

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра управления в технических системах

УТВЕРЖДАЮ:

Проректор по учебной работе

_____ Е.И. Луковникова

«_____» _____ 201__ г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
СЕТЕВЫЕ ТЕХНОЛОГИИ ВЫСОКОСКОРОСТНОЙ ПЕРЕДАЧИ
ДАННЫХ**

Б1.В.11

НАПРАВЛЕНИЕ ПОДГОТОВКИ

11.03.02 Инфокоммуникационные технологии и системы связи

ПРОФИЛЬ ПОДГОТОВКИ

Многоканальные телекоммуникационные системы

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ	4
3.1 Распределение объёма дисциплины по формам обучения.....	4
3.2 Распределение объёма дисциплины по видам учебных занятий и трудоемкости	4
4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	5
4.1 Распределение разделов дисциплины по видам учебных занятий	5
4.2 Содержание дисциплины, структурированное по разделам и темам	7
4.3 Лабораторные работы.....	32
4.4 Практические занятия.....	32
4.5 Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат	32
5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	33
6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ	34
7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	34
8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО – ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	34
9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....	35
9.1. Методические указания для обучающихся по выполнению лабораторных работ/ практических работ	35
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	50
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	50
Приложение 1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	51
Приложение 2. Аннотация рабочей программы дисциплины	56
Приложение 3. Протокол о дополнениях и изменениях в рабочей программе	57
Приложение 4. Фонд оценочных средств для текущего контроля успеваемости по дисциплине.....	57

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к экспериментально-исследовательскому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучающихся профессиональных компетенций в области построения и функционирования сетей передачи данных, базовых технологий организации локальных и территориальных компьютерных сетей, стека протоколов TCP/IP, принципов расчета характеристик отдельных участков сетей передачи данных, методы защиты от ошибок при передачи данных.

Задачи дисциплины

Ознакомление обучающихся с вопросами функционирования и настройки аппаратного и программного обеспечения сетевых технологий передачи данных

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОПК-3	Способность владеть основными методами, способами и средствами получения, хранения, переработки информации	Знать: - Основы технологии интегральных схем, микросхемотехнику и принцип работы базовых каскадов аналоговых и логических элементов цифровых схем. Уметь: - проводить самостоятельный анализ физических процессов, происходящих в электронных телекоммуникационных устройствах. Владеть: - навыками работы на компьютере и в компьютерных сетях, .
ПК-13	Способность осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты	Знать: - Базовые принципы построение типовых технических проектов в сфере сетевых технологий. Уметь: - проводить самостоятельный расчет физических процессов, происходящих в электронных телекоммуникационных устройствах, и проектировать их; Владеть: - навыками расчета внешних характеристик систем передачи данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.11 Сетевые технологии высокоскоростной передачи данных относится к вариативной части к обязательным дисциплинами .

Дисциплина сетевые технологии высокоскоростной передачи данных базируется на знаниях, полученных при изучении дисциплин Б1.Б.8 Информатика, Б1.Б.16 Вычислительная техника и информационные технологии, Б1.В.10 Направляющие среды электросвязи .

Основываясь на изучении перечисленных дисциплин, сетевые технологии высокоскоростной передачи данных представляет основу для изучения дисциплины: Б1.В.ОД.15 Проектирование и эксплуатация систем передачи, Б1.В.ДВ.11 Основы информационной безопасности сетей и систем

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	Курс	Семестр	Трудоемкость дисциплины в часах						Курсовая работа (проект), контрольная работа, реферат, РГР	Вид промежуточной аттестации
			Всего часов (с экз.)	Аудиторных часов	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа		
1	2	3	4	5	6	7	8	9	10	11
Очная	4	7	144	51	17	17	17	57	-	Экзамен
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	Трудоемкость (час.)	в т.ч. в интерактивной, активной, инновационной формах, (час.)	Распределение по семестрам, час
			7
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	51	17	51
Лекции (Лк)	17	-	17
Лабораторные работы (ЛР)	17	17	17
Практические работы (ПР)	17	-	17
Индивидуальные (групповые) консультации	+	-	+
II. Самостоятельная работа обучающихся (СР)	57	-	57
Подготовка к лабораторным работам	18	-	18
Подготовка к практическим работам	18	-	18
Подготовка к экзамену в течение семестра	21	-	21
III. Промежуточная аттестация экзамен	36	-	36
Общая трудоемкость дисциплины час.	144	-	144
зач. ед.	4	-	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий - для очной формы обучения:

№ раздела и темы	Наименование раздела и тема дисциплины	Трудоемкость, (час.)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)			
			учебные занятия			самостоятельная работа обучающихся
			лекции	лабораторные работы	практические работы	
1	2	3	4	5	6	7
1.	Принципы построения компьютерных сетей. Сетевые протоколы.	19	2	3	3	11
1.1.	Классификация компьютерных сетей.	5.6	0,6	1	1	3
1.2.	Международные организации. Модель OSI	6.7	0,7	1	1	4
1.3.	ATM. Основные идеи технологии ATM.	6.7	0,7	1	1	4
2.	Среды доступа и технологии локальных и глобальных сетей.	25	2	9	3	11
2.1.	Ethernet. Физическая среда Ethernet.	8.5	0,5	3	3	2
2.2.	Высокоскоростной Ethernet	6.5	0,5	3	-	3
2.3.	Технологии удалённого доступа.	6.5	0,5	3	-	3
2.4.	Стык по (последовательному) COM порту.	3.5	0,5	-	-	3
3.	Сетевая операционная система Unix и сети TCP/IP.	18	4	-	3	11
3.1.	История создания.	5.5	0,5	-	3	2
3.2.	Краткая история семейства протоколов TCP/IP	2.5	0,5	-	-	2
3.3.	Общие сведения об архитектуре семейства протоколов TCP/IP	3	1	-	-	2
3.4.	Уровень сетевого интерфейса	2.5	0,5	-	-	2
3.5	Уровень Internet. Протоколы IP, ICMP, ARP, RARP. Internet-адреса	2.5	0,5	-	-	2
3.6.	Транспортный уровень. Протоколы TCP и UDP. TCP и UDP сокет. Адресные пространства портов. Понятие encapsulation	2	1	-	-	1
4.	Адресация и маршрутизация в компьютерных сетях.	29	7	5	8	12
4.1.	Физические адреса	2.5	0,7	-	-	2
4.2.	IP-адресация	5.5	0,7	2	2	1
4.3.	Классы IP-сетей	6.5	0,8	2	2	2
4.4.	Маски подсетей	4.5	0,8	1	2	1
4.5.	Система доменных имен	1.4	0,8	-	-	1

4.6.	Универсальная идентификация ресурсов (URL)	2.4	0,8	-	-	2
4.7.	IP маршрутизация	1.4	0,8	-	-	1
4.8.	Статическая маршрутизация.	2.4	0,8	-	1	1
4.9.	Динамическая маршрутизация.	2.4	0,8	-	1	1
5.	Службы DNS и DHCP.	17	2	-	-	12
5.1.	DNS	5.7	0,7	-	-	4
5.2.	DHCP. Клиент DHCP и IP-адрес.	5.7	0,7	-	-	4
5.3	Проверка назначения IP-адреса	5.6	0,6	-	-	4
	ИТОГО	108	17	17	17	57

4.2. Содержание дисциплины, структурированное по разделам и темам

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ. СЕТЕВЫЕ ПРОТОКОЛЫ.

Под термином «Сеть» будем понимать систему связи со многими источниками и/или получателями сообщений. Места, где пути распространения сигналов в сети разветвляются или оканчиваются, называются узлами сети.

Компьютерная сеть – это сеть, в которой источниками и получателями сообщений являются компьютеры. Можно назвать несколько близких понятий, а именно, — вычислительная сеть, сеть передачи данных, распределённая система, различие между которыми определяется акцентами.

Классификация компьютерных сетей

Компьютерные сети как сложные и многопрофильные объекты принято классифицировать, исходя из разных точек зрения. Наиболее популярными являются следующие принципы классификации:

По «диаметру», т. е. расстоянию между наиболее удалёнными узлами сети:

Сотни метров — LAN (Local Area Network) или ЛВС (Локальная Вычислительная Сеть);

Километры — MAN/CAN (Metropolitan/Campus Area Network) или РВС (Региональная Вычислительная Сеть);

Сотни и тысячи километров — WAN (Wide Area Network) или ГВС (Глобальная Вычислительная Сеть).

Поскольку современные компьютерные сети практически всегда имеют выход в глобальную сеть Internet, классификация сетей по этому принципу носит довольно условный характер.

По физической топологии (звезда, кольцо, общая шина, сотовая, иерархическая (древовидная), комбинированная), показывающей физическое соединение линий связи между узлами сети.

По логической топологии (звезда, кольцо, общая шина), показывающей способ обмена сигналами

Физическая и логическая топологии слабо связаны между собой. Например, популярной технологии Ethernet на витой паре соответствует физическая топология звезда и логическая топология общая шина.

По виду кабельной системы – витая пара, оптический кабель, коаксиальный кабель, беспроводные сети.

По способу организации соединения и передачи информации сети делятся на сети с коммутацией

каналов (например, телефонная сеть общего пользования),

сообщений (информация перемещается от узла к узлу целиком)

пакетов (пакеты внутри сети перемещаются независимо друг от друга и собираются целиком в узле назначения).

По стекам протоколов – наборам правил формирования и передачи пакетов. Например, стек TCP/IP, стек IPX/SPX, X25 и пр. Стек отличается от совокупности тем, что стек подразумевает не только набор правил, но и определяет последовательность их применения.

По сетевым операционным системам, т. е. программным продуктам, обслуживающим запросы пользователей на ресурсы сети и обеспечивающим функционирование сети, её администрирование. Например, MS Windows, Novell NetWare, UNIX/Linux и пр.

По способу предоставления ресурсов

одноранговые (все компьютеры могут быть и источниками и потребителями ресурсов сети),

клиент – сервер (выделенные компьютеры являются источниками ресурсов – серверами, а остальные – клиентами, т. е. потребителями ресурсов).

Ресурсами сети могут быть устройства (принтеры, модемы, диски и пр.), файлы (текстовые, звуковые, видео и пр.), службы/сервисы (WWW, E-mail, базы данных и пр.).

Международные организации. Модель OSI

Глобальность охвата и интернациональный характер развития компьютерных сетей делает роль международных организаций в вопросах стандартизации определяющей. При этом, в большинстве случаев, принимаемые стандарты носят характер рекомендаций, однако «де факто» становятся обязательными и соблюдаются всеми производителями сетевого оборудования и программного обеспечения. Механизм создания рекомендаций, кроме собственных разработок, включает в себя и рассмотрение инициативных предложений крупных компаний, самостоятельно разрабатывающих и продвигающих те или иные сетевые технологии. Отличительной чертой рекомендация является их непрерывная модернизация, отслеживающая новейшие достижения в этой области.

Наиболее авторитетными организациями в области сетевых технологий являются:

ITU-T (International Telecommunications Union sector Telecommunication) Международный союз электросвязи, сектор телекоммуникаций. До 1993 года организация называлась ССИТТ (Consultative Committee for International Telephone and telegraphy), или в русском переводе МККТТ (Международный Консультативный Комитет по Телефонии и Телеграфии). Кроме сектора Т (Telecommunication), важными являются секторы R (распределения радиочастот) и D (развития).

ISO (International Organization for Standardization) Международная организация по стандартизации. Эта организация объединяет национальные институты стандартов из 89 стран (ANSI — США, DIN – Германия, BSI – Великобритания и др.).

IEEE (Institute of Electrical and Electronics Engineers) Институт инженеров по электротехнике и радиоэлектронике – национальный «профсоюз» «электрических» учёных и инженеров США.

Модель OSI (Open System Interconnection) — взаимодействия открытых систем была опубликована в 1983 г. по результатам совместных работ ISO и ITU-T. Согласно этой модели все процессы в сетях рассматриваются на семи (поэтому модель иногда называют «семиуровневой») относительно независимых уровнях для наилучшей реализации на каждом уровне по отдельности.

Обмен данными между двумя компьютерами в сети согласно семиуровневой модели иллюстрирует рисунок 1.

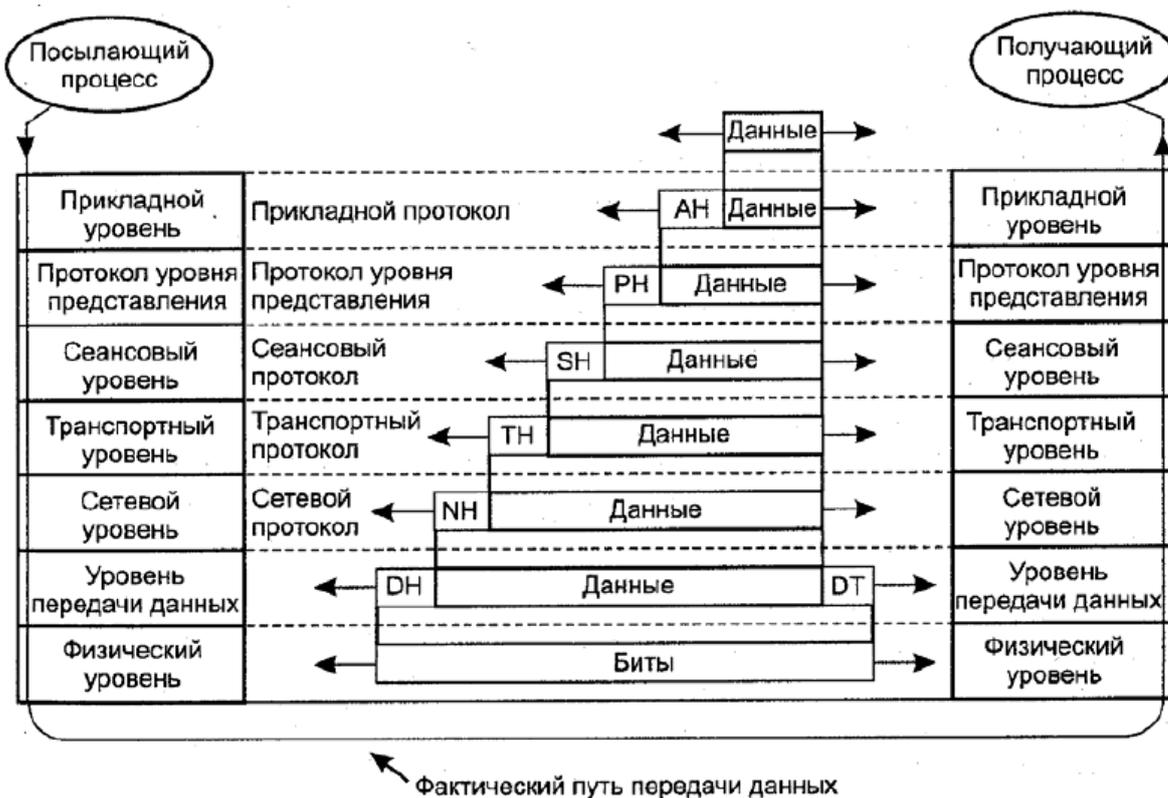


Рис. 1. Модель OSI.

На этом рисунке использованы следующие обозначения: АН (application header) заголовок прикладного уровня, РН (presentation) – заголовок уровня представлений, SH (session) – заголовок сеансового уровня, ТН (transport) – заголовок транспортного уровня, NH (network) – заголовок сетевого уровня, ДН (data link) – заголовок канального уровня, DT (data link tail) – хвостовик кадра канального уровня.

Основной принцип построения модели, обеспечивающий независимость уровней, состоит в том, что пакет вышележащего уровня на нижележащем уровне рассматривается как данные, а вся необходимая для работы информация добавляется в виде заголовка/хвостовика.

При невозможности формирования пакета на нижележащем уровне из-за ограничений на размер пакета используется фрагментация (дробление) пакетов. Пример фрагментации показан на рисунке 2, где для обозначения данных используется буква М (message), заголовка – Н (header) и хвостовика – Т (tail).

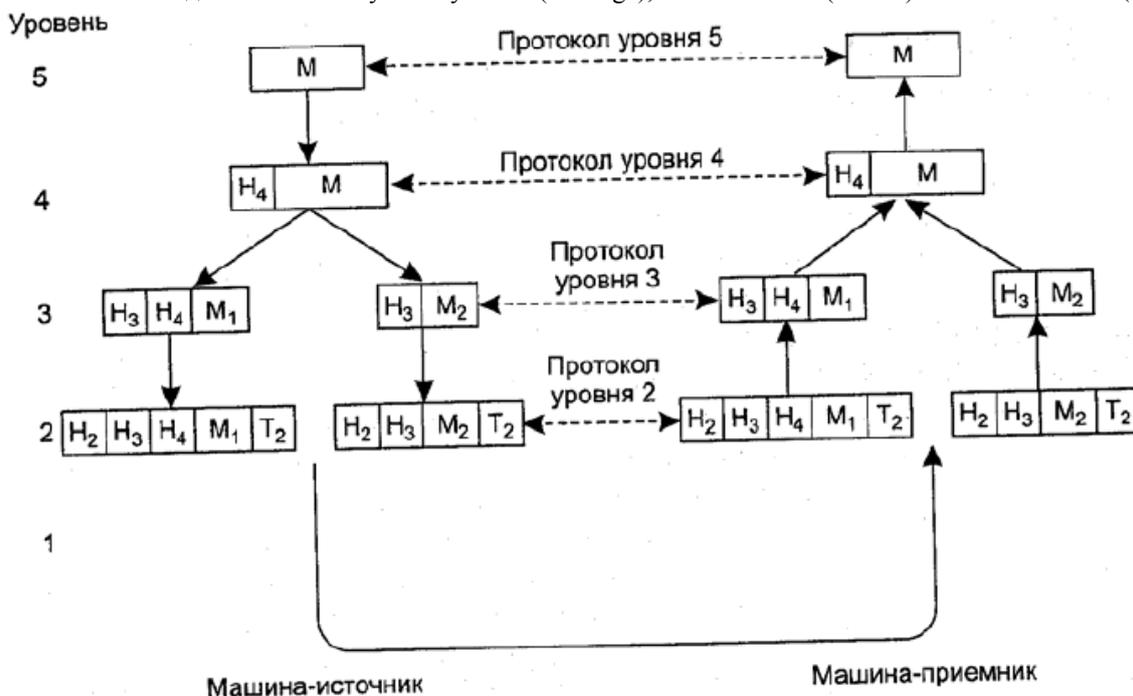


Рис. 2. Фрагментация.

На узлах внутри сети действуют три нижних уровня, как это показано на рисунке 1.2.3, где PDU (protocol data unit) означает пакет протокола соответствующего уровня.

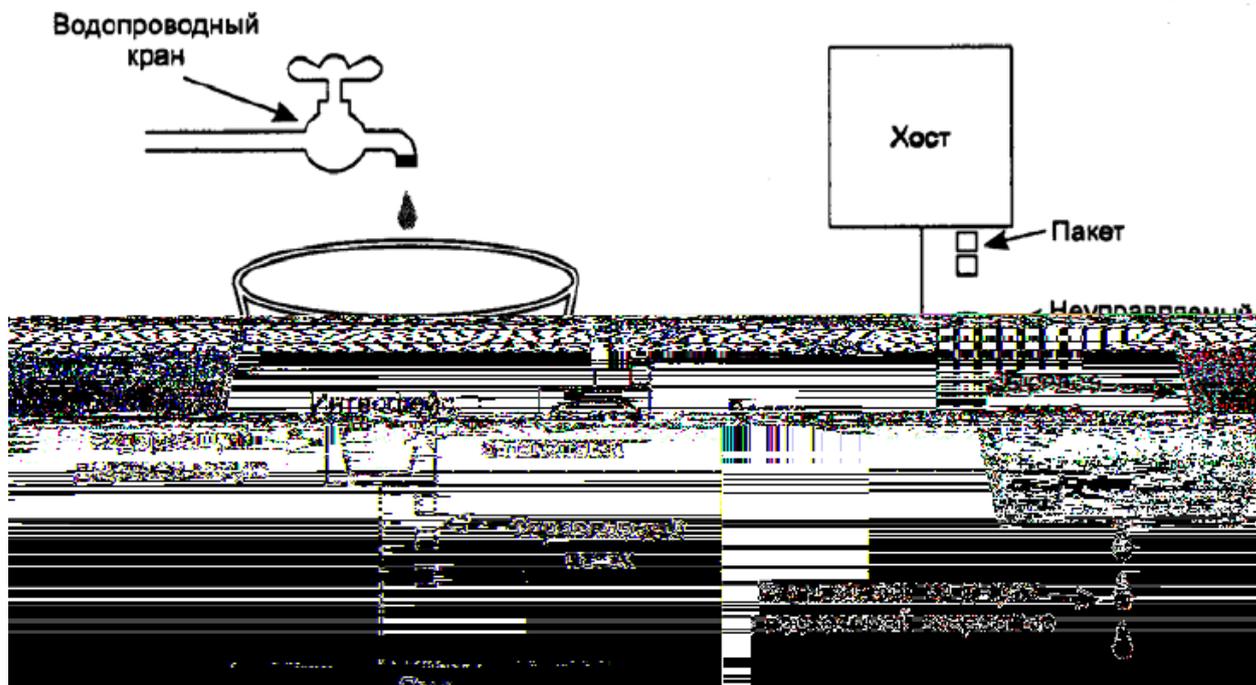


Рис. 4. «Дырявое ведро»

Широкий диапазон скоростей и их согласованность со стандартными скоростями. В таблице 2.2.1 приведены скорости и примерные характеристики физической среды АТМ для локальных компьютерных сетей, в следующей таблице 2.2.2 – для глобальных сетей.

Характеристики физической среды АТМ для ЛВС

Скорость Мбит/с	Физическая среда	Макс. расстояние между узлами м
25,6	UTP Cat. 3	100
51,84	UTP Cat. 3 Вол/опт. каб. Коаксиаль. каб.	100 2 000 400
100,0	Вол/опт. каб.	2 000
155,52	UTP Cat. 5, STP 1A Вол/опт. каб. Коаксиаль. каб.	100 2 000 200
622,08	Вол/опт. каб.	300

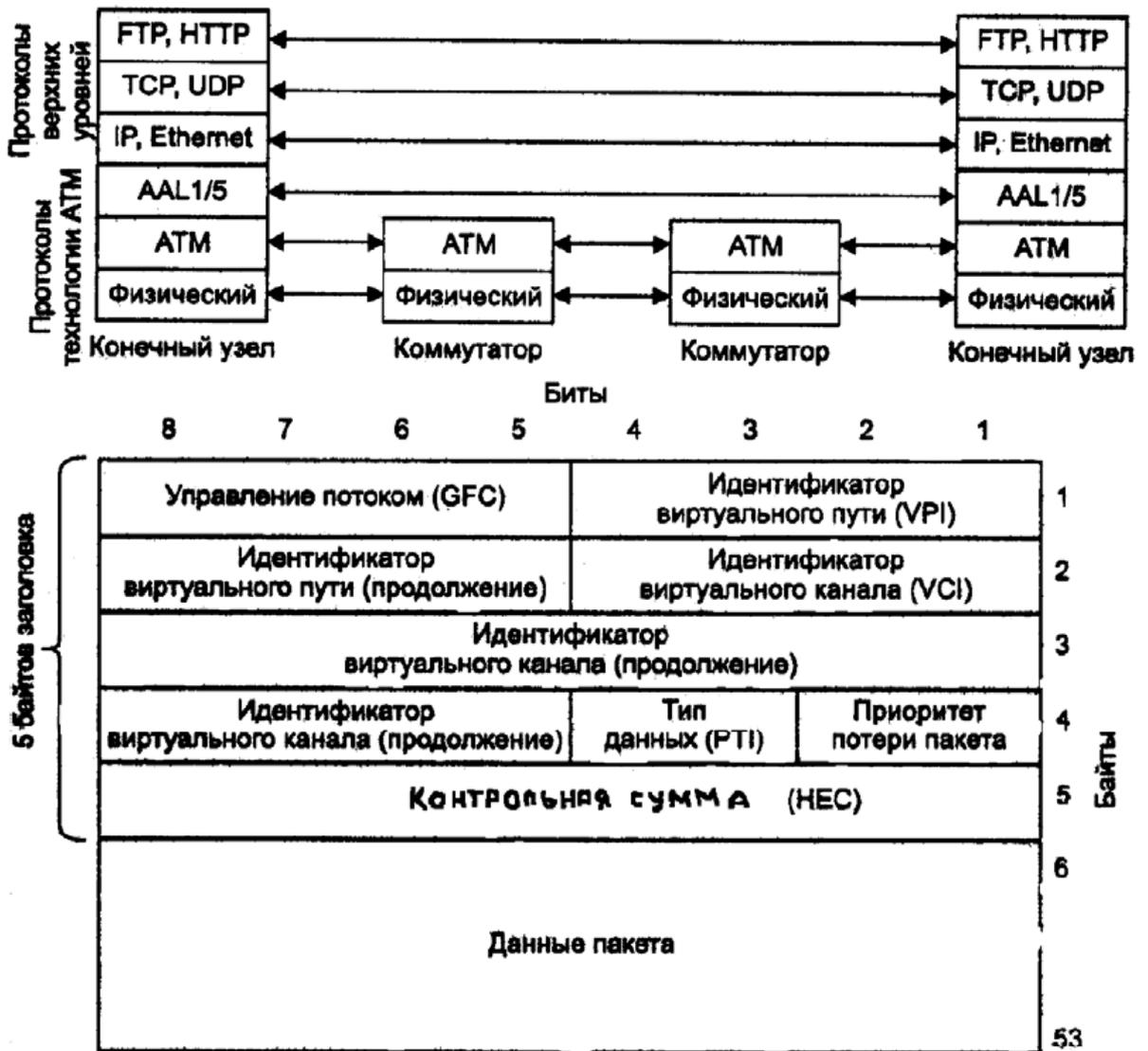
Характеристики физической среды АТМ для ГВС.

Скорость Мбит/с	Физическая среда	Макс. расстояние между узлами в км
1,544 (Т1)/2,048(Е1)	UTP Cat. 3	1,3
34,368(Т3)/44,736(Е3)	Твинаксиаль. каб.	0,4
51,84/155,52/622,08	Вол/опт. каб.	15 и более

Характеристики классов трафика в АТМ

Класс трафика	Пост. бит. скорость	Треб. временная синхр	Установ. соединения	Примеры
A	+	+	+	Голос, TV
B	-	+	+	Сжат. голос, TV
C	-	-	+	TCP
D	-	-	-	IP, Ethernet
X	Устанавлив-ся пользоват-ем			

Многообразие уровней адаптации технологии к протоколам верхних уровней. уровень адаптации АТМ представляет собой набор протоколов ААЛ1 – ААЛ5 преобразования пакетов верхних уровней в ячейки АТМ, структура которых показана на рисунке 2.3.4.



GFC (Generic Flow Control) – параметр взаимодействия конечного терминала и коммутатора.

VPI (Virtual Path Identifier) – идентификатор виртуального пути (общей части нескольких виртуальных каналов).

VCI (Virtual Channel Identifier) – идентификатор виртуального канала

PTI (Payload Type Identifier) – (3 бита) идентификатор типа ячейки – пользовательская или управляющая, имеет флаг перегрузки.

Приоритет потери ячейки CLP (Cell Loss Priority) – флаг кандидатов на удаление в случае необходимости.

HEC (Header Error Control) – контрольная сумма заголовка на базе расширенного кода Хэмминга.

В заключение следует отметить, что несмотря на несомненные преимущества ATM перед другими технологиями, её массовому применению в локальных сетях препятствует высокая стоимость оборудования, в особенности коммутаторов.

СРЕДЫ ДОСТУПА И ТЕХНОЛОГИИ ЛОКАЛЬНЫХ И ГЛОБАЛЬНЫХ СЕТЕЙ.

Ethernet

Ethernet/IEEE 802.3 (от лат. luminiferous ether — светоносный эфир) – самая популярная технология LAN с методом доступа CSMA/CD.

Технология была создана в 70-х гг. доктором Робертом Меткалфом (Robert Metcalfe) как часть проекта «офиса будущего» и обеспечивала скорость 3 Мбит/с. В 1980 г. фирмы DEC/Intel- Xerox довели скорость до 10 Мбит/с и в 1985 г. технология была официально утверждена 802-м комитетом IEEE. До сих пор можно встретить «фирменные» варианты Ethernet под названиями Ethernet II/Ethernet DIX (DEC, Intel, Xerox) и Raw 802.3 (Novell), отличающиеся друг от друга небольшими изменениями формата кадра (пакета).

Иерархия протоколов Ethernet.

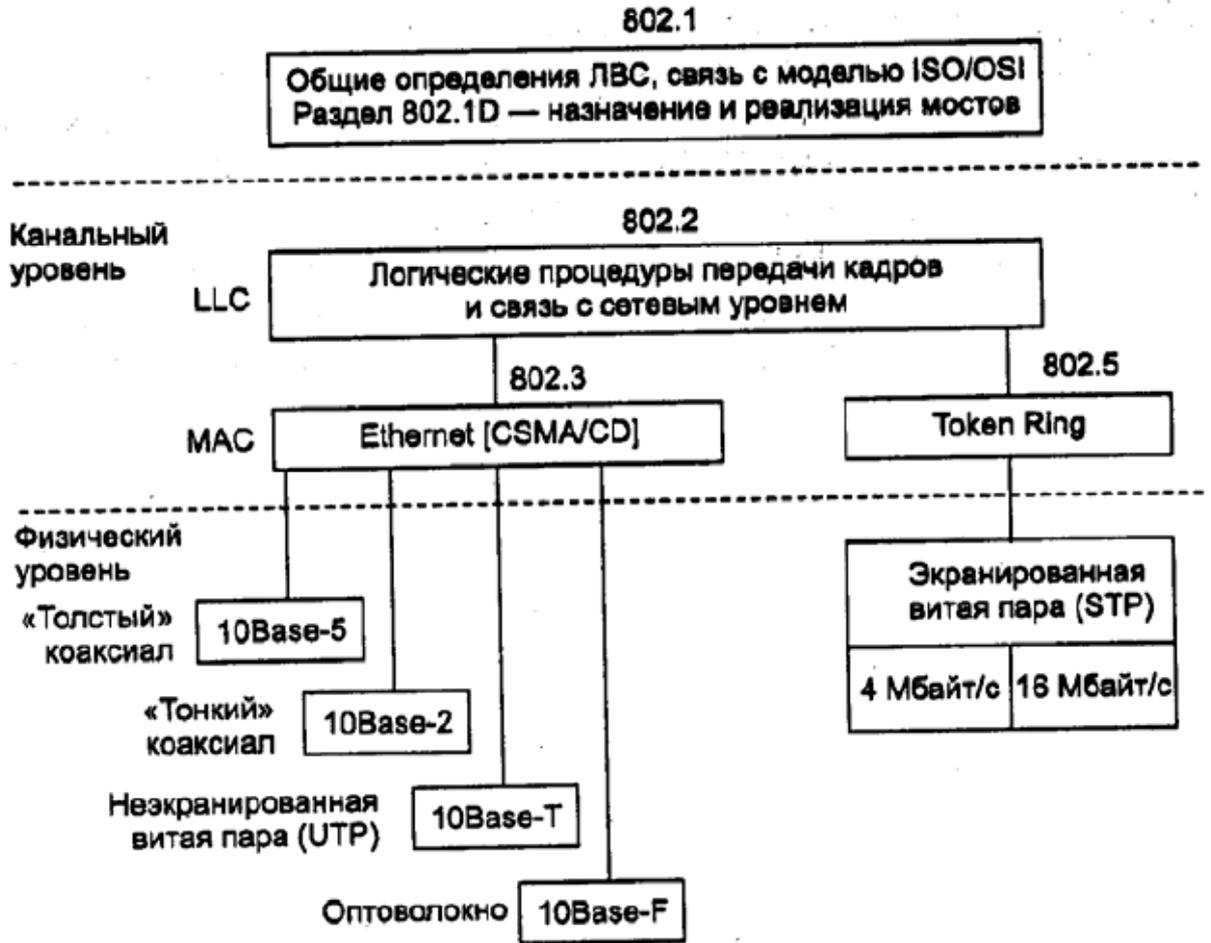
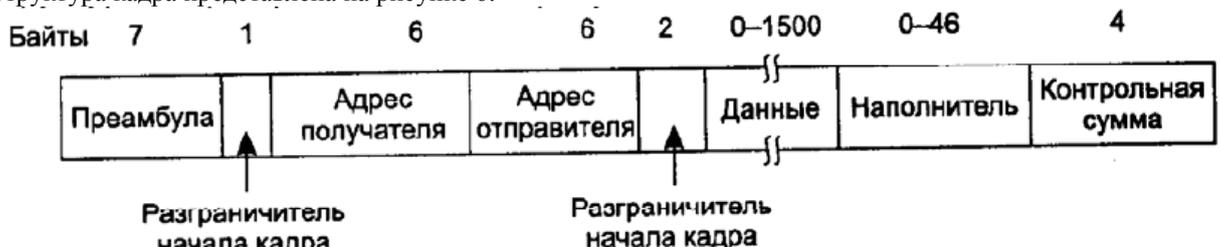


Рис. 5. Протоколы Ethernet

Согласно принятому IEEE стандарту канальный уровень технологии Ethernet делится на подуровень управления логическим каналом LLC (Logical Link Control), отвечающий за логику работы канального уровня, и подуровень доступа к среде MAC (Media Access Control), обеспечивающий формирование кадра.

Каждый узел сети снабжается уникальным MAC адресом из 6 байт, причём 3 байта (без двух старших бит) закрепляются в IEEE за производителем оборудования, а 3 оставшихся байта устанавливаются им самостоятельно.

Структура кадра представлена на рисунке 6.

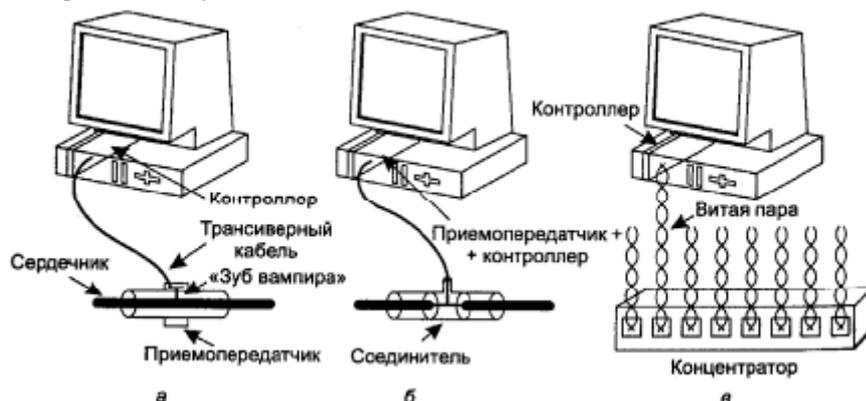


Принимая кадры, сетевые адаптеры устройств считывают MAC адрес получателя и при его совпадении с собственным адресом помещают кадр во входной буфер для последующей обработки, в противном случае – кадр отбрасывается.

Старшие два бита адреса получателя в зависимости от назначения кадра устанавливаются программно при его отправке. Например, у широковещательного кадра, обращённого ко всем узлам сети, старший бит устанавливается в 1, у кадра, адресованного группе узлов, в 1 устанавливается следующий бит адреса и, наконец, у кадра, предназначенного конкретному узлу, оба старших бита — нулевые.

Физическая среда Ethernet

Физическая среда играет важную роль как в формировании стоимости компьютерной сети, так и в потенциальных возможностях её развития. Как следует из рисунка базовые типы кабельных систем технологии Ethernet могут быть построены на двух вида коаксиального кабеля, оптического кабеля или витой пары.



Устаревшие коаксиальные кабельные системы обозначаются как 10Base5 и 10Base2. Первая цифра 10 означает «физическую» скорость передачи сигналов в 10 Мбит/с, слово «Base» – использование всего доступного частотного диапазона кабеля и, наконец, вторая цифра 5 или 2 — округлённый диаметр коаксиального кабеля в десятых долях дюйма. Кабели этих типов имеют волновое сопротивление 50 Ом, маркируются как RG 8/11 и RG58 и называются толстым (thick) и тонким (thin) Ethernet.

Оптические кабели обобщённо обозначаются как 10BaseF (Fiber). Различают стандарт 10BaseFL (доработка комитета IEEE 802.3 более ранней (80-е годы) технологии FOIRL (Fiber Optic Inter Repeater Link) для оптоволоконного соединения узлов сети) и 10BaseFB – для магистральных соединений оптических концентраторов и повторителей, отстоящих друг от друга на расстоянии до 2 км. По своим оптическим характеристикам кабели делят на одномодовые, рассчитанные на использование лазеров, и многомодовые, предназначенные для более дешёвых светодиодных излучателей. Из-за относительно высокой стоимости оптического кабеля и сложности его прокладки оптические кабельные системы редко используются в ЛВС.

Самым распространённым в ЛВС типом кабельной системы является витая пара 10BaseT (Twisted), представляющая собой заключённые в общую оболочку 8 разноцветных скрученных попарно проводов (IEEE 802.3i), из которых в классической технологии Ethernet используется только 2 пары для передачи и приёма сигналов. Альтернативным обозначением витой пары является UTP (Unshielded Twisted Pair) – неэкранированная витая пара.

Категории витой пары

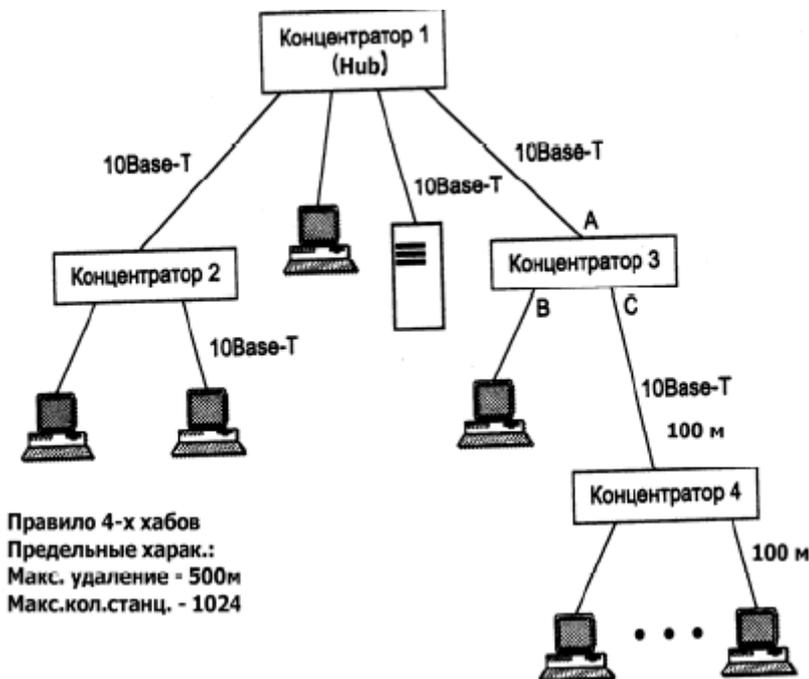
Категория	Верхняя частота (МГц)	Применение
1	0	Телефон, сигнализация
2	1	Телефон, ArcNet
3	16	Телефон, 10BaseT
4	20	Token Ring
5	110(200)	100BaseT
6	350	1000BaseT
7	400(750)	1000BaseT

Современный подход к созданию кабельных систем предполагает использование UTP как для компьютерных, так и учрежденческих телефонных сетей. Использование физической топологии «звезда» и организация всех необходимых для работы сети коммутаций в едином центре получило название «структурированная кабельная система» (СКС).

Стандарты Ethernet кроме UTP допускают применение более дорогой, используемой в технологии Token Ring, экранированной витой пары STP (Shielded Twisted Pair) Type 1A, отличающейся наличием общей экранирующей оболочки.

При построении ЛВС ограничение диаметра сети связано с явлениями затухания сигнала из-за неизбежных потерь, перекрёстными искажениями, отражениями и пр. Согласно принятым соглашениям для корректной работы сети длина соединительного кабеля не должна превышать 100 м. Для увеличения диаметра сети возможно использование последовательного соединения концентраторов (hub), которые усиливают поступивший от любого узла (другого концентратора) сигнал и повторяют его на всех остальных своих портах (выходах).

Для предотвращения неустраняемых коллизий рекомендуется придерживаться «правила 4-х хабов», т. е. в пределах коллизийного домена использовать не более 4 концентраторов.



Правило 4-х хабов не ограничивает размеры сети, т. к. коллизийный домен ограничивается коммутатором (Switch), посылающим пакеты в конкретный порт назначения и не дублирующий его в другие порты, или маршрутизатором (Router), реализующим функции коммутации пакетов на сетевом уровне. Различают также шлюзы (Gateway) – маршрутизаторы, связывающие разнородные сети.

Важным аспектом построения физической среды Ethernet является выбор сетевых адаптеров (NIC – Network Interface Card), устанавливаемых в компьютеры и осуществляющих физический доступ к сети.

Тип шины	Разрядность (бит)	Частота (МГц)	Скорость обмена Мбит/с-Мбайт/с
ISA (Industry Standard Architecture)	16	8,33	66,64-8,33
EISA (Enhanced ISA)	32	8,33	266,56-33,32
MCA (Micro Channel Architecture)	32	10,0	320,0-40,0
VLB (VESA Local Bus)	32	33,33	1066,56-133,33
PCI (Peripheral Connection Interface)	32	33,33	1066,56-133,33

По возможности прямой работы с оперативной памятью компьютера (Bus mastering)

По размеру буферной памяти (стандартно входные и выходные буферы имеют размер 2 кбайта)

По «интеллектуальным» способностям – remote wake up (удалённая активизация).

По режиму обмена: симплекс (только передача или приём), дуплекс (одновременная передача и приём) и полудуплекс (часть времени передача, часть – приём).

По возможности обработки приоритета пакета IEEE 802.1p (QoS – Quality of Service).

Высокоскоростной Ethernet

Fast Ethernet (IEEE 802.3u) – самая распространённая сейчас высокоскоростная технология LAN. С 1992 г. по 1995 г. коалиция фирм 3Com, SynOptics и др. усовершенствовала технологию Ethernet, сохраняя метод доступа CSMA/CD. В 1995 г. IEEE принял дополнение к 802.3 – стандарт 802.3u для скорости 100 Мбит/с, по которому допускается использование в одной сети двух скоростей одновременно (10 и 100 Мбит/с).

Успех технологии во многом связан с возможностью использования (как показано в таблице 2.3.2.1) уже проложенных для обычного Ethernet соединительных кабелей.

Наименование	Кабель	Макс. расстояние до конц. (м)
100BaseT4	UTP Cat.3	100
100BaseTX	UTP Cat.5	100
100BaseFX	Многомод. опт. вол.	2000

Среда 100BaseT4 с использованием UTP Cat.3 применяются довольно редко из-за необходимости одновременной замены всего активного оборудования (концентраторов, коммутаторов, сетевых адаптеров и т. д.) в коллизийном домене. В этом типе физической среды используются все 4 пары кабеля UTP.

Среда 100BaseTX допускает использования в коллизийном домене двухскоростного активного оборудования. Естественно, скорость в 100 Мбит/с будет достигнута только, если оба узла поддерживают эту скорость. Как и в обычном Ethernet сигналы передаются только по 2-м из 4-х пар проводов.

Среда 100BaseFX использует 2 оптические нити.

Концентраторы технологии Fast Ethernet делятся на два класса:

класс I требует наличия портов всех видов (100BaseT4, 100BaseTX/FX)

класс II имеет порты либо типа 100BaseT4, либо типов 100BaseTX/FX

Поскольку концентраторы класса I преобразуют электрические сигналы (увеличение задержки) в пределах коллизийного домена рекомендуется иметь либо 1 концентратор класса I, либо 2 концентратора класса II, расстояние между которыми не должно превышать 5 м. Тем не менее, размеры сети по-прежнему не ограничены, т. к. коллизийный домен ограничивается коммутатором, маршрутизатором или шлюзом.

Gigabit Ethernet (IEEE 802.3z/ав) – технология (1998-9 гг.) обеспечивает скорость 1000 Мбит/с и предназначена для локальных сетей с большим трафиком, возникающим, например, при широком использовании мультимедийных приложений, видеоконференций и т. д.

Физическая среда

Наименование	Кабель	Макс. расстояние до конц. (м)
1000BaseSX/LX	Вол/опт. кабель	200-500
Twinaх	Твинаксиальный кабель	25
1000BaseT	UTP Cat.5 и выше	100

Среда 1000BaseSX/LX согласно стандарту IEEE 802.3z (1998 г.) представляет собой коротковолновый (S – short) или длинноволновый (L – long) волоконно-оптический кабель

. Среда Twinaх – двойной коаксиальный кабель применяется для соединения концентраторов/маршрутизаторов.

Среда 1000BaseT по стандарту IEEE 802.3ав (1999 г.) есть витая пара на ниже 5 категории. Для передачи сигналов в этой среде используется все 4 пары проводов. При прокладке кабеля предъявляются особые требования по недопущению резких изгибов, близости силовых установок и т. д.

В пределах коллизийного домена рекомендуется иметь не более 1-го концентратора технологии Gigabit Ethernet.

В настоящее время комитетом 802 IEEE активно ведутся работы по стандартизации технологии 10 Gigabit Ethernet (IEEE 802.3ae).

Технологии удалённого доступа

Под удалённым доступом понимается предоставление ресурсов сети с использованием общедоступных, чаще всего телефонных каналов связи. Наиболее проблемным участком таких каналов является участок от абонента до телефонной станции. В городах это расстояние не превышает 1,5-2 км, т. е. около 1 мили, это и послужило причиной использования для обозначения участка термина «Последняя миля».

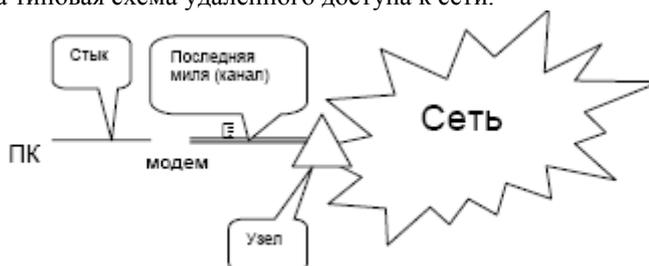
Проблема последней мили заключается в достижении возможно высокой скорости передачи информации при существующих ограничениях на полосу канала связи и величину отношения сигнал/шум, поскольку оба эти параметра по формуле Шеннона влияют на пропускную способность канала $C = F \log_2(1 + P_c/P_{ш})$ бит/с, где F — ширина полосы канала, $P_c/P_{ш}$ — отношение сигнал/шум.

К наиболее популярным и/или перспективным каналам относятся:

проводные каналы общественной телефонной сети

радиоканалы каналов сотовой связи

На рисунке представлена типовая схема удалённого доступа к сети.



Соединение персонального компьютера (ПК) с модемом (модулятором-демодулятором), осуществляющим обмен данными по каналу связи, называется стыком. Термин «стык» или «интерфейс» означает соединение двух отдельных устройств. В случае передачи данных для обозначения этих устройств используются аббревиатуры DTE (Data Terminal Equipment – цифровое терминальное устройство, т. е. ПК) и DCE (Data Circuit-Terminal Equipment – оконечное оборудование линии передачи данных, т. е. модем).

Наиболее популярными и/или перспективными стыками являются.

Стык по (последовательному) COM порту.

Название происходит от COMmunication Port и подразумевает обмен информацией последовательно бит за битом. Традиционные операционные системы персональных компьютеров поддерживают 4 COM порта, два из которых имеют 9 (DB-9) или 25 (DB-25) контактные разъёмы на задней стенке корпуса, а два других предназначены для работы со встраиваемыми устройствами. Стык рассчитан на скорости до 115,2 кбит/с и длину соединительного кабеля до 20 м (50 футов). Механические параметры разъёмов, а также назначения сигналов и их электрические характеристики описываются весьма близкими стандартами RS-232, V.24/V.28 и X.21.

Стандарт RS-232 принят EIA (Electronics Industries Association – Ассоциация электронной промышленности США). Наиболее распространённая версия обозначается как RS-232C.

Стандарты V.24/V.28 (электро-механические характеристики/назначение сигналов) приняты ITU-T (CCITT) в форме рекомендаций для устройств передачи данных, а стандарт X.21 принят ITU-T (CCITT) в рамках стека протоколов X.25 (физический уровень стека). Наиболее близка к перечисленным выше стандартам версия X.21bis.

Стык по порту USB (Universal Serial Bus) – универсальная последовательная шина, предусматривает обмен со скоростями 1,5 Мбит/с или 12 Мбит/с (USB версий 1.0 и 1.1 соответственно), а также 480 Мбит/с (USB версии 2.0). Стык допускает подключение до 127 различных устройств при длине соединительного кабеля 24 AWG до 14 м.

Стык Bluetooth (голубой зуб) получил своё название от прозвища датского короля X века н. э. Гарольда Блаатанда (Harald Blaatand), который принёс христианство в Скандинавию и объединил Данию и Норвегию. В качестве логотипа Bluetooth используется руническая запись инициалов короля.

Технология представлена компанией Ericsson в 1994 г. для соединения по радиоканалу гарнитуры и сотового телефона. Bluetooth предусматривает организацию пикосети (сверхмалой сети) из 7 узлов (1 узел главный и до 6 подчинённых узлов) с методом доступа опрос по логической топологии «звезда». Для соединения узлов пикосети может быть использовано до 79 радиоканалов в диапазоне 2,4 ГГц при скорости обмена до 720 кбит/с. Допустимые расстояния между узлами в основном зависят от мощности используемых передатчиков, которые делятся на 3 класса:

- класс 1 включает в себя передатчики с мощностью от 1 мВт до 100 мВт и обеспечивает соединение на расстоянии несколько сот метров
- класс 2 – передатчики с мощностями от 0,25 мВт до 2,4 мВт для соединения на десятки метров
- класс 3 – предусматривает мощность передатчика до 1 мВт для соединений до 10 метров

СЕТЕВАЯ ОПЕРАЦИОННАЯ СИСТЕМА UNIX И УРОВНИ TCP/IP.

История создания.

UNIX имеет долгую и интересную историю. Начавшись как несерьезный и почти "игрушечный" проект молодых исследователей, UNIX стал многомиллионной индустрией, включив в свою орбиту университеты, многонациональные корпорации, правительства и международные организации стандартизации.

UNIX зародился в лаборатории Bell Labs фирмы AT&T более 20 лет назад. В то время Bell Labs занималась разработкой многопользовательской системы разделения времени MULTICS (Multiplexed Information and Computing Service) совместно с MIT и General Electric, но эта система потерпела неудачу, отчасти из-за слишком амбициозных целей, не соответствовавших уровню компьютеров того времени, а отчасти и из-за того, что она разрабатывалась на языке PL/1, а компилятор PL/1 задерживался и вообще плохо работал после своего запоздалого появления. Поэтому Bell Labs вообще отказалась от участия в проекте MULTICS, что дало возможность одному из ее исследователей, Кену Томпсону, заняться поисковой работой в направлении улучшения операционной среды Bell Labs. Томпсон, а также сотрудник Bell Labs Денис Ритчи и некоторые другие разработали новую файловую систему, многие черты которой вели свое происхождение от MULTICS. Для проверки новой файловой системы Томпсон написал ядро ОС и некоторые программы для компьютера GE-645, который работал под управлением мультипрограммной системы разделения времени GECOS. У Кена Томпсона была написанная им еще во времена работы над MULTICS игра "Space Travel" - "Космическое путешествие". Он запускал ее на компьютере GE-645, но она работала на нем не очень хорошо из-за невысокой эффективности разделения времени. Кроме этого, машинное время GE-645 стоило слишком дорого. В результате Томпсон и Ритчи решили перенести игру на стоящую в углу без дела машину PDP-7 фирмы DEC, имеющую 4096 18-битных слов, телетайп и хороший графический дисплей. Но у PDP-7 было неважное программное обеспечение, и, закончив перенос игры, Томпсон решил реализовать на PDP-7 ту файловую систему, над которой он работал на GE-645. Из этой работы и возникла первая версия UNIX, хотя она и не имела в то время никакого названия. Но она уже включала характерную для UNIX файловую систему, основанную на индексных дескрипторах inode, имела подсистему управления процессами и памятью, а также позволяла двум пользователям работать в режиме разделения времени. Система была написана на ассемблере. Имя UNIX (Uniplex Information and Computing Services) было дано ей еще одним сотрудником Bell Labs, Брайаном Керниганом, который первоначально назвал ее UNICS, подчеркивая ее отличие от многопользовательской MULTICS. Вскоре UNICS начали называть UNIX.

Первыми пользователями UNIX'a стали сотрудники отдела патентов Bell Labs, которые нашли ее удобной средой для создания текстов.

Большое влияние на судьбу UNIX оказала переписка ее на языке высокого уровня C, разработанного Денисом Ритчи специально для этих целей. Это произошло в 1973 году, UNIX насчитывал к этому времени уже 25 инсталляций, и в Bell Labs была создана специальная группа поддержки UNIX.

Широкое распространение UNIX получил с 1974 года, после описания этой системы Томпсоном и Ритчи в компьютерном журнале CACM. UNIX получил широкое распространение в университетах, так как для них он поставлялся бесплатно вместе с исходными кодами на C. Широкое распространение эффективных C-компиляторов сделало UNIX уникальной для того времени ОС из-за возможности переноса на различные компьютеры. Университеты внесли значительный вклад в улучшение UNIX и дальнейшую его популяризацию. Еще одним шагом на пути получения признания UNIX как стандартизированной среды стала разработка Денисом Ритчи библиотеки ввода-вывода stdio. Благодаря использованию этой библиотеки для компилятора C, программы для UNIX стали легко переносимыми.

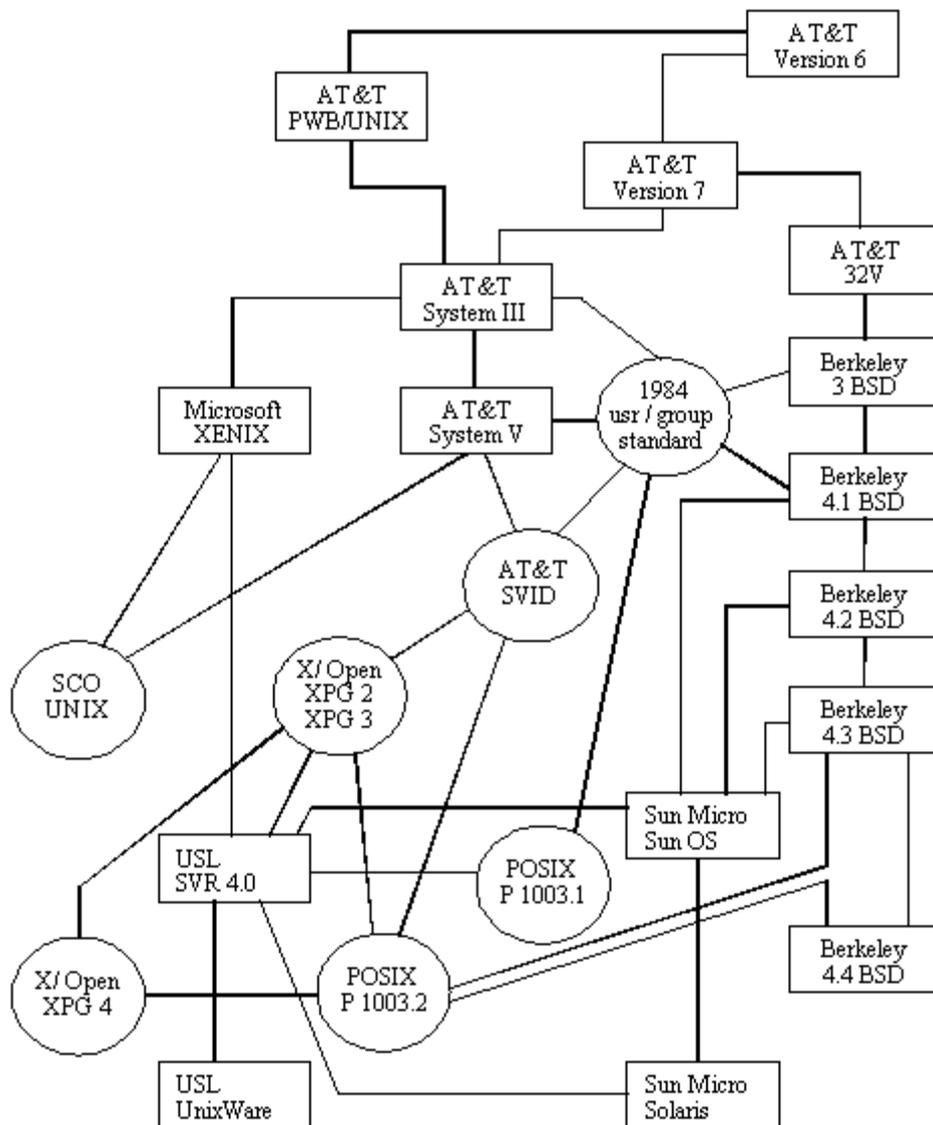


Рис. 5.1. История развития UNIX

Широкое распространение UNIX породило проблему несовместимости его многочисленных версий. Очевидно, что для пользователя весьма неприятен тот факт, что пакет, купленный для одной версии UNIX, отказывается работать на другой версии UNIX. Периодически делались и делаются попытки стандартизации UNIX, но они пока имели ограниченный успех. Процесс сближения различных версий UNIX и их расхождения носит циклический характер. Перед лицом новой угрозы со стороны какой-либо другой операционной системы различные производители UNIX-версий сближают свои продукты, но затем конкурентная борьба вынуждает их делать оригинальные улучшения и версии снова расходятся. В этом процессе есть и положительная сторона - появление новых идей и средств, улучшающих как UNIX, так и многие другие операционные системы, перенявшие у него за долгие годы его существования много полезного.

На рисунке 5.1 показана упрощенная картина развития UNIX, которая учитывает преемственность различных версий и влияние на них принимаемых стандартов. Наибольшее распространение получили две весьма несовместимые линии версий UNIX: линия AT&T - UNIX System V, и линия университета Berkeley-BSD. Многие фирмы на основе этих версий разработали и поддерживают свои версии UNIX: SunOS и Solaris фирмы Sun Microsystems, UX фирмы Hewlett-Packard, XENIX фирмы Microsoft, AIX фирмы IBM, UnixWare фирмы Novell (проданный теперь компании SCO), и список этот можно еще долго продолжать.

Наибольшее влияние на унификацию версий UNIX оказали такие стандарты как SVID фирмы AT&T, POSIX, созданный под эгидой IEEE, и XPG4 консорциума X/Open. В этих стандартах сформулированы требования к интерфейсу между приложениями и ОС, что дает возможность приложениям успешно работать под управлением различных версий UNIX.

Независимо от версии, общими для UNIX чертами являются:

- многопользовательский режим со средствами защиты данных от несанкционированного доступа,
- реализация мультипрограммной обработки в режиме разделения времени, основанная на использовании алгоритмов вытесняющей многозадачности (preemptive multitasking),
- использование механизмов виртуальной памяти и свопинга для повышения уровня мультипрограммирования,
- унификация операций ввода-вывода на основе расширенного использования понятия "файл",
- иерархическая файловая система, образующая единое дерево каталогов независимо от количества физических устройств, используемых для размещения файлов,

- переносимость системы за счет написания ее основной части на языке C,
- разнообразные средства взаимодействия процессов, в том числе и через сеть,
- кэширование диска для уменьшения среднего времени доступа к файлам.

Далее мы подробно остановимся на основных концепциях версии UNIX System V Release 4, которая вобрала в себя лучшие черты линий UNIX System V и UNIX BSD.

Версия UNIX System V Release 4 - это незаконченная коммерческая версия операционной системы, т.к. в ее кодах отсутствуют многие системные утилиты, необходимые для успешной эксплуатации ОС, например утилиты администрирования или менеджер графического интерфейса. Версия SVR4 является скорее стандартной реализацией кода ядра, вобравшая в себя наиболее популярные и эффективные решения из различных версий ядра UNIX, такие как виртуальная файловая система VFS, отображаемые в память файлы и т.п. Код SVR4 (частично доработанный) лег в основу многих современных коммерческих версий UNIX, таких как HP-UX, Solaris, AIX и т.д.

Краткая история семейства протоколов TCP/IP

Мы приступаем к последней теме наших семинарских и практических занятий – введению в сетевое *программирование* в операционной системе UNIX.

Все многообразие сетевых приложений и многомиллионная всемирная компьютерная *сеть* выросли из четырехкомпьютерной сети ARPANET, созданной по заказу Министерства Обороны США и связавшей вычислительные комплексы в Стэнфордском исследовательском институте, Калифорнийском университете в Санта-Барбаре, Калифорнийском университете в Лос-Анджелесе и университете Юты. Первая передача информации между двумя компьютерами сети ARPANET состоялась в октябре 1969 года, и эту дату принято считать датой рождения нелокальных компьютерных сетей. (Необходимо отметить, что дата является достаточно условной, так как первая *связь* двух удаленных компьютеров через коммутируемые телефонные линии была осуществлена еще в 1965 году, а реальные возможности для разработки пользователями ARPANET сетевых приложений появились только в 1972 году.) Эта *сеть* росла и почковалась, закрывались ее отдельные части, появлялись ее гражданские аналоги, они сливались вместе, и в результате "что выросло – то выросло".

При создании ARPANET был разработан протокол сетевого взаимодействия коммуникационных узлов – *Network Control Protocol (NCP)*, осуществлявший *связь* посредством передачи *датаграмм* (см. лекцию 14, раздел "*Связь с установлением логического соединения и передача данных с помощью сообщений*"). Этот протокол был предназначен для конкретного архитектурного построения сети и базировался на предположении, что *сеть* является статической и настолько надежной, что компьютерам не требуется умения реагировать на возникающие ошибки. По мере роста ARPANET и необходимости подключения к ней сетей, построенных на других архитектурных принципах (пакетные спутниковые сети, наземные пакетные радиосети), от этого предположения пришлось отказаться и искать другие подходы к построению сетевых систем. Результатом исследований в этих областях стало появление *семейства протоколов TCP/IP*, на базе которого обеспечивалась надежная доставка информации *понеоднородной* сети. Это *семейство протоколов* до сих пор занимает ведущее *место* в качестве сетевой технологии, используемой в операционной системе UNIX. Именно поэтому мы и выбрали его для практической иллюстрации общих сетевых решений, изложенных в лекции 14.

Общие сведения об архитектуре семейства протоколов TCP/IP

Семейство протоколов TCP/IP построено по "слоеному" принципу, подробно рассмотренному в лекции (лекция 14, раздел "*Многоуровневая модель построения сетевых вычислительных систем*"). Хотя оно и имеет многоуровневую структуру, его строение отличается от строения эталонной модели OSI, предложенной стандартом ISO. Это и неудивительно, так как основные черты *семейства TCP/IP* были заложены до появления эталонной модели и во многом послужили толчком для ее разработки. В *семействе протоколов TCP/IP* можно выделить четыре уровня:

- *Уровень сетевого интерфейса.*
- *Уровень Internet.*
- *Транспортный уровень.*
- *Уровень приложений/процессов.*

Соотношение уровней *семейства TCP/IP* и уровней модели OSI/ISO приведено на [рисунке 15–16.1](#).



Рис. 15-16.1. Соотношение моделей OSI/ISO и TCP/IP

На каждом уровне *семейства TCP/IP* присутствует несколько протоколов. *Связь* между наиболее употребительными протоколами и их принадлежность уровням изображены на [рисунке 15-16.2](#).

Давайте кратко охарактеризуем каждый уровень семейства.

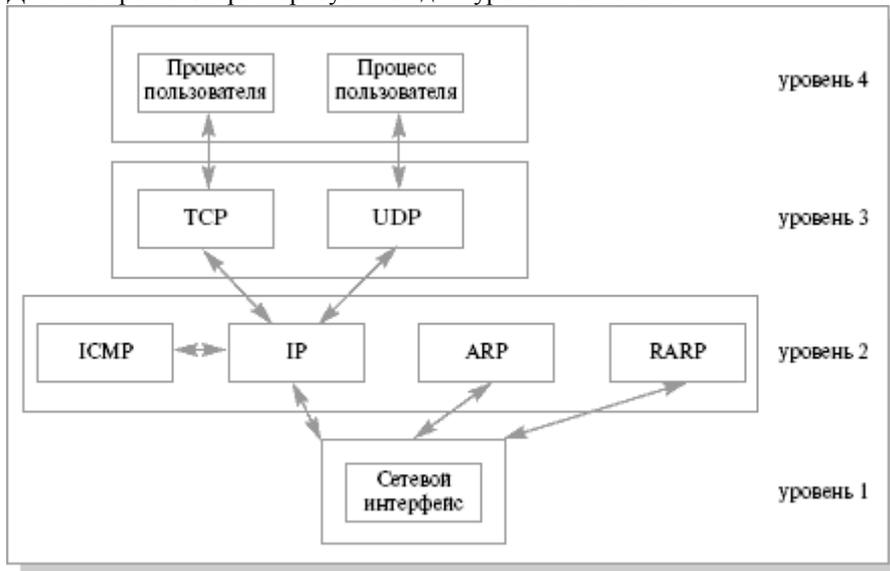


Рис. 15-16.2. Основные протоколы семейства TCP/IP

Уровень сетевого интерфейса

Уровень сетевого интерфейса составляют протоколы, которые обеспечивают передачу данных между узлами связи, физически напрямую соединенными друг с другом, или, иначе говоря, подключенными к одному сегменту сети, и соответствующие физические средства передачи данных. К этому уровню относятся протоколы Ethernet, Token Ring, SLIP, PPP и т.д. и такие физические средства как витая пара, коаксиальный кабель, оптоволоконный кабель и т.д. Формально *протоколы уровня сетевого интерфейса* не являются частью *семейства TCP/IP*, но существующие стандарты определяют, каким образом должна осуществляться *передача данных семейства TCP/IP* с использованием этих протоколов. На *уровне сетевого интерфейса* в операционной системе *UNIX* обычно функционируют драйверы различных сетевых плат.

Передача информации на *уровне сетевого интерфейса* производится на основании физических адресов, соответствующих точкам входа сети в узлы связи (например, физических адресов сетевых карт). Каждая точка входа имеет свой уникальный *адрес* – *MAC-адрес (Media Access Control)*, физически зашитый в нее на этапе

изготовления. Так, например, каждая сетевая *плата Ethernet* имеет собственный уникальный 48-битовый номер.

Уровень Internet. Протоколы IP, ICMP, ARP, RARP. Internet–адреса

Из многочисленных протоколов *уровня Internet* мы перечислим только те, которые будут в дальнейшем упоминаться в нашем курсе:

- **ICMP** – Internet Control Message Protocol. Протокол обработки ошибок и обмена управляющей информацией между узлами сети.

- **IP – Internet Protocol**. Это протокол, который обеспечивает доставку пакетов информации для *протокола ICMP* и протоколов *транспортного уровня* TCP и UDP.

- **ARP** – Address Resolution Protocol. Это протокол для отображения адресов *уровня Internet* в адреса *уровня сетевого интерфейса*.

- **RARP** – Reverse Address Resolution Protocol. Этот протокол служит для *решения обратной задачи*: отображения адресов *уровня сетевого интерфейса* в адреса *уровня Internet*.

Два последних протокола используются не для всех сетей; только некоторые сети требуют их применения.

Уровень Internet обеспечивает доставку информации от сетевого узла отправителя к сетевому узлу получателя без установления *виртуального соединения* с помощью *датаграмм* и не является надежным.

Центральным протоколом уровня является *протокол IP*. Вся информация, поступающая к нему от других протоколов, оформляется в виде *IP-пакетов* данных (*IP datagrams*). Каждый *IP-пакет* содержит адреса компьютера отправителя и компьютера получателя, поэтому он может передаваться *по* сети независимо от других пакетов и, возможно, *по* своему собственному маршруту. Любая ассоциативная *связь* между пакетами, предполагающая знания об их содержании, должна осуществляться на более высоком уровне семейства протоколов.

IP-уровень семейства TCP/IP не является уровнем, обеспечивающим надежную *связь*, так как он не гарантирует ни доставку отправленного пакета информации, ни то, что пакет будет доставлен без ошибок. *IP* вычисляет и проверяет контрольную сумму, которая покрывает только его собственный 20-байтовый заголовок для пакета информации (включающий, например, адреса отправителя и получателя). Если *IP-заголовок* пакета при передаче оказывается испорченным, то весь пакет просто отбрасывается. Ответственность за повторную передачу пакета тем самым возлагается на вышестоящие уровни.

IP протокол, при необходимости, осуществляет фрагментацию и дефрагментацию данных, передаваемых *по* сети. Если размер *IP-пакета* слишком велик для дальнейшей передачи *по* сети, то полученный пакет разбивается на несколько фрагментов, и каждый фрагмент оформляется в виде нового *IP-пакета* с теми же адресами отправителя и получателя. Фрагменты собираются в единое целое только в конечной точке своего путешествия. Если при дефрагментации пакета обнаруживается, что хотя бы один из фрагментов был потерян или отброшен, то отбрасывается и весь пакет целиком.

Уровень Internet отвечает за маршрутизацию пакетов. Для обмена информацией между узлами сети в случае возникновения проблем с маршрутизацией пакетов используется *протокол ICMP*. С помощью сообщений этого же протокола *уровень Internet* умеет частично управлять скоростью передачи данных – он может попросить отправителя уменьшить *скорость передачи*.

Поскольку на *уровне Internet информация* передается от компьютера-отправителя к компьютеру-получателю, ему требуются специальные *IP-адреса* компьютеров (а точнее, их точек подсоединения к сети – сетевых интерфейсов) – удаленные части полных адресов процессов (см. лекцию 14, раздел "Удаленная адресация и разрешение адресов"). Мы будем далее работать с *IP* версии 4 (*IPv4*), которая предполагает наличие у каждого сетевого интерфейса уникального 32-битового адреса. Когда разрабатывалось *семейство протоколов TCP/IP*, казалось, что 32 бита адреса будет достаточно для всех нужд сети, однако не прошло и 30 лет, как выяснилось, что этого мало. Поэтому была разработана версия 6 для *IP* (*IPv6*), предполагающая наличие 128-битовых адресов. С точки зрения сетевого программиста *IPv6* мало отличается от *IPv4*, но имеет более сложный *интерфейс* передачи параметров, поэтому для практических занятий был выбран *IPv4*.

Транспортный уровень. Протоколы TCP и UDP. TCP и UDP сокеты. Адресные пространства портов. Понятие encapsulation

Мы не будем вдаваться в детали реализации протоколов *транспортного уровня*, а лишь кратко рассмотрим их основные характеристики. К протоколам *транспортного уровня* относятся *протоколы TCP* и *UDP*.

Протокол TCP реализует *потокковую модель* передачи информации, хотя в его основе, как и в основе *протокола UDP*, лежит обмен информацией через пакеты данных. Он представляет собой ориентированный на установление логической связи (*connection-oriented*), надежный (обеспечивающий проверку контрольных сумм, передачу подтверждения в случае правильного приема сообщения, повторную передачу пакета данных в случае неполучения подтверждения в течение определенного промежутка времени, правильную последовательность получения информации, полный контроль скорости передачи данных) дуплексный способ связи между процессами в сети. **Протокол UDP**, наоборот, является способом связи ненадежным, ориентированным на передачу сообщений (*датаграмм*). От *протокола IP* он отличается двумя основными чертами: использованием для проверки правильности принятого сообщения контрольной суммы, насчитанной по всему сообщению, и передачей информации не от узла сети к другому узлу, а от отправителя к получателю.

Полный *адрес* удаленного процесса или промежуточного объекта для конкретного способа связи с точки зрения операционных систем определяется парой адресов: **<числовой адрес компьютера в сети, локальный адрес>**.

Такая пара получила название *socket* (гнездо, панель), так как *по* сути дела является виртуальным коммуникационным узлом (можно представить себе виртуальный *разъем* или ящик для приема/отправки писем), ведущим от объекта во внешний мир и наоборот. *Принепрямой адресации* сами промежуточные объекты для организации взаимодействия процессов также именуется *сокетами*.

Поскольку *уровень Internet семейства протоколов TCP/IP* умеет доставлять информацию только от компьютера к компьютеру, данные, полученные с его помощью, должны содержать тип использованного протокола *транспортного уровня* и локальные адреса отправителя и получателя. И протокол *TCP*, и *протокол UDP* используют *непрямую адресацию*.

Для того чтобы избежать путаницы, мы в дальнейшем термин "*сокет*" будем употреблять только для обозначения самих промежуточных объектов, а полные адреса таких объектов будем называть *адресами сокетов*.

Для каждого транспортного протокола в стеке *TCP/IP* существуют собственные *сокеты*: *UDP сокеты* и *TCP сокеты*, имеющие различные адресные пространства своих локальных адресов – **портов**. В *семействе протоколов TCP/IP* адресные пространства *портов* представляют собой положительные значения целого 16-битового числа. Поэтому, говоря о локальном *адресе сокета*, мы часто будем использовать термин "**номер порта**". Из различия адресных пространств *портов* следует, что *порт 1111 TCP* – это совсем не тот же самый локальный *адрес*, что и *порт 1111 UDP*. О том, как назначаются номера *портов* различным *сокетам*, мы поговорим позже.

Итак, мы описали иерархическую систему адресации, используемую в *семействе протоколов TCP/IP*, которая включает в себя несколько уровней:

- Физический пакет данных, передаваемый по сети, содержит физические адреса узлов сети (*MAC-адреса*) с указанием на то, какой протокол *уровня Internet* должен использоваться для обработки передаваемых данных (поскольку пользователя интересуют только данные, доставляемые затем на *уровень приложений/процессов*, то для него это всегда *IP*).
- *IP-пакет* данных содержит 32-битовые *IP-адреса* компьютера-отправителя и компьютера-получателя, и указание на то, какой вышележащий протокол (*TCP*, *UDP* или еще что-нибудь) должен использоваться для их дальнейшей обработки.
- Служебная информация транспортных протоколов (*UDP-заголовок* к данным и *TCP-заголовок* к данным) должна содержать 16-битовые номера *портов* для *сокета* отправителя и *сокета* получателя.

Добавление необходимой информации к данным при переходе от верхних уровней семейства протоколов к нижним принято называть английским словом *encapsulation* (дословно: герметизация). На [рисунке 15–16.5](#) приведена схема *encapsulation* при использовании *протокола UDP* на сети *Ethernet*.

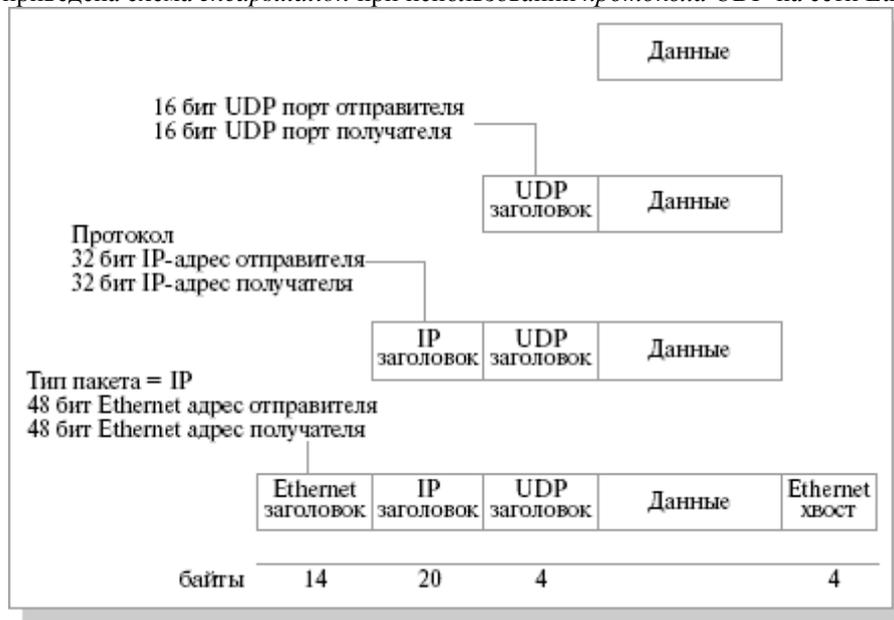


Рис. 15-16.5. Encapsulation для UDP-протокола на сети Ethernet

Поскольку между *MAC-адресами* и *IP-адресами* существует взаимно однозначное соответствие, известное *семейству протоколов TCP/IP*, то фактически для полного задания адреса доставки и адреса отправления, необходимых для установления двусторонней связи, нужно указать пять параметров:

<транспортный протокол, IP-адрес отправителя, порт отправителя, IP-адрес получателя, порт получателя>

АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

Виды адресации в компьютерных сетях

Для того, чтобы компьютеры могли идентифицировать друг друга в информационно-вычислительной сети, им присваиваются явные адреса. Основными типами адресов являются следующие:

- MAC-адрес;
- IP-адрес;
- доменный адрес;
- URL.

Физические адреса

MAC-адрес, который также называют *физическим адресом*, *Ethernet-адресом*, присваивается каждому сетевому адаптеру при его производстве. Его размер - 6 байт.

Этот сетевой адрес является уникальным, - фирмам-производителям выделены списки адресов, в рамках которых они обязаны выпускать карты. Адрес записывается в виде шести групп шестнадцатеричных цифр по две в каждой (шестнадцатеричная запись байта). Первые три байта называются префиксом (что определяет 2^{24} различных комбинаций или почти 17 млн адресов), и именно они закреплены за производителем.

Адаптер "слушает" сеть, принимает адресованные ему кадры и ширококвещательные кадры с адресом FF:FF:FF:FF:FF:FF и отправляет кадры в сеть, причем в каждый момент времени в сегменте узла сети находится только один кадр.

Собственно, MAC-адрес соответствует не компьютеру, а его сетевому интерфейсу. Таким образом, если компьютер имеет несколько интерфейсов, то это означает, что каждому интерфейсу будет назначен свой физический адрес. Каждой сетевой карте соответствует собственный MAC-адрес и IP-адрес, уникальный в рамках глобальной сети.

MAC-адреса используются на физическом и канальном уровнях, т.е. в "однородной" среде. Для того, чтобы могли связываться друг с другом компьютеры, входящие в большие составные сети, используется другой вид адресов - IP-адреса.

IP-адресация

IP-адрес является основным видом адресации в Internet. Он обозначает не только компьютер, но и сегмент сети, в котором находится данный компьютер. Например, адрес 192.123.004.010 соответствует узлу номер 10 в сети 192.123.004. У другого узла в этом же сегменте может быть номер 20 и т.д. Сети и узлы в них - это отдельные объекты с отдельными номерами.

IP-адрес -

представляет собой 32-разрядное двоичное число (например, 11000000 01111011 00001010). Для удобства оно разбивается на четыре восьмиразрядных поля, называемых *октетами*. TCP/IP представляет эти двоичные октеты их десятичными эквивалентами (в данном примере это 192.123.004.010), что облегчает использование IP-адресов для человека.

Классы IP-сетей

Эти четыре октета в разных сетях обозначают разные вещи. В некоторых организациях создается одна большая сеть, но с миллионами узлов. Здесь первый октет адреса используется для обозначения сети, а остальные три октета - для обозначения отдельных рабочих станций. Такой адрес называют адресом класса А. Самые частые потребители адресов класса А - поставщики сетевых услуг (провайдеры), которые обслуживают очень большие сети с тысячами конечных пунктов.

В некоторых организациях могут быть тысячи узлов, включенных в состав нескольких сетей. В таких случаях используются адреса класса В, в которых первые два октета (16 битов) используются для обозначения сети, а последние два - для обозначения отдельных узлов. Наиболее известные потребители адресов класса В - университеты и крупные учреждения.

Наконец, наиболее часто используется адрес класса С, в котором первые три октета (или 24 бита) служат для обозначения сегмента, а последний октет - для обозначения рабочих станций. Такие адреса лучше всего подходят для случая, когда имеется множество отдельных сетей, в состав каждой из которых входит всего несколько десятков узлов. Адреса такого типа чаще всего встречаются в локальных сетевых средах, где в одном сетевом сегменте в среднем бывает около 40 узлов.

При соединении сети класса А с сетью класса В маршрутизатору необходимо сообщить, как он должен отличать одну сеть от другой. В противном случае он подумает, что трафик, исходящий из сети класса С и предназначенный для узла класса, можно идентифицировать по последнему октету. На самом же деле узел класса А обозначается последними тремя октетами - а это большая разница. Не зная этого, маршрутизатор попытается найти трехоктетную сеть, к которой подключен однооктетный хост. На самом же деле ему нужно послать данные в однооктетную сеть, в которой находится трехоктетный хост.

Стек протоколов TCP/IP использует первые три бита первого октета для идентификации класса сети, позволяя устройствам автоматически распознавать соответствующие типы адресов. У адресов класса А первый бит установлен в 0, а остальные семь битов служат для идентификации сетевой части адреса (как вы помните, в адресах класса А первый октет служит для обозначения сети, а остальные три - для обозначения узлов). Поскольку можно использовать только семь битов, максимально возможное количество сетей - 128. Номера сетей 000 и 127 зарезервированы для использования программным обеспечением, поэтому это число уменьшается до 126 (001 - 126). Для обозначения узлов можно использовать 24 бита, поэтому для каждой из этих сетей максимальное число узлов составляет $16\,777\,216$.

У адресов класса В первый бит всегда устанавливается в 1, а второй в 0. Поскольку для обозначения сетей здесь используются два октета, то для каждого сетевого сегмента остается, таким образом, 14 битов. Следовательно, максимально возможное число адресов этого класса - 16 384, в диапазоне от 128.001 до 191.254 (номера 000 и 255 зарезервированы).

В адресах класса С первые два бита всегда равны 1, а третий установлен в 0. В этих адресах для обозначения сетей используются первые три октета, следовательно, остается 21 бит. Диапазон возможных номеров сетей - от 192.001.001 до 223.254.254, или 2 097 152 сегмента. При этом, однако, для обозначения узлов остается только один октет, поэтому в каждом сегменте может быть всего 254 устройства.

В таблице 1 приведены характеристики адресов сетей различных классов. Адреса класса D предназначены для широковещательной рассылки пакетов сразу группе машин. Адреса класса E пока не используются. Предполагается, что со временем они будут задействованы с целью расширения стандарта.

Таблица 1. Характеристика классов IP-адресов

Класс сети	Байт 1	Байт 2	Байт 3	Байт 4	
A	0	Номер сети	Номер хоста		
B	10	Номер сети		Номер хоста	
C	110	Номер сети			Номер хоста
D	1110				
E	11110				

Среди IP-адресов несколько зарезервировано под специальные случаи использования (табл. 2). Так, значение первого октета 127 зарезервировано для служебных целей, в основном, для тестирования сетевого оборудования, поскольку IP-пакеты, направленные на такой адрес, не передаются в сеть, а ретранслируются обратно управляющей надстройке сетевого программного обеспечения как только что принятые.

Таблица 2. Значение выделенных IP-адресов

IP-адрес	Значение
0.0.0.0	Данный компьютер
Номер сети.0	Данная IP-сеть
0.0.0.Номер узла	Узел в данной локальной сети
255.255.255.255	Все узлы в данной локальной сети
Номер сети.255	Все узлы указанной IP-сети

Централизованным распределением IP-адресов занимаются государственные организации. В США - Стенфордский международный научно-исследовательский институт (Stanford Research Institute), расположенный в г. Мэнло-Парк, штат Калифорния. Услуга по присвоению новой локальной сети IP-адресов бесплатная, и занимает она приблизительно неделю.

В небольших локальных сетях, использующих стек TCP/IP, можно назначать IP-адреса компьютерам произвольно - в том случае, если данные компьютеры не имеют непосредственного (прямого) выхода в Internet

Маски подсетей

Часто перед администраторами локальных сетей встает необходимость разбиения вверенной им сети на несколько подсетей. Делается это с помощью маски подсети. Маска подсети заставляет сетевое программное обеспечение иначе интерпретировать IP-адреса машин, входящих в сеть.

Рассмотрим, например, адрес хоста 192.123.004.010. Это адрес класса С, в котором первые 24 бита обозначают номер сети. Остальные 8 битов обозначают хост. Можно установить сетевую маску так, чтобы первые 25 битов обозначали сеть, а остальные 7 - хост.

Последние 8 битов администратор локальной сети может использовать так, как ему нужно. Можно их использовать обычным образом, для обозначения хост-машин. Но есть и другой вариант: назначить некоторые из оставшихся 8 битов подсетям. По сути дела, сетевая часть адреса получает еще одно поле, а диапазон номеров хостов сокращается.

Рассмотрим воображаемую компанию, Windows Inc., которая использует и сети Ethernet, и кольцевые сети с маркерным доступом. Ей выделен, однако, только один сетевой адрес класса С, 192.123.004. Вместо того чтобы использовать последний октет для обозначения 254 хостов в одной сети, компания решила ввести в адрес маску подсети, "позаимствовав" первый бит последнего октета. В результате создаются две подсети по 128 возможных хост-номера в каждой.

Изучая свои сетевые номера, Windows Inc. видит следующее:

Сегмент	Адрес сети	Адреса узлов*
Ethernet	192.123.004	001-127
Token Ring	192.123.004	128-254

*Номера 000 и 255 зарезервированы.

Следует, однако учесть, что устройства в сети не выполняют эту логическую разбивку автоматически. Основываясь на идентификаторе класса С в начале адреса, они продолжают считать, что последние 8 битов адреса обозначают хост. Поэтому о принятой маске нужно сообщить всем устройствам в сегменте сети.

В маске подсети используется очень простой алгоритм. Если бит маски установлен в 1, это часть номера сети. Если бит маски установлен в 0, это часть номера хоста. Следовательно, маска подсети для приведенного выше примера имеет вид 11111111 11111111 11111111 10000000.

Маска -

это число, двоичная запись которого содержит единицы в тех разрядах, которые должны интерпретироваться как номер сети.

В таблице 3 приведены стандартные маски подсетей для различных классов адресов сетей.

Таблица 3. Стандартные маски подсетей

Класс сети	Маска подсети	
	двоичное представление	десятичное представление
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Маска подсети должна применяться при обработке адреса маршрутизаторами. Если ранее маршрутизатор просто проверял, не совпадает ли адрес сети получателя, например, 192.123.004, с адресом какой-либо непосредственно подсоединенной к маршрутизатору сети, то теперь он должен использовать маску подсети, чтобы выделить адрес сети получателя. Чтобы маска подсети работала, ее должны поддерживать все устройства данной подсети.

Если сложить все возможные IP-адреса, то получится свыше 4,7 млрд. адресов хостов. Это очень много, но, к сожалению, четырехоктетной структуре присущи серьезные ограничения. Каждый раз, когда какой-то организации назначается адрес класса А, с ним уходит около 17 млн. адресов хостов. Если назначить все 126 адресов класса А, то свыше 3 млрд. из наличных 4,7 млрд. адресов окажутся занятыми. Если назначить все 16000 адресов класса В, уйдет еще миллиард. При этом не важно, используются ли выделенные адреса или нет: все они назначены конкретной сети и повторно использоваться не могут.

Самая большая проблема, однако, связана с классом С. Тому есть две причины. Во-первых, этих адресов меньше всего (имеется лишь около 500 млн. адресов узлов). Во-вторых, эти адреса самые популярные, потому что удовлетворяют размерам большинства локальных сетей. Каждый раз, когда сетевому сегменту выделяется адрес класса С, с ним уходит 254 возможных адреса узлов. Вспомним, что для каждой отдельной сети нужен новый номер. Поэтому люди, у которых три сегмента и всего 60 узлов, тратят впустую более 700 возможных адресов рабочих станций (3 сегмента \times 254 адреса узлов = 762 адреса - 60 активных узлов = 702 незадействованных адреса). Понятно, что при таких темпах "расходования" наличные хост-номера фактически уже закончились.

По действующей схеме (протокол IPv4) может быть всего 2113662 сети. Если бы для обозначения сегмента все сети применяли первые 24 бита (не используя "классовые" биты), то максимальное число сетей составило бы 16777216, по 254 узла в каждой.

Вспомним, однако, что сети TCP/IP изначально рассчитаны на использование маршрутизаторов. Естественно, узлам и маршрутизаторам проще запомнить несколько сетей, чем множество. Необходимость обработки 16 миллионов адресов сетей быстро переполнила бы базы данных маршрутизаторов, и сетевой трафик существенно замедлился бы. Наличие классов сетей позволяет маршрутизаторам легко работать с большими сетями, причем без ущерба для производительности.

Следует также помнить, что первоначально Internet состояла, в основном, из крупных сетей, соединенный друг с другом. Было удобно дать один адрес сети milnet (это сеть несекретных военных компьютеров), а другой - сети NSFnet (это сеть Национального научного фонда США). Благодаря этому маршрутизаторам, для того чтобы передавать данные буквально на миллионы хост-машин, достаточно было запомнить только адрес другого маршрутизатора.

На сегодняшний день, однако истощение запаса адресов порождает огромные проблемы. При отсутствии адресов ни одна новая организация не сможет подключиться к Internet, а существующие сети не смогут расширяться. Для решения большинства этих проблем разработана новая версия протокола IP - IPv6 (или IPng - IP next generation).

Система доменных имен

IP-адресация удобна для машинной обработки таблиц маршрутов, однако сложна для использования человеком. Система доменных имен (Domain Name System - DNS) позволяет присваивать компьютерам легко запоминаемые имена, например, yahoo.com, и отвечает за перевод этих имен в IP-адреса.

DNS строится по иерархическому принципу, однако эта иерархия не является строгой. Фактически нет единого корня всех доменов Internet. В 80-е гг. были определены первые домены (национальные, США) верхнего уровня: gov, mil, edu, com, net. Позднее появились национальные домены других стран: uk (Великобритания), jp (Япония), au (Австрия), cn (Китай) и т.п. Для СССР был выделен домен su, однако после приобретения республиками Союза суверенитета многие из них получили собственные домены: ua - Украина, ru - Россия и т.п.

В настоящее время существуют домены верхнего уровня **com** - для коммерческих компаний, **edu** - для школ и университетов, **org** - для прочих организаций, **net** - для сетевых организаций и т.д.

Вслед за доменами верхнего уровня следуют домены, определяющие либо регионы, либо организации; следующие уровни иерархии могут быть закреплены за небольшими организациями, либо за подразделениями больших организаций.

Таким образом, доменное имя компьютера имеет, по меньшей мере, два уровня доменов. Каждый уровень отделяется от другого точкой. Слева от домена верхнего уровня располагается другое имя и, возможно, не одно. Все, что находится слева, является поддоменом для общего домена. Так, например, в имени `somesite.russia.ru` слово `somesite` является поддоменом `russia`, который, в свою очередь, является поддоменом домена `ru`.

DNS-серверы, реализующие перевод IP-адресов в доменные и обратно, устанавливаются обычно на машинах, которые являются шлюзами для локальных сетей. Вообще говоря, сервер имен может быть установлен на любой компьютер локальной сети. При выборе машины для установки сервера имен следует принимать в расчет то обстоятельство, что многие реализации серверов держат базы данных имен в оперативной памяти. При этом часто подгружается информация и с других серверов. Все это может вызвать задержки при разрешении запроса на адрес по имени машины, если для сервера имен будет использоваться маломощный компьютер.

Универсальная идентификация ресурсов (URL)

Понятие URL

URL (Uniform Resource Locator - универсальный указатель ресурсов) -

система обозначений для однозначной идентификации компьютера, каталога или файла в Internet.

В систему URL заложены следующие принципы:

- *Расширяемость* - новые адресные схемы должны легко вписываться в существующий синтаксис URL; расширяемость достигается за счет выбора определенного порядка интерпретации адресов, который базируется на понятии "адресная схема". Идентификатор схемы стоит перед остатком адреса, отделен от него двоеточием и определяет порядок интерпретации остатка.

- *Полнота* - по возможности любая из существовавших схем должна описываться посредством URL.

- *Читаемость* - адрес должен легко пониматься человеком, что вообще характерно для технологии WWW, - документы вместе с ссылками могут разрабатываться в обычном текстовом редакторе.

Формат URL включает:

- схему адреса (тип протокола доступа - `http`, `gopher`, `wais`, `telnet`, `ftp` и т.п.);
- IP- или доменный адрес машины;
- номер TCP-порта;
- адрес ресурса на сервере (каталог или путь к файлу);
- имя HTML-файла или метку;
- критерий поиска данных.

Для каждого вида протокола приложений выбирается свое подмножество полей из представленного выше списка. Прежде чем рассмотреть различные схемы представления адресов, приведем пример простого адреса URL:

<http://astra.net.ru/master/index.html>

В данном случае путь состоит из доменного адреса машины, на которой установлен сервер HTTP, и пути от корня дерева сервера к файлу `index.html`.

Кроме подобной *полной* записи URL существует *упрощенная*, которая предполагает, что к моменту ее использования многие основные компоненты адреса ресурса уже определены (протокол, адрес машины в сети, некоторые элементы пути). В таком случае достаточно указывать только адрес, относительный определенных базовых ресурсов - *относительный адрес*.

Схемы URL

Рассмотрим несколько различных схем URL, с помощью которых можно обратиться к различным информационным ресурсам Internet.

Схема HTTP -

основная для Web. Она содержит идентификатор, адрес машины, TCP-порт, путь в директории сервера, поисковый критерий и метку.

Приведем несколько примеров URL для схемы `http`:

- В наиболее распространенном виде URL, применяемом в документах WWW, вслед за именем схемы (`http`) следует путь, состоящий из доменного адреса машины и полного адреса `html`-документа в дереве Web-сервера:

<http://astra.net.ru/vebmaster/quest/default.html>

- В качестве адреса машины допустимо использование и IP-адреса:

<http://144.206.160.40/risk/risk01.html>

- Если сервер протокола `http` запущен на обслуживание отличного от стандартного 80 порта, то это отражается в адресе:

<http://144.206.130.137:8080/alta/vista.html>

- При указании адреса ресурса возможна ссылка на точку внутри html-файла. Для этого вслед за именем документа может быть указана метка внутри html-документа:

<http://astra.net.ru/alta/volume04.html#first>

Символ "#" отделяет имя документа от имени метки.

- Другая возможность схемы http - передача параметров. Первоначально предполагалось, что в качестве параметров будут передаваться ключевые слова, но, по мере развития механизма CGI-скриптов, в качестве параметров стала передаваться и другая информация:

<http://astra.net.ru/index.html?keyword1+keyword2>

В данном примере предполагается, что файл index.html - документ с возможностью поиска по ключевым словам.

- При использовании Web-форм параметры передаются как именованные поля:

<http://astra.net.ru/index.html?field1=value1+field2=value2>

Схема ftp -

позволяет адресовать файловые FTP-архивы из программ-клиентов World Wide Web. При этом возможно указание не только имени схемы, адреса FTP-архива, но и идентификатора пользователя и даже его пароля.

- Наиболее часто данная схема используется для доступа к публичным архивам FTP:

<ftp://astra.net.ru/pub/index01.txt>

В данном случае записана ссылка на архив astra.net.ru с идентификатором "anonymous" (доступ для любых пользователей).

- Если необходимо указать идентификатор пользователя и его пароль, то можно это сделать перед адресом машины:

<ftp://login:password@users/local/>

В данном случае эти параметры отделены от адреса машины символом "@", а друг от друга - двоеточием.

Схема Gopher -

используется для ссылки на ресурсы распределенной информационной системы Gopher; состоит из идентификатора и пути, в котором указывается адрес Gopher-сервера, тип ресурса и команда Gopher:

- <gopher://gopher.com:70:7/software>

В данном примере осуществляется доступ к Gopher-серверу gopher.com через порт 70 для поиска (тип 7) слова software. Следует заметить, что тип ресурса, в данном случае - 7, передается не перед командой, а вслед за ней.

Схема mailto -

предназначена для отправки почты по стандарту RFC 822 (стандарт почтового сообщения). Общий вид схемы выглядит так:

<mailto:paul@quest.astra.com>

Схема news -

просмотр сообщений системы Usenet.

<news:comp.infosystems>

В данном примере пользователь получит идентификаторы статей из группы comp.infosystems в режиме уведомления. Можно получить и текст статьи, но тогда необходим ее идентификатор:

<news:086@comp.infosystems> (86-я статья из группы).

Схема nntp -

еще одна схема получения доступа к ресурсам Usenet, в которой, например, обращение к группе comp.infosystems для получения статьи 86 будет выглядеть так:

<nntp:comp.infosystems/086>

Следует обратить внимание на то, что адрес сервера Usenet не указан. Программа-клиент должна быть предварительно сконфигурирована на работу с одним из серверов Usenet. Сама служба Usenet является распределенным информационным ресурсом, и группа comp.infosystems на сервере в домене abc.com или где-либо еще в мире содержит одни и те же сообщения.

Схема telnet -

осуществляет доступ к ресурсу в режиме удаленного терминала. Обычно клиент вызывает дополнительную программу для работы по протоколу telnet. При использовании этой схемы необходимо указывать идентификатор пользователя, допускается использование пароля:

<telnet://login:password@astra.net.ru>

Схема wais -

предназначена для использования в распределенной информационно-поисковой системе WAIS, работающей в режимах поиска и просмотра. При поиске используется форма со знаком "?", отделяющим адресную часть от ключевых слов:

<wais://wais.think.com/wais?guide>

В данном случае обращаются к базе данных WAIS на сервере wais.think.com с запросом на поиск документов, содержащих слово guide. Сервер возвращает клиенту список идентификаторов документов, после получения которого можно использовать вторую форму схемы - wais-запрос на просмотр документа:

<wais://wais.think.com/wais/wtype/093=/user/letter.txt>, где 039 - идентификатор документа.

Схема file -

используется в локальном режиме:

<file:///C:/text/html/indes.htm>

В данном примере приведено обращение к локальному документу на персональном компьютере с ОС Windows.

Существует еще несколько схем URL. Однако они реально на практике не используются или находятся в стадии разработки, поэтому останавливаться на них мы не будем.

IP маршрутизация

Опр. Маршрутизация – это процесс передачи данных узлу адресата или промежуточному маршрутизатору.

Маршрутизация основана на таблицах маршрутов – это просто база данных, в которой хранятся соответствия между IP адресами сегментов и IP адресами интерфейсов маршрутизатора. Когда с какого-либо узла приходят данные, маршрутизатор проверяет таблицу маршрутов. Если данный узел-адресат (или его сетевой сегмент) не указан в таблице, то данные отправляются на шлюз по умолчанию. Если узел-адресат найден, данные отправляются адресату. Если узел-адресат не найден, то на узел-отправитель посылается сообщение об ошибке.

Пример процесса маршрутизации (рис. 8.1).

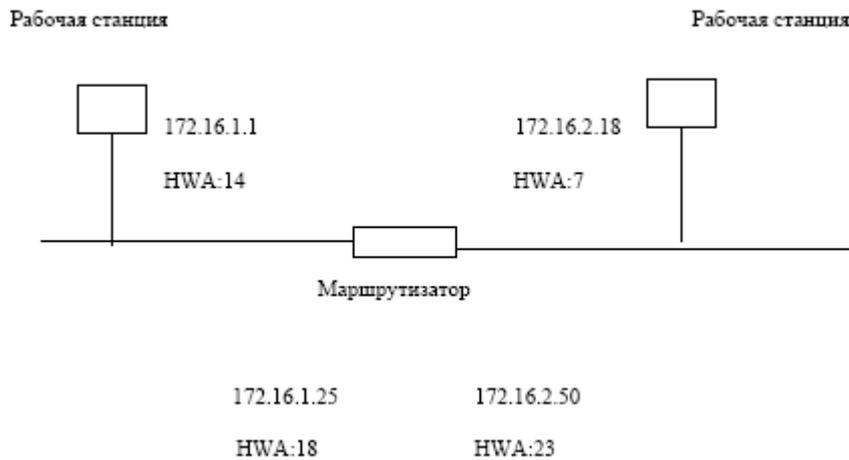


Рис.8.1 Простейшая маршрутизация

Существует два типа таблиц маршрутизации: статические и динамические. Системные администраторы должны создавать и обновлять статические таблицы маршрутизации вручную, поскольку таблицы не могут измениться без определенного вмешательства. Динамические таблицы маршрутизации создаются и поддерживаются автоматически при помощи протокола маршрутизации.

Статическая маршрутизация.

Статическая маршрутизация – встроенная функция IP и не требует каких-либо дополнительных служб для работы. Статическая таблица маршрутизации должна создаваться и поддерживаться на каждом маршрутизаторе вручную. Статическая таблица маршрутизации определяет связи между сетями и интерфейсами шлюза или маршрутизатора для доступа к ним. Статическая таблица маршрутизации состоит из следующих столбцов:

- Адрес сети. Адрес каждой известной сети, включая локальный адрес (0.0.0.0) и широковещательный адрес (255.255.255.255).
- Маска сети. Маска подсети, используемая для каждой из сетей.
- Адрес шлюза. IP –адрес входной точки (интерфейса маршрутизатора) для каждой сети.
- Интерфейс. IP, назначенный сетевому интерфейсу.
- Метрика. Число ретрансляций («хопов») для достижения сети.

В таблице. приведен пример таблицы маршрутизации

Таблица .

Сеть	Маска	Метрика	Интерфейс	Шлюз
0.0.0.0	0.0.0.0	1	10.57.11.169	10.57.8.2
127.0.0.0	255.0.0.0	1	127.0.0.1	127.0.0.1
10.57.8.0	255.255.248.0	1	10.57.11.169	10.57.11.169
10.57.11.169	255.255.255.255	1	127.0.0.1	127.0.0.1
10.57.255.255	255.255.255.255	1	10.57.11.169	10.57.11.169
224.0.0.0	224.0.0.0	1	10.57.11.169	10.57.11.169

Статический маршрутизатор может взаимодействовать только с теми сетями, которые были внесены в таблицу маршрутизации.

Команда route является утилитой TCP/IP, которая используется для создания или модификации статических таблиц маршрутизации. Эта команда имеет следующий синтаксис:

Route [-f] [-p] [команда [адресат] [маска] [шлюз] [метрика]]

Параметры имеют следующий смысл:

-f – удаление всех записей для шлюзов. Если этот параметр используется в сочетании с другими, то сначала производится удаление записей для шлюзов;

-p – добавить (при помощи команды add) постоянные записи. По умолчанию добавляемые записи не сохраняются при перезапуске системы. Все постоянные пути могут выведены на экран при помощи команды print.

команда – может быть указана одна из четырех команд: print (вывести список путей), add (добавить путь), delete (удалить путь), change (изменить существующий путь);

адресат – определяет компьютер, которому нужно послать указанную команду;

маска – определяет маску подсети для указанного пути. По умолчанию используется 255.255.255.255;

шлюз – шлюз для указанного пути;

метрика – установка поля метрики в таблице маршрутизации в указанное значение. Может быть задано любое значение от 1 до 9999.

Команда tracer – это утилита TCP/IP, используемая из командной строки и предназначенная для проверки маршрутизации и измерения времени прохождения пакетов. Эта команда имеет следующий синтаксис:

```
tracert [-d] [-h количество_ретрансляций][-j список_систем][-w тайм-аут] имя_системы
```

Параметры имеют следующий смысл:

-d – не переводить IP-адреса в имена системы;

-h – количество_ретрансляций – максимально допустимое количество ретрансляций («хопов») при поиске системы;

-j – список_систем – свободный выбор пути среди систем в указанном списке;

-w - тайм_аут – ожидать каждый ответ указанное число миллисекунд;

имя_системы – имя системы, поиск пути к которой осуществляется.

Tracert – отличная утилита для проверки пути. Также можно использовать ее для определения скорости действия путей.

Динамическая маршрутизация.

Динамическая маршрутизация обычно предпочтительнее статической в больших сетях со сложной архитектурой, поскольку она позволяет избежать утомительной ручной поддержки огромного количества таблиц маршрутизации. При динамической маршрутизации нагрузки на администратора сети минимальна и часто ограничивается просто указанием шлюза по умолчанию для каждого маршрутизатора. Все остальная настройка и создание таблицы маршрутизации происходит автоматически при помощи протокола маршрутизации.

Два наиболее часто используемых протокола для TCP/IP-маршрутизации – это RIP (Routing Information Protocol, протокол управления маршрутизацией) и OSPF (Open Shortest Path First, открой кратчайший путь первым). Оба эти протокола создают сетевой трафик при обновлении таблиц маршрутизации, но RIP является более «болтливым» протоколом по сравнению с OSPF (он передает по сети через регулярные промежутки времени все таблицы маршрутизации, в то время как OSPF передает по сети только изменения в таблицах).

Протокол RIP.

RIP – это ранний протокол, до сих пор распространенный ввиду простоты реализации. Таблица маршрутизации, поддерживаемая RIP, содержит следующую информацию:

- IP-адрес узла назначения;
- количество ретрансляций (хопов) от 1 до 15.;
- IP-адрес следующего маршрутизатора в пути;
- время доставки для каждого пути;
- время изменения информации в маршрутизации (время жизни).

Протокол RIP является дистанционно-векторным протоколом внутренней маршрутизации. RIP определяет количество ретрансляций для каждого из определенных путей и использует эту информацию для выбора наиболее эффективного пути. Если бы RIP не следил за количеством ретрансляций, могла бы возникнуть проблема подсчета бесконечности. В некоторых сетях, когда канал оказывается недоступным, RIP начинает последовательный поиск лучшего альтернативного пути, что может привести к возникновению логического цикла. Такой цикл может повторяться неограниченно. Чтобы избежать подобных ситуаций, RIP поддерживает счетчик ретрансляций, который может иметь значение от 1 до 15.

Протокол OSPF.

По сравнению с RIP OSPF является «протоколом второго поколения» и имеет множество преимуществ: OSPF создает меньшую нагрузку на сеть, поддерживает сети значительно большего размера, существенно менее «болтлив» и поддерживает множественные пути между узлом-отправителем и узлом-адресатом.

- Каждому каналу может быть присвоен свой вес (количество ретрансляций); - Ограничение на количество ретрансляций (хопов) – 65535;

- Каждый узел содержит базу сетевых путей в виде дерева, в вершине которого находится данный узел;

- Если существуют пути с одинаковым весом, нагрузка распределяется между ними;

- Широковещательные рассылки таблиц маршрутизации производится только при появлении изменений;

- Сообщения об изменениях в таблице маршрутизации отправляется только маршрутизатором, непосредственно связанным с данным метод «прочти сам и передай дальше» уменьшает нагрузку на сеть.

СЛУЖБА DNS И DHCP

DNS

Служба доменных имен (DNS) относится к прикладному уровню эталонной модели TCP/IP (рис. 10). Она переводит трудно воспринимаемые человеком IP-адреса в более удобочитаемый текстовый формат, а так же обеспечивает независимость от физического IP-адреса хоста. В самом деле, предположим, что владелец сайта решил сменить хост. Если бы поиск сайта осуществлялся по его IP, то пользователь, который знает прежний адрес сайта и ввел его в адресную строку в своем браузере, попал бы куда угодно, но не туда, куда ожидал. То же самое справедливо для электронной почты и прочих интернет-служб. Для того чтобы решить эти две проблемы, и была создана служба доменных имен.

В бытность существования ARPANET соответствия между IP-адресами и их текстовыми эквивалентами хранились в файле hosts.txt. Ежедневно все хосты получали этот файл, что обеспечивало актуальность (авторитетность) хранящихся в нем записей, и пока к сети было подключено несколько сотен машин, это было вполне приемлемым решением.

Но когда сеть разрослась до нескольких тысяч компьютеров, стало ясно, что этому механизму надо искать какую-то замену. В самом деле, размер файла становился слишком большим, а главное, в результате децентрализации неизбежно должны были возникнуть конфликты имен. Эту проблему была призвана решить служба доменных имен (Domain Name System, DNS).

Идея DNS состоит в разбиении всего адресного пространства на несколько непересекающихся зон (доменов), которые делятся на подзоны (поддомены).

Весь Интернет разделен на 200 доменов верхнего уровня, число которых постоянно увеличивается. Доменом называют множество хостов, объединенных в логическую группу. Каждый домен верхнего уровня подразделяется на поддомены, которые так же могут состоять из других доменов и т. д. (рис. 13,а).

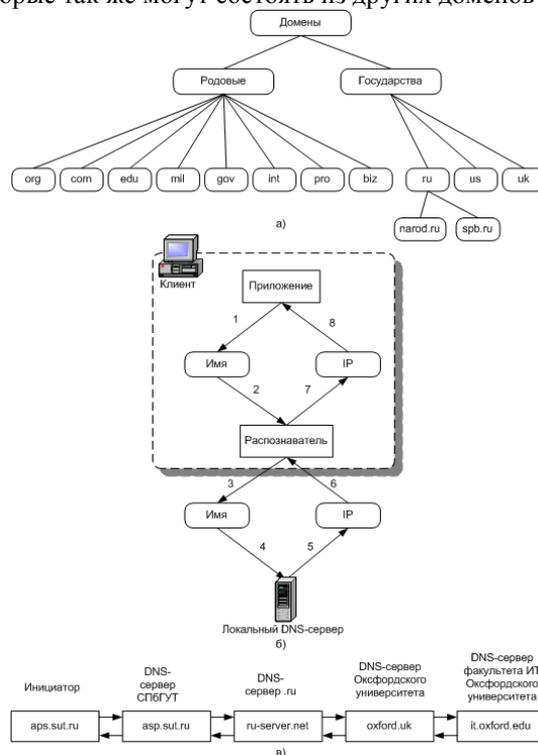


Рис. 13. Служба доменных имен (DNS)

Когда приложение, запущенное на машине клиента, хочет обратиться к хосту по его имени, то это имя передается распознавателю, который запущен на клиентской машине (рис. 13, б). Распознаватель обращается с запросом к одному из локальных DNS-серверов, и если требуемый домен относится к сфере ответственности данного DNS-сервера, то он сам передает распознавателю авторитетную запись ресурса. Если же DNS-сервер не имеет информацию о запрашиваемом домене, то он посылает сообщение с запросом серверу домена более высокого уровня.

Рассмотрим пример обработки запроса распознавателя, установленного на машине p.asp.sut.ru, подключенной к кафедральному серверу asp.sut.ru, к хосту a.it.oxford.edu (рис. 13,в). Сначала инициатор запроса p.asp.sut.ru посылает запрос кафедральному серверу asp.sut.ru, который переадресует его университетскому DNS-серверу sut.ru. Он ищет требуемую запись в собственной базе данных и, не найдя ее, передает запрос DNS-серверу зоны .ru. Последний находит адрес сервера Оксфордского университета (oxford.edu) и переадресует ему запрос, так как по принципу построения иерархических систем он не должен хранить имена доменов третьего уровня. DNS-сервер Оксфордского университета переадресует запрос DNS-серверу факультета информационных технологий (it.oxford.edu), который хранит запись с требуемым IP-адресом хоста a.it.oxford.edu, после чего результат передается назад по цепочке: it.oxford.edu – oxford.edu – ru-server.net – sut.ru – asp.sut.ru – p.asp.sut.ru (на самом деле, для повышения эффективности обработки запросов, DNS-серверы часто кэшируют информацию и хранят IP-адреса не только дочерних доменов, но и доменов не

находящихся в их прямой ответственности). Такая схема называется рекурсивным запросом, но возможны и другие схемы.

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) обеспечивает динамическую настройку параметров протокола TCP/IP на сетевых клиентах, чем существенно облегчает администрирование доменов службы каталогов Active Directory. При этом не только экономится время на настройку параметров системы, но и создается централизованный механизм изменения этих параметров. Для запуска службы DHCP в сети нужно настроить DHCP-сервер, предоставляющий клиентам сведения о сетевой конфигурации.

Знакомство с DHCP

DHCP - средство централизованного управления выделением IP-адресов, но этим его функции не ограничиваются. DHCP-сервер выдает клиентам основную информацию, необходимую для работы сети TCP/IP: IP-адрес, маску подсети, сведения о шлюзе по умолчанию, о первичных и вторичных DNS- и WINS-серверах, а также имя домена DNS.

Клиент DHCP и IP-адрес

Компьютер с динамическим IP-адресом называют *клиентом DHCP*. При загрузке компьютера DHCP-клиент запрашивает IP-адрес из пула адресов, выделенных данному DHCP-серверу, и использует адрес определенное время, называемое сроком аренды (lease). Спустя примерно половину этого срока клиент пытается возобновить аренду и повторяет эти попытки до успешного возобновления или до окончания срока аренды. Если возобновить аренду не удастся, клиент обращается к другому DHCP-серверу. Невозобновленный IP-адрес возвращается в пул адресов. Если клиент успешно связался с сервером, но его текущий IP-адрес не может быть возобновлен, DHCP-сервер присваивает клиенту новый IP-адрес.

DHCP-сервер обычно не влияет на процедуру загрузки или входа в сеть. Загрузка DHCP-клиента и регистрация пользователя в локальной системе возможна даже при неработающем DHCP-сервере.

Во время запуска DHCP-клиент пытается найти DHCP-сервер. Если это удалось, клиент получает от сервера нужную конфигурационную информацию. Если DHCP-сервер недоступен, а срок аренды клиента еще не истек, клиент опрашивает с помощью программы Ping стандартный шлюз, указанный при получении аренды. В случае успеха клиент считает, что, вероятно, находится в той же сети, в которой находился при получении аренды, и продолжает ею пользоваться. Неудачный опрос означает, что, возможно, клиент находится в другой сети. Тогда применяется автоконфигурация IP. Клиент также прибегает к ней, если DHCP-сервер недоступен, а срок аренды истек.

Авто конфигурация IP работает следующим образом.

1. Компьютер клиента выбирает IP-адрес из зарезервированной Microsoft подсети класса B - 169.254.0.0, маска подсети 255.255.0.0. Прежде чем задействовать IP-адрес, клиент проводит проверку по протоколу разрешения адресов (Address Resolution Protocol, ARP), чтобы убедиться, что выбранный IP-адрес не используется другим клиентом.
2. Если IP-адрес уже занят, клиент повторяет действие 1, пробуя до 10 IP-адресов, после чего сообщает об ошибке.
3. Если IP-адрес свободен, клиент настраивает сетевой интерфейс, используя этот адрес. Затем клиент пытается связаться с сервером DHCP, отправляя в сеть широковещательные запросы каждые 5 минут. Установив связь с сервером, клиент получает аренду и перенастраивает сетевой интерфейс.

Проверка назначения IP-адреса

Узнать выделенный компьютеру IP-адрес и другие сведения о конфигурации позволяет утилита Ipconfig. Чтобы получить информацию обо всех сетевых адаптерах компьютера, наберите в командной строке **ipconfig /all**. Если IP-адрес был назначен автоматически, вы увидите строку IP-адрес автонастройки (Autonfiguration IP Address). В приведенном ниже примере сетевому адаптеру автоматически назначен адрес 169.254.98.59:

Настройка протокола IP для Windows

```
Имя компьютера..... corpserver01
Основной DNS-суффикс..... mic rosoft. com
..... Тип узла гибридный
IP-маршрутизация включена. .... нет
WINS-прокси включен..... нет
..... Порядок просмотра суффиксов DNS microsoft. com
Подключение по локальной сети - Ethernet адаптер:
.....DNS-суффикс этого подключения .
.....Описание . NDC ND5300
PnP Ethernet адаптер
..... Физический адрес . 05-82-C6-F8-FD-67
```

..... DHCP включен	.	да
..... Автонастройка включена	.	да
..... IP-адрес автонастройки	.	169.254.98.59
..... Маска подсети	.	255.255.255.0
..... Основной шлюз	.	
..... DNS-серверы	.	

Области

Области (scopes) - это пулы IP-адресов, присваиваемых клиентам в процессе аренды и резервирования. Резервирование отличается от аренды тем, что назначенный компьютеру IP-адрес остается за этим компьютером, пока вы не отмените резервирование. Так можно присвоить постоянные адреса ограниченному кругу клиентов DHCP.

Посредством создания области вы ограничиваете диапазон IP-адресов, доступных клиентам DHCP. Например, для основной области предприятия можно выделить диапазон IP-адресов 192.168.12.2-192.168.12.250. В областях разрешается использовать открытые или частные IP-адреса:

- в сетях класса А:** 1.0.0.0-126.255.255.255;
- в сетях класса В:** 128.0.0.0-191.255.255.255;
- в сетях класса С:** 192.0.0.0-223.255.255.255;
- в сетях класса D:** 224.0.0.0-239.255.255.255.

4.3. Лабораторные работы

<i>№ п/п</i>	<i>Номер раздела дисциплины</i>	<i>Наименование лабораторной работы</i>	<i>Объем (час.)</i>	<i>Вид занятия в интерактивной, активной, инновационной формах, (час.)</i>
1	1.	Знакомство с учебным стендом. Основы коммутации.	3	Работа в малых группах (3 часа)
2	2.	Конфигурирование портов коммутатора.	3	Работа в малых группах (3 часов)
3	2.	Виртуальные локальные сети VLAN.	3	Работа в малых группах (3 часов)
4	2.	Применение алгоритма Spanning Tree.	3	Работа в малых группах (3 часов)
5	4.	Безопасность на основе сегментации трафика.	3	Работа в малых группах (3 часов)
6	4.	Адресация в IP-сетях. Основы коммутации третьего уровня.	2	Работа в малых группах (2 часов)
ИТОГО			17	17

4.4. Практические занятия

<i>№ п/п</i>	<i>Номер раздела дисциплины</i>	<i>Наименование практической работы</i>	<i>Объем (час.)</i>	<i>Вид занятия в интерактивной, активной, инновационной формах, (час.)</i>
1	1.	Эталонная модель взаимодействия открытых систем	3	-
2	2.	Расчет параметров кабельных сетей	3	-
3	3.	Сетевая операционная система UNIX.	3	-
4	4.	Адресация в компьютерных сетях, организация подсетей	3	-
5	4.	Таблицы маршрутизации, критерии маршрутизации.	3	-
6	4.	Функционирование системы доменных имен.	2	-
ИТОГО			17	-

4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

Учебным планом не предусмотрено

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<i>№, наименование разделов дисциплины</i>	<i>Компетенции</i>	<i>Кол-во часов</i>	<i>Компетенции</i>		Σ <i>комп.</i>	$t_{ср}$ час	<i>Вид учебных занятий</i>	<i>Оценка результатов</i>
			<i>ОПК</i>	<i>ПК</i>				
			3	13				
1	2	3	4	5	6	7	8	
1. Принципы построения компьютерных сетей. Сетевые протоколы.		19	+	+	2	9,5	Лк, ЛР, ПЗ, СРС	ЭКЗАМЕН
2. Среды доступа и технологии локальных и глобальных сетей.		25	+	+	2	12,5	Лк, ЛР, ПЗ, СРС	ЭКЗАМЕН
3. Сетевая операционная система Unix и сети TCP/IP.		18	+	+	2	9	Лк, ПЗ, СРС	ЭКЗАМЕН
4. Адресация и маршрутизация в компьютерных сетях.		29	+	+	2	14,5	Лк, ЛР, ПЗ, СРС	ЭКЗАМЕН
5. Службы DNS и DHCP.		17	+	+	2	8,5	Лк, СРС	ЭКЗАМЕН
<i>всего часов</i>		108	54	54	2	54		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц. (страницы 1-85)

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	Наименование издания	Вид занятия (Лк, ЛР, ПЗ)	Количество экземпляров библиотеке, шт.	Обеспеченность, (экз./чел.)
1	2	3	4	5
Основная литература				
1.	Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия-Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.	Лк, ЛР, ПЗ	10	0,67
2.	Берлин, А.Н. Высокоскоростные сети связи / А.Н. Берлин. – 2-е изд., испр. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 452 с. : ил. – Библиогр. В Н. ; То же [Электронный ресурс]. – URL: //biblioclub.ru/index.php?page=book&id=428941 (24.03.2017).	ЛК	ЭР	1
3	Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с..	Лк, ЛР, ПЗ	10	0,67
Дополнительная литература				
4	Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.	Лк, ПЗ, ЛР	50	1
5	Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.	Лк, ПЗ, ЛР	6	0,4
6	Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.	ЛР	50	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ
<http://ecat.brstu.ru/catalog> .

3. Электронно-библиотечная система «Университетская библиотека online»
<http://biblioclub.ru> .

4. Электронно-библиотечная система «Издательство «Лань»
<http://e.lanbook.com> .
5. Информационная система "Единое окно доступа к образовательным ресурсам"
<http://window.edu.ru> .
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru> .
7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
<https://uisrussia.msu.ru/> .
8. Национальная электронная библиотека НЭБ
<http://xn--90ax2c.xn--p1ai/how-to-search/> .

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1. Методические указания для обучающихся по выполнению лабораторных работ и практических работ

Лабораторная работа №1

Знакомство с учебным стендом. Основы коммутации

Цель работы:

Изучение структуры стенда, способов коммутации его составляющих. Получение навыков использования утилит для изучения трафика и мониторинга сети. Изучение основных принципов коммутации Второго уровня.

Задание:

1. Получение навыков использования утилит для изучения трафика и мониторинга сети
2. Изучение основных принципов коммутации Второго уровня

Порядок выполнения:

1. С помощью проводов соедините patch-панель и коммутаторы таким образом, чтобы получить топологию, представленную на рис. 1

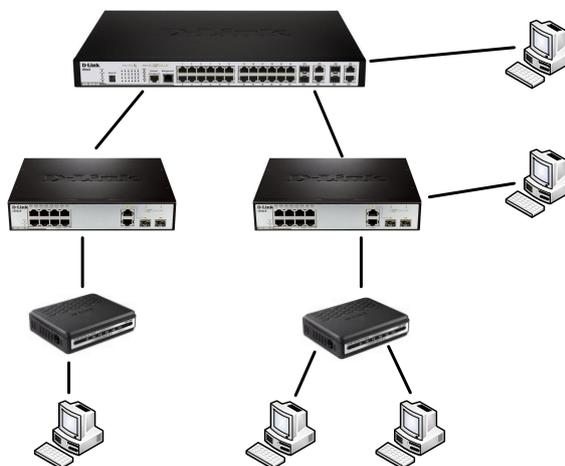


Рис. 1. Топология сети

2. Включите рабочие станции и зарегистрируйтесь на них
3. Задайте ip- адреса рабочим станциям.
4. Подключитесь к Web-интерфейсу управления коммутатором. Зарегистрируйтесь на коммутаторе.
5. Изучите раздел «Утилиты мониторинга сети» теоретического пособия.
6. С помощью утилиты ipconfig определите параметры вашего узла. Отметьте MAC и IP – адреса всех компьютеров.
7. С помощью утилиты ping проверьте связь каждой рабочей станции со всеми другими рабочими станциями созданной сети.
8. С помощью утилиты arp просмотрите таблицу ARP на каждой рабочей станции.

9. Назначьте коммутатору IP – адрес из диапазона свободных адресов IP- сети, в которой находятся рабочие станции. Определите MAC – адрес коммутатора.
10. С помощью системной утилиты коммутатора Ping test в разделе Monitoring проверить связь коммутатора с каждой машиной в сети.
11. С помощью утилиты arp просмотрите таблицу ARP на каждом коммутаторе.
12. Используя утилиту *tcpdump* на любой из машин в сети, убедиться в том, что до заданной машины доходят ICMP-запросы от коммутатора.
13. Сбросьте настройки коммутатора в заводские и перезагрузите его.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в первом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Для чего предназначена утилита ipconfig?
2. Для чего предназначена утилита arp?
3. Для чего предназначена утилита ping?

Лабораторная работа №2

Конфигурирование портов коммутатора

Цель работы:

Изучение конфигурирования портов, зеркалирование портов и построение магистральных линий связи.

Задание:

1. Изучить теоретический материал достаточный для выполнения лабораторной работы.
2. Произвести настройку портов.

Порядок выполнения:

1. Постройте топологию сети, показанную на рис.2.

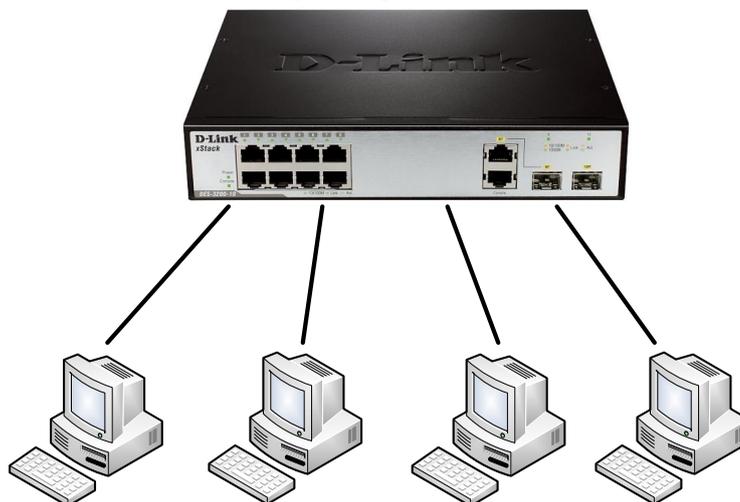


Рис. 2. Топология сети

2. С помощью утилиты `iperf` произвести тест скорости соединения с каждой рабочей станцией.
3. После этого задать портам коммутаторов, соответствующим двум рабочим станциям, скорость и режим работы 10М с полным дуплексом. Осуществить повторный тест скорости и сравнить результаты
4. С помощью меню «PortSettings» закрыть доступ к произвольной рабочей станции. С помощью утилит попробуйте осуществить взаимодействие между компьютерами.
5. Изучите раздел зеркалирования.
6. Настройте зеркало на любом из портов коммутатора, к которому подключена рабочая станция.
7. Запустите на рабочей станции, подключенной к порту- приемнику (зеркалом) утилиту `tcpdump`. Активизируйте сетевую активность.
8. Аналогично запустите данную утилиту на рабочей станции, подключенной к порту-источнику.
9. Сравните результаты работ утилит на обеих машинах.
10. Сбросьте настройки коммутатора в заводские настройки
11. Постройте топологию сети, показанную на рис. 3

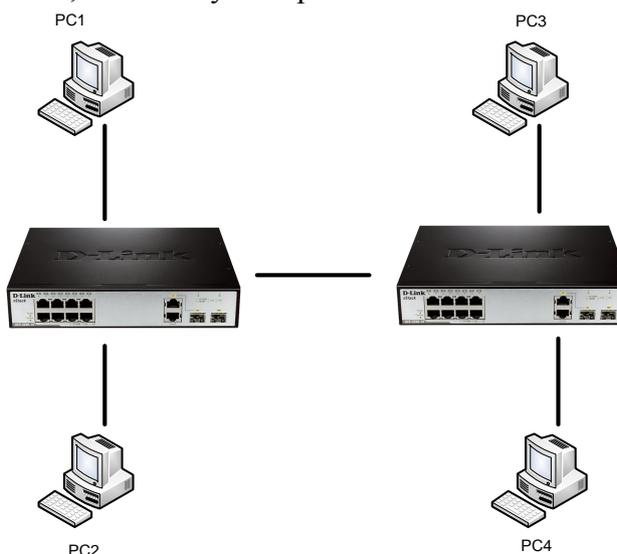


Рис. 3. Топология сети

12. С помощью утилиты `ftp`, одновременно запустить процесс передачи файла с PC1 на PC3 и с PC2 на PC4. С помощью данной утилиты замерить скорость и время передачи файла.
13. Создайте магистраль между коммутаторами, включающими 3 порта.

14. Одновременно запустите процесс передачи с PC1 на PC3 и с PC2 на PC4. Сравните скорость и время передачи с результатами пункта 13.
15. Удалите созданную магистраль и соедините коммутаторы через гигабитные порты.
16. Одновременно запустите процесс передачи с PC1 на PC3 и с PC2 на PC4. Сравните скорость и время передачи с результатами пункта 13 и 15. Сделайте вывод
17. Сбросьте настройки коммутатора в заводские и перезагрузите его.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным во втором разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Что такое зеркалирование портов?
2. Каким образом организуется магистральное соединение?
3. Для каких целей создается магистральное соединение?

Лабораторная работа №3

Виртуальные локальные сети VLAN

Цель работы:

Изучение технологий виртуальных сетей. Получение навыков настройки VLAN на основе тэгов IEEE 802.1q в сети, построенной на коммутаторах D-Link.

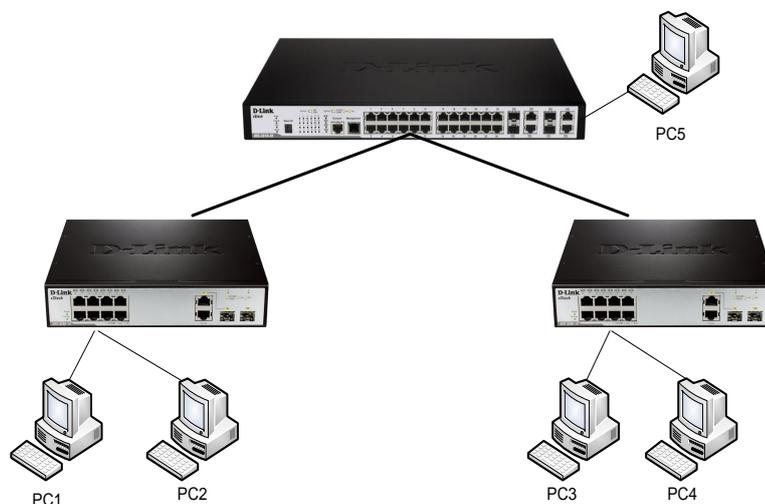
Задание:

1. Изучить работу VLAN.
2. Произвести настройку VLAN.

Порядок выполнения:

1. Постройте топологию сети, представленную на рис. 4

2. Сконфигурируйте VLAN на основе тегов таким образом, чтобы рабочие станции PC1 и PC3 принадлежали виртуальной сети №1, PC2 и PC4 – виртуальной сети №2, а PC5 являлась общедоступным ресурсом для обеих виртуальных сетей (таб. 1).
3. Проверьте правильность конфигурации сети. Результаты мониторинга покажите и поясните преподавателю.
4. Сбросьте настройки коммутатора в фабричные и перезагрузите его.



5. Рис .4. Топология сети

Таблица 1

№ станции	рабочей	Номер VLAN
1		1
2		2
3		1
4		2
5		1,2

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным во втором разделе данной дисциплины.

Основная литература

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Дать определение сетям VLAN.
2. Для чего необходимо использовать сети VLAN?
3. Как проверить правильность настройки сети VLAN?

Лабораторная работа №4

Применение алгоритма Spanning Tree.

Цель работы:

Изучения алгоритма Spanning Tree и Rapid Spanning Tree. Получение навыков построения сети с поддержкой резервных линий связи.

Задание:

1. Изучить принцип работы алгоритма Spanning Tree и Rapid Spanning Tree.
2. Построить сеть с поддержкой резервных линий связи.

Порядок выполнения:

1. Соберите сеть с топологией, представленной на рис 5.
2. Активизируйте на всех коммутаторах протокол Spanning Tree.
3. Настройте приоритеты коммутаторов и портов таким образом, чтобы получить сеть, показанную на рис. 6 (курсивом показана резервная связь).
4. С помощью системы мониторинга убедитесь, что через порт коммутатора DES-3200-10 #2 отмеченного черным квадратом, трафик не идет. Проверьте остальные задействованные в работе порты. Результаты мониторинга сохраните.
5. Имитируйте сбой в сети, нарушив соединение, выделенное на рис. 6 жирной линией. В соответствии с алгоритмом Spanning Tree сеть должна быть переконфигурирована. Убедитесь в этом с помощью системы мониторинга коммутаторов. Определите время сходимости сети. Результаты сохраните.

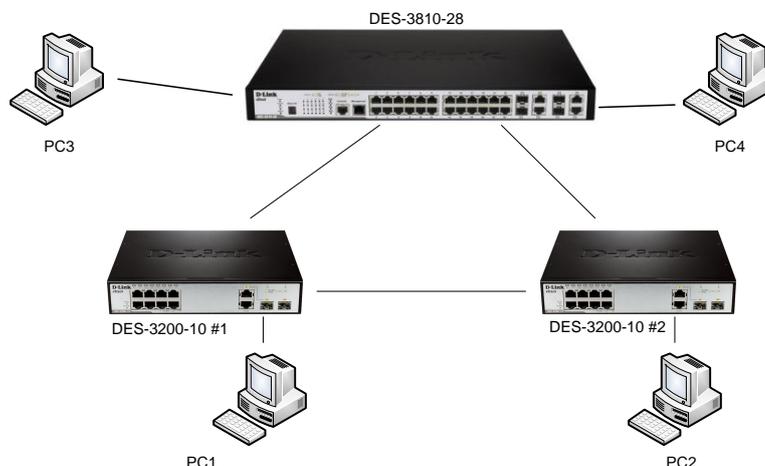


Рис. 5 Топология сети

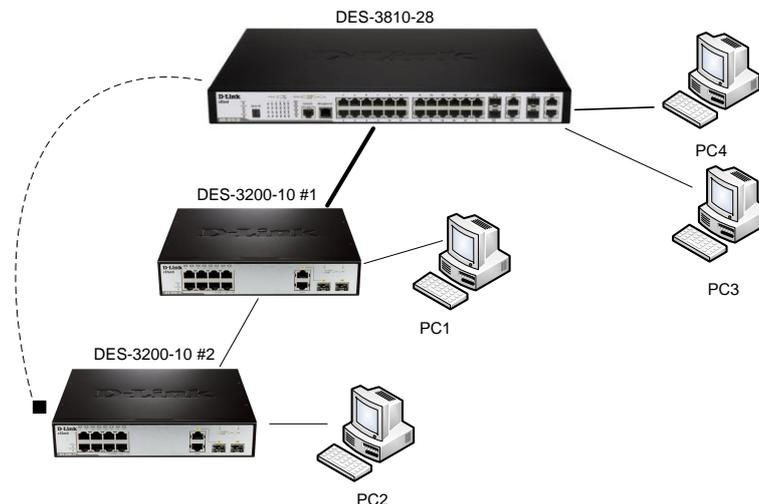


Рис.6. Топология сети

6. Активизируйте на всех коммутаторах протокол Rapid Spanning Tree.
7. Повторите действия пунктов 3-5.
8. Сравните времена сходимости, полученные при использовании двух протоколов: STP и RSTP. Сделайте выводы.
9. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным во втором разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Дать определение алгоритма Spanning Tree.
2. Дать определение алгоритма Rapid Spanning Tree.

3. В чем отличие между ними?

Лабораторная работа №5

Безопасность на основе сегментации трафика.

Цель работы:

Изучение механизма сегментации трафика.

Задание:

1. Изучить принцип работы механизма сегментации трафика.

Порядок выполнения:

1. Соберите топологию сети, представленную на рис.7

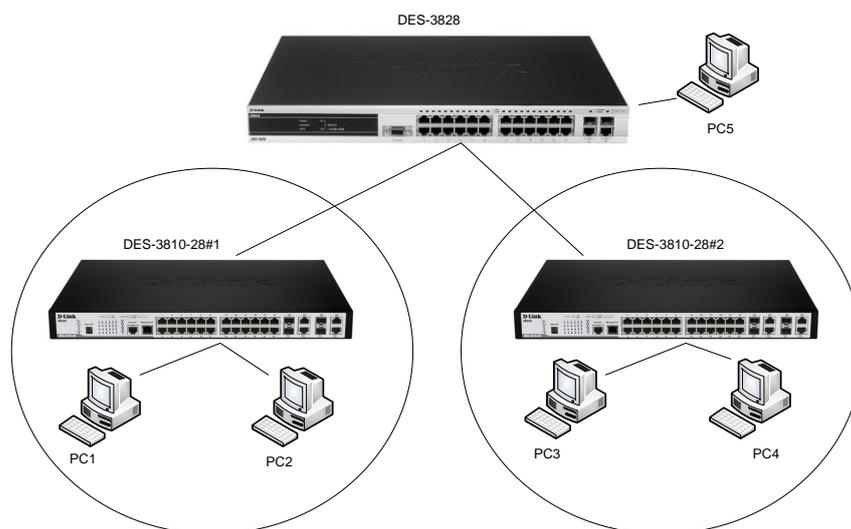


Рис. 7. Топология сети

2. Назначьте каждому компьютеру IP-адрес из одной подсети.
3. Организуйте работу сети таким образом, чтобы все рабочие станции не могли «видеть» друг друга, а только PC5 и PC6.
4. Подтвердите правильность сделанных настроек.
5. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в четвертом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Дать определение сегментации трафика?
2. Для чего применяется сегментация?
3. В чем преимущество данного метода перед остальными?

Лабораторная работа №6

Адресация в IP-сетях. Основы коммутации третьего уровня.

Цель работы:

Изучение принципов работы коммутатора уровня 3.

Задание:

1. Изучить принцип работы коммутатора уровня 3.

Порядок выполнения:

1. Соберите сеть с топологией, представленной на рис. 8.
2. Включите машины в виртуальные сети, а виртуальные сети в IP-подсети в соответствие с таблицей 2
3. Назначьте каждой машине IP-адрес из подсети, в которую она входит.
4. Проверить взаимодействие между всеми машинами.
5. С помощью утилиты traceroute выясните маршрут между любыми двумя машинами из разных подсетей.

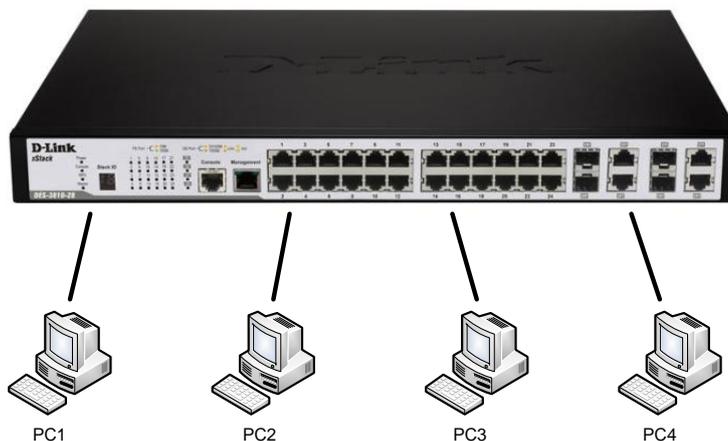


Рис. 8. Топология сети

Таблица 2

№ рабочей станции	VLAN	IP- подсеть
1	group1	192.168.2.1
2	group2	192.168.3.1
3	group2	192.168.3.1
4	group3	192.168.4.1

6. Просмотрите содержимое ARP таблицы на коммутаторе и выясните MAC-адреса машин по их IP-адресу.
7. Запустите FTP-сервер на машине № 1

8. Используя протокол FTP, скачайте файл (находится на рабочем столе) с машины №3 на машину № 1. Запомните время скачивания.
9. Соберите сеть с топологией, представленной на рис. 9 и повторите действия пункта 8.

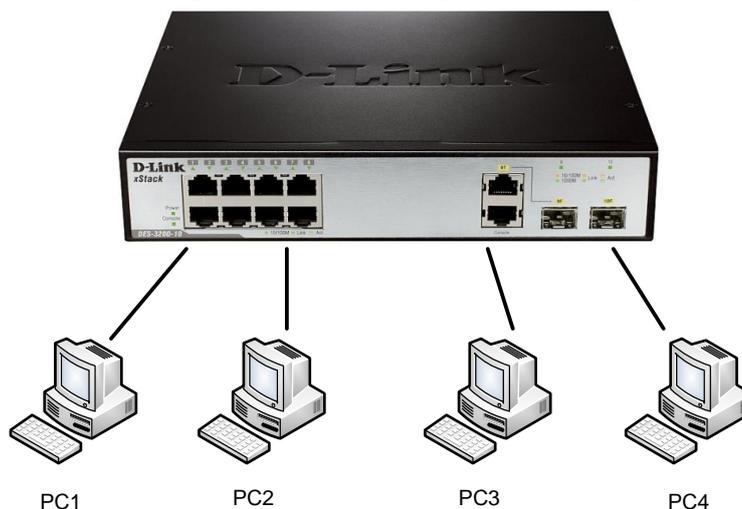


Рис. 9. Топология сети

10. Сравните времена скачивания одного и того же файла для сетей, построенных на различных принципах (уровнях) коммутации. Сделайте выводы.
11. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в четвертом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.
3. Колтыгин, Д. С. Сети ЭВМ и телекоммуникации : лабораторный практикум / Д. С. Колтыгин, И. А. Седельников. – Братск : БрГУ, 2013. – 85 с. – Б. ц.

Контрольные вопросы для самопроверки

1. Назначение утилиты traceroute ?

2. Что такое FTP сервер?
3. В чем отличии коммутации третьего уровня от остальных?

Практическое занятие №1

Эталонная модель взаимодействия открытых систем.

Цель работы:

Познакомиться с эталонной моделью взаимодействия открытых систем.

Задание:

1. Получить навыки работы с эталонной моделью взаимодействия открытых систем.

Порядок выполнения:

Изучить теоретические данные. Познакомиться с требованиями, предоставляемыми к системам электрической связи. Познакомиться с моделью взаимодействия открытых систем.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Ознакомиться с теоретическим материалом, представленным в первом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Какие требования предоставляются системам электрической связи?
2. Как эти требования классифицируются?
3. Что из себя представляет модель взаимодействия открытых систем?

Практическое занятие №2

Расчет параметров кабельных сетей.

Цель работы:

Приобрести навыки расчета параметров кабельных сетей.

Задание:

1. Познакомиться с основными параметрами кабельных сетей.

Порядок выполнения:

Изучить теоретические данные. Познакомиться со стандартом ISO/IEC 11801:2002. Изучить «парадокс стандартов». Изучить необходимое и достаточное условия нормального функционирования оптических трактов СКС.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Ознакомиться с теоретическим материалом, представленным во втором разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Что входит в стандарт ISO/IEC 11801:2002?
2. Что представляет собой «парадокс стандартов»
3. Перечислить необходимые и достаточные условия нормального функционирования оптических трактов СКС

Практическое занятие №3

Сетевая операционная система UNIX.

Цель работы:

Познакомиться с причинами возникновения операционной системы Unix.

Задание:

1. Познакомиться с ОС Unix.

Порядок выполнения:

Изучить теоретические данные. Изучить историю вопроса. Изучить основные отличия Unix от Windows. Изучить перспективы развития данной ОС.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Чем отличается ОС Unix от остальных ОС?
2. Когда был выпущен первый коммерческий образец данной ОС?
3. Для кого разрабатывалась данная ОС?

Практическое занятие №4

Адресация в компьютерных сетях, организация подсетей.

Цель работы:

Приобрести навыки работы с различными адресациями в компьютерных сетях, а также навыки организации подсетей.

Задание:

1. Изучить теоретические основы.
2. Получить навыки адресации ив компьютерных сетях и организации подсетей.

Порядок выполнения:

Изучить теоретические данные. Изучить основные принципы адресации. Познакомиться с основными требованиями к адресации. Изучить основные схемы адресации. Познакомиться с основами организации подсетей.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:
Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию
Ознакомиться с теоретическим материалом, представленным в четвертом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Основные принципы адресации.
2. Основными требованиями к адресации.
3. Основами организации подсетей.

Практическое занятие №5

Таблицы маршрутизации, критерии маршрутизации..

Цель работы:

Приобрести навыки организации различных схем маршрутизации. Изучить основные критерии маршрутизации.

Задание:

1. Изучить различные схемы маршрутизации.
2. Познакомиться с основными критериями маршрутизации.

Порядок выполнения:

Изучить теоретические данные. Изучить различные схемы маршрутизации и способы их реализации. Познакомиться с основными критериями маршрутизации

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:
Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию
Ознакомиться с теоретическим материалом, представленным в четвертом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.
2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Что такое маршрутизация?
2. Какие бывают схемы маршрутизации?
3. В чем их различия?

Практическое занятие №6

Функционирование системы доменных имен.

Цель работы:

Приобрести навыки работы с системой доменных имен.

Задание:

1. Изучить работу системы доменных имен.

Порядок выполнения:

Изучить теоретические данные. Изучить структуру системы доменных имен. Познакомиться с сервером доменных имен и клиентами ДНС.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Предусмотрены вариантом студента.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Ознакомиться с теоретическим материалом, представленным в четвертом разделе данной дисциплины.

Основная литература

1. Телекоммуникационные системы и сети. В 3 т. Т. 1-2 / под ред. В. П. Шувалова. – Москва : Горячая линия- Телеком. Т.1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. – 4-е изд., испр. И доп. – 2013. – 620 с.
2. Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учебник / А. И. Гусева, В. С. Киреев. – Москва : Академия, 2014. – 288 с.

Дополнительная литература

1. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : учебное пособие для вузов / С. В. Никифоров. – М. : Финансы и статистика, 2003. – 223 с.

2. Скляр, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляр. – 2-е изд., стереотип. – Санкт-Петербург : Лань, 2010. – 272 с.

Контрольные вопросы для самопроверки

1. Что такое система доменных имен?
2. В чем отличие прямой адресации и системы доменных имен?

12. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Информационно-коммуникационные технологии (ИКТ) – преподаватель использует для:

- получения информации при подготовке к занятиям,
- создания презентационного сопровождения лекций;
- интерактивного общения;
- ОС Windows 7 Professional;
- Microsoft Office 2007 Russian Academic OPEN No Level ;
- Антивирусное программное обеспечение Kaspersky Security

13. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

<i>Вид занятия</i>	<i>Наименование аудитории</i>	<i>Перечень основного оборудования</i>	<i>№ ЛР или ПЗ</i>
1	2	3	4
ЛР	Лаборатория «Управление в технических системах»	Лабораторный комплекс «Локальные сети ЭВМ» на 10 рабочих мест	ЛР 1-6
ПЗ	Лаборатория «Управление в технических системах»	Лабораторный комплекс «Локальные сети ЭВМ» на 10 рабочих мест	ПЗ 1-6
СР	ЧЗЗ	-	-

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ОПК-3	Способность владеть основными методами, способами средствами получения, хранения, переработки информации	1. Принципы построения компьютерных сетей. Сетевые протоколы.	1.1. Классификация компьютерных сетей.	Экзаменационный билет
			1.3. АТМ. Основные идеи технологии АТМ.	Экзаменационный билет
		2. Среда доступа и технологии локальных и глобальных сетей.	2.1. Ethernet. Физическая среда Ethernet.	Экзаменационный билет
			2.3. Технологии удалённого доступа.	Экзаменационный билет
		3. Сетевая операционная система Unix и сети TCP/IP.	3.1. История создания.	Экзаменационный билет
			3.3. Общие сведения об архитектуре семейства протоколов TCP/IP	Экзаменационный билет
			3.5. Уровень Internet. Протоколы IP, ICMP, ARP, RARP. Internet-адреса	Экзаменационный билет
		4. Адресация и маршрутизация в компьютерных сетях.	4.1. Физические адреса	Экзаменационный билет
			4.3. Классы IP-сетей	Экзаменационный билет
			4.5. Система доменных имен	Экзаменационный билет
			4.7. IP маршрутизация	Экзаменационный билет
			4.9. Динамическая маршрутизация.	Экзаменационный билет
		5. Службы DNS и DHCP.	5.1. DNS	Экзаменационный билет
			5.3. Проверка назначения IP-адреса	Экзаменационный билет
		ПК-13	Способность осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты	1. Принципы построения компьютерных сетей. Сетевые протоколы.
2. Среда доступа и технологии локальных и глобальных сетей.	2.2. Высокоскоростной Ethernet			
	3. Сетевая			2.4. Стык по (последовательному) COM порту.
3.2. Краткая история				Экзаменационный билет

		операционная система Unix и сети TCP/IP.	семейства протоколов TCP/IP	билет
			3.4. Уровень сетевого интерфейса	Экзаменационный билет
			3.6. Транспортный уровень. Протоколы TCP и UDP. TCP и UDP сокеты. Адресные пространства портов. Понятие encapsulation	Экзаменационный билет
		4. Адресация и маршрутизация в компьютерных сетях.	4.8. Статическая маршрутизация.	Экзаменационный билет
			4.6. Универсальная идентификация ресурсов (URL)	Экзаменационный билет
			4.4. Маски подсетей	Экзаменационный билет
			4.2. IP-адресация	Экзаменационный билет
		5. Службы DNS и DHCP.	5.2. DHCP. Клиент DHCP и IP-адрес.	Экзаменационный билет

2. Экзаменационные вопросы

№ п/п	Компетенции		ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ	№ и наименование раздела (
	Код	Определение		
1	2	3	4	5
1	ОПК-3	Способность владеть основными методами, способами средствами получения, хранения, переработки информации и	1. Основные понятия.	1. Принципы построения компьютерных сетей. Сетевые протоколы.
			2. Международные организации.	
			3. История ATM.	
			1. История Ethernet.	2. Среды доступа и технологии локальных и глобальных сетей.
			2. Высокоскоростной Ethernet.	
			4. Стык по (последовательному) COM порту.	3. Сетевая операционная система Unix и сети TCP/IP.
			1. История. Архитектура. Файлы.	
			2. История семейства протоколов TCP/IP.	
			4. Уровень сетевого интерфейса.	
			1. Виды адресации в компьютерных сетях.	4. Адресация и маршрутизация в компьютерных сетях.
			2. IP-адресация.	
			3. Маски подсетей.	
			4. Универсальная идентификация ресурсов (URL).	
			5. Статическая маршрутизация.	
1. Определение DNS.	5. Службы DNS и DHCP.			
2. Основные идеи DNS.				
3. Определение DHCP.				
4. Проверка назначения IP-адреса.				
2	ПК-13	Способность осуществлять	1. Классификация компьютерных сетей.	1. Принципы построения

	подготовку типовых технических проектов на различные инфокоммуникационные объекты	2. Модель OSI.	компьютерных сетей. Сетевые протоколы.
		3. Основные идеи технологии ATM.	
		1. Физическая среда Ethernet.	2. Среда доступа и технологии локальных и глобальных сетей.
		2. Технологии удалённого доступа.	
		1. Архитектура семейства протоколов TCP/IP.	3. Сетевая операционная система Unix и сети TCP/IP.
		2. Процессы.	
		1. Физические адреса.	4. Адресация и маршрутизация в компьютерных сетях.
		2. Классы IP-сетей.	
		3. Проблемы 4-х байтовой адресации.	
		4. IP маршрутизация.	
		5. Динамическая маршрутизация.	
		1. История развития DNS.	5. Службы DNS и DHCP.
		2. Домены верхнего уровня.	
		3. Клиент DHCP и IP-адрес.	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
<p>Знать: (ОПК-3) - Основы технологии интегральных схем, микросхемотехнику и принцип работы базовых каскадов аналоговых и логических элементов цифровых схем. (ПК-13): - Базовые принципы построения типовых технических проектов в сфере сетевых технологий.</p> <p>Уметь: (ОПК-3) - проводить самостоятельный анализ физических процессов, происходящих в электронных телекоммуникационных устройствах. (ПК-13): - проводить самостоятельный расчет физических процессов, происходящих в электронных телекоммуникационных устройствах, и проектировать их;</p> <p>Владеть: (ОПК-3) - навыками работы на компьютере и в компьютерных сетях, (ПК-13): - навыками расчета внешних характеристик систем передачи данных</p>	отлично	<p>Студент должен во время ответа показать знания: компьютерных сетей, историю их развития и современные тенденции в современных компьютерных сетях, основные термины используемые в научно-технической литературе по вычислительной технике. Студент должен иметь навыки владения: использования универсальных программных продуктов на ПК, понимания материала и способности высказывания мыслей на научно-техническом языке. Студент во время ответа должен продемонстрировать умения: использования навыков анализа топологии компьютерных сетей и законов их функционирования.</p>
	хорошо	<p>Ответ содержит неточности. Дополнительные вопросы требуются, но студент с ними справляется отлично.</p>
	удовлетворительно	<p>Ответил только на один вопрос, либо слабо ответил на оба вопроса. На дополнительные вопросы отвечает неуверенно.</p>
	неудовлетворительно	<p>На оба вопроса студент отвечает неубедительно. На дополнительные вопросы преподавателя также не может ответить.</p>

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина сетевые технологии высокоскоростной передачи данных направлена на ознакомление с основными элементами и процессами, протекающими в компьютерных сетях, и их практическим применением в современных системах телекоммуникаций; на получение теоретических знаний и практических навыков с различными топологиями компьютерных сетей для их дальнейшего использования в практической деятельности.

Изучение дисциплины вычислительная техника и информационные технологии предусматривает:

- лекции,
- лабораторные работы,
- практические занятия,
- самостоятельную работу студента,
- экзамен.

В ходе освоения раздела 1 «Принципы построения компьютерных сетей. Сетевые протоколы» студенты должны изучить: классификацию компьютерных сетей, международные организации, модель OSI, ATM, Основные идеи технологии ATM.

В ходе освоения раздела 2 «Среды доступа и технологии локальных и глобальных сетей» студенты должны изучить: Ethernet, физическую среду Ethernet, высокоскоростной Ethernet, технологию удалённого доступа, стык по (последовательному) COM порту.

В ходе освоения раздела 3 «Сетевая операционная система Unix и сети TCP/IP.» студенты должны изучить: историю создания UNIX, краткую историю семейства протоколов TCP/IP, общие сведения об архитектуре семейства протоколов TCP/IP, уровень сетевого интерфейса, уровень Internet, протоколы IP, ICMP, ARP, RARP, Internet–адреса, транспортный уровень.

В ходе освоения раздела 4 «Адресация и маршрутизация в компьютерных сетях.» студенты должны изучить: физические адреса, IP-адресация, классы IP-сетей, маски подсетей, систему доменных имен, универсальную идентификацию ресурсов (URL), IP маршрутизацию, статическая маршрутизацию, динамическая маршрутизацию.

В ходе освоения раздела 5 «Службы DNS и DHCP» студенты должны изучить: DNS, DHCP, клиент DHCP и IP-адрес, проверку назначения IP-адреса

В процессе проведения лабораторных работ происходит закрепление знаний, формирование умений и навыков реализации представления об различных способах коммутации и настройки различных компьютерных сетей.

В процессе проведения практических работ происходит закрепление знаний, формирование умений и навыков работы с различными протоколами в компьютерных сетях.

При подготовке к экзамену рекомендуется особое внимание уделить следующим вопросам: Ethernet, модель OSI, TCP/IP, маршрутизация.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

АННОТАЦИЯ
рабочей программы дисциплины
Сетевые технологии высокоскоростной передачи данных

1. Цель и задачи дисциплины

Целью изучения дисциплины является: формирование у обучающихся профессиональных компетенций в области построения и функционирования сетей передачи данных, базовых технологий организации локальных и территориальных компьютерных сетей, стека протоколов TCP/IP, принципов расчета характеристик отдельных участков сетей передачи данных, методы защиты от ошибок при передаче данных.

Задачей изучения дисциплины является: ознакомление обучающихся с вопросами функционирования и настройки аппаратного и программного обеспечения сетевых технологий передачи данных.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк – 17 часов, ЛР – 17 часов, ПЗ – 17 часов, СРС – 57 часов. Общая трудоемкость дисциплины составляет 144 часов, 4 зачетных единиц

2.2 Основные разделы дисциплины:

1. Принципы построения компьютерных сетей. Сетевые протоколы.
2. Среды доступа и технологии локальных и глобальных сетей.
3. Сетевая операционная система UNIX и сети TCP/IP.
4. Адресация и маршрутизация в компьютерных сетях
5. Службы DNS и DHCP

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующей компетенции:

ОПК-3 - Способностью владеть основными методами, способами и средствами получения, хранения, переработки информации.

ПК-13 - Способность осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты

4. Вид промежуточной аттестации: экзамен

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО
КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ**

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
1.	ОПК - 3	1. Принципы построения компьютерных сетей. Сетевые протоколы.	1.1. Классификация компьютерных сетей.	Отчеты по лабораторным работам, практическим занятиям
			1.3. АТМ. Основные идеи технологии АТМ.	Отчеты по лабораторным работам, практическим занятиям
		2. Среды доступа и технологии локальных и глобальных сетей.	2.1. Ethernet. Физическая среда Ethernet.	Отчеты по лабораторным работам, практическим занятиям,
			2.3. Технологии удалённого доступа.	Отчеты по лабораторным работам
		3. Сетевая операционная система Unix и сети TCP/IP	3.1. История создания	Отчеты по практическим занятиям
		4. Адресация и маршрутизация в компьютерных сетях.	4.3. Классы IP-сетей	Отчеты по лабораторным работам, практическим занятиям
4.9. Динамическая маршрутизация.	Отчеты по практическим занятиям			
2.	ПК-13	1. Принципы построения компьютерных сетей. Сетевые протоколы.	1.2. Международные организации. Модель OSI	Отчеты по лабораторным работам, практическим занятиям
			2.2. Высокоскоростной Ethernet	Отчеты по лабораторным работам
		3. Сетевая операционная система Unix и сети TCP/IP	3.1. История создания	Отчеты по практическим занятиям
		4. Адресация и маршрутизация в компьютерных сетях	4.8. Статическая маршрутизация.	Отчеты по практическим занятиям
			4.4. Маски подсетей	Отчеты по практическим занятиям
			4.2. IP-адресация	Отчеты по лабораторным работам, практическим занятиям

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
<p>Знать: (ОПК-3) - Основы технологии интегральных схем, микросхемотехнику и принцип работы базовых каскадов аналоговых и логических элементов цифровых схем. (ПК-13): - Базовые принципы построение типовых технических проектов в сфере сетевых технологий.</p>	зачтено	<p>Во время защиты лабораторных работ и практических работ студент ответил на поставленные преподавателем вопросы. Продемонстрировал знание построения компьютерных сетей, владение навыками разработки технического задания.</p>
<p>Уметь: (ОПК-3) - проводить самостоятельный анализ физических процессов, происходящих в электронных телекоммуникационных устройствах. (ПК-13): - проводить самостоятельный расчет физических процессов, происходящих в электронных телекоммуникационных устройствах, и проектировать их;</p> <p>Владеть: (ОПК-3) - навыками работы на компьютере и в компьютерных сетях, (ПК-13): - навыками расчета внешних характеристик систем передачи данных</p>	не зачтено	<p>Во время защиты лабораторных работ и практических работ студент не смог дать ответы на поставленные преподавателем вопросы. Либо отчет имеет ряд замечаний.</p>

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи от «6» марта 2015 г. №174

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015г. № 475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» июня 2016г. № 429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «6» марта 2017г. № 125

для набора 2018 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018г. № 130

Программу составил (и):

Ульянов А.Д. старший преподаватель кафедры УТС
Ф.И.О., должность, ученое звание, (степень)

(подпись)

Рабочая программа рассмотрена и утверждена на заседании кафедры
от «28» декабря 2018 г., протокол № 6

УТС

(сокращенное наименование)

Заведующий кафедрой УТС
(разработчик)

(подпись)

Игнатьев И.В.
(Ф.И.О.)

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой

(подпись)

Игнатьев И.В.
(Ф.И.О.)

Директор библиотеки

(подпись)

Сотник Т.Ф.

Рабочая программа одобрена методической комиссией ЭиА факультета
от «28» декабря 2018 г., протокол № 6

(сокращенное наименование)

Председатель методической комиссии факультета

(подпись)

Ульянов А.Д.
(Ф.И.О.)

СОГЛАСОВАНО:

Начальник
учебно-методического управления

Г.П. Нежевец

Регистрационный № _____