Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

Е.С. Белоусова

КОМПЬЮТЕРНЫЕ СЕТИ

IPV4 И IPV6 АДРЕСАЦИЯ

ПРАКТИКУМ

Минск БГУИР 2020

СОДЕРЖАНИЕ

ПРАКТИЧЕСКАЯ РАБОТА №2
СЕТЕВАЯ И УЗЛОВАЯ ЧАСТЬ IPV4-АДРЕСА

Цель: овладеть навыками определения адреса сети, первого IP-адреса сети и широковещательного адреса; изучить классификацию IP-адресов, научиться определять тип IPv4-адреса и его класс.

2.1 Теоретическая часть

IP-адрес является иерархическим адресом и состоит из двух частей: сетевой и узловой. При настройке оконечного устройства ему присваивается не только IP-адрес, но и маска подсети. Маска также как и IP-адрес состоит из 32 бит и определяет, какая часть IP-адреса относится к сети и к узлу. Маска подсети для простоты использования также представляется в десятичном формате с разделительными точками. Маска подсети настраивается на узловом устройстве в сочетании с IPv4-адресом и необходима для того, чтобы узел мог определить, к какой сети он принадлежит. Для этого устройство сравнивает маску с IP-адресом побитно, слева направо, единицы в маске соответствуют сетевой части, а нули – адресу узла. Таким образом, в маске подсети единицы в каждой позиции бита обозначают сетевую часть. Размещение нуля в каждой позиции бита маски подсети обозначает узловую часть IP-адреса (рисунок 2.1). Необходимо отметить, что маска подсети не содержит сетевую или узловую часть IPv4-адреса; она необходима устройствам для определения узловой и сетевой части в IPv4-адресах.

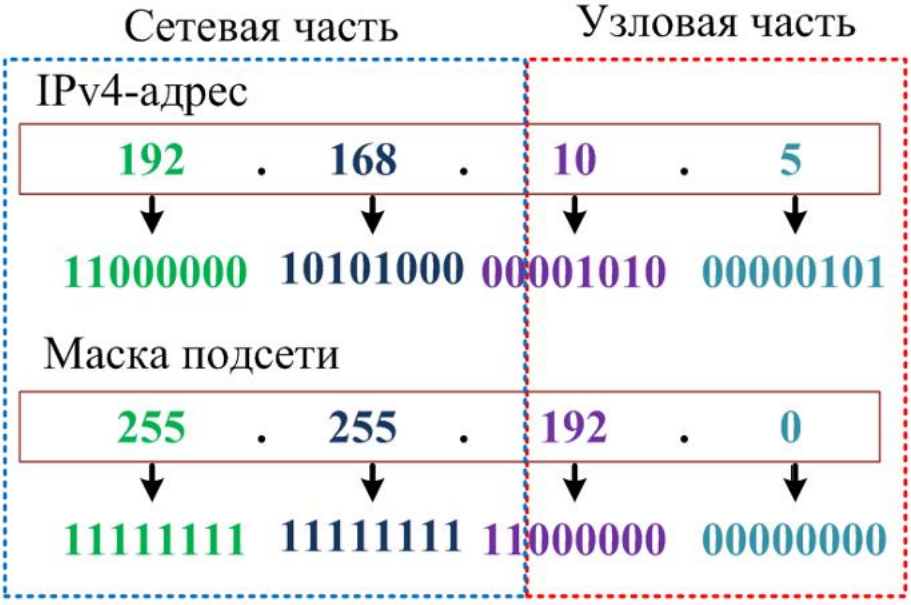

Рисунок 2.1 – Сетевая и узловая часть IPv4-адреса

Биты в сетевой части адреса должны быть одинаковыми для всех устройств, которые находятся в одной и той же сети. Биты в узловой части адреса должны быть уникальными, чтобы можно было определить конкретный узел в сети. Независимо от того, совпадают ли десятичные числа в двух IPv4-адресах, если два узла имеют одну битовую комбинацию в определённой сетевой части 32-битного потока, то эти два узла находятся в одной и той же сети.

Префикс – это способ представления маски подсети. Значение префикса означает количество бит, установленных в единицу в маске подсети. Она обозначается наклонной чертой вправо («/»), после которой идёт набор единиц. Например, если маска подсети 255.255.255.0, то в двоичной версии маски подсети первые 24 бита единицы, поэтому значение префикса составляет 24 бита и обозначается /24. Например, для адреса 192.168.10.5 на рисунке 2.1, префикс может обозначаться следующим образом: /18, так как 18 первых бит в маске подсети установлены в единицу. По сути, назначение префикса и маска подсети одинаковое – представление сетевой части адреса.

В зависимости от количества узлов в сети префикс может отличаться. Различный префикс приводит к изменению диапазона узлов и широковещательного адреса для каждой сети.

В сети узлы могут взаимодействовать одним из трёх следующих способов:

– **одноадресная рассылка** – процесс отправки пакета с одного узла на другой;

– **широковещательная рассылка** – процесс отправки пакета с одного узла на все узлы в сети;

– **многоадресная рассылка** – процесс отправки пакета с одного узла выбранной группе узлов.

Эти три типа связи используются в сетях передачи данных для различных целей. Во всех трёх типах IPv4-адрес исходного узла размещён в заголовке пакета в качестве адреса источника.

Одноадресная передача используется для обычного обмена данными между узлами. Для одноадресной рассылки пакетов в качестве адреса назначения используются адреса целевого устройства. Во время процесса инкапсуляции исходный узел размещает свой IPv4-адрес в заголовке пакета одноадресной рассылки в качестве адреса источника, а IPv4-адрес узла назначения – в заголовке пакета в качестве адреса назначения.

В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы. Это означает, что пакеты получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих сетевых протоколах, например в протоколе DHCP. Когда узел получает пакет, отправленный на сетевой широковещательный адрес, узел обрабатывает этот пакет так же, как обрабатывает пакет, отправленный по одноадресной рассылке.

Многоадресная передача предназначена для сохранения пропускной способности IPv4-сети. Такая передача сокращает трафик, позволяя узлу отправлять один пакет выбранной группе узлов, которые являются частью подписной группы мультивещания. Чтобы достичь множества целевых узлов с помощью одноадресной связи, узел-источник должен отправлять отдельный пакет на каждый адрес. В случае с многоадресной рассылкой узел-источник может отправлять один пакет, который достигает нескольких тысяч узлов назначения.

Независимо от того, является ли пункт назначения, определивший пакет, одноадресным, широковещательным или многоадресным, источник всегда является индивидуальным адресом исходного узла.

В каждой сети IPv4 существуют три типа адресов:

– сетевой адрес;

– узловые адреса;

– широковещательный адрес

Сетевой адрес – это стандартный способ обозначения сети. Маска подсети или префикс используются при обозначении сетевого адреса. Сеть, показанную на рисунке 2.2, можно обозначить как 192.168.10.0 с маской 255.255.255.0 или 192.168.10.0/24. Все узлы в сети 192.168.10.0/24 будут иметь одинаковую сетевую часть.

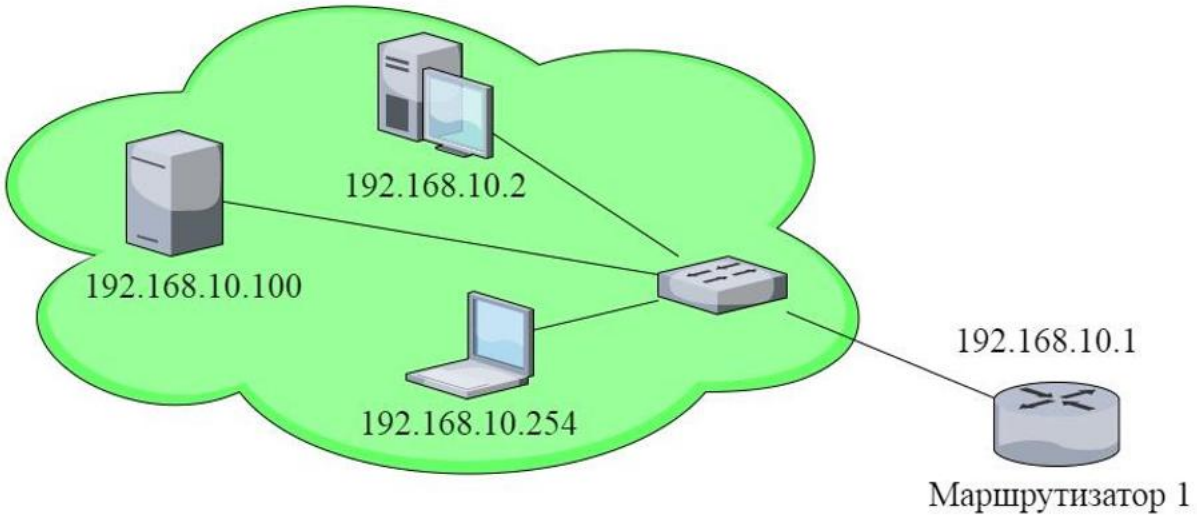

Рисунок 2.2 – Пример сети с адресом 192.168.10.0/24

Как показано на рисунке 2.2, в диапазоне IPv4-адресов первый из них (192.168.10.0) зарезервирован для обозначения всей сети в целом. В каждом узловом бите узловой части адреса указан ноль.

Для обмена данными по сети каждому оконечному устройству необходим уникальный адрес. В IPv4-адресах значения между сетевым и широковещательным адресами могут быть назначены оконечным устройствам в сети. В узловой части адрес 192.168.10.0/24 может иметь любую комбинацию

нулей и единиц, но при этом не может состоять только из нулей или только из единиц. Таким образом для примера сети, показанном на рисунке 2.2 узловые адреса могут иметь значение в последнем октете от 1 до 254. Обычно первый IP-адрес присваивается устройству, ограничивающем данную сеть (маршрутизатор).

Широковещательный IPv4-адрес – это особый адрес для каждой сети, который осуществляет связь для всех узлов, расположенных в этой сети. Для единовременной отправки данных на все узлы в сети узел может отправить один пакет, назначенный широковещательному адресу сети, а каждый узел в этой сети, который получит этот пакет, обработает его содержимое.

Для широковещательной рассылки используется наивысший адрес диапазона сети. В этом адресе все части узла представлены единицами (1). Сумма единиц октета в двоичной форме равняется значению 255 в десятичном формате. Таким образом, для сети 192.168.10.0/24, в которой последний октет используется для узловой части, широковещательный адрес будет равен 192.168.10.255. Также этот адрес называют прямой широковещательной рассылкой. Необходимо отметить, что узловая часть не всегда представлена всем октетом целиком.

Чтобы не возникало проблем в сети, всем узлам в сети назначаются уникальный IP-адрес внутри диапазона сети, для того важно уметь определять адреса первого и последнего узлов. Узловая часть первого адреса узла будет содержать все нулевые биты с единицей в крайнем справа бите. Значение этого адреса всегда на единицу больше сетевого адреса. Часто во многих схемах адресации первый адрес узла используется для маршрутизатора или шлюза по умолчанию.

Узловая часть последнего адреса узла будет содержать все единицы с нулём в крайнем справа бите. Значение этого адреса всегда на единицу меньше, чем значение широковещательного адреса.

На рисунке 2.3 представлен пример определения адреса сети, первого и последнего возможного IP-адреса устройств. В данном примере известен только IP-адрес одного из устройств 192.168.10.5 с префиксом /18.

Если устройству назначен IPv4-адрес, то это устройство использует маску подсети, чтобы определить, к какому сетевому адресу оно принадлежит. Сетевой адрес представляет все устройства в одной и той же сети.

При отправке данных по сети устройство использует эту информацию, чтобы определить, может ли оно пересылать пакеты локально, либо оно должно отправлять пакеты на шлюз по умолчанию для удалённой отправки. Когда узел отправляет пакет, он сравнивает сетевые части собственного IP-адреса и IP-адреса назначения, который зависит от маски подсети. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если биты не совпадают, отправляющий узел передаёт пакет на шлюз по умолчанию для отправки в другую сеть.

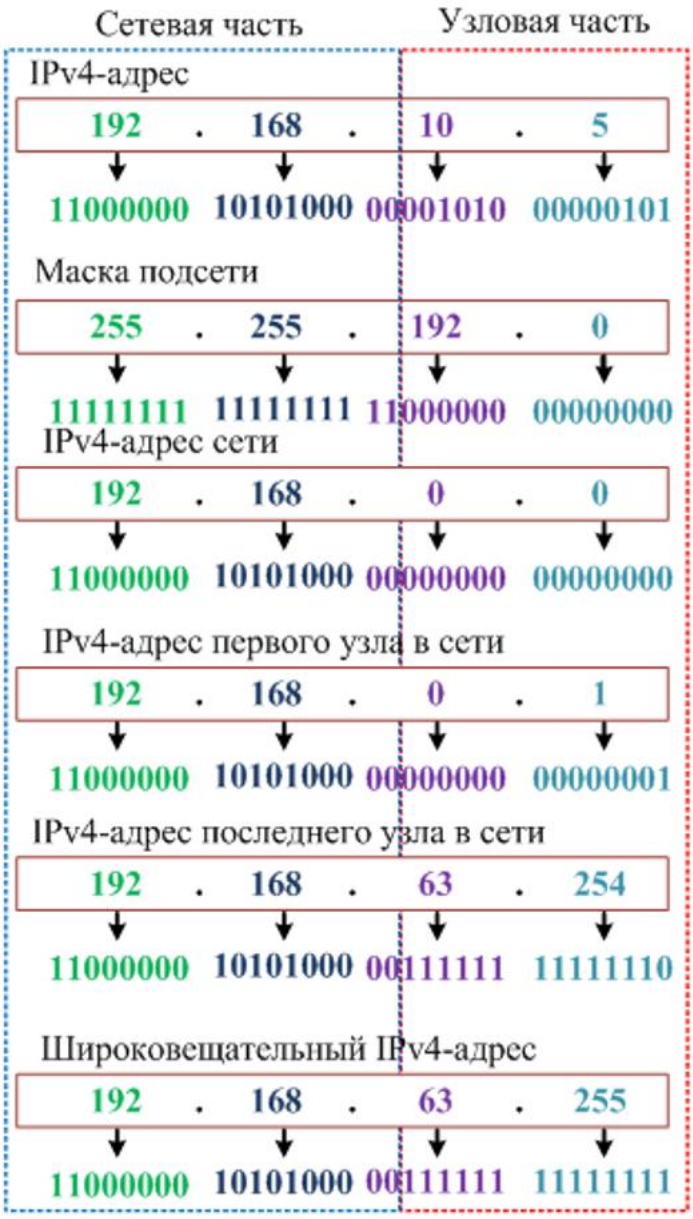

Рисунок 2.3 – Определение первого и широковещательного IPv4-адреса

Для определения способа отправки устройство использует операцию дискретной логики логическое умножение (операция **AND**), которая заключается в сравнение двух битов, как показано на рисунке 2.4. Например, 1 AND 1 = 1, 0 AND 1 = 0, 0 AND 0 = 0.

Классовая IP адресация – это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т. к. не возможно использование различных масок подсетей. В классовом методе адресации используется фиксированная маска подсети, поэтому класс сети всегда можно идентифицировать по первым битам.

В соответствии с документом RFC1700 все IPv4-адреса сгруппированы в диапазоны (рисунок 2.5), которые называются классами A, B, C, D (групповые), E (экспериментальные). К классам A, B и C относятся коммерческие адреса, присваиваемые узлам. Индивидуальным адресам классов A, B и C определены

сети особого размера и блоки особых адресов для этих сетей. Компании или организации назначается целая сеть из блоков адресов класса A, B или C.

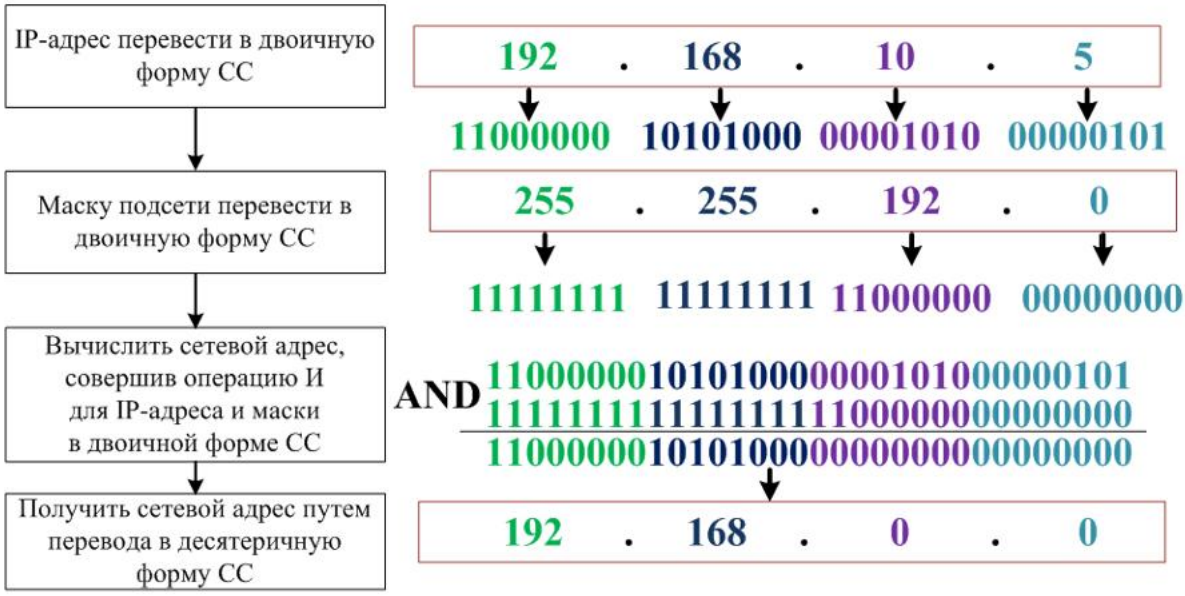

Рисунок 2.4 – Вычисление сетевого адреса

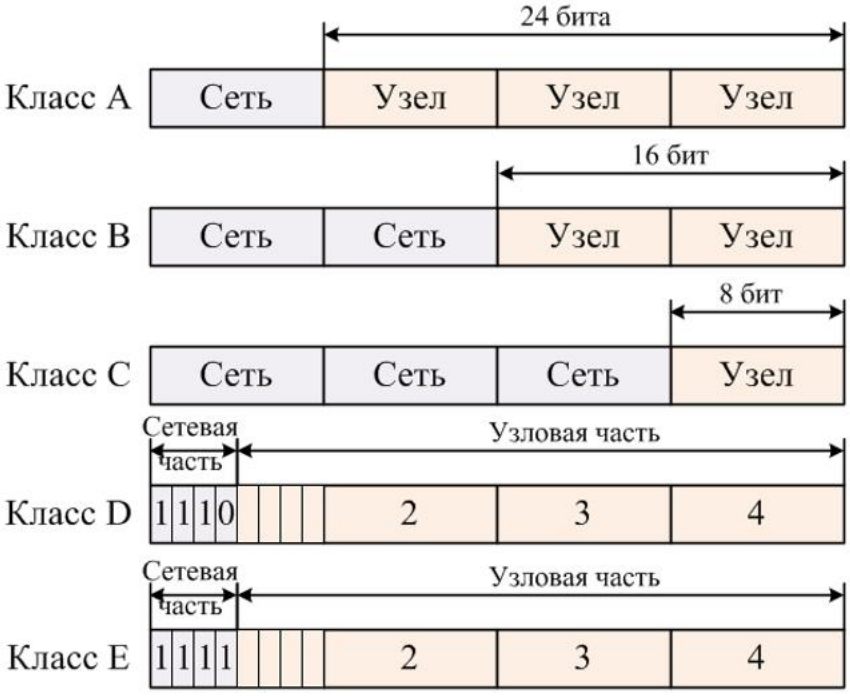

Рисунок 2.5 – Классы IPv4-адресов

Блок адресов класса A разработан для поддержки очень крупных сетей, содержащих более чем 16 миллионов адресов узлов. Для обозначения сетевого адреса IPv4-адреса класса A использовали фиксированный префикс /8 с первым октетом. Остальные три октета использовались для адресов узлов. Все адреса класса A требуют, чтобы самый старший разряд старшего октета был равен

нулю. Это означает, что существовало только 128 возможных сетей класса A, от 1.0.0.0/8 до 127.0.0.0 /8 (таблица 2.1). Даже если адреса класса A зарезервировали половину адресного пространства, в связи с их ограничением до 128 сетей они могут быть назначены только приблизительно 120 компаниям или организациям.

Адресное пространство класса B разработано для поддержки потребностей небольших и крупных сетей, содержащих приблизительно 65 000 узлов. IP-адрес класса B использовал два старших октета для обозначения сетевого адреса. Оставшиеся два октета определяли адреса узлов. Как и в случае с классом A, адресное пространство для оставшихся классов адресов должно быть зарезервированным. Для адресов класса B два самых старших разряда старшего октета равны 10. Это ограничивает блок адресов для класса B от 128.0.0.0/16 до 191.255.0.0/16 (таблица 2.1). Назначение адресов класса B немного более эффективно по сравнению с классом A, поскольку 25 % его общего пространства IPv4-адресов было разделено среди примерно 16 000 сетей.

Адресное пространство класса C было доступно чаще всех остальных классов адресов. Это адресное пространство предназначено для предоставления адресов небольшим сетям с максимальным количеством узлов не более 254. Блоки адресов класса C использовали префикс /24. Это означает, что сеть класса C использовала только последний октет в качестве адресов узлов с тремя старшими октетами, используемыми для обозначения сетевых адресов. Блоки адресов класса C отделяли адресное пространство с помощью фиксированного значения 110 самых старших разрядов старшего октета. Это ограничило блок адресов класса C от 192.0.0.0/24 до 223.255.255.0/24 (таблица 2.1). Хотя этот блок занял только 12,5 % от общего объёма адресного IPv4-пространства, он предоставил адреса 2 миллионам сетей.

Таблица 2.1 – Диапазон первого октета классов адресов

Класс адреса	Диапазон первого октета в десятичном формате	Маска подсети
A	1-127	255.0.0.0
B	128-191	255.255.0.0
C	192-223	255.255.255.0
D	224-239	
E	240-255	

На сегодняшний день более распространено разделение IPv4-адресов на публичные и частные. Подавляющее большинство адресов в диапазоне узлов одноадресной IPv4-рассылки являются публичными адресами. Эти адреса предназначены для использования в узлах с открытым доступом из Интернета. Даже в диапазоне этих блоков IPv4-адресов существует множество адресов, предназначенных для других особых целей.

Частные адреса определены в документе RFC 1918 «Присвоение адресов для частного Интернета» (таблица 2.2). Узлы, которые не требуют доступа в Интернет, могут использовать частные адреса. Узлы в различных сетях могут использовать одни и те же адреса частного пространства. Пакеты, использующие эти адреса в качестве источника или назначения, не должны появляться в публичном Интернете. Маршрутизатор должен блокировать или преобразовывать эти адреса. Даже если бы пакеты сами прокладывали свой путь через Интернет, у маршрутизаторов в любом случае не появилось бы маршрутов для пересылки их в соответствующую частную сеть.

В документе RFC 6598 IANA (Администрация адресного пространства Интернет) зарезервировала другую группу адресов, которая называется общим адресным пространством. Так же, как и в пространстве частных адресов RFC 1918, адреса общего адресного пространства недоступны глобально. Однако эти адреса предназначены только для использования в сетях операторов связи. Блок общих адресов – 100.64.0.0/10.

Таблица 2.2 – Диапазоны адресов для частных сетей

Класс адреса	Сети	Маска подсети	Диапазон адресов
A	10.0.0.0	255.0.0.0	10.0.0.0 –10.255.255.255
B	172.16.0.0 – 172.31.0.0	255.240.0.0	172.16.0.0 – 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 – 192.168.255.255

Также существуют особые адреса, которые не могут быть назначены узлам, такие адреса называются сетевым и широковещательным.

К таким адресам также относится IPv4-адрес логического интерфейса loopback (127.0.0.1). Loopback – это особый адрес, который используют узлы, чтобы направлять трафик самим себе. Адрес обратной связи позволяет создавать ускоренный метод взаимодействия для приложений и сервисов TCP/IP, которые работают на одном и том же устройстве. С использованием loopback-адреса вместо назначенного IPv4-адреса узла два сервиса на одном узле могут обойти нижние уровни стека протоколов TCP/IP. Для проверки настройки TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес.

Хотя используется только адрес 127.0.0.1, резервируются адреса с 127.0.0.0 до 127.255.255.255. Любой адрес из этого блока даст обратную связь с локальным узлом. Ни один адрес из этого блока не должен быть назначен устройствам в сети.

В качестве локальных адресов канала используются IPv4-адреса в блоке адресов от 169.254.0.0 до 169.254.255.255 (169.254.0.0/16). Эти адреса могут быть автоматически присвоены операционной системой локальному узлу в средах, где настройка IP-сети недоступна. Они могут использоваться в

небольшой одноранговой сети или для узла, который не может автоматически получить адрес от DHCP-сервера.

Коммуникация с помощью локальных IPv4-адресов подходит только для обмена данными с другими устройствами, подключёнными к той же сети. Узел не должен отправлять пакет с локальным IPv4-адресом назначения какому-либо маршрутизатору для пересылки. Локальные адреса не предоставляют сервисы за пределами локальной сети. Однако многие приложения типа клиент-сервер и одноранговые приложения будут работать надлежащим образом с локальными IPv4-адресами.

Адреса в блоке от 240.0.0.0 до 255.255.255.254 указаны в качестве зарезервированных для использования в будущем (RFC 3330). В настоящее время эти адреса могут использоваться только в исследовательских или экспериментальных целях, но не могут использоваться в IPv4-сети. Тем не менее, в соответствии с документом RFC 3330, в будущем технически они могут быть преобразованы в доступные адреса.

Блок адресов от 192.0.2.0 до 192.0.2.255 (192.0.2.0/24) предназначен для обучающих и учебных целей. В отличие от экспериментальных адресов сетевые устройства принимают эти адреса в свои конфигурации.

Если необходимо определить относятся ли к одной сети IP-адреса узлов, то необходимо выполнить следующие действия (рисунок 2.6):

1 перевести IP-адреса в двоичную форму;

2 перевести маску подсети в двоичную форму;

3 осуществить операцию AND каждого IP-адреса с маской подсети

4 определить сетевой адрес для каждого IP-адреса

5 сравнить сетевые адреса

6 сделать вывод о том, какие IP-адреса находятся в одной сети.

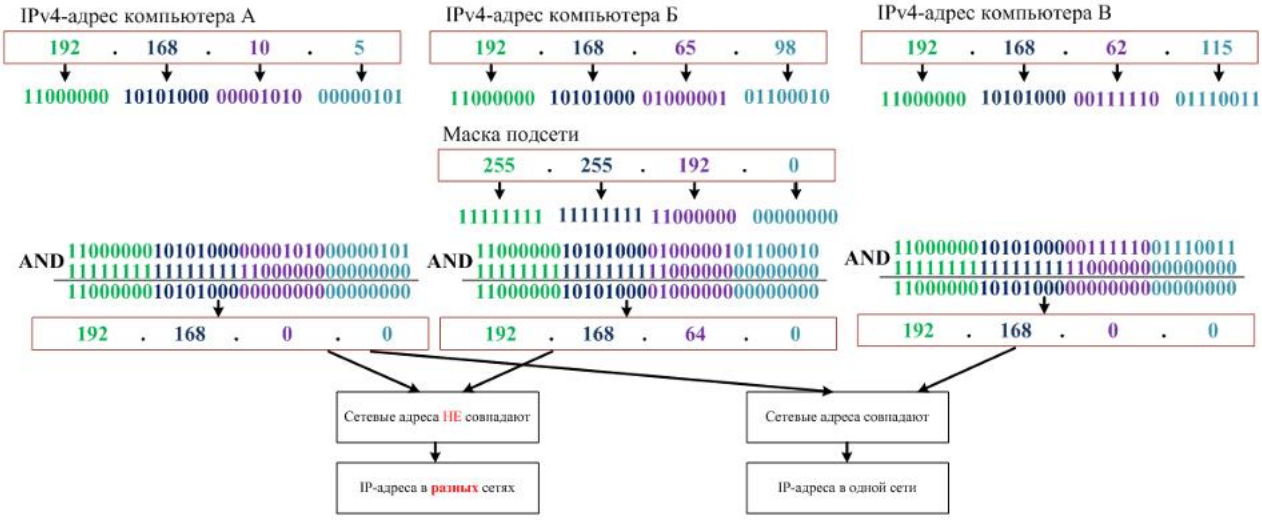

Рисунок 2.6 – Определение отношения IP-адресов к одной сети

2.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. Определить первый, широковещательный адреса и адрес сети. В соответствии со второй цифрой шифра из таблицы 2.3 выбрать IP-адреса и маски сети и определить адрес подсети, IP-адрес первого узла, широковещательный IP-адрес. Результаты представить в виде таблицы 2.4.

Таблица 2.3 – IP-адреса для расчета широковещательного адреса и адреса сети

Номер второй цифры шифра	IP-адреса и маски подсети
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

Таблица 2.4 – Результаты расчета IP-адресов

IP-адрес	В двоичной СС	В десятичной СС
Маска подсети		
IP-адрес с префиксом		
IP-адрес сети		
IP-адрес первого узла		
Широковещательный IP-адрес		

2. В соответствии с третьей цифрой шифра выбрать из таблицы 2.5 IP-адреса и маску подсети и определить IP-адреса, находящиеся в одной сети. Результаты оформить виде таблицы 2.6.

Таблица 2.5 – IP-адреса для расчета первого, широковещательного адреса и адреса сети

Номер третьей цифры шифра	IP-адреса	Маска подсети
0		
1		
2		
3		
4		
5		
6		
7		
8		
9		

Таблица 2.6 – Результаты сравнения IP-адресов

	Первый IP-адрес	Второй IP-адрес	Третий IP-адрес
В десятичном формате			
В двоичном формате			
Маска подсети в десятичном формате			
Маска подсети в двоичном формате			
Результат операции AND			
Сетевой адрес в десятичном формате			
IP-адреса в одной сети			

3. В соответствии с первой цифрой шифра выбрать из таблицы 2.7 IP-адреса и определить, какие из IP-адресов являются адресом сети, оконечного устройства или адрес широковещательной рассылки. Результат оформить виде таблице 2.8.

Таблица 2.7 – IP-адреса для расчета широковещательного адреса и адреса сети

Номер первой цифры шифра	IP-адреса
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

Таблица 2.8 – Результаты определения вида IP-адреса

Вид адреса	IP-адрес	Маска подсети
Адрес сети		
Широковещательный адрес		
Адрес узла		

4. Из таблицы 2.9 выбрать IP-адреса в соответствии со второй цифрой шифра и определить тип и класс IP-адреса. По результатам выполнения заполнить таблицу 2.10.

Таблица 2.9 – IP-адреса для определения типа и класса

Номер второй цифры шифра	IP-адреса
0	
1	
2	
3	
4	
5	
6	

Продолжение таблицы 2.9

Номер второй цифры шифра	IP-адреса
7	
8	
9	

Таблица 2.10 – Результаты определения вида IP-адреса

IP-адрес	Класс	Тип

2.3 Содержание отчета

1. Цель работы, исходные данные из таблиц 2.3, 2.5, 2.7, 2.9.

2. Результаты вычислений (заполненная таблица 2.4 для всех заданных IP-адресов из таблиц 2.3, 2.5, заполненные таблицы 2.6, 2.8, 2.10).

3. Вывод по работе.

4. Ответы на контрольные вопросы.

2.4 Контрольные вопросы

1. Определение адреса сети по IPv4-адресу и маске подсети. Определение сетевой и узловой части IPv4-адреса. Назначение префикса.

2. Способы взаимодействия устройств в сети.

3. Типы адресов IPv4.

4. Назначение широковещательного адреса сети, способы его определения по заданному IPv4-адресу и маске подсети.

5. Применение операции и для определения способа отправки.

6. Отличие частных и публичных IPv4-адресов. Назначение логического интерфейса loopback.

7. Локальные IPv4-адреса. Зарезервированные IPv4-адреса и адреса для учебных целей.

8. Последовательность действий при проверке IPv4-адресов на принадлежность к одной сети.