ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

федеральное государственное бюджетное образовательное учреждение высшегопрофессионального образования

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙСООБЩЕНИЯ»

СОГЛАСОВАНО:
:
Выпускающей кафедрой «Железнодорожная автоматика,
телемеханика и связь»
Зав. кафедрой
_____А.В. Горелик
(подпись, Ф.И.О.)

« ___ » _____ 20 ____ г.

Кафедра: «Железнодорожная автоматика, телемеханика и связь»

(название кафедры)

Авторы: Ермакова О.П., к.т.н, доц.

(ф.и.о., ученая степень, ученое звание)

ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ ПО ДИСЦИПЛИНЕ
«Нано технологии в телекоммуникациях»

(название дисциплины)

Направление/специальность: **23.05.05. Системы обеспечения движения поездов**

(код, наименование специальности /направления)

Профиль/специализация: **«Телекоммуникационные системы и сети железнодорожного транспорта (СТ)»,**

Квалификация (степень) выпускника: **специалист**

Форма обучения: **заочная**

Москва 2016г.

ОБЩИЕ УКАЗАНИЯ

Контрольная работа состоит из трех задач. Ее цель - закрепить знания, полученные студентами, при изучении дисциплины.

Прежде чем приступать к выполнению контрольной работы студент должен тщательно проработать материал соответствующих разделов курса.

Контрольная работа выполняется на листах формата А4. На титульном листе должны быть указаны наименование дисциплины, данные студента и его учебный шифр.В контрольной работе должны быть приведены исходные данные, схемы и формулы, поясняющие ход решения, а также сделаны выводы по решениям задач.

Проверенная и допущенная к защите контрольная работа предъявляется преподавателю на защите. Без защиты контрольной работы студент не допускается к сдаче экзамена.

ЗАДАЧА 1

В контрольной работе по заданному IP адресу и маске подсети необходимо определить: адрес сети; адрес широковещательной рассылки; первый и последний доступные IP адреса для этой сети. Вариант исходных данных задачи определяется по последней цифре шифра студента в соответствии с табл. 1.

Таблица 1

Последняя цифра шифра	Вариант	IP адрес	Маска подсети
1	2	3	4
0	1	80.207.148.126	255.255.255.240
	2	114.72.126.117	255.240.0.0
	3	105.13.52.47	255.248.0.0
	4	4.56.169.76	255.224.0.0
1	1	107.154.150.74	255.255.224.0
	2	77.16.148.215	255.252.0.0
	3	63.130.131.104	255.255.0.0
	4	32.26.40.6	255.255.224.0
2	1	104.77.24.152	255.224.0.0
	2	115.38.132.245	255.255.224.0
	3	38.4.60.21	255.255.252.0
	4	61.12.74.12	255.252.0.0
3	1	153.41.246.188	255.255.255.252
	2	130.95.102.138	255.255.254.0
	3	113.83.34.54	255.254.0.0
	4	50.41.211.6	255.252.0.0
4	1	15.22.220.104	255.240.0.0
	2	65.43.28.58	255.255.240.0
	3	170.37.142.72	255.255.252.0
	4	19.116.75.228	255.192.0.0

Продолжение табл.1

1	2	3	4
5	1	78.62.54.131	255.224.0.0
	2	29.196.70.9	255.224.0.0
	3	12.99.44.87	255.192.0.0
	4	104.53.78.172	255.224.0.0
6	1	14.92.177.54	255.255.255.252
	2	67.27.4.236	255.255.252.0
	3	148.95.99.156	255.255.224.0
	4	37.34.106.93	255.240.0.0
7	1	187.172.44.10	255.255.255.240
	2	82.22.224.20	255.248.0.0
	3	79.90.17.195	255.252.0.0
	4	47.93.175.209	255.240.0.0
8	1	117.243.81.226	255.192.0.0
	2	51.30.64.132	255.255.255.224
	3	38.222.151.248	255.252.0.0
	4	53.6.199.60	255.255.252.0
9	1	88.4.233.130	255.252.0.0
	2	15.4.143.163	255.255.224.0
	3	180.81.42.129	255.255.192.0
	4	64.241.23.209	255.255.255.128

Примечание. Приведенные в табл. 1 IP адреса могут совпадать с адресом сети или широковещательным адресом.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

1. Классы и структура IP-адресов

В сетях TCP/IP любое сетевое устройство должно иметь уникальный *IP- адрес*, который представляет собой 32-х разрядное двоичное число (четыре байта). Обычно он представляется в виде четырех десятичных чисел, лежащих в диапазоне от 0 до 255, разделенных точками, например, 198.87.118.17. IP- адрес состоит из двух частей: адреса сети и адреса хоста в этой сети. Соотношения между адресом сети и хоста зависит от класса IP-адреса.

Существует пять классов IP- адресов: A, B, C, D и E. Адреса класса D, для которых отведен диапазон адресов с 224 по 239, используются для обращения к группам компьютеров, а E – зарезервированы. Классы отличаются друг от друга количеством битов, отведенных на адрес сети и адрес хоста. В табл. 2 приведены структуры адресов для этих классов в виде четырех десятичных чисел w. x. y. z.

Таблица 2. Структура IP- адресов

Класс	W	Адрес сети	Адрес узла	Максимальное число сетей	Максимальное число узлов в сети
A	1…126	w	x.y.z	126	16 777 214
B	128…191	w.x	y.z	16 382	65 534
C	192…223	w.x.y	z	2 097 151	254

В двоичной нотации первый октет (байт) всегда начинается с 0 для адресов класса A, с 10 – для класса B и с 110 – для адресов класса C.

Адреса класса A используются в очень больших сетях общего пользования, класса B – в сетях среднего размера, а большинство сетей Internet попадают в категорию C, количество узлов в которых не превышает 254 хоста. Количество хостов в сети рассчитывается по формуле:

$$N_{хостов} = 2^n - 2,$$

где n – число разрядов “хостовой” части IP-адреса. Уменьшение максимального числа узлов в сети на 2 обусловлено тем, что адрес, в котором все разряды “хостовой” части равны 0, является адресом сети, а адрес, у которого эти же разряды равны 1 является**широковещательным** и предназначен для широковещательной рассылки уровня 3 всем хостам, входящим в эту сеть.

Сетевой адрес 127.0.0.0 является выделенным и предназначен для тестирования программ и взаимодействия процессов, функционирующих на данном компьютере. Для локальных целей зарезервированными являются адреса: для класса A – это сеть 10.0.0.0, в классе B – это диапазон из 16 номеров сетей 172.16.0.0…172.31.0.0, в классе C – это диапазон из 255 сетей – 192.168.0.0…192.168.255.0. Адреса 0.0.0.0, а также диапазон 224.0.0.0...255.0.0.0 зарезервированы для специальных целей.

2. Маски подсетей

Для установления связи по протоколу IP кроме IP-адреса необходимо еще два компонента: маска подсети и адрес шлюза, используемого по умолчанию. Маска подсети определяет, какая часть адреса относится к хосту, а какая часть – к сети. Маска подсети представляет собой 32-битовое число, представленное, как и IP- адрес, в виде четырех десятичных чисел. В табл.3 приведены стандартные маски подсетей для IP- адресов классов A, B, C как в десятичной нотации, так и в виде двоичных чисел.

Таблица 3. Стандартные маски подсетей

Класс	Маска подсети	
	Десятичное значение	Двоичное значение
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Для определения адреса сети необходимо выполнить логическое умножение IP-адреса и маски подсети, т.е. выполнить логическую операцию “И” (AND) над всеми двоичными разрядами. На рис. 1 показан процесс

определения адреса сети для хоста, имеющего IP-адрес 172.16.6.27 и маской подсети 255.255.0.0. Вначале адрес и маска переводятся в двоичную форму. Затем выполняется поразрядная операция логического “И”. После чего полученное двоичное число переводится в десятичную форму.

172.16.6.27 - IP-адрес
255.255.0.0 - маска подсети

10101100.00010000.00000110.00011011 - IP-адрес
× 11111111.11111111.00000000.00000000 - маска подсети
10101100.00010000.00000000.00000000 - адрес сети
(результат операции И)

172.16.0.0 - адрес сети

Рисунок 1 - Определение адреса сети с помощью операции “И”

Кроме разбиения IP- адреса на сетевую и узловую части, маски подсети используются для сегментации сети на несколько локальных подсетей. Предположим, что большой компании присвоен IP-адрес класса B, например, 191.100.0.0. Сеть компании представляет собой 10 различных локальных сетей, каждая из которых состоит из 200 узлов. Использование маски 255.255.255.0 позволит разбить сеть на 254 отдельных подсетей с адресами от 191.100.1.0 до 191.100.254.0. В каждой из 254 подсетей может быть до 254 хостов.

Маска подсети не обязательно должна состоять из целых октетов. Узловая часть маски может быть как больше, так и меньше 8 бит. Проиллюстрируем сказанное еще одним примером. Пусть компания располагается в 6 зданиях, в каждом из которых расположено не более 30 хостов. Для их адресации используется блок адресов класса C - 200.10.1.0. При использовании стандартной маски подсети, младшие восемь разрядов определяют адрес хоста, а старших три байта – адрес сети (рис. 2, а).

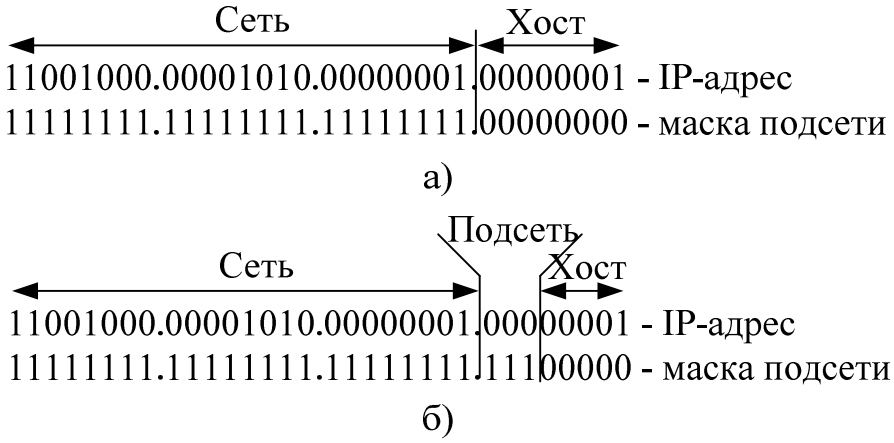

Рисунок 2 - Разбиение сети на подсети с помощью маски

Так как в каждой подсети будет использоваться не более 30 хостов, то для задания их адресов достаточно всего 5 двоичных разрядов ($2^5 - 2 = 30$). Тогда оставшихся старших три разряда можно использовать для маски

подсети (рис.2, б), которая в десятичной форме будет равна 255.255.255.224. В некоторых случаях, маска подсети может записываться через косую черту (/). Этот стиль записи намного компактнее и предусматривает указание после IP-адреса количество подряд идущих единиц в маске вместо записи маски в точечном десятичном формате. Например, чтобы представить сеть 172.16.1.0 с маской 255.255.224.0, ее можно записать в виде 172.16.1.0/19.

ЗАДАЧА 2

В сети действуют три маршрутизатора: RouterA, RouterB,RouterC, каждый из которых содержит один порт Ethernet и два последовательных порта. Маршрутизаторы, связаны последовательной линией со скоростью передачи 256 Кбит (рисунок 3).

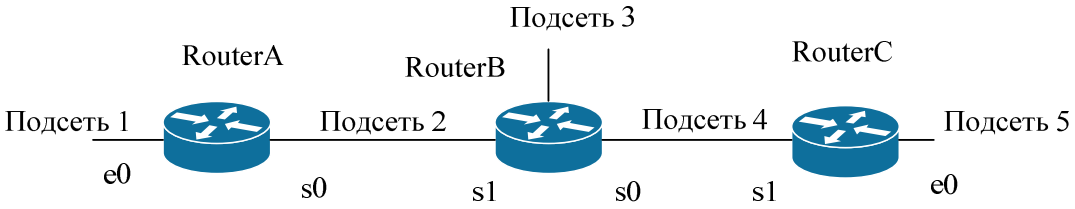

Рисунок 3 – Схема конфигурируемой сети

Все хосты имеют одинаковую маску 255.255.0.0. По данным приведенным в таблице 4 назначить действующие адреса интерфейсам маршрутизаторов и хостам сети, а также составить таблицы статической маршрутизации.

Таблица 4

Вариант	Сетевой адрес
0	72.0.0.0
1	182.17.0.0
2	105.0.0.0
3	14.0.0.0
4	227.14.22.0
5	172.23.0.0
6	176.24.0.0
7	240.25.18.0
8	172.30.0.0
9	172.27.0.0

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

Основной функцией маршрутизаторов является передача пользовательских пакетов из сети отправителя в сеть получателя в соответствии с адресами, содержащимися в заголовке IP пакета. Для этого используются таблицы маршрутизации, которые формируются с помощью следующих двух основных способов:

1. Статическая маршрутизация.
2. Маршрутизация по умолчанию.
3. Динамическая маршрутизация.

При статической маршрутизации администратор сети вручную вводит пути передачи пакетов в таблицы маршрутизации всех маршрутизаторов. Статическая маршрутизация, как правило, используется в сетях небольшого размера, а также в пограничных маршрутизаторах (маршрутизатор, непосредственно соединенный с сетью провайдера).

Статическая маршрутизация обладает следующими достоинствами:

1. В линиях связи между маршрутизаторами отсутствует служебный трафик, а, следовательно, эффективность линий связи повышается;
2. Поскольку только администратор устанавливает маршруты передачи данных к определенным сетям, то обеспечивается хорошая защита информации.

Однако статическая маршрутизация не лишена недостатков, основными из которых являются:

1. Администратор должен хорошо понимать особенности объединенной сети и правильно настроить каждый маршрутизатор;
2. Если в объединенную сеть добавляется новая сеть, то администратору придется добавить новые пути во все маршрутизаторы;
3. Статическая маршрутизация неприменима в крупных сетях, поскольку требует большого объема работы.

Маршрутизация по умолчанию используется для пересылки пакетов в удаленную сеть назначения, которая не отмечена в таблице маршрутизации через маршрутизатор следующего участка. Можно использовать маршрутизацию по умолчанию в тупиковых сетях (stubnetwork), т.е. сетях, имеющих только один выходной порт.

При динамической маршрутизации таблицы маршрутизации формируются с помощью протоколов маршрутизации (routingprotocols). Для формирования и обновления таблиц маршрутизации эти протоколы обмениваются служебной информацией, объем которой существенно зависит от количества маршрутизаторов в сети. При существенном росте объединенной сети (прежде всего Internet) в ней возникают следующие проблемы:

1. Производительность протоколов маршрутизации значительно снижается;
2. Объем служебного трафика, которым обмениваются маршрутизаторы для поддержания своих таблиц маршрутизации, растет, что требует все больших ресурсов маршрутизатора и все большей пропускной способности сети;
3. Большое число маршрутизаторов, работающих с протоколами маршрутизации, делают поддержку механизмов обнаружения и изоляции сбоев в сети практически невозможной.

Для того чтобы в какой-то степени снизить влияние этих факторов сеть Internet разделили на отдельные автономные системы (AutonomousSystem – AS). Автономная система представляет собой группу сетей и маршрутизаторов, находящихся под единым административным управлением.

В качестве примера настройки статической маршрутизации рассмотрим сеть с адресом 172.16.0.0 и маской 255.255.255.0, фрагмент которой показан на рисунке 4.

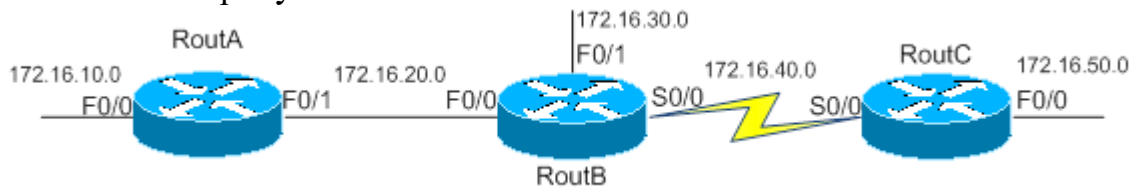

Рисунок 4 – Схема сети

Как видно из рисунка необходимо сконфигурировать пять сетей, как различные подсети.

Схема выбранных адресов и таблицы маршрутизации показаны на рисунке 5.

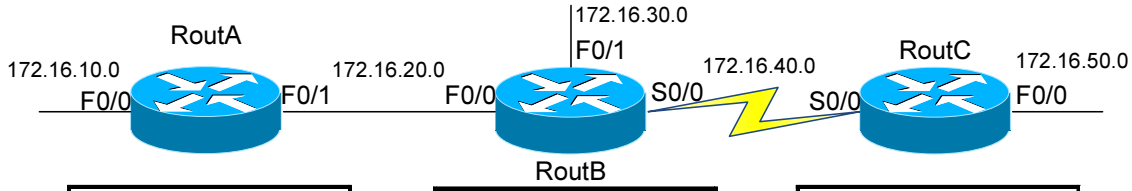

Таблица маршрутизации		
172.16.10.0	F0/0	0
172.16.20.0	F0/1	0
172.16.30.0	F0/1	1
172.16.40.0	F0/1	1
172.16.50.0	F0/1	2

Таблица маршрутизации		
172.16.20.0	F0/0	0
172.16.30.0	F0/1	0
172.16.40.0	S0/0	0
172.16.10.0	F0/0	1
172.16.50.0	S0/0	1

Таблица маршрутизации		
172.16.40.0	S0/0	0
172.16.50.0	F0/0	0
172.16.30.0	S0/0	1
172.16.20.0	S0/0	1
172.16.10.0	S0/0	2

Рисунок 5- Схема выбранных адресов и таблицы маршрутизации

ЗАДАЧА 3

1. Рассчитать коэффициент использования канала связи для двух скоростей передачи данных, если для установления соединения используется протокол ARQ, который работает в режиме останова и ожидания и с избирательным повторением. Исходные данные для расчета приведены в таблицах 5, 6

Таблица 5

Параметр	Последняя цифра шифра									
	0	1	2	3	4	5	6	7	8	9
Длина информационного поля, байт	100	150	200	250	300	350	400	450	500	550
Длина подтверждения, байт	10	9	8	11	12	16	15	14	13	17
Задержка распространения сигналов в канале связи, мс	100	90	80	70	60	50	55	65	75	85
Скорость передачи данных, кбит/с	19,2	9,6	4,8	12	16	20	22	24	33,6	28,8
Вероятность потери кадра, 10^{-3}	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5

Таблица 6

Параметр	Предпоследняя цифра шифра									
	0	1	2	3	4	5	6	7	8	9
Длина заголовка, байт	25	24	23	22	21	20	19	18	17	16
Тайм-аут подтверждения, мс	50	60	70	80	90	100	110	120	130	140
Скорость передачи данных, кбит/с	700	750	800	850	900	950	650	600	550	500
Вероятность потери подтверждения, 10^{-4}	5,5	5	4,5	4	3,5	3	2,5	2	1,5	1

Примечание. При максимальной скорости передачи данных время тайм-аута уменьшить на порядок.

2. Построить график зависимости коэффициента использования канала связи, если длина информационного поля пакета данных изменяется от 1 до 100000 бит. Вероятность потери кадра описывается экспоненциальным законом $p_F = 1 - \exp(-\lambda \cdot m)$. Значения коэффициента λ определяется по таблице 7.

Таблица 7

Коэффициент $\lambda \cdot 10^{-5}$	Последняя цифра шифра									
	0	1	2	3	4	5	6	7	8	9
	9	8	7	6	5	4	3	2	1	1,5

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

В каналах связи с установлением соединения для защиты от ошибок передачи данных широко используется протокол автоматического запроса повторной передачи ARQ (AutomaticRepeatrequest). Вариант с остановом и ожиданием является самым простым, который состоит из следующих шагов (рисунок 6):

1. Отправитель (передатчик) посылает данные и заголовок получателю (приемнику) информации, одновременно запуская таймер тайм-аута, и переходит в состояние ожидания до тех пор пока не получит подтверждения от приемника или до истечения времени тайм-аута.

2. Приемник, получив данные и заголовок, посылает передатчику подтверждение (ACK – acknowledgement) приема информации.

3. Передатчик, получив подтверждение ACK, посылает приемнику следующую порцию информации. Если же по каким-либо причинам передатчик не получает подтверждение, то после обнуления таймера тайм-аута, он осуществляет повторную передачу ранее переданных данных.

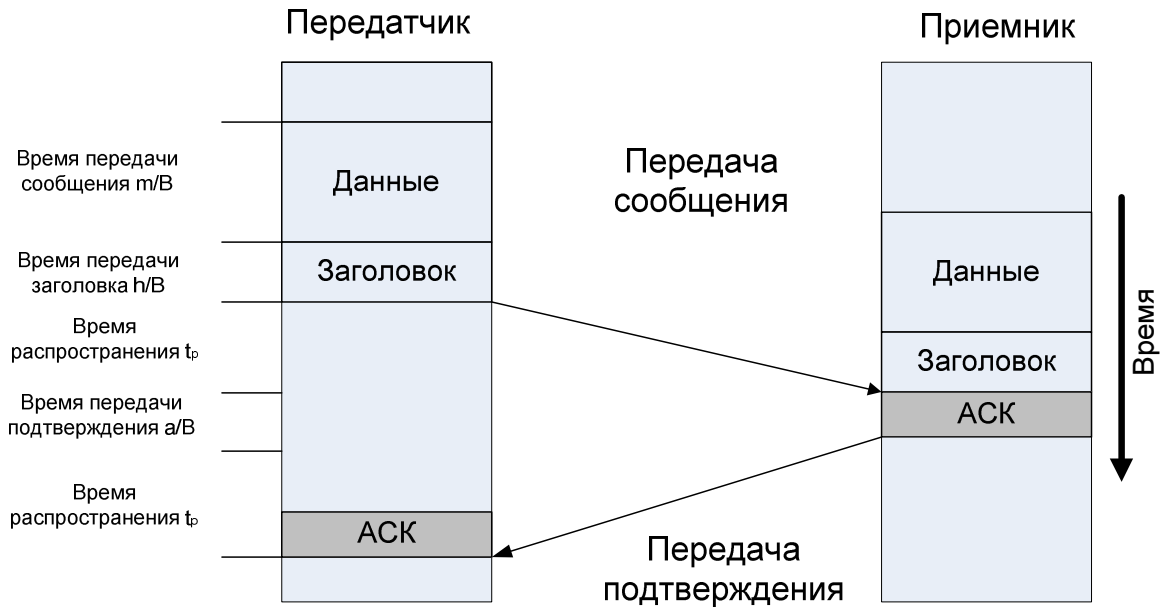

Рисунок 6 - Передача данных в протоколе ARQ с остановом и ожиданием

Для передачи кадра, содержащего *m*битов сообщения и*h*битов заголовка, по идеальному каналу связи, в котором отсутствуют ошибки и скорость передачи данных равна *B*бит/с, а задержка распространения сигнала равна t_P, потребуется время равное

$$(m+h)/B + t_P .$$

Аналогично, время, необходимое для передачи подтверждения длиной *a*бит от приемника к передатчику, будет равно

$$a/B + t_P .$$

Тогда полное время, требуемое для передачи одного кадра, будет равно

$$t_K = \frac{h+m+a}{B} + 2t_P .$$

В течение этого периода времени передается *m*бит полезной информации. Тогда, коэффициент использования канала связи K_C, равный отношению полезного времени, т.е. времени, необходимого для передачи *m*битов информации, к общему времени, затрачиваемому на передачу всего кадра, можно определить по формуле (1)

$$K_C = \frac{m}{m+h+a+2\cdot B\cdot t_P}. \qquad (1)$$

Практически во всех реальных каналах связи действуют помехи, которые приводят к возникновению ошибок при передаче данных. Если предположить, что вероятность потери кадра равна p_F, а вероятность потери подтверждения – p_A, то вероятность правильного приема кадра будет равна

$$p_s = (1-p_F)(1-p_A) .$$

Причем, чем больше длина информационного поля кадра, тем выше вероятность его потери в процесс передачи по каналу связи. Чаще всего вероятность потери кадра описывается экспоненциальным законом вида

$p_F = 1 - \exp(-\lambda \cdot m)$. При этом полезная пропускная способность (в кадрах) реального канала связи будет определяться как $m \times p_S$, а коэффициент K_C – согласно выражению (2)

$$K_C = \frac{m \cdot p_S}{m + h + a + 2 \cdot B \cdot t_P}. \quad (2)$$

Приведенные выше рассуждения справедливы для протокола ARQ с остановом и ожиданием, в котором время тайм-аута равно $2t_P + a/B$ (время, которое обычно требуется для возврата подтверждения). В этом случае кадры будут передаваться с одним и тем же интервалом, независимо от того возникает ошибка или нет.

Для повышения коэффициента использования канала связи, в случае использования протокола ARQ с остановом и ожиданием, необходимо, чтобы заголовок и подтверждение были короткими, а время распространения сигнала– небольшим.

Для преодоления неэффективности ARQ с остановом и ожиданием можно продолжать передавать новые кадры, не ожидая получения никаких подтверждений. Для числа[1] кадров, ожидающих получения подтверждения, устанавливается некоторый максимум, а соответствующий протокол называют *ARQ-протоколом со скользящим окном.* Использование таких окон обеспечивает определенную степень управления потоком данных.

В случае потери подтверждений, можно для каждого кадра использовать тайм-аут (как в ARQ с остановом и ожиданием). Если подтверждение не было своевременно получено, то интервал тайм-аута завершается по таймеру, а передатчик предполагает, что кадр потерян, и что нужно повторно передать только что переданный кадр. В качестве альтернативного способа обнаружения потерянных кадров можно отслеживать на принимающем конце канала связи перерывы в их последовательности.

Существуют два режима повторной передачи: или передатчик передает только тот кадр, в котором была ошибка (избирательная повторная передача), или он также повторно передает все кадры, которые были переданы после потери кадра (повторная передача с возвратом *N* кадров).

В *избирательной схеме* передатчик повторно посылает только тот кадр, который был ошибочным. Преимущество этой схемы заключается в том, что она менее расточительна с точки зрения пропускной способности канала связи, но зависит от способности приемника гарантировать, что кадры поставляются сетевому уровню в правильном порядке. Это означает, что сетевой уровеньдолжен правильно буферизовать полученные кадры во время ожидания повторно передаваемых кадров.

Всхеме с *возвратом N кадров,* передатчик “возвращается назад” к потерянному кадру и от этой точки снова посылает *все* кадры. Преимущество этого подхода состоит в том, что в приемнике не

[1]Это число называют *окном* (window)

требуется буферизации или повторного построения последовательности кадров. Но вследствие того, что этасхема ARQ требует повторной передачи даже тех кадров, которые, возможно,былиприняты правильно, она не столь эффективна в случае ошибок, каксхема с избирательной повторной передачей.

Всистеме с возвратом N кадров для определения того момента, когда произошла ошибка или когда были приняты дубликаты кадра, приемник проверяет порядковые номера кадров. Если был получен правильный кадр с порядковым номером N, то следующий полученный кадр должен иметь номер N+1. Если номер следующего принятого кадра равен N+2, то кадр с номером N+ 1 считается потерянным.

В протоколах со скользящим окном роль порядковых номеров является решающей. Когда передается кадр, ему приписывается номер, который определяет порядок его вывода по отношению к другим кадрам. Эти номера используются приемником для того, чтобы гарантировать, что кадры, передаваемые на сетевой уровень, расположены в правильном порядке.Диапазон допустимых порядковых номеров является функцией размера окна и метода повторной передачи. В случае протокола со скользящим окном размера 1 требуется одноразрядный порядковый номер. В общем случае для окнаразмером Wкадров, диапазон требуемых порядковых номеров простирается от 0 до $2W$+1 для системы, использующей избирательную повторнуюпередачу, а для систем с возвратом N кадров – от0 до W+1. Для указанияномера в каждом кадре обычно задается специальное полеразмером в 3 или 8 разрядов.

Вычисление коэффициента использования канала связи для протоколов со скользящимокном несколько сложнее. Здесь различают два случая. При большом окне его размер оказывается достаточным для непрерывной передачи в условияхотсутствия ошибок. В случае маленького окна его размер не достаточен для непрерывной передачи, но можно использовать эффективную схему ARQ с остановом и ожиданием, позволяющую одновременно передавать несколько кадров.Пусть на передачу кадра затрачивается $\frac{h+m}{B}$ секунд, а на прием подтверждения- $2t_P + \frac{a}{B}$ секунд. Это означает, что при ожидании подтверждения можно передавать $\frac{(2t_P + a/B)}{(h+m)/B} = \frac{2Bt_P + a}{h+m}$ кадров. Если размер окна на 1 (или на еще большую величину) больше, чем это значение, то возможна непрерывная передача. В случае небольшого окна его размер Wдолжен удовлетворять следующему условию:

$$W < (2Bt_P + a)/(h+m).$$

Тогда за каждый временной интервал, равный $\frac{h+m+a}{B} + 2t_P$, можно передать Wкадров. При этом эффективность свободной от ошибок передачи возрастает и ее можно вычислять по формуле

$$K_{CW} = \frac{m}{h+m} \times \frac{W(h+m)}{(h+m+a+2Bt_P)} = \frac{m \cdot W}{h+m+a+2Bt_P}.$$

В случае реального канала связи, для ARQсо скользящим окном можно использовать подход, который был использован для ARQ с остановом и ожиданием. В условиях низкой интенсивности ошибок для ARQ с избирательным повторением передачи можно сделать некоторое упрощение, состоящее в том, что повторные передачи потерянных пакетов – это еще не сами потери, и что система должна уменьшить число пакетов, которые она посылает вследствие переполнения буферов. В этом случае, коэффициент использования канала связи для случая большого окна будет равен $mp_S/(h+m)$,а для случая малого окна – равным $mWp_S/(h+m+a+2Bt_P)$.

Для ARQ с возвратом *N* кадров рассмотренный подход использовать нельзя, потому что в дополнение к тому, что нужно снова посылать более одного кадра *(N*кадров в случае большого окна и *W*кадров – вслучае малого окна), ошибка в повторной передаче сбойного кадра заставит протокол остановиться. Однако если допустить упрощение, состоящее в том, что этого не случится, то каждый потерянный кадр вызоветповторную передачу*N* или *W*кадров. Среднее число передач, требуемых для того, чтобы получить успешно переданный кадр, равно $1/p_S$. Средне число повторных передач на 1 меньше, чем эта величина, т. е. $1/p_S - 1$, так что общее количество переданных кадров будет равно $(1/p_S - 1)N + 1$для большого окна или $(1/p_S - 1)W + 1$ – для малого. Из-за этого множителя коэффициент использования канала связи уменьшается и становится равным

$$K_C = \frac{m}{h+m}\left((1/p_S - 1)N + 1\right) - \text{для большого окна;}$$

$$\frac{mWp_S}{h+m+a+2Bt_p}((1/p_S - 1)W + 1) - \text{длямалого окна.}$$

На рисунке 7 показаны графики зависимости коэффициента использования канала связи от размера данных протоколаARQ с остановом и ожиданием (1) и с избирательным повторением (2) для системы со следующими характеристиками:

- скоростью передачи 1 Мбит/с;
- 40-разрядным заголовком;
- 40-разрядным пакетом подтверждения;
- задержкой распространения 10 мс;
- вероятность потери подтверждения равна 10^{-4}.

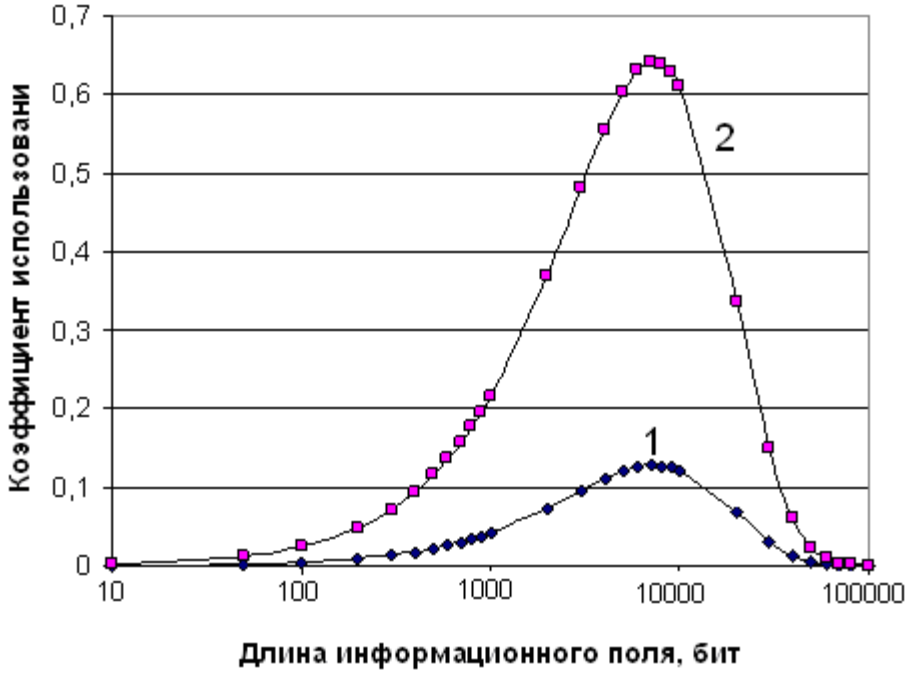

Рисунок - 7Графики зависимости коэффициента использования канала