

31/40/1

Одобрено кафедрой
«Транспортная связь»

Утверждено деканом факультета
«Управление процессами
перевозок»

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ДАнных

Рабочая программа и задание
на контрольную работу

для студентов V курса

специальности

**190402 АВТОМАТИКА, ТЕЛЕМЕХАНИКА И СВЯЗЬ
НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ (АТС)**



Москва – 2007

Программа составлена в соответствии с Государственным образовательным стандартом высшего профессионального образования в соответствии с государственными требованиями к минимуму содержания и уровня подготовки инженера по специальности 190402 Автоматика, телемеханика и связь на железнодорожном транспорте.

С о с т а в и т е л и : кандидаты техн.наук, доценты Губенко М.Л. и
Филенков В.В.

Р е ц е н з е н т — д-р техн. наук, проф. Алексеев В.М.

РАБОЧАЯ ПРОГРАММА

1. ЦЕЛЬ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цель – изучение принципов построения, функционирования и эксплуатации локальных и глобальных сетей, основанных на современных технических и программных средствах.

Задача – изучение теоретических основ построения сетей, глубокое понимание протоколов, функционирующих на конкретных уровнях сети, изучение современных технологий, аппаратной и программной базы, а также приобретение практических навыков в конфигурировании систем, расчет сетевых адресов, обеспечение программной и аппаратной защиты.

2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Изучив дисциплину «Системы и сети передачи данных» студент должен:

2.1. Знать и уметь использовать теорию построения и анализа современных систем и сетей, межсетевое взаимодействие и функционирование сетей, современную аппаратную и программную базу.

2.2. Владеть методами и практическими навыками конфигурирования реальных систем, поиском неисправностей в системах, методами декомпозиции и повышения качества функционирования систем. Иметь навыки модернизации существующих сетей и проектирования вновь создаваемых.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Всего часов – 75.

Аудиторные занятия – 12 ч.

Лекционные занятия – 4 ч.

Лабораторно-практические занятия – 8 ч.

Контрольные работы (количество) – 1.

Зачеты (количество) – 1.

Дифференцированный зачет – 1 (количество).

Самостоятельная работа – 48 ч.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Перечень тем лекционных занятий

Перечень тем лекционных занятий совпадает с содержанием курса. Продолжительность лекции 4 часа.

№ п/п	Тема	Кол-во часов
1	Введение в объединенные сети. Основы объединения сетей	0,5
2	Сегментирование локальных сетей	0,5
3	Семейство протоколов TCP/IP базовая модель DOD	0,5
4	IP-адресация	0,5
5	Основы маршрутизации	0,5
6	Динамическая маршрутизация	0,5
7	Управление трафиком с помощью списков доступа	0,5
8	Глобальные сети	0,5

4.2. Содержание разделов дисциплины

Программа по дисциплине «Системы и сети передачи данных» для удобства пользования представлена в виде перечня тем, каждая из которых объединяет логически заверченный материал.

Раздел 1

Введение в объединенные сети

Основы объединения сетей.

Устройство локальных сетей. Устройство глобальных сетей. Базовая модель OSI. Многоуровневый коммутационный подход. Уровни модели OSI. Инкапсуляция данных. Технология локальных сетей. Сеть Ethernet и стандарт IEEE 802.3.

Раздел 2

Сегментирование локальных сетей

Снижение перегрузки сети. Сегментирование сети с помощью мостов. Сегментирование сети с помощью маршрутизаторов. Сегментирование сети с помощью коммутаторов. Протокол покрывающего дерева. Виртуальные локальные сети. Идентификация кадров. Полнодуплексные сети Ethernet. Конструкция полудуплексной сети Ethernet. Конструкция полнодуплексной сети Ethernet. Сеть 100BaseT Fast Ethernet. Достоинства сетей Fast Ethernet. Спецификация 100BaseT.

Раздел 3

Семейство протоколов TCP/IP базовая модель DOD

Базовая модель DOD. Протоколы уровня процессов/приложений. Протоколы уровня взаимодействия хостов. Протоколы уровня Интернета. Протоколы уровня доступа к сети. Определение IP адресов. Локальное определение адресов. Определение IP адресов при удаленном доступе.

Раздел 4 IP-адресация

Иерархическая IP-адресация. Дополнительные классы сетей. Назначение адресов сетей. Подсети. Выделение подсетей. Маски подсетей.

Раздел 5 Основы маршрутизации

Процесс IP-маршрутизации. Статическая и динамическая маршрутизация, маршрутизация по умолчанию.

Раздел 6 Динамическая маршрутизация

Маршрутные протоколы и протоколы маршрутизации. Протоколы внутренней маршрутизации. Протоколы вектора расстояния. Протоколы маршрутизации по состоянию связи. Сравнение алгоритмов вектора расстояния и маршрутизации по состоянию связи. Протокол RIP. Протокол IGRP. Протокол OSPF. Протокол EIGRP. Протоколы внешней маршрутизации. Протокол EGP. Протокол BGP.

Раздел 7 Управление трафиком с помощью списков доступа

Списки доступа. Стандартные списки доступа. Расширенные списки доступа. Ограничение доступа к ресурсу и разграничение прав. Стратегии по обеспечению безопасности ресурсов. Идентификация и аутентификация. Схемы парольной защиты. Шифрование данных в информационно-вычислительных сетях. Шифрование данных (криптографическое преобразование). Классические методы шифрования. Дополнительные средства защиты информации.

Раздел 8 Глобальные сети

Использование телефонных сетей для удаленного доступа. Протокол SDLC. Протокол HDLC. Режимы передачи данных, поддерживаемые HDLC. Маршрутизация DDR. Протокол X.25. Сеансы X.25. Виртуальные соединения в сети X.25. Набор протоколов X.25. FRAME RELAY. Характеристики FRAME RELAY. Преобразование FRAME RELAY. Протокол “точка-точка” (PPP). Служба ISDN. Терминалы ISDN. Точки соединения ISDN. Протоколы ISDN. Служба BRI. Служба PRI.

4.3. Лабораторный практикум

№ п/п	Название и краткое содержание работы	Кол-во часов
1	Изучение маршрутизаторов и основных команд конфигурирования	2
2	Настройка интерфейсов маршрутизаторов, задание IP адресов на его интерфейсах	2
3	Динамическая маршрутизация. Настройка протоколов RIP. Поиск неисправностей в сетях с динамической маршрутизацией	2
4	Настройка протоколов межсетевого взаимодействия (на примере протокола FRAME-RELAY)	2

5. ПЕРЕЧЕНЬ ТЕМ ДЛЯ САМОСТОЯТЕЛЬНОЙ ПРОРАБОТКИ

Для самостоятельной проработки рекомендуется ряд тем, связанных с углубленным изучением протоколов маршрутизации, конфигурированием протоколов динамической маршрутизации (в частности, протоколов OSPF, EIGRP, BGP).

1. Протокол OSPF. Инициализация отношений соседства и смежности. Условия, при которых устанавливаются отношения смежности. Процедура выбора DR и BDR. Лавинные рассылки LSA. Вычисления дерева SPF. Метрика OSPF. Особенности сетей с NBMA. Широковещательная сеть. Не широковещательная сеть. Сеть с двухточечным соединением. Сеть с многоточечным соединением. Масштабируемость сетей OSPF. Взаимодействие между областями OSPF.

2. Протоколы IGRP и EIGRP. Маркировка маршрутов. Распространение маршрутов в сеанс IGRP. Настройка EIGRP. Тонкая настройка EIGRP. Распределение нагрузки. Распространение маршрутов.

3. Протокол BGP. Автономные системы. Тупиковые автономные системы. Транзитные автономные системы. Внутренний протокол BGP. Внешний протокол BGP. Фильтрация маршрутов. Поддержка масштабируемых сетей протоколом BGP. Фильтры. Организация политик BGP.

4. Списки рассылки. Префиксные списки. Карты маршрутов. Рефлекторы маршрутов. Конфедерации. Группы партнеров и сообщества. Многолинейные подключения к сервис-провайдерам. Оптимизация обновления маршрутов. Распространение маршрутов. Расширенные возможности метода распространения маршрутов. Настройка каналов по требованию. Настройка каналов E1 и ISDN.

6. КОНТРОЛЬНЫЕ РАБОТЫ

Студенты V курса выполняют контрольную работу на тему «Декомпозиция локальных сетей и определение масок и подмасок сетей».

В состав контрольной работы входят две задачи и пояснительная записка.

7. ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Обязательная литература

1. О д о м У. Компьютерные сети. – М.-СПб.-Киев: Cisco Press, 2006.

2. Лэммл Т., Портер Д., Челлис Д. CCNA: Учеб. руководство. – М.: Изд-во «Лори», 2002.

3. Джером Ф. Димарцио. Маршрутизаторы CISCO. – СПб.: Изд-во «Символ-Плюс», 2003.

4. Руководство по технологиям объединенных сетей. – 3-е изд. – М.: Издат. дом «Вильямс», 2002.

5. Хабаркен Д. Маршрутизаторы CISCO. Практическое применение: Пер. с англ. – М.: ДМК ПРЕСС, 2001.

6. Амато Вито. Основы организации сетей CISCO. Т. 1 и 2.: Пер. с англ. – М.: Издат. дом «Вильямс», 2002.

7.2. Дополнительная литература

7. Кэтрин Пакет, Дайана Тир. Создание масштабируемых сетей CISCO. – М.: Издат. дом «Вильямс», 2002.

7.3. Компьютерные программы

Программный эмулятор компьютерных сетей фирмы BOSON.

7.4. Аппаратное обеспечение

Комплект аппаратуры фирмы CISCO по программе CNA (сетевая академия CISCO CCNA/CCNP)

ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ

Задача 1

По исходным данным, приведенным в табл. 1, выполнить задание, определенное в каждом из вариантов. Обосновать причины и необходимость декомпозиции сети. Выполняемый вариант соответствует последней цифре учебного шифра.

Таблица 1

Выполняемый вариант	Задание
<i>1</i>	<i>2</i>
0	В сети с адресом 172.16.10.5 и маской подсети 255.255.255.128 определить подсеть, широковещательный адрес и диапазон допустимых хостов
1	В сети с адресом 10.10.10.5 и маской подсети 255.255.255.252 определить подсеть, широковещательный адрес и диапазон допустимых хостов
2	В сети с адресом 192.168.100.17 и маской подсети 255.255.255.248 определить подсеть, широковещательный адрес и диапазон допустимых хостов
3	В сети с адресом 192.168.100.17 и маской подсети 255.255.255.240 определить подсеть, широковещательный адрес и диапазон допустимых хостов
4	В сети с адресом 172.16.10.33 и маской подсети 255.255.255.224 определить подсеть, широковещательный адрес и диапазон допустимых хостов

Окончание табл. 1

1	2
5	В сети с адресом 172.16.10.65 и маской подсети 255.255.255.192 определить подсеть, широковещательный адрес и диапазон допустимых хостов
6	В сети с адресом 172.16.10.33 и маской подсети 255.255.255.240 определить подсеть, широковещательный адрес и диапазон допустимых хостов
7	В сети с адресом 192.168.100.25 и маской подсети 255.255.255.252 определить подсеть, широковещательный адрес и диапазон допустимых хостов
8	В сети с адресом 172.16.10.17 и маской подсети 255.255.255.240 определить подсеть, широковещательный адрес и диапазон допустимых хостов
9	В сети с адресом 172.16.10.33 и маской подсети 255.255.255.240 определить подсеть, широковещательный адрес и диапазон допустимых хостов

Задача 2

В сети класса В действуют 3 маршрутизатора: RouterA, RouterB, RouterC каждый из которых содержит один порт Ethernet и два последовательных порта. Маршрутизаторы связаны последовательной линией со скоростью передачи 56 Кбит/с. Все хосты имеют одинаковую маску. По данным, приведенным в табл.2, обосновать необходимое количество сетевых адресов, назначить действующие адреса интерфейсам маршрутизаторов и хостам сети, а также составить таблицы статической маршрутизации, привести схему сети и адреса соответствующих интерфейсов.

Таблица 2

Вариант	Сетевой адрес
0	172.10.0.0
1	172.20.0.0
2	172.30.0.0
3	172.40.0.0
4	172.50.0.0
5	172.60.0.0
6	172.70.0.0
7	172.80.0.0
8	172.90.0.0
9	172.95.0.0

Примечание. Адреса 10.0.0.0 – для сети класса А; 172.16.0.0 – 172.31.0.0 – для сети класса В; 192.168.0.0 – для сети класса С – резервированы и недоступны в Интернете, поэтому были выбраны в качестве учебных.

IP- адресация. Форматы IP-адресов

IP-адрес – число, однозначно определяющее TCP/IP узел. В TCP-IP терминологии «узлом» называется любая машина, имеющая сетевой интерфейс, настроенный на использование PCP/IP. Узлом может быть Windows NT Server, рабочая станция UNIX или один из множества маршрутизаторов, используемых для передачи информации из одной сети в другую.

IP-адрес состоит из двух компонентов: идентификатора сети и идентификатора узла. Идентификатор сети обозначает конкретную сеть (или сегмент сети), в которой узел физически находится. Этот адрес должен быть уникальным по всей PCP/IP сети, вне зависимости от того, является ли сеть глобальной TCP/IP сетью или это просто небольшая локальная сеть, в которой реализован TCP/IP. Идентификатор сети используется для передачи информации на нужный сетевой интерфейс маршру-

тизатора. После того как информация попадает в нужную подсеть (нужный сегмент сети), данные передаются нужному узлу – в соответствии с идентификатором узла. Все узлы, использующие один и тот же идентификатор сети, должен быть физически расположен в одном сегменте сети, чтобы информация могла достичь их. Если узел переносится из одного сетевого сегмента в другой, его сетевой адрес должен быть изменен.

Идентификатор узла определяет конкретный узел в данной сети. Эта часть адреса не должна повторяться для узлов одной подсети. Узлы обычно имеют один сетевой интерфейс или сетевую карту. Однако, такие узлы как маршрутизаторы, могут быть настроены на использование нескольких сетевых интерфейсов. Каждый сетевой интерфейс узла должен иметь свой собственный уникальный IP-адрес.

Форматы IP-адресов могут представляться как двоичным, так и десятичным форматом. Когда IP-адрес записан в десятичном формате, он состоит из четырех групп цифр, называемых октетами, каждая из которых отделена от соседней точкой. Для компьютера IP-адрес является 32-битовым числом (или 4-х байтовым) каждый октет в десятичной записи может принимать значение от 0 до 255 и представляется восьмью битами в двоичном формате, что объясняет название “октет”.

Например: число слева представляет собой двоичную запись адреса, записанного слева: 11000000.10101000.00000000.00000001 - 192.168.0.1

Преобразование между двоичными и десятичными форматами

Как уже было упомянуто, каждый IP-адрес делится на 4 октета. Октет состоит из восьми бит. В двоичном формате каждый бит имеет значение 0,1, что соответствует десятичным числам равным 2 в степени $n-1$, где n -обозначает положение единицы в числе, считая справа налево. Десятичное значение октета может быть число от 0 до 255, т.е. сумма десятичных значений всех битов октета не может быть больше чем 255. В табл.1 приведены примеры двоичных и десятичных значений некоторых октетов.

Таблица 3

Двоичное значение октета	Значения битов октета	Десятичное значение октета
00000000	0	0
10000000	128	128
11000000	128+64	192
11100000	128+64+32	224
11110000	128+64+32+16	240
11111000	128+64+32+16+8	248
11111100	128+64+32+16+8+4	252
11111110	128+64+32+16+8+4+2	254
11111111	128+64+32+16+8+4+2+1	255

Получение IP- адресов

Каждый IP-адрес должен быть уникальным, вне зависимости от количества узлов, находящихся в сети. В том случае, если сеть настроена на использование ТСР/IP и не соединена с Интернетом, то назначение и использование неповторяющихся адресов из пространства IP-адресов выбирается произвольно. Однако если сеть имеет выход в Интернет, то за получением IP-адреса необходимо обратиться в сетевой информационный центр Интернета, который выделяет для организации сетевой идентификатор, позволяющий создать в данной сети (подсети) необходимое количество узлов. Организация может устанавливать идентификаторы узлов в своей подсети по собственному усмотрению.

Классы адресов

Общее адресное пространство IP-адресов позволяет использовать примерно 4,3 миллиарда адресов. Разделив доступное адресное пространство на классы, можно выделить блоки

адресов, в соответствии с общим количеством узлов, которые должны поддерживаться в организации.

В табл. 2 показаны классы адресов, значение старших битов адреса (старших битов первого октета), диапазон десятичных значений первого октета в данном классе и доступное количество сетей и узлов, поддерживаемых в данном классе.

В адресах класса А первый октет представляет идентификатор сети. В адресах класса В первые два октета используются для идентификатора сети, в классе С первые три октета используются для идентификатора сети. Таким образом, каждый адрес можно разделить на два компонента (табл. 4).

Таблица 4

Класс адреса	Старшие биты	Диапазон десятичных значений 1 октета	Доступное количество сетей	Доступное количество узлов
Класс А	0	1-126.X.Y.Z.	126	16777214
Класс В	10	128-191. X.Y.Z	16384	65534
Класс С	110	192-233. X.Y.Z	2097152	254

Таблица 5

Класс адреса	IP-адрес	Идентификатор-сети	Идентификатор узла
Класс А	W.X.Y.Z.	W	X.Y.Z
Класс В	W.X.Y.Z	W.X	Y.Z
Класс С	W.X.Y.Z	W.X.Y	Z

Разделение IP-адреса на компоненты проведено в соответствии с его классом.

Адреса класса А

Класс А использует для идентификации сети только первый октет и три оставшихся октета для идентификации узла. Старший бит первого октета адреса этого класса всегда равен нулю, позволяя определить, что это адрес класса А.

Поскольку старший адрес всегда равен нулю, для идентификации сети остается только семь бит. Эти семь бит позволяют создать максимум 127 различных сетевых адресов, но сетевой идентификатор зарезервирован для локального сетевого адаптера. Таким образом, в классе А доступны только 126 различных сетевых адресов (табл. 6).

Таблица 6

Класс адреса	IP- адрес	Идентификатор сети	Идентификатор узла
Класс А	124.29.88.7	124	29.88.7

Примечание. Здесь и далее адреса сетей приведены в качестве иллюстрации.

Оставшиеся 24 бита доступны для использования в идентификаторе узла. Это позволяет использовать 16777214 адресов узлов. Поскольку этот класс позволяет использовать столь большое количество узлов в сети, эти адреса выдаются только организациям, которым требуется обеспечить доступ к чрезвычайно большому количеству узлов.

Адреса класса В

Класс В использует для идентификатора сети первый и второй октеты, а два оставшихся октета для идентификатора узла. Два старших бита первого октета адреса этого класса всегда равны 10 (единица-ноль), позволяя определить, что это адрес класса В (см. табл. 6). Так как старшие биты всегда равны 10, то для идентификации остается только 14 бит. Эти 14 бит позво-

ляют создать максимум 16384 различных сетевых устройства.

Оставшиеся 16 бит доступны для использования в идентификаторе узла, что позволяет использовать 65534 адреса узла. Этот класс адресов предназначен для средних или больших сетей.

Таблица 7

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс В	130.29.88.7	130.29	88.7

Адреса класса С

Класс С использует для идентификатора сети первые три октета и оставшийся октет для идентификатора узла. Три старших бита первого октета адреса этого класса всегда равны 110, позволяя определить, что это адрес класса С. Поскольку старшие биты равны 110, для идентификатора сети остается 21 бит. Это позволяет создать максимум 2097152 различных сетевых адреса (табл.8).

Оставшиеся 8 бит доступны для использования в идентификаторе узла. Это позволяет получить 254 адреса узла. Этот класс адресов предназначен для небольших сетей, которым требуется ограниченное количество узлов.

Таблица 8

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс А	192.29.88.7	192.29.88	7

Адреса класса D

Адресация класса D используется для широкоэмитальных сообщений, которые используются для отправки информации

определенной группе узлов. Эти узлы включаются в группы после того, как они регистрируют себя на локальном маршрутизаторе, используя широковещательный адрес - один из адресов класса D. Старшие биты адреса класса D всегда устанавливаются в 1110; оставшиеся биты используются для обозначения логической группы узлов.

Адреса класса E

Класс E – экспериментальный класс адресов, зарезервированный для будущего использования. Адреса в этом классе определяются четырьмя старшими битами, установленными в 1111.

Разделение сетей: подсети и маски подсетей

Дополнительное подразделение блоков адресов на подсети возникает тогда, когда блоки выделенных адресов не соответствуют топологии существующей сети. Поскольку все пространство IP-адресов делится на три класса, то количество доступных идентификаторов сети и узла в каждом классе является функцией количества бит, выделенных на образование соответствующего компонента адреса.

Например, в адресах класса B два старших бита установлены в 10, что позволяет использовать только 14 бит для идентификатора сети и 16 бит для идентификатора узла. Проверив старшие биты адреса, можно легко определить, какая часть адреса составляет идентификатор сети, а какая идентификатор узла. Однако если необходимо провести дальнейшее разделение части адресного пространства, понадобится передать часть бит выделенных исходно для идентификатора узла, идентификатору сети. После выполнения указанного разделения, определение длины идентификатора сети по адресу, становится неочевидным. Для облегчения этого процесса предназначены маски подсетей.

Маски подсетей

Маска подсети – это 32-битный адрес, позволяющий определить, сколько бит в адресах используется для идентификации сети, используя все единицы в позициях, соответствующих идентификатору сети (табл. 9).

Таблица 9

Класс адресов	Дополнительное значение маски	Двоичное значение маски
Класс А	255.0.0.0	11111111.00000000.00000000.00000000
Класс В	255.255.0.0	11111111.11111111.00000000.00000000
Класс С	255.255.255.0	11111111.11111111.11111111.00000000

При инициализации каждый ТСР/IP-узел сравнивает свой собственный IP-адрес с заданной маской подсети при помощи процесса логического «И» (табл. 10) и сохраняет результат. Когда узлу необходимо определить, предназначен ли пакет для локальной сети или удаленной, он сравнит IP-адрес узла адресата со своей маской подсети, а затем сравнит результат с тем, что было получено при инициализации. Если результаты совпадают, то пакет предназначен для локального узла и не маршрутизируется. Если результаты различны, пакет предназначен для узла в другой подсети и передается маршрутизатору.

Операция сравнения (логическое «И») выполняется поразрядно.

В том случае, если принято решение о разделении сети (например, класса С) на две различных подсети требуется расширить маску, чтобы она показывала, какие биты были добавлены к идентификатору сети. Для того, чтобы создать две дополнительные подсети в рамках сети класса С, обычно используется маска 255.255.255.192. Число 192 показывает, что два старших бита октета используются для идентификатора сети. В принципе, два добавочных бита позволяют создать четыре различные комбинации, но поскольку идентификатор сети не может состоять из одних единиц или нулей, остаются только две возможности подсети – 64 и 128.

Адресация подсетей

Маршрутизаторам между любыми двумя узлами не требуется знание точного расположения узлов в сети. Вместо этого они используют идентификатор сети, входящий в состав IP-адреса для того, чтобы отправить пакет маршрутизатору, соединенному с соответствующей сетью. Затем этот маршрутизатор самостоятельно определит, какому из узлов локальной сети можно передать пакеты. По умолчанию граница между идентификатором сети и узла располагается между двумя октетами. В табл.9 приведен пример идентификаторов сети и узла по умолчанию для адреса класса В.

Таблица 10

Класс адреса	IP-адрес	Идентификат. сети	Идентификат. узла
Класс В	130.29.88.7	130.29	88.7

Положение границы по умолчанию между идентификаторами сети и узла соответствует одному из трех классов адресов. Классы используются для разделения всего 32-битового адресного пространства на группы адресов, которые могут поддерживать различное количество узлов. Идентификаторами узлов в выделенном блоке адресов организация может распоряжаться по собственному усмотрению. Однако обычно выделяется только один идентификатор сети на организацию. Это подходит для небольшой организации, получившей сетевой адрес класса С (что позволяет поддерживать до 254 узлов), если сеть состоит из одного сегмента и не планируется создавать новые сегменты. Однако большинство организаций имеют несколько сетей, и наблюдается тенденция к их увеличению. Следовательно, одного сетевого идентификатора недостаточно. Дополнительные сетевые идентификаторы могут быть получены при помощи разделения выделенного адресного пространства.

IP-маршрутизация

IP-маршрутизация является процессом передачи данных от хоста, расположенного в некоторой сети удаленному хосту, принадлежащему другой сети, через один или несколько маршрутизаторов. Путь, по которому маршрутизатор передает пакет, определяется по таблице маршрутизации. Эта таблица содержит IP-адреса интерфейсов маршрутизаторов, соединенных с сетями, с которыми должен взаимодействовать маршрутизатор. Таблица маршрутизации помогает найти путь к сети, определяемой адресом получателя из передаваемого пакета. Если путь не найден, пакет отправляется по адресу маршрутизатора, выбранного по умолчанию, при наличии такового. По умолчанию маршрутизатор может посылать пакеты в любую сеть, с которой связаны его настроенные интерфейсы. Когда некоторый хост пытается взаимодействовать с хостом из другой сети, IP-протокол использует адрес шлюза, выбранного по умолчанию, для доставки пакета соответствующему маршрутизатору. Если маршрутизатор найден, пакет посылается в нужную сеть, а затем достигает хоста получателя. Если маршрут не найден, то сообщение об ошибке возвращается на хост-источник.

Процесс маршрутизации

Процесс маршрутизации ясен, если получатель датаграммы находится в соседней сети. В этом случае маршрутизатор выполняет простую процедуру по пересылке пакета.

Когда рабочая станция посылает пакет хосту-получателю, всегда проверяется IP-адрес получателя. Если оказывается, что в локальной сети такого адреса нет, пакет должен быть маршрутизирован. С помощью протокола ARP станция определяет аппаратный адрес шлюза выбранного по умолчанию. Затем IP отправляет пакет по аппаратному адресу маршрутизатора, выбранного по умолчанию. Информация, используемая для адресации пакета, включает в себя:

аппаратный адрес источника;
IP- адрес источника;
аппаратный адрес получателя;
IP- адрес получателя.

Для того чтобы маршрутизатор «знал», через какой интерфейс он должен отправить пакет, необходимо составить таблицу маршрутизации, которую поддерживает IP-маршрутизатор. Именно по ней IP-протокол определяет путь к нужной сети. Таблицы маршрутизации сложных объединенных сетей должны содержать не только доступные пути к сети получателя, но и данные, позволяющие оценить эффективность предполагаемого маршрута. В таблицах маршрутизации должны содержаться записи о расположении сетей, а не хостов.

Статическая и динамическая маршрутизация, маршрутизация по умолчанию

Таблицы маршрутизации хранят информацию о маршрутах, алгоритмы маршрутизации создают и поддерживают эти таблицы. На начальном этапе работы маршрутизатор знает только, как достичь сетей или подсетей, с которыми он связан непосредственно.

Маршрутизаторы обнаруживают пути в другие сети тремя различными способами:

- с помощью статической маршрутизации;
- с помощью маршрутизации по умолчанию;
- с помощью динамической маршрутизации.

Статическая маршрутизация. Таблицы статических маршрутизаторов создаются и обновляются вручную. При изменении маршрута статические маршрутизаторы не информируют об этом друг друга. Администратор сети должен вручную модифицировать запись статической таблицы всякий раз, когда в топологии объединенной сети возникают изменения. Достоинством статической маршрутизации является неизменная полоса пропускания, так как не приняты широковещательные рассылки сообщений об изменении маршрутов. Другое поло-

жительное качество – безопасность. При статической маршрутизации маршрутизаторы знают только о тех сетях, которые прописаны в таблицах. Это не позволяет пользователям получать доступ к ресурсам, доступ к которым им запрещен. К положительным свойствам можно также отнести ограничение статических маршрутов к удаленным получателям одним путем, пролегающим через единственный маршрутизатор. Статическую маршрутизацию следует использовать также в тех случаях, когда сеть достижима только по одному пути (так называемая *stab* сеть). Создание статических маршрутов для таких тупиковых сетей позволяет оптимизировать расходы, свойственные динамической маршрутизации.

Маршрутизация по умолчанию. Путь по умолчанию должен быть задан для каждого маршрутизатора, установленного в сети; в том случае если этого не сделать, то маршрутизатор выбирает путь по умолчанию самостоятельно. Задание маршрута по умолчанию выполняется аналогично указанию путей при статической маршрутизации, однако запись в таблице маршрутизации для маршрута, выбранного по умолчанию, содержит сеть и маску сети, состоящую из одних нулей (применительно к маршрутизаторам Cisco). Поскольку задачи динамической маршрутизации выходят за рамки данного задания, то в данной работе не рассматриваются.

Пример решения контрольной работы № 1

При решении задачи следует учесть следующее. В случае, если маска сети отличается от стандартной, это свидетельствует о том, что сеть разбита на N подсетей. На первом шаге ре-

шения определяют, сколько бит в маске отводится под подсети. Далее определяют, к какой подсети относится данный сетевой адрес. Определение выполняют путем логического умножения маски на сетевой адрес (предварительно необходимо преобразовать адрес и маску в двоичную систему исчисления). Диапазон допустимых адресов будет лежать в диапазоне между адресами подсетей. Следует учесть, что адрес со всеми единицами является широковещательным и является запрещенным.

Пример решения контрольной работы № 2

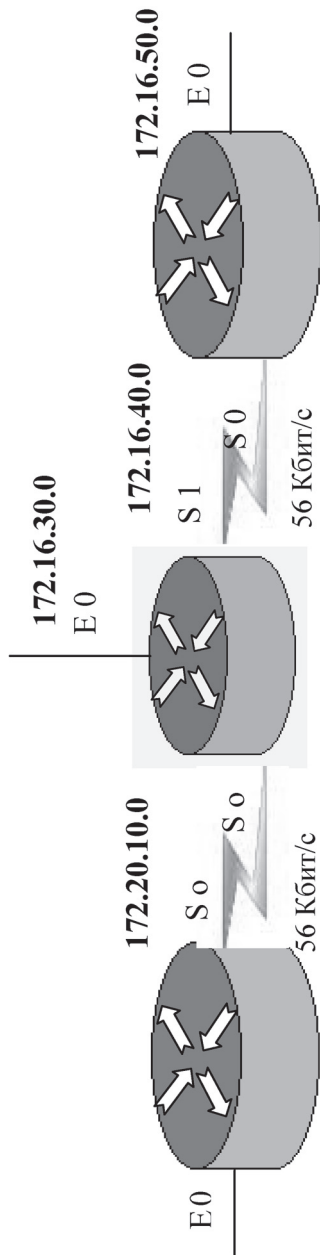
Рассмотрим сеть с адресом 172.16.0.0 в качестве номера сети. Вся сеть состоит из трех сетей Ethernet и двух последовательных линий. Это означает, что необходимо сконфигурировать пять сетей, как различные подсети.

Если применить маску 255.255.255.0, получаем 254 подсети, каждая из которых содержит до 254 хостов. Обозначим подсети как 172.16.10.0, 172.16.20.0, 172.16.30.0, 172.16.40.0, и 172.16.20.50.0, всем хостам присвоим одинаковую маску 255.255.255.0 (объединенные адреса нанесены на рисунок).

Теперь необходимо назначить действительные адреса хостов интерфейсам маршрутизаторов и всем хостам сети. Схемы выбранных адресов приведены в табл. 11.

Таблица 11

Маршрутизатор А	Маршрутизатор В	Маршрутизатор С
Ethernet0=172.16.10.1	Ethernet0=172.16.30.1	Ethernet0=172.16.50.1
Serial0=172.16.20.1	Serial0=172.16.20.2	Serial0=172.16.40.2
Хост А=172.16.10.2	Serial1=172.16.40.1	Хост В=172.16.50.2



Маршрутизатор А Маршрутизатор В Маршрутизатор С

Объединенная сеть с IP-адресами

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ДАННЫХ

Рабочая программа и задание на контрольную работу

Редактор *В.И. Чучева*
Компьютерная верстка *А.Ю. Байкова*

Тип. зак.	Изд. зак.265	Тираж 300 экз.
Подписано в печать	Гарнитура NewtonC	Офсет
Усл. печ. л.		Формат 60×90 ¹ / ₁₆

Издательский центр РГОТУПСа,
125993, Москва, Часовая ул., 22/2

Участок оперативной печати РГОТУПСа,
125993, Москва, Часовая ул., 22/2