	105.213.190.0/23	169.22.0.0/15
9	80.243.8.200/31	7.81.247.0/21	40.127.40.54/31	222.117.148.0/22

10	32.10.0.0/9	95.81.1-8.0/18	68.111.8.0/22	52.96.0.0/11
11	43.51.83.162/27	21.96.100.0/11	105.49.54.226/31	164.0.0.0/7
12	122.0.0.0/5	67.109.141.105/30	161.249.88.0/25	104.184.0.0/13
13	33.245.254.0/22	152.0.0.0/6	46.126.200.209/30	155.80.0.0/18
14	147.0.0.0/8	138.182.0.0/14	7.117.120.60/32	112.0.0.0/6
15	127.160.0.0/11	27.100.136.87/29	17.91.200.10/21	166.51.64.0/19
16	236.181.31.134/31	108.21.68.0/23	159.0.0.0/7	178.190.114.180/30
17	6.30.97.0/28	87.104.0.0/14	153.11.102.90/29	96.0.0.0/4
18	182.0.0.0/5	55.204.36.75/30	116.200.156.0/24	128.0.0.0/5
19	104.14.0.0/16	81.0.0.0/10	192.76.12.0/25	135.87.12.0/22
20	157.207.130.0/25	127.3.108.0/23	96.30.0.0/5	128.0.0.0/5
21	121.156.142.0/22	139.128.0.0/9	213.195.0.0/13	144.0.0.0/5
22	48.85.174.0/20	135.128.0.0/10	207.0.0.0/4	4.121.231.192/26
23	196.118.169.133/30	188.128.0.0/10	32.20.0.0/6	128.0.0.0/2
24	112.98.0.0/16	232.159.229.89/29	33.64.0.0/14	87.180.176.0/23
25	106.212.235.0/25	104.200.76.0/31	10.200.0.0/8	117.60.0.0/14
26	194.0.0.0/7	105.227.0.0/11	191.134.130.192/28	239.134.0.0/13

5) Принадлежат ли указанные IP-адреса к одной подсети: *(чтобы узнать принадлежат ли адреса к одной подсети, необходимо получить адрес сети для каждого из адресов и сравнить адреса сетей)*

Вариант		
1	229.52.17.190 - 229.50.17.191/30	226.144.183.64 - 226.128.186.152/9
2	223.62.19.244 - 223.67.176.98/14	67.50.242.243 - 67.50.200.172/18
3	127.73.18.240 - 137.114.177.17/9	195.94.59.188 - 195.94.59.191/30
4	185.63.56.182 - 85.63.239.16/16	199.57.36.63 - 199.57.5.169/15
5	136.61.83.119 - 111.181.218.52/5	125.60.255.103 - 125.34.169.199/9
6	133.206.62.249 - 133.105.92.88/11	192.243.42.162 - 192.243.42.246/25
7	94.176.91.111 - 94.176.92.80/20	4.244.159.102 - 4.246.125.165/12
8	47.88.172.145 - 47.88.178.192/21	203.40.171.158 - 203.40.141.180/18
9	244.23.38.153 - 244.23.78.154/29	28.3.34.25 - 19.109.158.253/4
10	123.65.168.74 - 123.65.164.72/27	110.71.140.119 - 110.67.85.239/9
11	116.75.124.87 - 116.75.124.85/20	135.143.91.179 - 135.143.87.229/20
12	253.130.198.145 - 253.130.198.145/22	37.125.13.168 - 37.125.15.13/21
13	108.11.214.167 - 108.11.223.5/19	246.235.45.207 - 246.235.45.215/29
14	74.28.237.200 - 74.28.237.203/25	181.84.249.67 - 181.65.130.204/9
15	199.123.3.50 - 199.123.3.101/23	100.101.216.145 - 100.182.234.25/5
16	24.52.254.96 - 24.52.252.93/21	206.240.138.123 - 206.242.138.65/26
17	125.160.27.126 - 125.160.27.104/29	90.11.41.223 - 90.11.36.71/20
18	245.147.217.10 - 245.137.208.239/20	8.215.223.7 - 8.215.221.121/22
19	203.229.237.163 - 203.229.236.44/24	50.140.6.93 - 50.137.106.16/12
20	138.38.89.122 - 138.38.89.102/27	33.57.125.225 - 33.105.28.206/10
21	1.155.84.168 - 1.155.87.159/25	218.21.244.169 - 218.21.247.183/21
22	107.105.106.169 - 107.121.225.62/12	150.135.197.141 - 150.175.141.163/6
23	219.115.4.199 - 219.113.224.101/14	194.104.201.41 - 194.112.152.83/14
24	128.77.223.26 - 128.77.220.172/18	136.95.4.150 - 136.96.221.49/15
25	111.44.22.209 - 111.231.92.245/8	50.22.147.220 - 50.22.147.221/21

26	243.212.122.21 - 243.204.143.79/10	242.251.231.41 - 242.251.231.42/19

6) Определить максимальную длину маски сети, чтобы указанные IP-адреса находились в одной сети: *(чтобы определить максимальную длину маски сети необходимо перевести в двоичное представление оба адреса и посчитать число совпадающих бит, начиная со старшего бита до первого различия)*

Вариант		
1	221.220.88.73 - 223.222.74.206	32.102.0.46 - 32.102.0.47
2	102.244.10.49 - 102.244.10.26	235.41.199.239 - 235.41.41.139
3	251.252.230.152 - 251.250.29.97	54.134.17.147 - 54.10.33.193
4	162.235.231.229 - 160.93.14.253	18.10.124.128 - 18.10.124.169
5	99.149.26.16 - 99.149.26.16	199.225.66.216 - 199.225.66.247
6	250.54.84.49 - 214.7.75.249	149.182.180.56 - 151.66.167.26
7	231.81.216.237 - 231.81.212.30	177.77.34.213 - 191.35.196.43
8	115.115.32.253 - 114.14.56.227	62.225.77.124 - 62.225.76.103
9	184.155.179.54 - 184.155.66.71	251.106.185.206 - 251.126.234.156
10	246.168.67.154 - 246.169.9.220	48.107.202.223 - 48.107.203.56
11	23.115.247.150 - 23.48.37.248	95.129.111.1 - 95.129.111.3
12	207.234.120.181 - 207.234.120.181	38.23.81.102 - 38.127.45.239
13	150.27.130.246 - 150.18.140.87	166.220.34.180 - 166.220.34.183
14	51.79.155.111 - 51.75.182.175	112.56.206.224 - 112.56.202.104
15	236.74.83.193 - 236.75.195.217	12.95.127.35 - 12.131.135.175
16	123.157.136.13 - 123.165.203.131	196.200.12.115 - 196.200.12.116
17	91.1.129.158 - 91.1.172.242	220.225.247.23 - 220.225.71.91
18	5.35.95.106 - 9.58.248.150	226.4.22.186 - 226.163.205.38
19	159.218.202.36 - 159.218.156.20	141.85.107.17 - 141.85.107.97
20	247.242.52.247 - 247.66.88.19	2.57.42.80 - 2.56.92.124
21	120.149.163.181 - 120.186.35.7	41.0.254.221 - 47.86.238.81
22	179.76.216.76 - 179.76.216.76	0.42.239.218 - 19.83.23.66
23	182.133.171.215 - 182.133.221.50	122.186.87.171 - 122.186.87.170
24	11.204.240.150 - 11.204.240.222	225.185.154.217 - 225.185.154.208
25	226.61.98.224 - 226.61.18.215	24.173.207.45 - 24.177.233.169
26	35.115.185.74 - 35.113.230.137	208.114.254.251 - 208.114.254.203

ПРИМЕР ОТВЕТА К ЗАДАНИЮ «**Изучение IP-адреса»**

Задание 1.

По данным IP-адресам определить к сети какому классу они принадлежат, получить IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети: **110.157.233.184**

Решение:

первый октет = 0000 0110, поэтому это адрес класса A
адрес сети 110.0.0.0
маска сети 255.0.0.0
адрес шир. расс. 110.255.255.255

Задание 2.

Используйте IP-адреса из задания 1 и соответствующую длину маски сети, чтобы получить

IP-адрес сети, маску сети и IP-адрес широковещательной рассылки в данной сети: **110.157.233.184/12**

Сначала необходимо получить маску сети в явном виде:
/12 — это 12 единичных бит от 31 бита направо

11111111.11110000.00000000.00000000 или в десятичном виде 255.240.0.0

Так как результат логического И/ИЛИ байтового значения с 0 и 255 очевиден, то нам необходимо получить представление в двоичном виде лишь байта **157** нашего IP-адреса.

Чтобы получить адрес сети, нам необходимо выполнить операцию логического И между IP-адресом и маской сети:

110.10011101.233.184 И
255.11110000. 0. 0

110.10010000. 0. 0 = 110.144.0.0 — адрес сети

Чтобы получить адрес широковещательной рассылки, необходимо выполнить операцию логического ИЛИ между IP-адресом и инверсией маски сети.

Получим инверсию маски сети:
00000000.00001111.11111111.11111111 или в десятичном виде 0.15.255.255

Тогда:
110.100111012.233.184 ИЛИ
0.000011112.255.255

110.100111112.255.255 = 110.159.255.255 — адрес широковещательной рассылки

Задание 3.
Является ли данная маска сети правильной, и какова ее длина в битах: **255.254.0.0**

По определению маска сети является непрерывной последовательностью битов 1 от старшего разряда, после которых идут только биты 0. Поэтому необходимо перевести в двоичное представление указанные маски и проверить этот факт.

В двоичном виде **255.254.0.0** представимо как:

11111111.11111110.00000000.00000000

Как мы видим последовательность единиц идет от старшего бита IP-адреса и является непрерывной, следовательно эта маска является правильной и имеет длину 15 бит.

Задание 4.
Является ли данный IP-адрес адресом сети с указанной длиной маски сети: **228.0.0.0/3**

Получим маску сети в явном виде:

/3 — это 3 единичных бит от 31 бита направо

111000002.0.0.0 = 224.0.0.0

Нам необходимо получить адрес сети по данному IP-адресу.

11100100.0.0.0 И
11100000.0.0.0

11100000.0.0.0 = 224.0.0.0 — адрес сети

Так как 224.0.0.0 не равен 228.0.0.0, то 228.0.0.0 не может выступать в качестве адреса сети с маской /3.

Задание 5.
Принадлежат ли указанные IP-адреса к одной подсети: **135.95.4.150 - 135.96.221.49/15**

Чтобы узнать принадлежат ли адреса к одной подсети, необходимо получить адрес сети для каждого из адресов и сравнить адреса сетей.

Получим маску сети в явном виде:

/15 — это 15 единичных бит от 31 бита направо

11111111.11111110.0.0 = 255.254.0.0

Так как в нашей маске отличным от 0 и 255 является второй байт, то при выполнении операции логического И нам необходимо расписывать в двоичном виде только второй байт IP-адресов.

135.01011111. 4.150 И
255.11111110. 0. 0

135.01011110. 0. 0 = 135.94.0.0 — адрес сети для 1-ого IP-адреса

135.01100000.221. 49 И
255.11111110. 0. 0

135.01100000. 0. 0 = 135.96.0.0 — адрес сети для 2-ого IP-адреса

Адреса сетей не совпадают, значит указанные в задании IP-адреса не могут лежать в одной подсети с длиной маски 15 бит.

Задание 6.
Определить максимальную длину маски сети, чтобы указанные IP-адреса находились в одной сети: **24.177.20.45 - 24.177.23.169**
Чтобы определить максимальную длину маски сети необходимо перевести в двоичное представление оба адреса и посчитать число совпадающих бит, начиная со старшего бита, до первого различия.

В нашем задании первые два байта IP-адресов совпадают, и поэтому их не нужно переводить в двоичное представление. Так как каждый байт — это 8 бит, то мы уже имеем 8 * 2 = 16 совпадающих бит.

Рассмотрим третий байт IP-адресов. В двоичном виде (не забываем про незначащие разряды, которые равны 0!):

20 = 00010100
23 = 00010111

В третьем байте совпадают 6 бит. Таким образом, всего совпадает 16 + 6 = 22 бит. Поэтому максимальная длина маски сети, при которой оба указанных IP-адреса будут лежать в одной подсети — это 22 бит.

1***-**Дейтаграмма (датаграмма)** - пакет, передаваемый через сеть без предварительной организации пути его следования и независимо от других пакетов.

При ***дейтаграммной передаче*** соединение не устанавливается, и все передаваемые пакеты ***продвигаются*** (передаются от одного узла сети другому) ***независимо*** друг от друга на основании одних и тех же правил. Процедура обработки пакета определяется только значениями параметров, которые он несет в себе, и текущим состоянием сети (например, в зависимости от ее нагрузки пакет может стоять в очереди на обслуживание большее или меньшее время). Однако никакая информация об уже переданных пакетах в сети (устройствах) не хранится и в ходе обработки очередного пакета во внимание не принимается. То есть каждый отдельный пакет рассматривается сетью как совершенно новый и как независимая единица передачи — **дейтаграмма.**