Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Севастопольский государственный университет»

ИССЛЕДОВАНИЕ ПРОТОКОЛА IP И ТЕХНОЛОГИИ МАРШРУТИЗАЦИИ

Методические указания
к выполнению лабораторной работы №2
по дисциплине **«Архитектура инфокоммуникационных систем и сетей»**

Для студентов, обучающихся по направлению 09.03.02
"Информационные системы и технологии"
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

Севастополь
2017

Исследование протокола IP и технологии маршрутизации. Методические указания к лабораторным занятиям по дисциплине «Архитектура (структуры и протоколы) инфокоммуникационных систем и сетей» / Сост. В.С. Чернега, А.В. Волкова – Севастополь: Изд-во СевГУ, 2017 – 21 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Архитектура (структуры и протоколы) инфокоммуникационных систем и сетей». Целью методических указаний является помощь студентам в исследовании технологии маршрутизации и принципов работы системного программного обеспечения на сетевом уровне модели взаимодействия открытых систем. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем (протокол № 10 от 21 апреля 2017 г.)

Рецензент: Моисеев Д.В., канд. техн. наук, доцент кафедры ИТиКС

1 Цель работы

Исследовать особенности функционирования и формат пакета протокола IP, технологию маршрутизации и принцип работы системного программного обеспечения на сетевом уровне модели взаимодействия открытых систем, приобрести практические навыки по конфигурации маршрутизаторов.

2 Теоретическая часть

2.1 Адресация хостов, сетей и подсетей с использованием IP

Протокол межсетевого взаимодействия *IP (Internet Protocol)* определяет правила передачи пакетов (для IP они называются *дейтаграммами*) между рабочими станциями (хостами) находящимися в одной или разных *IP-сетях* или *IP-подсетях*. Для адресации отправителей и получателей дейтаграмм IP использует четырехбайтовый адрес, значение каждого байта которого записывается в десятичной системе в виде `X.X.X.X`, где `X=0-255`. IP-адрес состоит из двух частей – адреса сети (старшие биты IP-адреса) и адреса хоста (младшие биты IP-адреса). Например, в адресе `192.168.1.1` можно выделить сетевую часть – три старшие цифры `192.168.1` адреса и хостовую часть – одну младшую цифру `1` адреса, этот адрес принадлежит IP-сети с диапазоном адресов `192.168.1.0` – `192.168.1.255`. Адресом всей сети для приведенного примера является адрес `192.168.1.0`, и он не может назначаться сетевым интерфейсам в качестве их адреса. В результате такого подхода становится возможной адресация групп компьютеров – *сетей* и *подсетей*, что позволяет с помощью *маршрутизаторов (Router)* – устройств, соединяющих сети/подсети в единую *составную сеть*, реализовать технологию маршрутизации дейтаграмм между сетями/подсетями. Под *маршрутизацией* понимают определение маршрутизаторами оптимального пути передачи дейтаграммы по направлению к ее получателю на основе информации об адресах сетей/подсетей. На рисунке 1 приведен пример составной сети, состоящей из четырех IP-сетей, организованных на коммутаторах Ethernet, которые объединены с помощью двух маршрутизаторов (участок между маршрутизаторами является пятой IP-сетью). Рядом с коммутаторами и возле линий связи между маршрутизаторами указаны IP-адреса сетей и так называемые *маски подсети (Subnet Mask)*, позволяющие делить IP-сети на IP-подсети. В состав сетей входят не только сетевые интерфейсы хостов, подсоединенных к коммутатору, но и сетевой интерфейс маршрутизатора, через который он подключен к данной сети, на рисунке 1 такие интерфейсы маршрутизаторов помечены стрелками. Эти интерфейсы маршрутизаторов называются *шлюзами (Gateway)*, дейтаграммы проходят через шлюз только в случае, если они адресованы получателям, находящимся в другой сети/подсети (то есть в случае, когда IP-адреса сети/подсети отправителя и сети/подсети получателя различаются). IP-адрес шлюза указывается при конфигурировании сетевых интерфейсов всех хостов сети/подсети.

Кроме адресации интерфейсов хостов, сетей/подсетей и маршрутизации, маршрутизатор может выполнять *фрагментацию/дефрагментацию дейтаграмм* при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров канального уровня – так называемой *максимальной единицы передачи MTU* (*Maximum Transfer Unit*). На практике

фрагментация/дефрагментация может происходить, когда маршрутизатор объединяет сети с разной технологией канального уровня, например, при объединении сетей Ethernet и Token Ring. Для Token Ring характерно отличное от Ethernet значение MTU. При этом фрагментацию/дефрагментацию могут осуществлять как маршрутизаторы, так и хосты.

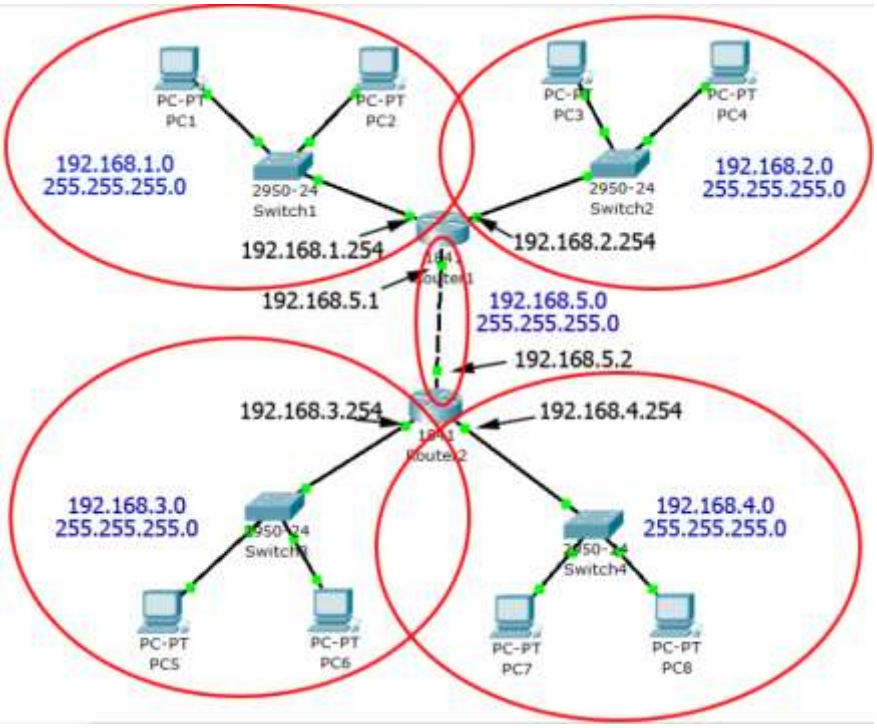

Рисунок 1 – Пример составной IP-сети

В IP отсутствуют механизмы, гарантирующие доставку дейтаграммы получателю и ее целостность. Эти функции возлагаются на транспортный уровень модели взаимодействия открытых систем.

Поскольку размер адреса протокола IP 4-й версии составляет 4 байта=32 бита, то пространство адресов составляет 2^{32}≈4,3 млрд. адресов. Из этого адресного пространства пользователям выделяются блоки смежных адресов – IP-сети (IP-подсети) и отдельные адреса. Выделение адресов координирует Международная организация IANA (Internet Assigned Numbers Authority) через пять организаций *региональных интернет-регистраторов*: AfriNIC (African Network Information Centre), ARIN (American Registry for Internet Numbers), APNIC (Asia-Pacific Network Information Centre), LACNIC (Latin American and Caribbean Internet Addresses Registry), RIPE NCC (Reseaux IP Europeens Network Coordination Centre). Эти организации выделяют блоки IP-адресов *локальным интернет-регистраторам (провайдерам услуг Интернет)*. Последние выделяют из своих блоков субблоки IP-адресов и отдельные IP-адреса конечным пользователям. Поскольку каждый из Региональных Интернет-провайдеров и Локальных Интернет-провайдеров обладает неперекрывающимися блоками IP-адресов, обеспечивается уникальность IP-адреса в глобальном масштабе.

Поскольку для разных пользователей существует потребность в сетях различного масштаба, в протоколе IP предусмотрена классификация IP-сетей. Предусмотрено пять классов IP-адресов: основные классы A, B, C и дополнительные классы D и E. Идентификация класса сети, к которому принадлежит IP-адрес, выполняется по старшему байту адреса (рисунок 2).

Класс A определяет самые крупные сети, 2, 3 и 4 байты IP-адреса этого класса содержат адрес хоста в сети (максимальное количество адресов в такой сети равно $2^{24} \approx$ 16,8 млн). Сети класса A принадлежат региональным интернет-провайдерам, крупным компаниям и организациям (в основном американским, что связано с историей развития Интернета). Признаком IP-адреса класса A является равный нулю старший бит старшего байта адреса, семь младших бит определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса класса A лежит в диапазоне от `0` до `127` (максимальное количество сетей класса A равно 128).

Класс	1 байт		2 байт	3 байт	4 байт	1 дес. число	Примечание
A	0	№ сети	№ хоста			0 – 127	128 сетей по 16 777 216 адресов
B	1	0	№ сети	№ хоста		128 – 191	16,384 сетей по 65,536 адресов
C	1	1	0	№ сети	№ хоста	192 – 223	2,097,152 сетей по 256 адресов
D	1	1	1	0		224 – 239	Multicast
E	1	1	1	1	0	220 – 247	резерв

Рисунок 2 – Классы IP-адресов

Класс B определяет средние по масштабу сети, 3 и 4 байты IP-адреса этого класса содержат адрес хоста в сети (максимальное количество адресов в такой сети равно $2^{16} \approx$ 65,6 тыс.). Сети класса B принадлежат в основном локальным интернет-провайдерам (провайдерам услуг Интернета) и крупным компаниям и организациям. Признаком IP-адреса класса B являются биты `10` в старших разрядах старшего байта адреса, шесть младших бит старшего байта (первого) и все биты второго байта определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса класса B лежит в диапазоне от `128` до `191` (максимальное количество сетей класса B равно $2^{14} \approx$ 16,4 тыс.).

Класс C определяет сети минимального масштаба, только 4-ый байт (младший) IP-адреса этого класса содержит адрес хоста в сети (максимальное количество адресов в такой сети равно $2^8 \approx$ 256 адресов). Сети класса C принадлежат в основном провайдерам услуг Интернета, различным компаниям и организациям. Признаком IP-адреса класса C являются биты `110` в старших разрядах старшего байта адреса, пять младших бит старшего байта (первого), все биты второго и третьего байтов определяют адрес сети. Таким образом, десятичное значение старшего байта IP-адреса класса C лежит в диапазоне от `192` до `223` (максимальное количество сетей класса C равно $2^{21} \approx$ 2,1 млн.).

Имеется возможность выяснить, кто является владельцем сети, в которую входит произвольный IP-адрес, а также координаты администратора этой сети, выполнив запрос к базе данных регионального или локального регистратора. Для

европейских адресов это можно сделать на сайте RIPE NCC http://www.db.ripe.net/whois.

Класс D служит для обозначения групповых IP-адресов, представляющих собой так называемые *мультикастовые группы* (*Multicast Group*), использующиеся технологией рассылки одного и того же потока дейтаграмм нескольким получателям одновременно. При этом вплоть до шлюза сети получателя этот поток не дублируется, а в качестве IP-адреса получателя в дейтаграммах указывается адрес мультикастовой группы. Признаком IP-адреса класса D являются биты `1110` в старших разрядах старшего байта адреса, четыре младших бита старшего байта (первого) и все биты второго, третьего и четвертого байтов определяют адрес мультикастовой группы. Таким образом, десятичное значение старшего байта IP-адреса класса D лежит в диапазоне от `224` до `239` (максимальное количество мультткастовых групп равно $2^{28} \approx 268$ млн.).

Класс E характеризуется адресом, старшие биты старшего байта которого равны `11110`, десятичное значение старшего байта IP-адреса класса E лежит в диапазоне от `240` до `247`, адреса этого класса зарезервированы для будущих применений.

Оставшиеся адреса с десятичным значением старшего байта от `248` до `255` также зарезервированы. В адресном пространстве IP v4 также зарезервированы следующие адреса под специальные нужды:

– `0.0.0.0` – адрес хоста, сгенерировавшего пакет (используется только в некоторых сообщениях протокола управляющих сообщений Интернета – ICMP);

– `255.255.255.255` – пакет с таким IP-адресом получателя рассылается всем хостам, находящимся в той же сети, что и отправитель этого пакета *широковещательное сообщение*;

– в поле номера сети IP-адреса получателя все биты равны нулю – хост-получатель принадлежит той же сети, что и хост-отправитель (например, `0.0.0.X, X=1-224`);

– в поле номера хоста IP-адреса получателя все биты равны нулю – такой адрес является адресом сети с заданным в поле номера сети адресом (например, `X.X.X.0, X=1-224`);

– в поле номера хоста IP-адреса получателя все биты равны единице – пакет рассылается всем хостам сети с заданным в поле номера сети адресом – широковещательное сообщение (например, `X.X.X.255, X=1-224`);

– старший байт IP-адреса = `127` – *кольцевой адрес* (*Loopback Address*) – петля (обычно используется адрес `127.0.0.1`) – используется для тестирования программ и взаимодействия процессов в пределах одного хоста;

– блоки частных адресов, зарезервированные для локальных сетей (без выхода в Интернет или использующих сетевую трансляцию адресов) – одна сеть класса A `10.0.0.0-10.255.255.255`, 16 сетей класса B `172.16.0.0-172.31.255.255`, 256 сетей класса C `192.168.0.0` - `192.168.255.255`.

Любой маршрутизатор, работающий в Интернет, не будет передавать пакеты с адресами из диапазонов адресов для локальных сетей. В то же время такие адреса удобны, поскольку они могут присваиваться хостам локальных сетей их администраторами без согласования с провайдерами услуг Интернет. Для выхода в Интернет с этих адресов используется технология *сетевой*

трансляции адресов NAT (*Network Address Translation*), подменяющая локальный IP-адрес отправителя на разрешенный для передачи в Интернет адрес, полученный от провайдера. Таким образом, достигается существенная экономия адресов (и средств, оплачиваемых провайдерам за их аренду). При этом все хосты с локальными адресами в Интернете видны как один хост с разрешенным для работы в Интернете адресом, что не позволяет размещать на внутренних хостах общедоступные для пользователей Интернета сервисы. Последнее обстоятельство одновременно является преимуществом с точки зрения безопасности: внутренние хосты с локальными адресами не видны из Интернета.

Недостатком выделения IP-адресов по классовой схеме является невозможность экономного выделения групп IP-адресов. Действительно, если в небольшой компании всего несколько компьютеров (например, 6), то она вынуждена арендовать сеть класса C как сеть минимально возможного масштаба. Однако при этом, даже, если компания увеличит парк компьютеров вдвое, более 240 адресов (с учетом зарезервированных под специальные нужды) останутся неиспользованными. Поэтому в настоящее время классовая схема адресации вытеснена бесклассовой схемой, согласно которой выделение блоков IP-адресов основано на использовании *маски подсети*.

Маска подсети – это двоичное число с количеством разрядов, равным количеству разрядов IP-адреса, используемое вместе с IP-адресом. Маска содержит единицы в тех разрядах IP-адреса, которые должны интерпретироваться как номер подсети. Количество адресов в IP-подсети $N=2^m$, где m – количество нулевых битов в маске подсети (заметим, что речь идет именно об IP-адресах, включающих и специальные адреса, а не только об адресах хостов).

Снабжая адрес маской, можно отказаться от понятия классов адресов для возможности более гибкого распределения адресов, например, разбиения полученной организацией сети класса C на подсети подразделений нужного размера с целью обеспечения локализации трафика подразделений и реализации внутрикорпоративной политики безопасности. При этом для внешних хостов и маршрутизаторов сеть организации по-прежнему выглядит как сеть класса C и отсутствует необходимость добавления маршрутов к подсетям на внешних маршрутизаторах.

На рисунок 3 приведены возможные маски подсети для сети класса C и количество доступных адресов в подсети для каждой из них. Количество адресов для нумерации хостов на два меньше, поскольку первый адрес – это адрес самой подсети, а последний адрес – широковещательный адрес этой подсети. Кроме того, один из доступных адресов хостов (часто первый или последний) обычно назначают интерфейсу маршрутизатора шлюза, соединяющего данную подсеть с другими сетями.

С использованием технологии создания подсетей для небольшой компании с 6 компьютерами вместо 256 адресов сети класса C с помощью маски подсети `255.255.255.240` могут быть выделены 16 адресов, из которых для нумерации хостов и шлюза останутся 14. Однако, использование `255.255.255.248` маски обеспечит только 6 адресов, которых хватит на нумерацию хостов, но IP-адреса для шлюза этой сети уже не хватит.

Маска (дес)	Маска (двоичн)	Хостов	Подсетей	Примечание
255.255.255.255	11111111.11111111.11111111.11111111	все	нет	
255.0.0.0	11111111.00000000.00000000.00000000	16777214	126	Класс A
255.255.0.0	11111111.11111111.00000000.00000000	16382		Класс B
255.255.255.0	11111111.11111111.11111111.00000000	254		Класс C
Деление на подсети с количеством хостов менее 254				
255.255.255.254	11111111.11111111.11111111.11111110	0 (2 адреса)	128	не имеют смысла
255.255.255.252	11111111.11111111.11111111.11111100	2 (4 адреса)	64	
255.255.255.248	11111111.11111111.11111111.11111000	6 (8 адр.)	32	
255.255.255.240	11111111.11111111.11111111.11110000	14 (16 адр.)	16	
255.255.255.224	11111111.11111111.11111111.11100000	30 (32 адр.)	8	
255.255.255.192	11111111.11111111.11111111.11000000	62 (64 адр.)	4	
255.255.255.128	11111111.11111111.11111111.10000000	126 (128 адр.)	2	

Рисунок 3 – Маскирование IP-адресов класса C

На рисунке 4 показан пример планирования подсетей для четырех подразделений организации, в которых находится 77, 50, 29 и 15 компьютеров, соответственно. Для каждой подсети приведены ее адрес, маска подсети, широковещательный адрес, адрес, зарезервированный для шлюза, диапазон адресов хостов и диапазон резервных адресов (для будущих подключений). Механизм масок широко используется в технологии IP-маршрутизации. При получении маршрутизатором IP пакета из IP-адреса получателя определяется адрес подсети назначения путем логического умножения (операция AND) IP-адреса получателя на маску подсети, например:

```
      192.168.3.5 AND 255.255.255.240 =
      11000000 10101000 00000011 00000101
AND   11111111 11111111 11111111 11110000
=     11000000 10101000 00000011 00000000      = 192.168.3.0
```

Полученный номер подсети используется для нахождения маршрута (т.е. адреса следующего маршрутизатора по пути к хосту-получателю) с помощью таблицы маршрутизации маршрутизатора.

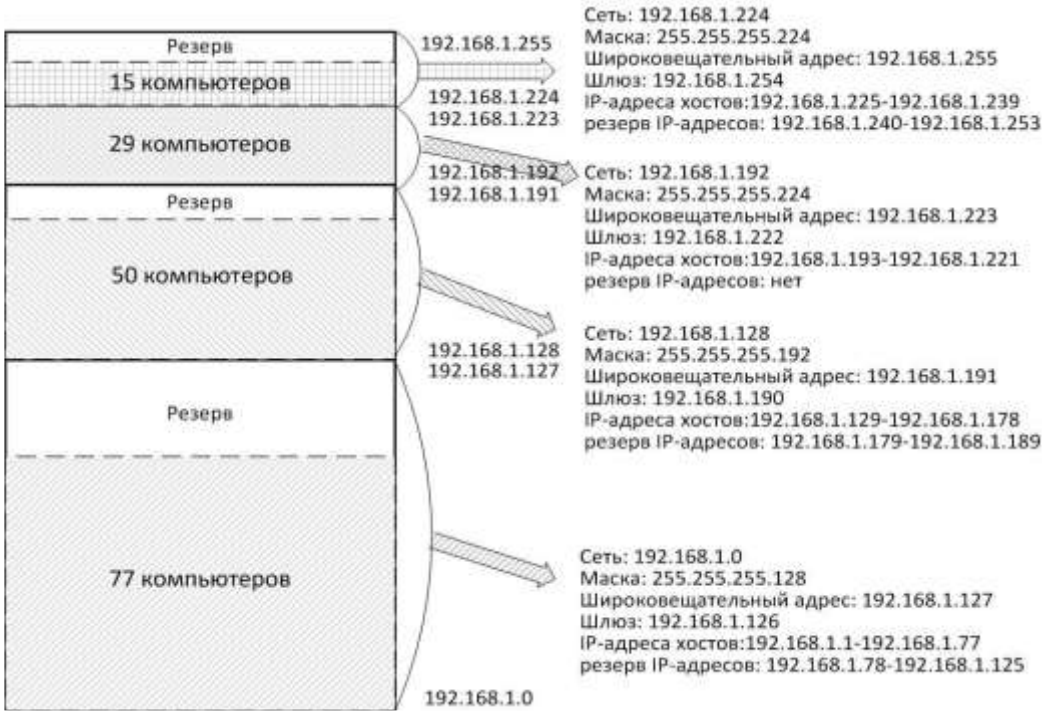

Рисунок 4 – Пример планирования IP-адресов для четырех подсетей

При планировании подсетей адресное пространство каждой следующей смежной подсети не может быть больше адресного пространства предыдущей. Для правильного планирования подсетей в приведенном примере (рисунок 5) необходимо выделение 16-адресной подсети спланировать на границе 16-адресного блока, например, выделить ей блок `192.168.1.16 - 192.168.1.31`.

Оставшийся незанятым блок адресов `192.168.1.8 - 192.168.1.15` можно выделить третьей подсети с таким количеством хостов или оставить пустым. Результат умножения любого из адресов подсети на маску приводит к получению для всех адресов всех подсетей IP-адреса данной подсети. Маршрутизация будет работать правильно. Фактически, при планировании подсетей количеством адресов предыдущей подсети задаются границы следующей смежной подсети, которые не должны пересекаться адресным полем следующей подсети. Для того чтобы избежать ошибочного планирования, рекомендуется в начале адресного пространства размещать более крупные подсети, а затем более мелкие по мере уменьшения необходимого им количества адресов.

Net→	192	168	1	0	Broad Cast→	192	168	1	7
Net→	11000000	10101000	00000001	00000000	Broad Cast→	11000000	10101000	00000001	00000111
Mask→	11111111	11111111	11111111	11111000	248	11111111	11111111	11111111	11111000
IP ⊗ MASK	11000000	10101000	00000001	00000000	IP ⊗ MASK	11000000	10101000	00000001	00000000
IP ⊗ MASK	192	168	1	0	IP ⊗ MASK	192	168	1	0
Net→	192	168	1	8	Broad Cast→	192	168	1	15
Net→	11000000	10101000	00000001	00001000	Broad Cast→	11000000	10101000	00000001	00001111
Mask→	11111111	11111111	11111111	11111000	248	11111111	11111111	11111111	11111000
IP ⊗ MASK	11000000	10101000	00000001	00000000	IP ⊗ MASK	11000000	10101000	00000001	00001000
IP ⊗ MASK	192	168	1	8	IP ⊗ MASK	192	168	1	8
Net→	192	168	1	16	Broad Cast→	192	168	1	31
	11000000	10101000	00000001	00010000	Broad Cast→	11000000	10101000	00000001	00011111
Mask→	11111111	11111111	11111111	11110000	240	11111111	11111111	11111111	11110000
IP ⊗ MASK	11000000	10101000	00000001	00010000	IP ⊗ MASK	11000000	10101000	00000001	00010000
IP ⊗ MASK	192	168	1	16	IP ⊗ MASK	192	168	1	16

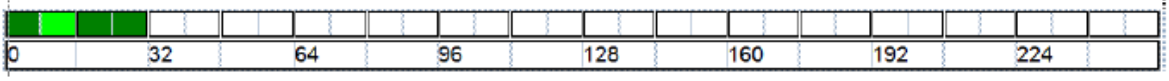

Рисунок 5 – Пример правильного планирования
IP-адресного пространства с помощью масок

Механизм масок в настоящее время используется не только для разбиения классовых сетей на подсети, но и для выделения сетей произвольного размера с помощью маски с любым необходимым количеством нулевых битов, определяющих размер сети, в любом месте адресного пространства. Такая технология получила название *бесклассовой междоменной маршрутизации CIDR* (*Classless*

InterDomain Routing), она позволяет гибко распределять адресное пространство и упрощать маршрутизацию. Технология CIDR предлагает описывать маску подсети добавленным к адресу сети суффиксом, в котором указано количество единичных битов маски. Например, запись `192.168.0.0/22` – определяет так называемую *суперсеть* с маской `11111111.11111111.11111100.00000000 = 255.255.252.0` с диапазоном адресов `192.168.0.0 - 192.168.3.255`, эквивалентную четырем смежным сетям класса С. Такая сеть может быть выделена на бесклассовой основе организации, которой необходимо до 1024 адресов (вместо выделения сети класса В с 65536 адресами с использованием классов).

2.2 Маршрутизация IP-дейтаграмм

Важнейшей задачей сетевого уровня является *маршрутизация* (*Routing*) дейтаграмм в составной сети, суть которой сводится к поиску маршрутизаторами оптимального пути (маршрута) к получателю дейтаграммы. Маршрутизация выполняется сетевыми устройствами, называемыми *маршрутизаторы* (*Router*). Любой маршрутизатор обладает более чем одним сетевым интерфейсом, к которым подключены сети/подсети, которые он соединяет. Например, маршрутизатор R1 на рисунке 6 связывает сети N1, N2 и N7, имеющие маски подсети M1, M2 и M7, соответственно, через свои интерфейсы R1(1), R1(2) и R1(3). Следует отметить, что даже если в сети отсутствуют пользовательские хосты, она все равно считается сетью/подсетью, имеет свой адрес и обладает другими свойствами, характерными для сетей/подсетей (такими сетями/подсетями являются сети с адресами N7, N8 и N9 *связей «точка – точка»* (*Point-to-Point*) между маршрутизаторами на рисунке 6).

Под *маршрутом* понимается последовательность маршрутизаторов, которые должна пройти дейтаграмма от хоста-отправителя до хоста-получателя. Выбор следующего шага маршрута выполняется каждым маршрутизатором и конечными хостами на основании имеющейся у них информации об адресах сетей/подсетей, записанных в так называемой *таблице маршрутизации,* и некоторого критерия выбора маршрута.

Критериями могут быть: количество маршрутизаторов на маршруте (hops), время прохождения тестового пакета до следующего по пути маршрутизатора, пропускная способность линии связи к следующему маршрутизатору и другие. Для каждой записи в первом столбце таблицы маршрутизации (см. рисунок 6) указывается адрес сети/подсети/хоста назначения дейтаграммы, во втором – маска подсети назначения, в третьем – сетевой адрес следующего по маршруту маршрутизатора, на который необходимо направить дейтаграмму, чтобы она продвигалась по рациональному маршруту к получателю. В четвертом столбце указывается сетевой адрес порта текущего маршрутизатора, через который должна уйти по выбранному маршруту дейтаграмма. В пятом столбце указывается метрика маршрута – один из приведенных выше критериев выбора маршрута (в таблицах маршрутизации на рисунке 6 в качестве метрики приведено количество промежуточных маршрутизаторов на маршруте – hops). Метрика маршрута указывается для выбора оптимального маршрута при наличии в таблице маршрутизации нескольких строк с маршрутами к одной и той же сети (например, маршруты к сети N4 в таблице маршрутизации маршрутизатора R2 на рисунке 6).

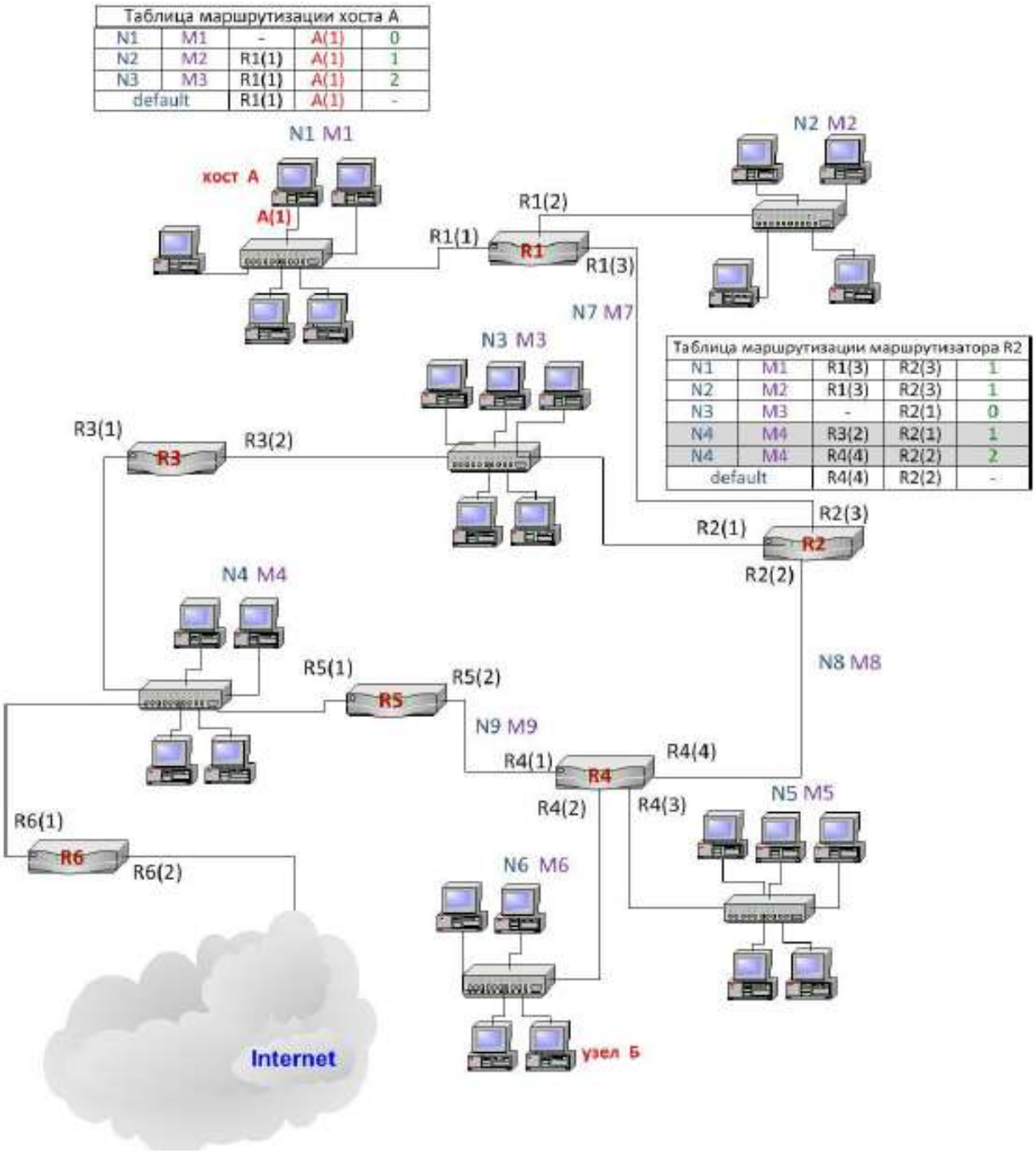

Рисунок 6 – Пример маршрутизации в составной сети

Количество записей в таблице маршрутизации может быть достаточно большим даже для относительно небольшой составной сети вследствие наличия альтернативных маршрутов, кроме того, в больших составных сетях адреса удаленных сетей/подсетей просто неизвестны. Поэтому обычно в последней строке таблиц маршрутизации указывается так называемый *маршрут по умолчанию* (*default route*), по которому будет направлена дейтаграмма в случае неудачного поиска адреса сети назначения дейтаграммы в первом столбце таблицы маршрутизации. Для хостов в маршруте по умолчанию в качестве следующего маршрутизатора по маршруту обычно указывается адрес шлюза локальной сети (как для хоста A на рисунке 6), а для маршрутизаторов – адрес маршрутизатора, следующего по маршруту, который используется большей частью исходящих дейтаграмм (как для маршрутизатора R2 на рисунке 6). Достаточно часто маршрут по умолчанию граничного маршрутизатора организации указывает на маршрутизатор провайдера Интернета для этой организации, маршрутизатор этого провай-

дера Интернета в качестве маршрута по умолчанию может использовать маршрут к маршрутизатору Интернет-провайдера более высокого уровня и т.д.

Записи в таблицу маршрутизации заносятся либо вручную, в этом случае маршрутизация называется статической (статическая маршрутизация обычно используется в относительно небольших составных сетях), или записи заносятся в результате работы протоколов динамической маршрутизации, задача которых – изучение топологии и адресной информации сетей/подсетей, формирующих составную сеть, и обмен записями маршрутных таблиц между маршрутизаторами составной сети. Популярными в настоящее время протоколами динамической маршрутизации являются *протокол маршрутной информации RIP* (*Routing Information Protocol*), *протокол кратчайшего пути OSPF* (*Open Shortest Path First*) и *протокол граничного шлюза BGP* (*Border Gateway Protocol*).

Маршрутизаторы определяют следующий от них шаг маршрута дейтаграммы по следующему алгоритму:

– из заголовка дейтаграммы извлекается сетевой адрес получателя и выполняется поиск его значения в первом столбце таблицы маршрутизации, если адрес найден, дейтаграмма направляется по адресу следующего на пути маршрутизатора, указанный в третьем столбце строки с найденным адресом;

– если адрес получателя в первом столбце не найден, из адреса получателя восстанавливается адрес сети получателя путем умножения адреса получателя на маску подсети назначения во втором столбце первой строки;

– после получения адреса сети выполняется его сравнение с адресом сети/подсети назначения в первом столбце первой строки;

– если адреса совпадают, в качестве следующего адреса маршрута выбирается адрес из третьего столбца первой строки;

– если адреса не совпадают, адрес получателя умножается на маску подсети из второй строки и полученный адрес сети/подсети сравнивается с адресом сети назначения в первом столбце второй строки и если совпадение адресов получено, дейтаграмма передается по адресу маршрутизатора, указанному в третьем столбце второй строки;

– если адреса не совпадают, алгоритм вычисления сети/подсети и сравнения повторяются для остальных строк таблицы, пока не будет найдено совпадение;

– в последней строке таблицы указывается маршрут по умолчанию, для него в первом и втором столбце заносятся адреса `0.0.0.0` и `0.0.0.0`. Умножение любого IP-адреса на маску `0.0.0.0` приведет к получению адреса сети `0.0.0.0`, поэтому совпадение будет достигнуто для любого адреса, для которого не получено совпадение в предыдущих строках таблицы маршрутизации и дейтаграмма будет направлена маршрутизатору, адрес которого указан в третьем столбце строки с маршрутом по умолчанию.

На рисунке 7 показан пример, иллюстрирующий обработку таблицы маршрутизации при поиске маршрута для дейтаграммы с адресом назначения `192.168.3.25` (`11000000 10101000 00000011 00011001`). Сравнение адресов выполняется побитово с помощью логической операции `XOR`, а ее нулевой результат свидетельствует о совпадении сравниваемых адресов. Совпадение вычисленного адреса сети назначения и адреса сети в первом столбце таблицы маршрутизации достигнуто в третьей строке, поэтому следующим маршрутизатором по пути будет выбран `192.168.2.2`, а маршрут по умолчанию прове-

ряться не будет. Однако если бы он проверялся, то совпадение было бы получено для любых проверяемых адресов хоста получателя.

Отправка дейтаграммы следующему по пути маршрутизатору, адрес которого найден в таблице маршрутизации, не означает замены адреса получателя в заголовке дейтаграммы. Такая замена сделала бы невозможным поиск дальнейших шагов маршрута. Полученный из третьего столбца таблицы маршрутизации адрес используется для определения адреса канального уровня этого порта (например, MAC адреса Ethernet) с помощью ARP-запроса. Заменяются только MAC-адрес отправителя (на MAC-адрес исходящего интерфейса маршрутизатора) и MAC-адрес получателя (на MAC-адрес, полученный с помощью ARP). Таким образом, IP-адреса отправителя и получателя не изменяются на всем протяжении маршрута, который проходит дейтаграмма, в то время как MAC-адреса (или другие адреса канального уровня) изменяются в каждой локальной сети, которую пересекает дейтаграмма.

Сеть назначения	Маска подсети назначения	Следующий маршрутизатор	Исходящий интерфейс	Метрика
192.168.1.0	255.255.255.0	192.168.5.1	192.168.4.1	2
192.168.3.0	255.255.255.240	192.168.2.1	192.168.4.2	1
192.168.3.16	255.255.255.240	192.168.2.2	192.168.4.3	1
0.0.0.0	0.0.0.0	192.168.5.2	192.168.4.1	–

обработка 1-й строки

```
        11000000 10101000 00000011 00011001   =  192.168.3.25
   AND  11111111 11111111 11111111 00000000   =  255.255.255.0
        --------------------------------------
        11000000 10101000 00000011 00000000   =  192.168.3.0
   XOR  11000000 10101000 00000001 00000000   =  192.168.1.0
        --------------------------------------
        00000000 00000000 000000 10 00000000  ≠  0
```

обработка 2-й строки

```
        11000000 10101000 00000011 00011001   =  192.168.3.25
   AND  11111111 11111111 11111111 11110000   =  255.255.255.240
        --------------------------------------
        11000000 10101000 00000011 00010000   =  192.168.3.16
   XOR  11000000 10101000 00000011 00000000   =  192.168.3.0
        --------------------------------------
        00000000 00000000 00000000 0001 000   ≠  0
```

обработка 3-й строки

```
        11000000 10101000 00000011 00011001   =  192.168.3.25
   AND  11111111 11111111 11111111 11110000   =  255.255.255.240
        --------------------------------------
        11000000 10101000 00000011 00010000   =  192.168.3.16
   XOR  11000000 10101000 00000011 00010000   =  192.168.3.16
        --------------------------------------
        00000000 00000000 00000000 00000000   =  0
```

Рисунок 7 – Пример обработки записей таблицы маршрутизации для адреса 192.168.3.25

В примере на рисунке 8 IP-адреса отправителя (IP1) и получателя (IP2) не меняются на всем маршруте дейтаграммы, в то время как MAC-адреса меняются в каждой сети. IP-адреса маршрутизаторов используются только для ARP-запросов.

Задачу маршрутизации также решают пользовательские хосты. Так, если номер сети назначения совпадает с сетью, к которой принадлежит сам компьютер, то задачу маршрутизации решать не требуется и пакет просто передается канальному уровню вместе с определенным по протоколу ARP адресом каналь-

ного уровня получателя. Если не совпадает, то необходима маршрутизация и узел-отправитель просматривает свою таблицу маршрутизации.

Рисунок 8 – Изменение адресов канального уровня при передаче дейтаграммы в составной сети

Команда `route print` в Windows выводит эту таблицу на экран, а также позволяет задавать и удалять маршруты (рисунок 9).

```
C:\WINNT\system32>route print
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 d0 b7 69 21 71 ...... Intel(R) PRO Adapter
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети       Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0   192.168.1.129   192.168.1.130       1
        127.0.0.0        255.0.0.0         127.0.0.1       127.0.0.1       1
    192.168.1.128  255.255.255.128   192.168.1.130   192.168.1.130       1
    192.168.1.130  255.255.255.255         127.0.0.1       127.0.0.1       1
    192.168.1.255  255.255.255.255   192.168.1.130   192.168.1.130       1
        224.0.0.0        224.0.0.0   192.168.1.130   192.168.1.130       1
  255.255.255.255  255.255.255.255   192.168.1.130   192.168.1.130       1
Основной шлюз:        192.168.1.129
===========================================================================

C:\WINNT\system32> route ADD 192.168.1.16 MASK 255.255.255.240  192.168.1.1
```

Рисунок 9 – Пример таблицы маршрутизации хоста и команда добавления маршрута

Хосты в большей степени, чем маршрутизаторы пользуются маршрутом по умолчанию, обычно в качестве следующего по маршруту маршрутизатора для маршрута по умолчанию указывается шлюз локальной сети хоста (с IP-адресом 192.168.1.129 для примера на рисунке 9). Следует отметить, что в таблицу маршрутизации автоматически заносится адрес сети `127.0.0.0`. Если в поле IP-адрес получателя находится адрес этой сети, то передачи пакета на канальный уровень (и, следовательно, в сеть) не происходит, а этот пакет возвращается отправителю (путем обмена адресов отправителя и получателя в соответствующих полях пакета). Аналогично может вноситься запись для сетевых адресов соб-

ственных портов маршрутизатора для них адресом следующего маршрутизатора и выходного интерфейса указывается адрес `127.0.0.1` – loopback.

Также в таблицу автоматически заносятся записи для сети с адресом `224.0.0.0` – они требуются для обработки *групповых адресов (multicast address)*. Кроме того, в таблицу могут быть занесены адреса, предназначенные для обработки широковещательных рассылок в сетях, подсоединенных к портам маршрутизатора, – это адреса, заканчивающиеся на последовательность единиц (`255`).Одни указывают маршрут для отправки широковещательных сообщений в составной сети для определенных подсетей – сетевой адрес подключенного к этим сетям порта маршрутизатора, адрес `255.255.255.255` – адрес ограниченной широковещательной рассылки – пакет с таким адресом рассылается всем узлам, находящимся в той же подсети, что и отправитель.

2.3 Формат заголовка IP-пакета

IP-дейтаграмма состоит из заголовка (обычно 20 байт) и поля данных, максимальная длина пакета – заголовок + данные составляет 65535 байтов, минимальная – определяется минимальным размером переносящего IP-пакет кадра канального уровня (для Ethernet 64 байта). Структура IP-пакета приведена на рисунке 10.

0 3	4 7	8 15	16 31
Номер версии	Длина заголовка	Тип сервиса	Общая длина пакета
Идентификатор пакета		Флаги 3 бита	Смещенные флаги 13 бит
Время жизни		Протокол верхнего уровня	Контрольная сумма заголовка
IP-адрес отправителя			
IP-адрес получателя			
Опции и выравнивание			
Данные			

Поле «Тип сервиса»

0	1	2	3	4	5	6	7
Приоритет			Задержка	Пропускная способность	Надежность доставки	Резерв (0)	

Поле «Флаги»

0	1	2
Резерв (0)	Do not Fragment	More Fragment

Поле «Протокол верхнего уровня»

Значение поля	$0=00_н$	$1=01_н$	$2=02_н$	$4=04_н$	$6=06_н$	$8=08_н$	$17=11_н$	$88=58_н$	$89=59_н$
Протокол	Резерв	ICMP	IGMP	IP	TCP	EGP	UDP	IGRP	OSPF

Рисунок 10 – Структура IP-пакета

Поле *Номер версии* (*Version*) указывает версию протокола IP. Напомним, что в настоящее время широко используется 4 версия IPv4 и начинается переход на 6 версию IPv6 (формат заголовка IPv6 отличается от рассматриваемого заголовка IPv4).

Поле *Длина заголовка* (*Header Length*) указывает значение длины заголовка IP-пакета в 32-битных (четырехбайтовых) словах. Обычно длина заголовка составляет 5 таких слов (20 байт), но может быть больше за счет дополни-

тельных байтов в поле Опции (максимальная длина заголовка 60 байт = 15 четырехбайтовых слов).

Младшие три бита поля (0-2) *Тип сервиса* (*Type of Service*) задают приоритет пакета от самого низкого `000` (нормальный пакет) до самого высокого `111` (пакет с управляющей информацией). Биты 3-5 определяют критерий выбора маршрута, используемый в протоколах маршрутизации *OSPF* и *BGP*. Выбор осуществляется между тремя альтернативами: малой задержкой передачи дейтаграмм (бит 3 *Delay=1*), высокой пропускной способностью линии связи (бит 4 *Throughput=1*) и высокой надежностью передачи дейтаграмм (бит 5 *Reliability=1*). Обычно улучшение одного параметра вызывает ухудшение другого, следовательно, выбирается один критерий выбора маршрута. Хосты обычно не используют возможность определения типа сервиса отправляемой дейтаграммы и указывают значение этого поля $00_н$.

Поле *Общая длина* (*Total Length*) содержит общую длину IP-пакета вместе с заголовком. Исходя из разрядности поля (2 байта), максимальная длина пакета составляет 65535 байт. Однако в большинстве случаев такие большие пакеты не используются, а размер пакета выбирается с учетом максимального поля данных несущего этот пакет кадра канального уровня (MTU). Для сетей Ethernet MTU ≈ 1500 байт, для сетей FDDI размер MTU ≈ 4096 байт.

При перенаправлении IP-пакета из одной сети в другую маршрутизатор может столкнуться с проблемой различных значений MTU в соседних сетях. В этом случае ему необходимо выполнить фрагментацию дейтаграммы (т.е. разбиение ее на несколько самостоятельных дейтаграмм) при передаче в сеть с меньшим значением MTU и дефрагментацию (то есть объединение нескольких дейтаграмм, полученных при фрагментации, в одну исходную) при передаче пакета в сеть с большим значением MTU. В целях распознавания пакетов, образованных в результате фрагментации используется поле *Идентификатор пакета* (*Identification*). Все фрагменты фрагментированного пакета имеют одинаковое значение этого поля.

Поле *Флаги* (*Flags*) содержит биты: 0 бит - резерв = `0`, 1 бит - *DF* – *Do not Fragment* в случае установки в `1` запрещает фрагментацию пакета, 2 бит – *MF* – *More Fragments* в случае установки в `1` свидетельствует о том, что данная дейтаграмма является промежуточным (не последним) фрагментом.

В поле *Смещение фрагмента* (*Fragment Offset*) указывается смещение в 8-байтных блоках поля данных этого пакета-фрагмента от начала общего поля данных исходного пакета, подвергнутого фрагментации (8 байт × 2^{13} = 2^{16} – максимальный размер пакета). Первый фрагмент имеет значение этого поля, равное `0`.

Поле *Время жизни* *TTL* (*Time To Live*) указывает предельный срок времени, в течение которого дейтаграмма может перемещаться по сети. Это время задается отправителем дейтаграммы в секундах. При пересылке пакета через маршрутизатор значение TTL уменьшается на 1 (даже если время передачи через маршрутизатор менее 1 секунды). Поэтому иногда говорят, что это время измеряется в количестве переходов через маршрутизаторы (hops). При достижении этим значением 0 пакет далее не передается.

Поле *Протокол верхнего уровня* (*Protocol*) содержит идентификатор протокола, переносящего информацию, размещенную в поле данных IP-пакета. Наиболее популярными идентификаторами являются $06_{н}$ – для *протокола управления транспортированием пакетов TCP* (*Transport Control Protocol*), $11_{н}$ – для *протокола пользовательских дейтаграмм UDP* (*User Datagram Protocol*) и $01_{н}$ – для *протокола управляющих сообщений Интернет ICMP* (*Internet Control Message Protocol*).

Поле *Контрольная сумма* (*Header Checksum*) рассчитывается только для заголовка IP-дейтаграммы. При каждом изменении полей заголовка промежуточными маршрутизаторами контрольная сумма заголовка пересчитывается.

Поля *IP-адрес отправителя* (*Source IP Address*) и *IP-адрес получателя* (*Destination IP Address*) содержат соответствующие адреса.

Поле *Опции* (*IP Options*) является необязательным и обычно не используется. В нем могут указываться точный маршрут прохождения дейтаграммы, данные о безопасности, различные временные отметки и т.д. Поле может иметь произвольную длину в пределах от 0 до 40 байтов, для выравнивания размера дейтаграммы по 32-битной границе используется поле *Выравнивание* (*Padding*). Это поле, например, используется для дополнения размера дейтаграммы нулевыми байтами до минимального размера поля данных кадра канального уровня (для сетей Ethernet 64 байта).

3 Описание лабораторной установки

В качестве лабораторного стенда используется персональный компьютер с установленной программой Cisco Packet Tracer. Работа с этим пакетом детально описана в предыдущей лабораторной работе.

4 Программа выполнения работы

1. В программе Cisco Packet Tracer постройте составную сеть, изображенную на рисунке 1. По аналогии с примером на рисунке 5 выполните планирование адресного пространства для составной компьютерной сети, состоящей из четырех IP-подсетей сетей с N_1, N_2, N_3 и N_4 хостами и пятой подсетью между маршрутизаторами. Количество пользовательских хостов в подсетях вычисляется следующим образом:

```
N1 = порядковому номеру студента в журнале;
N2 = N1 + 15;
N3 = N1 + 2N2;
N4 = N1 + N2 + N3.
```

Количество адресов в подсетях должно быть минимально возможным для рассчитанного числа хостов с учетом шлюза подсети. Используйте диапазон адресов 192.168.v.0 – 192.168.v.255 (при необходимости используйте следующую сеть класса C – 192.168.(v+1).0), где v – номер студента по списку в журнале группы. Количество адресов в пятой подсети выбирайте равным четырем: первый – адрес подсети, последний – широковещательный, оставшиеся два – для интерфейсов маршрутизаторов, соединенных связью «точка – точка». Адресное пространство

подсети между маршрутизаторами должно находиться за адресным пространством последней из пользовательских подсетей.

2. Приведите в отчет адресную информацию по всем подсетям, указав для каждой подсети адрес подсети, маску подсети, широковещательный адрес подсети, адрес шлюза, диапазон адресов хостов подсети, диапазон резервных адресов для хостов подсети, заполнив представленную ниже таблицу.

№ подсети	Кол-во хостов	IP-адрес подсети	Маска подсети	Broadcast адрес	Шлюз	Диапазон IP-адресов хостов	Диапазон IP-адресов резерва
1							
2							
3							
4							
5							

3. Выполните конфигурирование сетевых интерфейсов пользовательских хостов IP-подсетей в программе Packet Tracer в соответствии с разработанным планом адресов. Адрес шлюза подсети указывайте в строке *Gateway* (*Шлюз*) вкладки *Config* (*Конфигурирование*). Выполните проверку правильности конфигурирования хостов пересылкой пакетов утилиты `ping` между хостами подсети внутри каждой пользовательской подсети.

4. Выполните настройку интерфейсов маршрутизаторов. Выберите интерфейс, к которому подключена первая сеть и назначьте этому интерфейсу IP-адрес шлюза и маску первой подсети. После чего включите интерфейс. Обратите внимание на команды Cisco IOS, автоматически отображаемые в нижнем поле при конфигурировании. Приведите эти команды в отчет и поясните их назначение.

5. Повторите конфигурирование для остальных интерфейсов маршрутизатора, которые связаны со второй подсетью и вторым маршрутизатором. Приведите в отчет команды Cisco IOS, выполняющие конфигурацию интерфейсов.

6. Исследуйте проверку функционирования сети посылкой пакетов утилиты `ping`:

– от хоста первой подсети интерфейсу шлюза этой подсети;

– от хоста первой подсети интерфейсу шлюза второй подсети;

– от хоста первой подсети хосту второй подсети.

7. Аналогичным образом выполните конфигурирование интерфейсов второго маршрутизатора – шлюзов третьей, четвертой подсети и интерфейса связи с первым маршрутизатором. Исследуйте их функционирование с помощью утилиты `ping`.

8. На маршрутизаторах задайте правила маршрутизации для возможности передачи данных между всеми пятью подсетями.

9. Исследуйте работоспособность всей составной сети посылкой пакетов утилиты `ping` от хоста первой подсети хостам остальных подсетей.

10. Приведите в отчет листинги команд `sh ip int brief` (выводит адресную информацию интерфейсов) и `sh ip route` для обоих маршрутизаторов.

5 Методика настройка статической маршрутизации

Для настройки на оборудовании Cisco интерфейсов маршрутизаторов в меню глобальной конфигурации маршрутизатора следует выбрать тот интерфейс, к которому подключена необходимая подсеть и назначить этому интерфейсу IP-адрес шлюза и маску данной подсети. После чего «поднять» (включить) интерфейс командой *no shutdown*.

Выполнив конфигурирование интерфейсов двух маршрутизаторов, проверив наличие связи между всеми четырьмя подсетями с помощью утилиты *ping* окажется, что связь между первой и второй подсетями, а также между третьей и четвертой подсетями организуется без всяких дополнительных настроек, только заданием IP-адресов и включением интерфейсов. Это происходит потому, что маршрутизатор фактически участвует в соседних сетях своими интерфейсами и «знает» об их существовании. В то же время первый маршрутизатор ничего «не знает» о существовании удаленных от него третьей и четвертой подсетях. Адреса этих сетей необходимо сообщить ему путем ввода двух правил статической маршрутизации, задающих маршруты к этим сетям. В этих правилах указывается:

– IP-адрес удаленной подсети назначения (он будет фигурировать в первом столбце таблицы маршрутизации);

– маска этой удаленной подсети (она появится во втором столбце);

– IP-адрес следующего по пути в эту удаленную подсеть маршрутизатора (он будет указан в третьем столбце таблицы маршрутизации).

Для задания правил маршрутизации необходимо открыть вкладку *Config (Конфигурирование)* маршрутизатора и выбрать из меню *Routing (Маршрутизация)* команду *Static (Статическая)*. В полях *Network (Сеть)*, *Mask (Маска)* и *Next Hop (Следующий маршрутизатор)* необходимо указать, соответственно, IP-адрес подсети назначения, ее маску и адрес следующего по пути к ней маршрутизатора и нажать на кнопку *Add (Добавить)*. Маршрут будет добавлен в список маршрутов (см. рисунок 11).

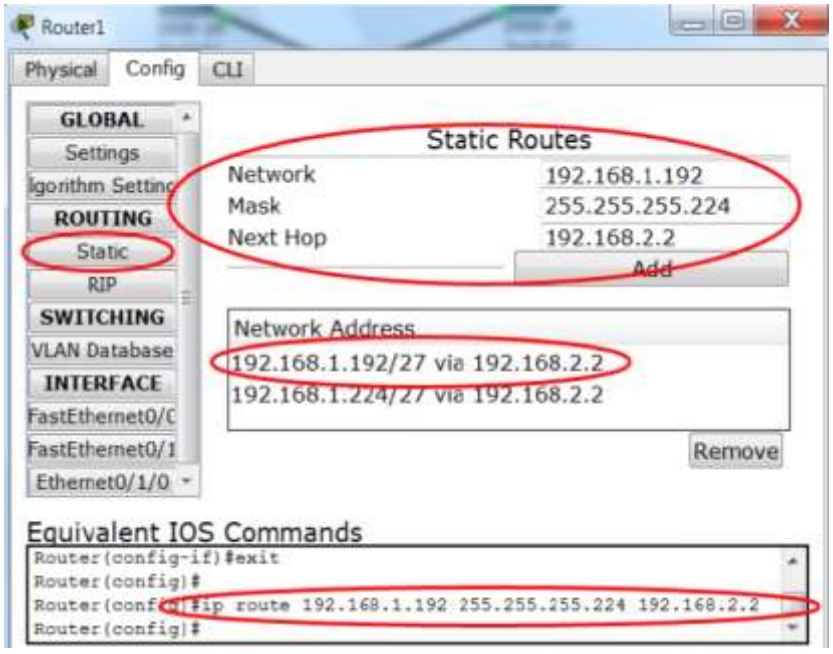

Рисунок 11 – Задание правил маршрутизации

Для просмотра конфигурации маршрутизаторов используйте инструмент *Inspect (Инспектировать)*, выполнив щелчок по маршрутизатору, необходимо

выбрать команду *Routing Table (Таблица маршрутизации)* (см. рисунок 12). Эту информацию также можно просмотреть командой Cisco IOS *show ip route*.

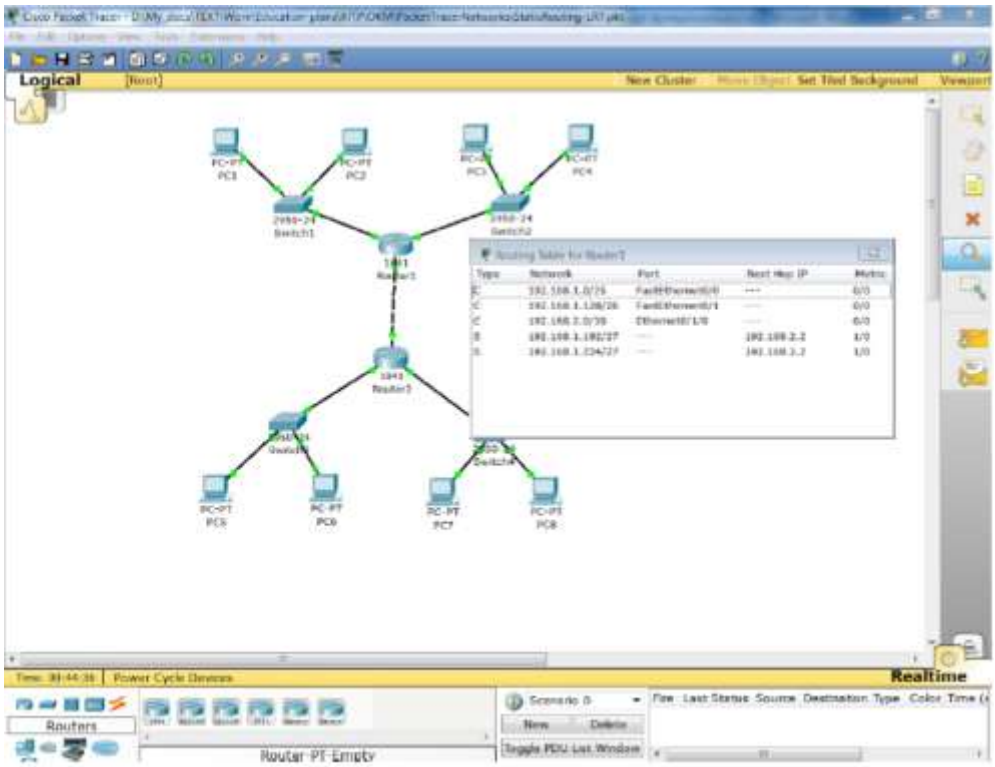

Рисунок 14 – Просмотр таблицы маршрутизации маршрутизатора

6 Содержание отчета

1. Титульный лист.
2. Исходные данные в соответствии с индивидуальным вариантом.
3. Описание всех использованных команд.
4. Скриншоты топологии, реализованных настроек строек и результатов исследования функционирования сети.
5. Выводы.

7 Контрольные вопросы

1. Опишите основное назначение протокола IP. Сравните пределы передачи IP-дейтаграмм и Ethernet-кадров.
2. Опишите формат IP-адреса протокола IPv4, назовите его принципиальное отличие от MAC-адреса.
3. Дайте определение технологии маршрутизации.
4. Что называют шлюзом сети/подсети. В каком случае пакеты проходят через шлюз?
5. Что представляет собой фрагментация/дефрагментация дейтаграмм? В каком случае она выполняется? Что такое MTU?
6. Оцените объем пространства адресов IP v4 и опишите, как организовано их выделение конечным пользователям.
7. Назовите классы IP адресов и их характеристики. Каким образом маршрутизаторы определяют принадлежность IP-адреса получателя к тому или иному классу?
8. Опишите особые (выделенные под специальные нужды) IP-адреса и их назначение.

9. Что представляют собой локальные IP-адреса, назовите диапазоны сетей таких адресов. Для чего служит технология сетевой трансляции адресов?

10. Опишите формат и использование маски подсети. Как по значению маски определить количество адресов, которое она выделяет? Перечислите известные Вам маски и их характеристики для сети класса C.

11. Определите, входят ли два IP-адреса (например, `192.168.1.67` и `192.168.117`) в одну и ту же подсеть с маской `255.255.255.192`.

12. Что представляет собой технология бесклассовой междоменной маршрутизации? Запишите адрес и маску суперсети для 2000 хостов.

13. Опишите структуру таблицы маршрутизации и способ нахождения маршрута маршрутизатором по IP-адресу получателя.

14. Что представляет собой маршрут по умолчанию, для чего он используется? Каким образом маршрут по умолчанию указывается в таблице маршрутизации?

15. Что такое метрика маршрута, какие параметры могут служить метрикой?

16. Чем отличается статическая маршрутизация от динамической? Приведите названия популярных протоколов динамической маршрутизации.

17. Опишите алгоритм нахождения маршрутизаторами следующего от них шага маршрута. Каким образом адресуется интерфейс, на который необходимо переслать пакет, на следующем шаге маршрута?

18. Выведите на экран Вашего компьютера таблицу маршрутизации для его интерфейсов.

19. Опишите формат заголовка IP и назначение его полей. Какова минимальная и максимальная длина IP пакета?

20. Опишите, каким образом выполняется фрагментация и дефрагментация пакетов при пересечении ними сетей с различным значением MTU.

21. Что такое время жизни пакета и для чего служит этот параметр?

22. Укажите идентификаторы наиболее популярных протоколов, пакеты которых переносятся в поле данных IP.