Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Курский государственный университет»

Колледж коммерции, технологий и сервиса

Методические рекомендации
по выполнению практических работ
по дисциплине:
«КОМПЬЮТЕРНЫЕ СЕТИ»

для студентов специальности
09.02.07 Информационные системы и программирование

Практическая работа №1.

Тема: Монтаж кабельных сред технологий Ethernet.

Цели: обобщить и систематизировать знания по теме «Монтаж кабельных сред технологий Ethernet».

Теоретический материал

На сегодняшний день подавляющая часть компьютерных сетей использует для соединения провода и кабели. Существуют различные типы кабелей, но на практике в большинстве сетей применяются только три основные группы:

1. Коаксиальный кабель (coaxial cable).
2. Витая пара (twisted pair).

- неэкранированная;
- экранированная.

3. Оптоволоконный кабель (fiber cable).

Назначение и структура коаксиального кабеля. Коаксиальный кабель предназначен для передачи высокочастотных сигналов в различной электронной аппаратуре, особенно в радио- и ТВ-передатчиках, компьютерах, трансмиттерах.

Рисунок 1. Конструкция коаксиального кабеля

Конструкция коаксиального кабеля состоит из медной жилы или стальной жилы плакированной медью, изоляции, ее окружающей, экрана в виде герметичного слоя фольги и металлической оплетки, внешней оболочки (см. рис. 1). При наличии сильных электромагнитных помех в месте прокладки сети можно воспользоваться кабелем с трехкратной (фольга + оплетка + фольга) или четырехкратной (фольга + оплетка + фольга + оплетка) экранизацией. Экран защищает передаваемые по кабелю данные, поглощая внешние электромагнитные сигналы - помехи или шумы. Таким образом, экран не позволяет помехам исказить данные. Трехкратный экран рекомендуется использовать в условиях сильного электромагнитного шума, например в городских индустриальных районах. Четырехкратный экран разработан для использования в местах с чрезвычайно высоким уровнем электромагнитного шума, например, вблизи от электрических машин, магистралей, в метро или поблизости от организаций оборудованных мощными радиопередатчиками.

Электрические сигналы, кодирующие данные, передаются по жиле.

Жила - это один провод (сплошная) или пучок проводов. Сплошная жила изготавливается, из меди или стали плакированной медью. Жила окружена изоляционным слоем, который отделяет ее от металлической оплетки. Оплетка играет роль заземления и защищает жилу от электрических шумов и перекрестных помех (электрические наводки, вызванные сигналами в соседних проводах). Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдет короткое замыкание, помехи проникнут в жилу, и данные разрушатся. Снаружи кабель покрыт непроводящим слоем - из резины, тефлона или пластика.

Коаксиальный кабель более помехоустойчив, затухание сигнала в нем меньше чем в витой паре. Ввиду того, что плетеная защитная оболочка поглощает внешние электромагнитные сигналы, не позволяя им влиять на передаваемые по жиле данные, то коаксиальный кабель можно использовать при передаче на большие расстояния и в тех случаях, когда высокоскоростная передача данных осуществляется на несложном оборудовании.

Существует два типа коаксиальных кабелей:

1. **Тонкий коаксиальный кабель** - гибкий кабель диаметром около 0,5 см, прост в применении и годится практически для любого типа сети, способен передавать сигнал на расстояние до 185 м без его заметного искажения, вызванного затуханием. Основная отличительная особенность — медная жила. Она может быть сплошной или состоять из нескольких переплетенных проводов.

2. **Толстый коаксиальный кабель** - относительно жесткий кабель с диаметром около 1 см. Иногда его называют «стандартный Ethernet», поскольку он был первым типом кабеля, применяемым в Ethernet — популярной сетевой архитектуре. Медная жила толстого коаксиального кабеля больше в сечении, чем тонкого, поэтому он передает сигналы на расстояние до 500 м. Толстый коаксиальный кабель иногда используют в качестве основного кабеля, который соединяет несколько небольших сетей, построенных на тонком коаксиальном кабеле.

Сравнение двух типов коаксиальных кабелей. Как правило, чем толще кабель, тем сложнее его прокладывать. Тонкий коаксиальный кабель гибок, прост в установке и относительно недорог. Толстый коаксиальный кабель трудно гнуть, следовательно, его сложнее монтировать, это очень существенный недостаток, особенно в тех случаях, когда необходимо проложить кабель по трубам или желобам.

Выбор того или иного типа коаксиальных кабелей зависит от места, где этот кабель будет прокладываться. Существуют поливинилхлоридные и пленумные классы коаксиальных кабелей.

Поливинилхлорид – это пластик, который применяется в качестве изолятора или внешней оболочки у большинства коаксиальных кабелей. Его прокладывают на открытых участках помещений. Однако при горении он выделяет ядовитые газы.

Пленумные коаксиальные кабели – прокладываются в вентиляционных шахтах, между подвесными потолками и перекрытиями пола.

Монтирование кабельной системы. Для подключения к толстому коаксиальному кабелю применяют специальное устройство – трансивер. Он снабжен специальным коннектором пронзающим ответвителем, который проникает через слой изоляции и вступает в контакт с проводящей жилой.

Для подключения тонкого коаксиального кабеля используются BNC-коннекторы. BNC коннектор (рисунок 2), BNC T коннектор (рисунок 3) и BNC баррел коннектор.

Рисунок 2. BNC коннектор

Рисунок 3. BNC T коннектор

Назначение и структура витой пары. Самая простая витая пара – это два перевитых изолированных медных провода. Согласно стандарту различают два вида витых пар:

- UTP - кабель на основе неэкранированной медной пары;
- STP - кабель на основе экранированной медной пары.

Неэкранированная витая пара (UTP, unshielded twisted pair) - это кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводников уменьшает электрические помехи извне при распространении сигналов по кабелю.

Кабель на основе неэкранированной медной пары различают по его пропускной способности, выделяя тем самым несколько категорий:

Категория 3: Кабель этой категории имеет частоту передачи сигналов до 16 МГц и предназначен для использования в сетях скоростью до 10 Мбит/с.

Категория 4: Кабель 4-й категории передает данные с частотой до 20 МГц, используется в сетях Token Ring (скорость передачи до 16 Мбит/с)

Категория 5:, Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 100М\бит 4 витые пары.

Категория 5е Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 1000М\бит для сетей 1000BaseT, Gigabit Ethernet.

Категория 6: Кабель этой категории является одной из наиболее совершенных сред передачи данных среди вышеперечисленных категорий. Его частота передачи сигнала доходит до 250 МГц, что почти в два раза больше пропускной способности категории 5е. Улучшена помехозащищенность.

Монтаж кабельной системы на основе витой пары. *Прямая разводка* – применяется, когда кабель соединяет ПК с концентратором или концентратор с концентратором

Кросс-разводка – применяется для соединения ПК друг с другом.

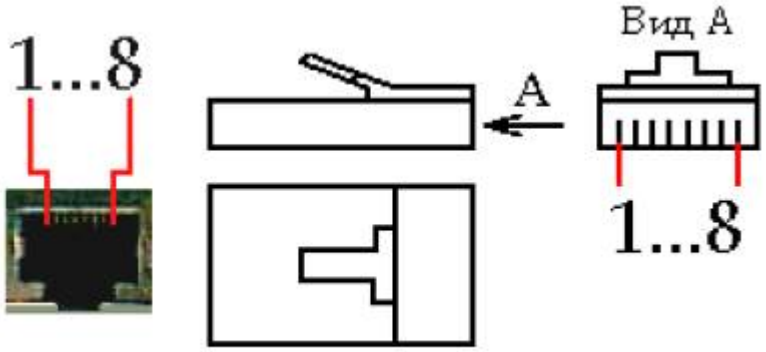


Рисунок 4. Порт MDI/MDI-X и разъем RJ-45

Таблица 1.Прямая разводка кабеля

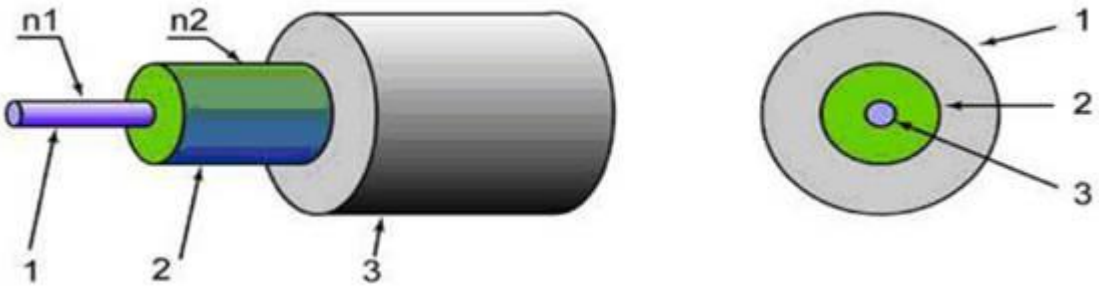
№ контакта коннектора	Цвет проводника
1.	Бело-зеленый
2.	Зеленый
3.	Бело-оранжевый
4.	Синий
5.	Бело-синий
6.	Оранжевый
7.	Бело-коричневый
8.	Коричневый

Таблица 2.Кросс-разводка кабеля

№ контакта коннектора	Первый конец	Второй конец
1.	Бело-зеленый	Бело-оранжевый
2.	Бело-синий	Оранжевый
3.	Бело-оранжевый	Бело-зеленый
4.	Синий	Синий
5.	Бело-синий	Бело-синий
6.	Оранжевый	Бело-синий
7.	Бело-коричневый	Бело-коричневый
8.	Коричневый	Коричневый

После подключения коннекторов кабель следует проверить с помощью специального тестера, который определит, правильно ли проводники витых пар подсоединены к контактам коннекторов, а также целостность самого кабеля.

Назначение и функции оптоволокна. В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов. Это относительно защищенный способ передачи, поскольку при нем не используются электрические сигналы. Следовательно, к оптоволоконному кабелю невозможно подключиться, не разрушая его, и перехватывать данные, от чего не



застрахован любой кабель, проводящий электрические сигналы.

Рисунок 5. Структура оптоволоконного кабеля: 1 – сердцевина с показателем преломления n_1; 2 – отражающая оболочка с показателем преломления n_2, $n_1 > n_2$; 3 – защитное покрытие.

Кабель содержит несколько световодов, хорошо защищенных пластиковой изоляцией. Он обладает сверхвысокой скоростью передачи данных (до 2 Гбит), и абсолютно не подвержен помехам. Расстояние между системами, соединенными оптиковолокном, может достигать 100 километров. Казалось бы, идеальный проводник для сети найден, но стоит оптический кабель чрезвычайно дорого, и для работы с ним требуется специальные сетевые карты, коммутаторы и т.д. Без специального оборудования оптоволокно практически не подлежит ремонту. Данное соединение применяется для объединения крупных сетей, высокосортного доступа в Интернет (для провайдеров и крупных компаний), а также для передачи данных на большие расстояния. В домашних сетях, если требуется

высокая скорость соединения, гораздо дешевле и удобнее воспользоваться гигабитной сетью на витой паре.

Лучи, входящие под разными углами в оптоволокно называются модами, а волокно, поддерживающее несколько мод - многомодовым. По одномодовому волокну распространяется только один луч.

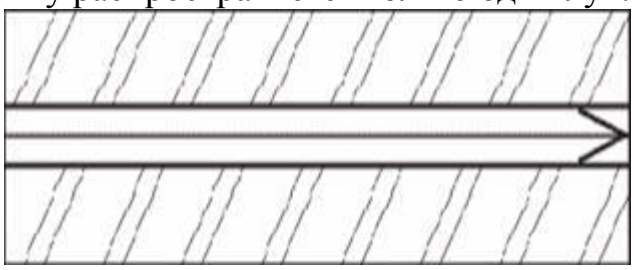
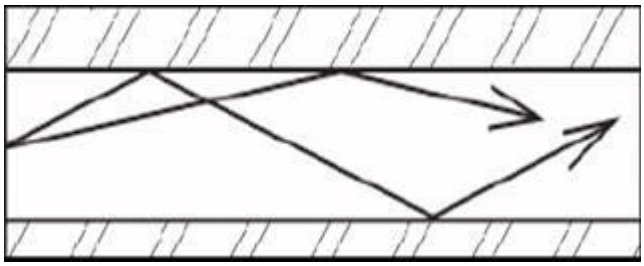


Рисунок 6. Одномодовое оптоволокно

Рисунок 7. Многомодовое оптоволокно

Задания к работе

Осуществите обжим витой пары по типу прямой разводки и кросс-разводки, используя таблицы 1, 2.



Контрольные вопросы:

1. Коаксиальный кабель: назначение и структура.
2. Неэкранированная витая пара: назначение и структура.
3. Экранированная витая пара: назначение и структура.
4. Оптоволоконный кабель: назначение и структура.

Практическая работа №2.
Тема: Подключение и настройка сетевого адаптера. Подключение и настройка модема.

Цели: обобщить и систематизировать знания по теме «Подключение и настройка сетевого адаптера. Подключение и настройка модема.»; научиться определять параметры сетевого адаптера, настраивать и устанавливать его.

Краткие теоретические сведения

Сетевые карты должны отвечать определенным требованиям в зависимости от того, в какие серверы они устанавливаются. Серверы с сетевыми картами можно разделить на три категории:

1. Сети, в состав которых входит не более 10 станций, используют серверы-десктопы. На таких небольших серверах функционирует небольшое количество информации: не очень объемная база данных или бухгалтерские программы, могут храниться архивы. С таким количеством информации может легко справиться обычная PCI-карта, обеспечивающая скорость 10 или 100 Мбит/сек.

2. Большие локальные сети, насчитывающие 200-300 рабочих станций, используют LAN-серверы. Это более высокий класс серверов, способных выполнять гораздо больший объем работы. Они обладают возможностью разделения файлов и печати, обеспечения межсервисных коммуникаций, функционирования электронной почты. Сетевые карты для больших серверов должны отвечать более высоким требованиям.

3. Суперсерверы, обслуживающие тысячи пользователей, выполняют все приложения, даже самые ресурсоемкие. Такие серверы могут обслуживать бизнес-процессы крупных предприятий. Суперсерверы используют сетевые карты, сравнимые по своим возможностям с сетевыми процессорами.

Исходя из своего предназначения, сетевая карта должна отвечать определенным требованиям. Производительность карты определяется тремя составляющими: микросхемным, конструктивным и программным уровнем карты.

Чем выше микросхемный уровень карты, тем больше она может выполнять функций, ранее выполнявшихся процессором. Серверные сетевые карты, разгружая процессор, значительно оптимизируют работу сети.

Конструктивный уровень карты определяется тем, сколько сегментов сети к нему возможно присоединить. Чем больше портов имеет карта, тем производительнее ее работа. Конструкция карты должна учитывать, что сеть работает в круглосуточном режиме. При замене карты не должна останавливаться работа сервера.

Программное обеспечение карты позволяет значительно расширить функции управления сетью, вести мониторинг, разделять трафик, группировать порты в логические каналы.

Задание к работе

1. Определите тип сетевой карты (тип шины, тип среды для

передачи данных).

Осмотрите сетевую карту. Определите тип шины, к которой она подключается (для этого посмотрите на ту часть сетевой карты, которая имеет контакты):

- карта подключается к шине PCI (Peripheral Component Interconnect - соединение периферийных компонент), если длина контактной пластины менее 10 см;

- карта подключается к шине ISA (Industry Standard Architecture - стандартная промышленная архитектура), если длина контактной пластины более 10 см.

Определите тип физической среды, с которой работает сетевая карта. Посмотрите на металлическую пластину, к которой крепится карта.

Круглый коннектор свидетельствует о том, что эта карта для коаксиального кабеля; разъем RJ-45 - для работы с витой парой.

Визуально определите на карте наличие микросхемы для загрузки компьютера по сети.

2. Установите сетевой адаптер в компьютер.

Выключите компьютер и откройте системный блок.

Вставьте сетевую карту в соответствующий разъем на материнской плате и закрепите ее в корпусе.

Закройте системный блок и включите компьютер.

В процессе загрузки ОС определяет подключенное оборудование. Если сетевая карта соответствует стандарту Plug and Play, то она будет найдена ОС и автоматически настроена. Если ОС не сможет определить установленную сетевую карту, то потребуется вручную установить ее драйвера.

Проверьте установку сетевой карты:

- откройте диалоговое окно Диспетчер устройств (Пуск/Панель управления/Система/Оборудование/Диспетчер устройств);

- раскройте список Сетевые платы.

Если в этом списке есть название адаптера, то установка прошла успешно.

3. Изучите параметры сетевого адаптера.

Откройте окно параметров сетевого адаптера (воспользуйтесь Диспетчером устройств).

Определите физический (MAC, Medium Access Control - управление доступом к носителю) адрес сетевой карты помощью команды ipconfig:

- запустите консоль (командную строку) любым способом (например, Пуск/Программы/Стандартные/Командная строка);

- введите команду ipconfig с параметром all;

- в полученном списке найдите строку Физический адрес.

Физический адрес и будет являться MAC-адресом сетевого адаптера.

Например, выведенный системой список может выглядеть так:

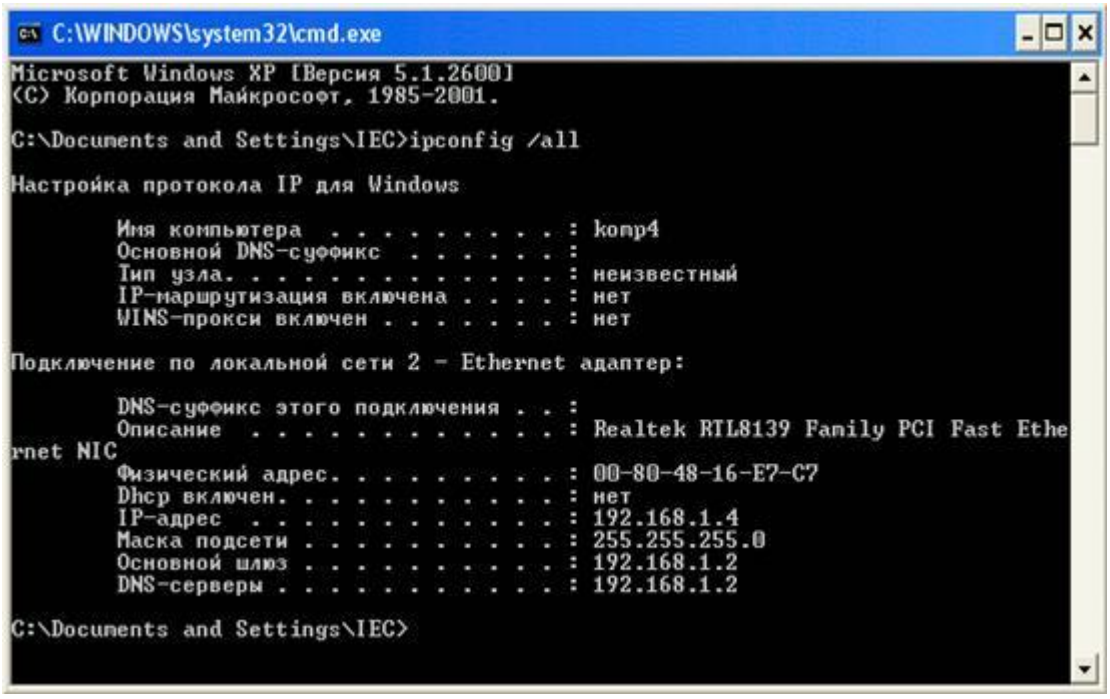


Рисунок 1. Результат работы команды ipconfig /all

Контрольные вопросы:

1. Классификация сетевых адаптеров.
2. Основные характеристики сетевых адаптеров.
3. Основные функции сетевых адаптеров.

Практическая работа №3.
Тема: Модель OSI. Модель TCP/IP

Цели: изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети.

Теоретические сведения:

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных - совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

IP - адреса представляют собой 32-х разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса (для удобства будем записывать точки и в двоичном изображении).

Например, IP–адрес 192.168.200.47 является десятичным эквивалентом двоичного адреса 11000000.10101000.11001000.00101111

Иногда применяют десятичное значение IP-адреса. Его легко вычислить: $192*256^3+168*256^2+200*256+47=3232286767$

Существует несколько правил об особенностях IP-адресов:

- если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;
- если в поле номера сети стоят 0, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;
- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);
- если в поле адреса назначения стоят сплошные 1, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);

адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback Адрес получателя должен содержать в себе:

1. адрес (номер) подсети;
2. адрес (номер) хоста (узла) внутри подсети

Часто (например, маршрутизация осуществляется на основании номера сети) возникает необходимость разделить IP - адрес на эти две части: номер подсети и номер узла. Для разделения IP - адреса используют один из способов:

1. использование фиксированной границы - (не нашел применения; весь адрес делится на 2 части фиксированной длины, в одной из них всегда размещается номер сети, в другой - номер узла)
2. использование маски, которая позволяет максимально гибко установить границу между номером сети и номером узла.
3. использование классов адресации (самый распространенный, компромисс между первым и вторым способом). Вводится 5 классов: A,B,C,D,E. A,B,C - используют для адресации сетей; D,E - имеют специальное назначение. Для каждого класса определены границы между номером сети и номером узлов, которые хранятся в таблицах:

Диапазоны адресов для всех классов сетей:

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число машин в сети
A	0	1.0.0.0	126.0.0.0	$2^{24} = 16\,777\,216$
B	10	128.0.0.0	191.255.0.0	$2^{16} = 65\,536$
C	110	192.0.1.0	223.255.255.0	$2^{8} = 256$
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано для будущих применений

Диапазон адресов сетей и хостов классов A и C:

Класс	Диапазон номера сети	Диапазон номеров узлов
A	1 – 126	0.0.1 – 255.255.254
B	128.0 – 191.255	0.1 – 255.254
C	192.0.0 – 223.255.255	1-254

Чтобы получить из IP-адреса номер сети и номер узла надо разбить адрес на 2 соответствующие части (см. таблицу) и дополнить каждую из них нулями до полных 4 байт.

Пример: Дан IP-адрес класса B: 129.64.134.5. Так как для класса B IP-адрес разбивается пополам, то номер сети равен **129.64**.0.0; номер узла равен 0.0.**134.5**.

Использование масок в IP-адресации

Маска - это 4-байтное число, которое используется в паре с IP-адресом. Двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресах использоваться как номер сети.

Маска - это число, применяемое в паре с IP - адресом, причем двоичная запись маски содержит

непрерывную последовательность единиц в тех разрядах, которые должны в IP - адресе интерпретироваться

как номер сети, а остальные - нули.

Поэтому маску часто записывают в виде числа единиц в ней содержащихся. 255.255.248.0 (11111111.11111111.11111000.00000000) - является правильной маской подсети (/21), а 255.255.250.0 (11111111.11111111.11111010.00000000) - является неправильной, недопустимой.

Если маску «наложить» на IP - адрес, то граница между единицами и нулями в маске станет границей

номер сети и номер узла IP - адреса.

Для стандартных классов сетей маски имеют следующие значения:

255.0.0.0 - маска для сети класса A,

255.255.0.0 - маска для сети класса B,

255.255.255.0 - маска для сети класса C.

В масках, которые использует администратор для увеличения числа подсетей, количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

Пример1: IP-адрес - 194.110.345.185, маска - 255.255.255.192. Если не учитывать маску подсети: номер сети - 194.110.245.0, а номер узла - 0.0.0.185. С учетом маски - номер сети - 194.110.345.128, а номер узла 0.0.0.57

Пример2: маска имеет значение 255.255.192.0 (11111111 11111111 11000000 00000000). И пусть сеть имеет номер 129.44.0.0 (10000001 00101100 00000000 00000000), из которого видно, что она относится к классу B. После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 до 18, то есть администратор получил возможность использовать вместо одного, централизованно заданного ему номера сети, четыре:

129.44.0.0 (10000001 00101100 00000000 00000000) 129.44.64.0 (10000001 00101100 01000000 00000000) 129.44.128.0 (10000001 00101100 10000000 00000000) 129.44.192.0 (10000001 00101100 11000000 00000000)

Пример3: IP-адрес 129.44.141.15 (10000001 00101100 10001101 00001111), который по стандартам IP задает номер сети 129.44.0.0 и номер узла 0.0.141.15, теперь, при использовании маски, будет интерпретироваться как пара:

129.44.128.0 - номер сети, 0.0. 13.15 - номер узла.

Таким образом, установив новое значение маски, можно заставить маршрутизатор по-другому интерпретировать IP-адрес.

Пример4: пусть ваша сеть относится к классу B. В одной сети циркулирует единый трафик. Но среди

всех станций сети есть некоторые, слабо взаимодействующие между собой. Эти станции желательно бы

изолировать в разных сетях. Пусть это будут узел 129.34.17.15 и узел 129.34.20.01, которые в исходной ситуации

относятся к одной сети класса B с номером 129.34. Если задать в качестве маски число 255. 255.255.0, то адреса

этих двух узлов будут интерпретироваться маршрутизаторами как адреса узла 15 сети класса C с номером

129.34.17 и узла 01 сети класса C с номером 129.34.20. Извне сеть по-прежнему будет выглядеть как единая сеть

класса B, а на местном уровне это будет несколько отдельных сетей класса C.

Нетрудно увидеть, что максимальный размер подсети может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

При передаче пакетов используются правила маршрутизации, главное из которых звучит так: «Пакеты участникам своей подсети доставляются напрямую, а остальным – по другим правилам маршрутизации».

Таким образом, требуется определить, является ли получатель членом нашей подсети или нет.

Алгоритм определения диапазона адресов подсети (из определения маски).

1. Перевести и записать IP-адрес в двоичной системе счисления.
2. Перевести маску и записать ее в двоичной системе счисления.
3. «Наложить» маску на IP-адрес и записать диапазон номеров подсети в двоичной системе счисления.
4. Перевести и записать диапазон из двоичной системы счисления в десятичную.

Задача. Дан IP-адрес 192.168.200.47 /20 (маска подсети 20). Определить диапазон номеров (адресов) подсети.

Решение.

1. 192.168.200.47 переведем в двоичную систему счисления:

* Алгоритм перевода числа из десятичной системы счисления в двоичную:

1. Делим число на 2, остаток от деления может быть 1 или 0, значение остатка присваивается младшему (самому правому) знаку искомой двоичной записи.
2. Полученное число вновь делим на 2, остаток равен значению следующего по старшинству знака.
3. Повторить п.2 пока частное не станет меньше двух, частное от последнего деления равно значению старшего знака, остаток – второму по старшинству знаку.

Перевод числа 192 из десятичной записи в двоичную:

192	96	48	24	12	6	3	1
0	0	0	0	0	0	1	1

Пояснения: 24/2=12 – четное, пишем – 0;
192 – четное, значит, пишем – 0; 12/2=6 – четное, пишем – 0;
192/2=96 – четное, пишем – 0; 6/2=3 – нечетное, пишем 1;
96/2=48 – четное, пишем – 0; 3/2=1 – нечетное, пишем 1.

Результат записываем из таблицы слева направо: 11000000.

Аналогично переводим 168 в двоичную систему счисления и получаем: 10101000.

Аналогично переводим 200 в двоичную систему счисления и получаем: 11001000

Аналогично переводим 47 в двоичную систему счисления и получаем: 00101111 (впереди недостающие

разряды дописываем нулями до 4 байт)

Записываем 192.168.200.47 в двоичной форме:

11000000.10101000.11001000.00101111 – IP-адрес

2. **Записываем маску 20 в двоичной форме.** Для этого пишем 20 нулей с разделением на 4 байта,

оставшиеся 12 знаков дописываем нулями:

11111111.11111111.11110000.00000000 – маска 20.

3. **«Накладываем» маску на IP-адрес и выявляем диапазон номеров подсети:**

11000000.10101000.11001000.00101111

11111111.11111111.11110000.00000000 Граница единиц и нулей попадает на середину третьего числа; все что оказалось под единицами остается без изменений, значит первые два числа в IP-адресе останутся без изменений и надо получить только третье число и четвертое.

Для того чтобы определить начало диапазона надо в IP-адресе все числа от границы заполнить нулями, для того, чтобы определить конец диапазона надо в IP-адресе все числа от границы заполнить единицами, то есть: Диапазон адресов подсети будет такой: от 11000000.10101000.11000000.00000000 до 11000000.10101000.11001111.11111111

4. **Переведем и запишем полученный диапазон номеров подсети из двоичной системы счисления в десятичную:**

11000000 = $1*2^7 + 1*2^6 + 0*2^5 + 0*2^4 + 0*2^3 + 0*2^2 + 0*2^1 + 0*2^0 = 2^7 + 2^6 = 192$

00000000 = 0

11001111 =

$1*2^7 + 1*2^6 + 0*2^5 + 0*2^4 + 1*2^3 + 1*2^2 + 1*2^1 + 1*2^0 = 2^7 + 2^6 + 2^3 + 2^2 + 2^1 + 2^0 = 207$

11111111 = 1

Значит, диапазон адресов подсети будет такой: от 192.168.192.0 до 192.168.207.255

Задания для выполнения:

1. Какие адреса из приведенного ниже списка являются допустимыми адресами хостов и почему:

0.10.10.10

10.0.10.10

10.10.0.10

10.10.10.10
127.0.127.127
127.0.127.0
255.0.200.1
1.255.0.0

2. Перечислите все допустимые маски, по какому принципу они получаются.
3. Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети):

10.212.157.12/24 27.31.12.254/31 192.168.0.217/28 10.7.14.14/16

4. Какие из адресов

241.253.169.212 243.253.169.212 242.252.169.212 242.254.168.212 242.254.178.212 242.254.170.212 242.254.169.211 242.254.179.213 будут достигнуты напрямую с хоста 242.254.169.212/21. Определите диапазон адресов в его подсети.

5. Посмотрите параметры IP на своем компьютере с помощью команды ipconfig. Команда ipconfig отображает краткую информацию, т.е. только IP-адрес, маску подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры, и какие сетевые параметры выбрали бы Вы.

6. Определить к какому классу относятся IP - адреса:

1.	8.
2.	9. 128.10.2.30
3.	10. 129.64.134.5
4.	11. 132.13.34.15
5.	12.
6. 14.0.0.6	связи
7	

- зарезервирован для обозначения обратной

Результаты представить в виде таблицы (все расчеты ниже таблицы)

№ примера	**Десятичная форма IP - адреса**	**Двоичная форма IP - адреса**	**Принадлежность к классу IP - адресов**	**Диапазон IP–адресов этого класса**	**Максимальное количество ПК в сети этого класса**

7. Выделить номер подсети и номер узла по заданному IP - адресу и маске подсети:

IP - адрес: 129. 64. 134. 5
Маска подсети: 255. 255. 128. 0

8. Дан IP-адрес 198.65.12.67 и маска этой подсети - 255.255.255.240. Определить номер подсети и максимальное число узлов этой подсети.
9. Какие из приведенных ниже адресов не могут быть использованы для узлов Интернета? Ответ обоснуйте. Для верных адресов определите их класс: A,B,C,D,E. Результат представить в виде таблицы.

1.127.0.0.1 7. 193.256.1.16

2.201.13.123.245
3.226.4.37.105
4.103.24.254.0
5.10.234.17.25
6.154.12.255.255
8. 194.87.45.0
9. 195.34.116.255
10. 161.23.45.305
11. 13.13.13.13
12. 204.0.3.1

10.* Какое максимальное количество подсетей теоретически можно иметь, если в вашем распоряжении имеется сеть класса С? Какое значение при этом может иметь маска? Ответ обосновать.

Контрольные вопросы:

1. Какой адрес называется неопределенным IP – адресом?
2. Что обозначает неопределенный IP – адрес?
3. Какой адрес может быть использован **только** в качестве адреса отправителя?
4. Какой адрес называется ограниченным широковещательным?
5. Какой адрес называется широковещательным?
6. Чем отличается ограниченный широковещательный адрес от широковещательного?
7. Какой адрес является внутренним адресом стека протоколов ПК?
8. Для чего он используется?
9. Какая операция называется разделением на подсети?
10. Какая операция называется объединением подсетей?
11. Какой класс IP – адресов используется для корпоративных внутренних сетей предприятия?
12. Чем занимается сетевой уровень?
13. Какие требования предъявляются к сетевой адресации?
14. Можно ли использовать в качестве сетевого MAC-адрес?
15. Что такое маска подсети?
16. Какова структура IP-адреса?
17. Чем определяется размер подсети?
18. Как определить диапазон адресов в подсети?
19. Как определить размер подсети?

Примечание:

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие:

0 в первом или последнем байте,

255 в любом байте (это широковещательные адреса),

127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня). Поэтому доступный диапазон адресов будет несколько меньше. Диапазон адресов:

10.X.X.X – для больших локальных сетей;

172.16.X.X – для больших локальных сетей, но применяется реже,

192.168.X.X – для маленьких (небольших) локальных сетей, не может быть использован в сети Internet, т.к. эти адреса отданы для использования в сетях непосредственно не подключенных к глобальной сети.

Практическая работа №4.

Тема: Преобразование форматов IP-адресов

Цель: Познакомиться с принципами адресации в IP-сетях

Теоретическая часть

Internet Protocol

Протокол IP (Internet Protocol) используется как в глобальных распределенных системах, например в сети Интернет, так и в локальных сетях. Впервые протокол IP применялся еще в сети ArpaNet, являвшейся предтечей современного Интернета, и с тех пор он уверенно удерживает позиции в качестве одного из наиболее распространенных и популярных протоколов межсетевого уровня.

Поскольку межсетевой протокол IP является универсальным стандартом, он нередко применяется в так называемых составных сетях, то есть сетях, использующих различные технологии передачи данных и соединяемых между собой посредством шлюзов. Этот же протокол «отвечает» за адресацию при передаче информации в сети. Как осуществляется эта адресация?

Каждый человек, живущий на Земле, имеет адрес, по которому его в случае необходимости можно разыскать. Думаю, ни у кого не вызовет удивления то, что каждая работающая в Интернете или локальной сети машина также имеет свой уникальный адрес. Адреса в компьютерных сетях разительно отличаются от привычных нам почтовых. Боюсь, совершенно бесполезно писать на отправляемом вами в Сеть пакете информации нечто вроде «Компьютеру Intel Pentium III 1300 Mhz, эсквайру, Пэнни-Лэйн 114, Ливерпуль, Англия». Увидев такую надпись, ваша персоналка в лучшем случае фундаментально зависнет. Но если вы укажете компьютеру в качестве адреса нечто вроде 195.85.102.14, машина вас прекрасно поймет.

Именно стандарт IP подразумевает подобную запись адресов подключенных к сети компьютеров. Такая запись носит название IP-адрес.

Из приведенного примера видно, что IP-адрес состоит из четырех десятичных идентификаторов, или октетов, по одному байту каждый, разделенных точкой. Левый октет указывает тип локальной интрасети (под термином «интрасеть» (intranet) здесь понимается частная корпоративная или домашняя локальная сеть, имеющая подключение к Интернету), в которой находится искомый компьютер. В рамках данного стандарта различается несколько подвидов интрасетей, определяемых значением первого октета. Это значение характеризует максимально возможное количество подсетей и узлов, которые может включать такая сеть. В табл. 1 приведено соответствие классов сетей значению первого октета IP-адреса.

Таблица 1 . Соответствие классов сетей значению первого октета IP-адреса.

класс сети	Диапазон значений первого октета	Возможное количество подсетей	Возможное количество узлов
A	1-126	126	16777214

B	128-191	16382	65534
C	192-223	2097150	254
D	224-239	-	2-28
E	240-247	-	2-27

Адреса класса A используются в крупных сетях общего пользования, поскольку позволяют создавать системы с большим количеством узлов. Адреса класса B, как правило, применяют в корпоративных сетях средних размеров, адреса класса C — в локальных сетях небольших предприятий. Для обращения к группам машин предназначены широковещательные адреса класса D, адреса класса E пока не используются: предполагается, что со временем они будут задействованы с целью расширения стандарта. 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. Кроме того, существует набор так называемых «выделенных» IP-адресов, имеющих особое значение. Эти адреса приведены в табл.2.

Таблица 2. Значение выделенных IP-адресов

IP-адрес	**Значение**
0.0.0.0	Данный компьютер
Номер сети.0.0.0	Данная IP-сеть
0.0.0.номерхоста	Конкретный компьютер в данной локальной IP-сети
1.1.1.1	Все компьютеры в данной локальной IP-сети
Номер сети.1.1.1	Все компьютеры в указанной IP-сети

Как уже упоминалось ранее, небольшие локальные сети могут соединяться между собой, образуя более сложные и разветвленные структуры. Например, локальная сеть предприятия может состоять из сети административного корпуса и сети производственного отдела, сеть административного корпуса, в свою очередь, может включать в себя сеть бухгалтерии, планово- экономического отдела и отдела маркетинга. В приведенном выше примере сеть более низкого уровня является подсетью системы более высокого уровня, то есть локальная сеть бухгалтерии — подсеть для сети административного корпуса, а та, в свою очередь, — подсеть для сети всего предприятия в целом.

Однако вернемся к изучению структуры IP-адреса. Последний (правый) идентификатор IP-адреса обозначает номер компьютера в данной локальной сети. Все, что расположено между правым и левым октетами в такой записи, — номера подсетей более низкого уровня. Непонятно? Давайте разберем на примере. Положим, мы имеем некий адрес в Интернете, на который хотим отправить пакет с набором свеженьких анекдотов. В качестве примера возьмем тот же IP-адрес — 195.85.102.14. Итак, мы отправляем пакет в 195-ю подсеть сети Интернет, которая, как видно из значения первого октета,

относится к классу С. Допустим, 195-я сеть включает в себя еще 902 подсети, но наш пакет высылается в 85-ю. Она содержит 250 подсетей более низкого порядка, но нам нужна 102-я. Ну и, наконец, к 102-й сети подключено 40 компьютеров. Исходя из рассматриваемого нами адреса, подборку анекдотов получит машина, имеющая в этой сетевой системе номер 14. Из всего сказанного выше становится очевидно, что IP-адрес каждого компьютера, работающего как в локальной сети, так и в глобальных вычислительных системах, должен быть уникален.

Централизованным распределением IP-адресов в локальных сетях занимается государственная организация — Стенфордский международный научно- исследовательский институт (Stanford Research Institute, SRI International), расположенный в самом сердце Силиконовой долины — городе Мэнло-Парк, штат Калифорния, США. Услуга по присвоению новой локальной сети IP-адресов бесплатная, и занимает она приблизительно неделю. Связаться с данной организацией можно по адресу SRI International, Room EJ210, 333 Ravenswood Avenue, Menio Park, California 94025, USA, no телефону в США 1-800-235-3155 или по адресу электронной почты, который можно найти на сайте http://www.sri.com. Однако большинство администраторов небольших локальных сетей, насчитывающих 5-10 компьютеров, назначают IP-адреса подключенным к сети машинам самостоятельно, исходя из описанных выше правил адресации в IP-сетях. Такой подход вполне имеет право на жизнь, но вместе с тем произвольное назначение IP-адресов может стать проблемой, если в будущем такая сеть будет соединена с другими локальными сетями или в ней будет организовано прямое подключение к Интернету. В данном случае случайное совпадение нескольких IP-адресов может привести к весьма неприятным последствиям, например к ошибкам в маршрутизации передаваемых по сети данных или отказу в работе всей сети в целом.

Небольшие локальные сети, насчитывающие ограниченное количество компьютеров, должны запрашивать для регистрации адреса класса С. При этом каждой из таких сетей назначаются только два первых октета IP-адреса, например 197.112.X.X, на практике это означает, что администратор данной сети может создавать подсети и назначать номера узлов в рамках каждой из них произвольно, исходя из собственных потребностей.

Большие локальные сети, использующие в качестве базового межсетевой протокол IP, нередко применяют чрезвычайно удобный способ структуризации всей сетевой системы путем разделения общей IP-сети на подсети. Например, если вся сеть предприятия состоит из ряда объединенных вместе локальных сетей Ethernet, то в ней может быть выделено несколько структурных составляющих, то есть подсетей, отличающихся значением третьего октета IP-адреса. Как правило, в качестве каждой из подсетей используется физическая сеть какого-либо отдела фирмы, скажем, сеть Ethernet, объединяющая все компьютеры бухгалтерии. Такой подход, во-первых, позволяет излишне не расходовать IP-адреса, а во-вторых, предоставляет определенные удобства с точки зрения администрирования:

например, администратор может открыть доступ к Интернету только для одной из вверенных ему подсетей или на время отключить одну из подсетей от локальной сети предприятия. Кроме того, в случае если сетевой администратор решит, что третий октет IP-адреса описывает номер подсети, а четвертый — номер узла в ней, то такая информация записывается в локальных таблицах маршрутизации сети вашего предприятия и не видна извне. Другими словами, данный подход обеспечивает большую безопасность.

В локальных сетях, работающих под управлением межсетевого протокола IP, помимо обозначения IP-адресов входящих в сеть узлов принято также символьное обозначение компьютеров: например, компьютер с адресом 192.112.85.7 может иметь сетевое имя localhost. Таблица соответствий IP-адресов символьным именам узлов содержится в специальном файле hosts, хранящемся в одной из системных папок; в частности, в операционной системе Microsoft Windows XP этот файл можно отыскать в папке AMCK:\Windows\system32\drivers\etc\. Синтаксис записи таблицы сопоставлений имен узлов локальной сети IP-адресам достаточно прост: каждый элемент таблицы должен быть расположен в новой строке, IP-адрес располагается в первом столбце, а за ним следует имя компьютера, при этом IP-адрес и имя должны быть разделены как минимум одним пробелом. Каждая из строк таблицы может включать произвольный комментарий, обозначаемый символом #. Пример файла hosts приведен ниже:

192.112.85.7	localhost	# этот компьютер
192.112.85.1	server	# сервер сети
192.112.85.2	director	# компьютер директора
192.112.85.5	admin	# компьютер администратора

Как правило, файл hosts создается для какой-либо конкретной локальной сети, и его копия хранится на каждом из подключенных к ней компьютеров. В случае, если один из узлов сети имеет несколько IP-адресов, то в таблице соответствий обычно указывается лишь один из них, вне зависимости от того, какой из адресов реально используется. При получении из сети IP- пакета, предназначенного для данного компьютера, протокол IP сверится с таблицей маршрутизации и на основе анализа заголовка IP-пакета автоматически опознает любой из IP-адресов, назначенных данному узлу.

Помимо отдельных узлов сети собственные символьные имена могут иметь также входящие в локальную сеть подсети. Таблица соответствий IP-адресов именам подсетей содержится в файле networks, хранящемся в той же папке, что и файл hosts. Синтаксис записи данной таблицы сопоставлений несколько отличается от предыдущего, и в общем виде выглядит следующим образом:

<сетевое имя> <номер сети > [псевдонимы...] [#<комментарий >]

где сетевое имя — имя, назначенное каждой подсети, номер сети —

часть IP-адреса подсети (за исключением номеров более мелких подсетей, входящих в данную подсеть, и номеров узлов), псевдонимы — необязательный параметр, указывающий на возможные синонимы имен подсетей: они используется в случае, если какая-либо подсеть имеет несколько различных символьных имен; и, наконец, комментарий — произвольный комментарий, поясняющий смысл каждой записи. Пример файла networks приведен ниже:

loopback 127
marketing 192.112.85 # отдел маркетинга
buhgaltena 192.112.81 # бухгалтерия
workshop 192.112.80 # сеть производственного цеха workgroup 192.112.10 localnetwork # основная рабочая группа

Обратите внимание на то обстоятельство, что адреса, начинающиеся на 127, являются зарезервированными для протокола IP, а подсеть с адресом 192.112.10 в нашем примере имеет два символьных имени, используемых совместно.

Файлы hosts и networks не оказывают непосредственного влияния на принципиальный механизм работы протокола IP и используются в основном прикладными программами, однако они существенно облегчают настройку и администрирование локальной сети.

TCP/IP

Правила межсетевой передачи информации были разработаны еще в начале 1970-х годов в рамках проекта американского проекта ARPANET. В 1974 году они были зафиксированы в протоколах заседаний межсетевой рабочей группы, работавшей под руководством Винтона Серфа (Vinton Cerf). Вскоре был опубликован документ, получивший название протокол TCP/IP (Transmission Control Protocol / Internet Protocol). Этот документ и стал основным стандартом Интернета. Предложенные в нем принципы таковы:

Каждый компьютер в сети (или на сетевом жаргоне хост (host) - узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую) имеет уникальный двоичный 4-х байтовый адрес, идентифицирующий его в Интернет. Например, 10111110101001110010001000000010. Во избежание ошибок принято после каждого октета адреса, кроме последнего, ставить точку. Тогда адрес запишется как 10111110.10100111.00100010.00000010. или 190.167.34.2, если перевести каждый октет в десятичную систему счисления. Таким образом, адрес компьютера записывается в формате A.B.C.D, где 0<=A<=255, 0<=B<=255, 0<=C<=255, 0<=D<=255. Этот адрес называют IP-адресом.

Задания к практической работе.

Задание 1.

а) Проверьте правильность примера, приведенного выше.

б) Запишите двоичный IP-адрес 11111110101111110110001000000111 в стандартном формате.

Задание 2. Подсчитайте, сколько всего компьютеров может быть в Интернете. Расчет с необходимыми пояснениями запишите в отчет.

Задание 3. При помощи любой известной вам поисковой системы определите число документов Интернет, в которых цитируется описание протокола IP. Попробуйте найти собственно описание протокола.

Указание. Этот документ называется RFC-791 (Request For Comments-791).

Задание 4. Укажите классы следующих IP-адресов.

Адрес	
1. 126.102.128.0 2. 1.191.248.0 3. 185.74.41.184 4. 96.247.128.0	5. 168.224.0.1 6. 201.76.98.5 7. 186.112.0.10 8. 28.0.0.0

Задание 5. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

1. 131.107.256.80 2. 222.222.255.222 3. 31.200.1.1 4. 126.1.0.0	5. 190.7.2.0 6. 127.1.1.1 7. 198.121.254.255 8. 255.255.255.255

Задание 6. Преобразуйте следующие доменные имена в IP-адреса: ***www.mail.ru***, ***www.google.com, www.bsu.edu.ru, ns.mmf.rsu.ru, ns.rsu.ru, krinc.rsu.ru, math.rsu.ru, www.rsu.ru, ftp.rsu.ru, uic.rsu.ru, rsu.ru. C***делайте выводы.

Задание 7. Даны имена веб-серверов:

Южная Америка	www.uba.ar	www.castelobranko.br	www.univalle.edu.co	www.ucv.ve
Австралия и Океания	www.usyd.edu.au	www.usp.ac.fj	www.adelaide.edu.au	www.vu.edu.a
Африка	www.uz.ac.zw	www.unisa.ac.za	www.bau.edu.lb	www.aast.edu
Азия	www.mu.ac.in	www.ntu.edu.tw	www.sharjah.ac.ae	www.kimep.k
Европа	www.us.es	www.sorbonne.fr	www.ox.ac.uk	www.unizh.ch
Северная Америка	www.stanford.edu	www.ufl.edu	www.nmt.edu	www.yale.edu
Россия	www.kubstu.ru	www.kbsu.ru	www.spbu.ru	www.festu.ru

•Выберите по одному серверу из каждой строки таблицы. Следующие действия нужно выполнять для каждого выбранного сервера, результаты оформлять в виде таблицы.

•Определите IP-адрес.

•Выясните название владельца IP-адреса.

•Определите название и местонахождение организации, которой принадлежит веб-сервер.

Контрольные вопросы:

1.Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2.Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?
3.Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?
4.Когда необходим уникальный идентификатор сети?
5.Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Практическая работа №5.

Тема: Адресация в IP-сетях. Подсети и маски.

Цель: получить практические навыки по работе с пространством IP-адресов, масками и управления адресацией в IP сетях.

Теоретические сведения

1) Все пространство IP адресов делится на логические группы – IP-сети. Они нужны для организации иерархической адресации в составной IP-сети, например Интернете. Каждой локальной сети присваивается своя IP-сеть, маршрут до IP-узлов, находящихся в этой локальной сети строится на маршрутизаторах как маршрут до их IP-сети. И только после того, как пакет попал в конкретную IP-сеть, решается задача его доставки на отдельный узел.
2) В IP-адресе выделяются две части – адрес сети и адрес узла. Деление происходит с помощью маски – 4-х байтного числа, которое поставлено в соответствие IP-адресу. Макса содержит двоичные 1 в тех разрядах IP-адреса, которые определяют адрес сети и двоичные 0 в тех разрядах IP адреса, которые определяют адрес узла.
3) Адресом IP-сети считается IP-адрес из этой сети, в котором в поле адреса узла содержатся двоичные 0. Этот адрес обозначает сеть целиком в таблицах маршрутизации.

Есть еще служебный IP-адрес – адрес ограниченного широковещания – в поле адреса узла он содержит двоичные 1. Оба эти адреса не используются для адресации реальных узлов сети, однако входят в диапазон адресов IP-сети.

4) Рассмотрим пример: есть адрес 192.168.170.15 с маской 255.255.252.0. Определим адрес сети, адрес широковещания и допустимый для данной IP-сети диапазон адресов.

DEC IP	192	168	170	15
DEC MASK	255	255	252	0
BIN IP	11000000	10101000	10101010	00001111
BIN MASK	11111111	11111111	11111100	00000000
BIN IP сети (скопируем сетевую часть IP и заполним узловую часть 0)	11000000	10101000	10101000	00000000
DEC IP сети	192	168	168	0
BIN IP широковещания (скопируем сетевую часть IP и заполним узловую часть 1)	11000000	10101000	10101011	11111111
DEC IP широковещания	192	168	171	255
Начало диапазона IP-адресов для узлов (значение поля узла +1 к IP адресу сети)	192	168	168	1

Окончание диапазона IP-адресов для узлов (значение поля узла -1 от IP-адреса широковещания)	192	168	171	254

5) если имеется сеть, составленная из нескольких локальных сетей, соединенных между собой маршрутизаторами, то нужно каждой из этих локальных сетей назначить отдельную IP-сеть. В случае, если вам для такой сети выдается большая IP-сеть в управление (например, такую сеть может назначить провайдер Интернет), то эту сеть необходимо разделить с помощью масок на части. (необходимо отметить, что подобная ситуация может иметь место, если вам необходимо назначить узлам вашей сети реальные IP адреса, для того чтобы ваши компьютеры были «видны» из Интернета каждый под своим адресом).

Порядок выполнения работы:

В работе даны 4 варианта задания (Табл. 1). Необходимо сделать все варианты. На приведенной схеме представлена составная локальная сеть. Отдельные локальные сети соединены маршрутизаторами. Для каждой локальной сети указано количество компьютеров. Провайдер, для вас выдал IP-сеть (данные о сети представлены в табл. 2). Ваша задача установить IP-адрес сети и допустимый диапазон адресов. Разделить вашу сеть на части, используя маски. Маску надо выбирать так, чтобы в отделяемой IP подсети было достаточно адресов. Помните, что и порт маршрутизатора, подключенный к локальной сети, имеет IP адрес! Некоторые маски представлены в табл.3.

Таблица 1

Вариант	IP- адрес из сети
1	192.169.168.70
2	172.21.25.202
3	83.14.53.9
4	190.23.23.23

Таблица 2

маска	Сеть 1	Сеть 2	Сеть 3
255.255.248.0	500 комп.	16 комп.	19 комп.
255.255.255.224	1 комп.	4 комп.	2 комп.
255.255.255.128	10 комп.	12 комп.	8 комп.
255.255.255.192	5 комп	3 комп.	3 комп.

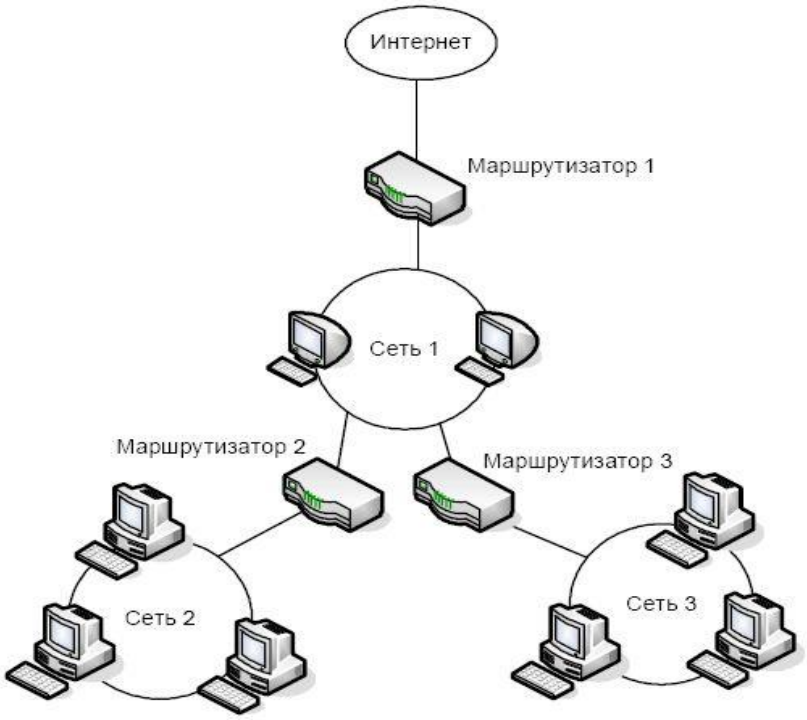


Рис 1.

Таблица 3

Маска	Количество двоичных 0	Количество всех адресов в IP сети с такой маской
255.255.255.252	00	4
255.255.255.248	000	8
255.255.255.240	0000	16
255.255.255.224	00000	32
255.255.255.192	000000	64
255.255.255.128	0000000	128
255.255.255.0	00000000	256
255.255.254.0	0.00000000	512

В отчете заполняем таблицу:

Вариант:	1		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	2		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	3		
Сеть	Сеть 1	Сеть 2	Сеть 3

IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			
Вариант:	4		
Сеть	Сеть 1	Сеть 2	Сеть 3
IP-сети, маска			
Количество IP адресов в IP-сети			
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров.			

Практическая работа №6.

Тема: Определение IP-адресов.

ЦЕЛЬ: Приобретение навыков классификации и анализа IP-адресов.

Теоретический материал.

IP-АДРЕСА. ВВЕДЕНИЕ

В IP-сетях все сетевые устройства (хосты, серверы, шлюзы, маршрутизаторы и т.д.) получают уникальные IP-адреса.

IP-адрес состоит из 4-х байтов (32 битов). Этот адрес используется на сетевом уровне эталонной модели OSI. Он делится на две части.

Первая часть IP-адреса задаёт сеть, в которой располагается сетевое устройство.

Вторая часть IP-адреса однозначно задаёт само сетевое устройство. Для обозначения сетевых устройств используют различные термины:

хост;

сетевой интерфейс.

0 1 2 …		… 29 30 31
Ключ	Номер сети	Номер устройства в сети

Адресное пространство IP-протокола делится на три класса -**A**, **B**, **C**.

Адрес класса **A**:

0	1 2 3 … 7	8 … … 29 30 31
0		
Номер сети		Номер устройства

Адрес класса **B**:

0 1	2 3 4 … …15	16… … 29 30 31
10		
Номер сети		Номер устройства

Адрес класса **C**:

0 1 2	3 4 5 … …23	24… … 29 30 31
110		
Номер сети		Номер устр-ва

IP-АДРЕСА КЛАССА **A.**

Сети класса А имеют 8-битный сетевой префикс «/8».

Структура адреса класса **A**:

0	1 2 3 … 7	8 … … 29 30 31
0		
Номер сети		Номер устройства

Максимальное число сетей класса **A** составляет $2^{7} - 2 = 126$.

Каждая сеть класса **A** поддерживает до $2^{24} - 2 = 16\ 777\ 214$ сетевых устройств.

Адресное пространство, выделенное классу **A,** занимает 50%общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **A** приведён ниже.

Класс адреса	Диапазон значений
A	**1.0.0.0–126.255.255.255**

Примеры адресов сетей класса А:

1.100.120.148
98.180.220.250
121.196.244.198

IP-АДРЕСА КЛАССА **В.**

Сети класса В имеют 16-битный сетевой префикс «/16».

Структура адреса класса **В**:

0 1	2 3 4 … …15	16… … 29 30 31
1 0		
Номер сети		Номер устройства

Максимальное число сетей класса **В** составляет $2^{14} = 16384$.

Каждая сеть класса **В** поддерживает до $2^{16} - 2 = 65\ 534$ сетевых устройств.

Адресное пространство, выделенное классу **В,** занимает 25%общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **В** приведён ниже.

Класс адреса	Диапазон значений
В	**128.0.0.0–191.255.255.255**

Примеры адресов сетей класса **В**:

128.100.120.148
164.180.220.250
190.196.244.198

IP-АДРЕСА КЛАССА **С.**

Сети класса С имеют 24-битный сетевой префикс «/24».

Структура адреса класса **С**:

0 1 2	3 4 5 … …23	24… … 29 30 31
1 1 0		
Номер сети		Номер устр-ва

Максимальное число сетей класса **С** составляет
$2^{21} = 2\ 097\ 152$.

Каждая сеть класса **С** поддерживает до $2^{8} - 2 = 254$ сетевых устройств.

Адресное пространство, выделенное классу **С,** занимает 12.5%общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **С** приведён ниже.

Класс адреса	Диапазон значений
С	**192.0.0.0–223.255.255.255**

Примеры адресов сетей класса **С**:

192.100.120.148

212.180.220.250
223.196.244.198

ОСТАЛЬНЫЕ IP-АДРЕСА.

Оставшийся резерв IP-адресов отводится следующим классам сетей:

Класс адреса	Диапазон значений
D	**224.0.0.0–239.255.255.255**
E	**240.0.0.0–247.255.255.255**
Резерв	**248.0.0.0–254.255.255.255**

В сетях класса **D** первые (0..3) биты адреса имеют значение **1110**. Адреса этого класса используются для поддержки групповой передачи данных.

В сетях класса **E** первые (0..4) биты адреса имеют значение **11110**. Адреса этого класса зарезервированы для экспериментального использования.

ЗАПИСЬ IP-АДРЕСА В РАЗЛИЧНЫХ НОТАЦИЯХ.

Запись IP-адресов.

Примеры записи IP-адресов

в 2-ой,
16-ой,
точечно-десятичной нотациях:

0111 1001	**1100 0100**	**1111 0100**	**1100 0110**
79	**C4**	**F4**	**C6**

121.196.244.198

1001 1001	**1110 0110**	**1101 1010**	**1011 0111**
99	**E6**	**DA**	**B7**

153.230.218.183

1101 1110	**0110 0101**	**0111 0101**	**1100 0110**
DE	**65**	**75**	**78**

222.101.117.120

МАСКА СЕТИ.

Маска сети представляет собою 32-разрядный адрес, 8, 16, 24старших разрядов которого заполнены "1"**.**

Маски сетей классов **A**, **B**, **C** представлены ниже:

Маска IP-адресов класса **A**:

0 1 2 3 … 7	8 … … 29 30 31
11111111	**00000000 00000000 00000000**
FF	**00 00 00**
255.0.0.0	
Маска сети	Номер устройства

Маска IP-адресов класса **B**:

0 1 2 3 4… …15	16… … 29 30 31

11111111 11111111	**00000000 00000000**
FF FF	**00 00**
255.255.0 . 0	
Маска сети	Номер устройства

Маска IP-адресов класса **C**:

0 1 2 3 4 5… …23	24… … 29 30 31
11111111 11111111 11111111	**00000000**
FF FF FF	**00**
255.255.255. 0	
Маска сети	Номер устр-ва

ПРИМЕРЫ МАСОК СЕТЕЙ:

IP-адрес	Маска
192.100.120.148	**255.255.255.0**
10.190.178.177	**255.0.0.0**
144.100.137.125	**255.255.0.0**
123.119.137.223	**255.0.0.0**
222.110.170.190	**255.255.255.0**

СПЕЦИАЛЬНЫЕ IP-АДРЕСА.

Некоторые IP-адреса используются для специальных целей.

IP-адрес	Пояснение
0.0.0.0	**Данный хост (любой сети)**
0.200.150.100	**Хост данной сети (класс A)**
0.0.150.100	**Хост данной сети (класс B)**
0.0.0.100	**Хост данной сети (класс C)**
100.0.0.0	**IP-адрес сети (класс A)**
150.200.0.0	**IP-адрес сети (класс B)**
200.220.240.0	**IP-адрес сети (класс C)**
255.255.255.255	**Широковещание в данной сети(любого класса)**
100.255.255.255	**Широковещание в удаленнойсети класса A**
150.200.255.255	**Широковещание в удаленнойсети класса B**
200.220.240.255	**Широковещание в удаленнойсети класса C**
127.X.X.X	**Тестирование сетевого программного обеспечения**

IP-АДРЕСАЦИЯ В ПОДСЕТЯХ

По мере роста сети Интернет всё острее стала ощущаться нехватка сетевых адресов. В 1985 году данная проблема была разрешена посредством введения подсетей.

Подсети формировались посредством деления IP-адреса на части, именно: номер сетевого устройства сети делится на 2 части:

- номер подсети;
- номер сетевого интерфейса в этой подсети.

2-х уровневая сетевая иерархия (без подсетей):

№ сети	№ хоста в сети

3-х уровневая сетевая иерархия (с подсетями):

№ сети	№ подсети	№ хоста в подсети

Внешние маршрутизаторы (внешние по отношению к сети с заданным №) используют деление IP-адреса на 2 части: № сети и № хоста в сети (как будто никаких подсетей нет).

Внутренние маршрутизаторы (функционирующие внутри сети с заданным №) используют деление IP-адреса на 3 части: № сети, № конкретной подсети и № конкретного хоста в конкретной подсети.

Внешние маршрутизаторы используют в качестве сетевого префикса только адрес сети:

Сетевой префикс	
№ сети	№ хоста в сети

Внутренние маршрутизаторы используют так называемыйрасширенный сетевой префикс, включающий как адрес сети, так и подсети:

Расширенный сетевой префикс		
№ сети	№ подсети	№ хоста в подсети

Пример.

Предположим, в сети класса **B**, сетевой префикс которой имеет значение **150.160.0.0**, сетевой администратор 3-ий байтсетевого адреса отвёл под адреса подсетей:

1-ый и 2-ой байты	3-ий байт	4-ый байт0
№ сети	№ подсети	№ хоста

В этом случае мы получаем следующие параметры сетевой архитектуры:

- класс сети: **B**;
- размер сетевого префикса: 16 разрядов;
- маска сети: **255.255.0.0**;
- адрес сети: **150.160.0.0/16**;
- размер расширенного сетевого префикса: 24 разряда;
- маска подсетей: **255.255.255.0**;
- адреса подсетей:
- **150.160.0.0/24**;
- **150.160.1.0/24**;
- **150.160.2.0/24**;
- **...** ;
- **150.160.254.0/24**;
- **150.160.255.0/24**.

ТИПОВОЕ ЗАДАНИЕ

Условие:

По заданному IP-адресу:

120.140.160.170/14

определить следующие параметры сетевой архитектуры:

1. Класс сети.
2. Маску сети.
3. Адрес сети.
4. Размер расширенного сетевого префикса.

5. Маску подсети.
6. Адрес подсети.
7. Адрес хоста.

Решение:

1. Класс **A** (так как **0 < 120 < 127**).
2. Маска сети: **255.0.0.0**.
3. Адрес сети: **120.0.0.0**.
4. Размер расширенного сетевого префикса: **14** разрядов.
5. Так как размер расширенного сетевого префикса составляет**14** разрядов, маска подсети, представленная в 2-ой системе счисления, состоит из **14** "**1**" и (32 - 14 = 18) **18** "**0**":

14 разрядов маски подсети		**18** разрядов сетевого адреса хоста	
1111 1111	1111 1100	0000 0000	0000 0000
F F	F C	0 0	0 0
255.	252.	0.	0

6. Адрес подсети определяется первыми **14** разрядами заданного IP-адреса. Остальные **18** разрядов заполняются "**0**":

14 сетевых разрядов		**18** разрядов хоста	
0111 1000	1000 1100	0000 0000	0000 0000
7 8	8 C	0 0	0 0
120.	140.	0.	0

7. Адрес хоста определяется первыми **14** "**0**" и **18** остальными разрядами заданного IP-адреса:

14 сетевых разрядов		**18** разрядов хоста	
0000 0000	0000 0000	1010 0000	0000 0000
0 0	0 0	A 0	A A
0.	0.	160.	170

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Определить параметры сетевой архитектуры:

1. Класс сети.
2. Маску сети.
3. Адрес сети.
4. Размер расширенного сетевого префикса.
5. Маску подсети.
6. Адрес подсети.
7. Адрес хоста.

по заданному IP-адресу:

1. **100.110.120.130/10**
2. **140.160.180.200/18**
3. **160.180.200.220/22**
4. **180.200.220.240/26**
5. **200.210.220.230/27**

Практическая работа №7

Тема: Работа с протоколами сетевого уровня

Цель работы: Исследовать вероятностно-временные характеристики сети Internet с использованием утилиты **ping.** Провести анализ состояния фрагментов топологии Internet с использованием утилит **tracer**t и **pathping**.

Краткие теоретические сведения

Утилита ping

Утилита **ping** (*Packet Internet Groper*) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу программ TCP/IP на удаленных машинах, адреса устройств в локальной сети, адрес и маршрут для удаленного сетевого устройства. В выполнении команды **ping** участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на зондируемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание зондируемой машины включено, и машина не отказала ("не висит").

Утилита **ping** имеется в большинстве реализаций TCP/IP для различных операционных систем. В Windows утилита **ping** имеется в комплекте поставки, но представляет собой программу, выполняющуюся в сеансе DOS из командной строки.

Запросы утилиты **ping** передаются по протоколу ICMP (*Internet Control Message Protocol*). Получив такой запрос, программное обеспечение, реализующее протокол IP у адресата, немедленно посылает эхо-ответ. Эхо-запросы посылаются заданное количество раз (ключ **-n**) или по умолчанию до тех пор, пока пользователь не введет команду прерывания (Ctrl+C или Ctrl+Break), после чего выводятся статистические данные.

*Обратите внимание: поскольку с утилиты **ping** начинается хакерская атака, некоторые серверы в целях безопасности могут не посылать эхо-ответы (например,* www.microsoft.com*). Не ждите напрасно, введите команду прерывания.*

Формат команды:

ping [**-t**] [**-a**] [**-n** *число*] [**-l** *размер*] [**-f**] [**-i** *TTL*] **[-v** *TOS*][**-r** *число*] [**-s** *число*] [[**-j** *списокУзлов*]|[**-k** *списокУзлов*]][**-w** *таймау т*] *конечноеИмя*

Параметры утилиты ping

Параметр	Назначение
-t	Отправка пакетов(эхо-запросов) на указанный узел до команды прерывания: Ctrl+Break - для вывода статистики и продолжения работы утилиты; Ctrl+C - для прекращения работы утилиты.
-a	Определение IP-адресов по именам узлов.
-n *число*	Число отправляемых эхо-запросов; по умолчанию – 4.
-l *размер*	Размер поля данных в отправленных пакетах с эхо-запросом; по умолчанию – 32 байта. Максимально – 65527.
-f	Установка флага, запрещающего фрагментацию пакета.
-i *TTL*	Задание времени жизни **в секундах** отправляемого пакета (поле TTL в заголовке пакета) с эхо-запросом. По умолчанию берется значение TTL, заданное по умолчанию для узла. Для узлов **Windows XP** это значение равно **128.** Максимально – 255.
-v *TOS*	Задание типа службы (поле "Type Of Service") в заголовке отправляемого пакета. По умолчанию значение *TOS* – 0. Максимально – 255.
-r *число*	Запись маршрута с эхо-запросом для указанного *числа* переходов. Параметр *число* имеет значение от 1 до 9.
-s *число*	Вариант штампа времени Интернета в заголовке пакета для записи времени прибытия пакета для каждого перехода. Параметр *число* имеет значение от 1 до 4.
-j *списокУзлов*	*Свободный* выбор маршрута по списку узлов; последовательные узлы могут быть разделены шлюзами. *списокУзлов* – это набор IP-адресов (в точечно-десятичной форме), разделенных пробелами.
-k *списокУзлов*	*Жесткий* выбор маршрута по списку узлов; последовательные узлы не могут быть разделены шлюзами.
-w *таймаут*	Интервал времени **в миллисекундах** ожидания эхо-ответа; по умолчанию – 4000 ms. При превышении интервала следует сообщение об ошибке: "Request time out".
конечноеИмя	Имя узла или IP-адрес, в котором маршрут заканчивается

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть: **ping** *конечноеИмя*.

Пример:**tracert**

Утилита **tracert** предназначена для определения маршрута до точки назначения с помощью посылки в точку назначения эхо-запросов протокола Internet Control Message Protocol (ICMP) с различными значениями срока жизни - **TTL** (Time-To-Live). Таким образом, **tracert** позволяет выявлять последовательность шлюзов, через которые проходит IP-пакет на пути к пункту своего назначения.

Формат команды:

tracert [**-d**] [**-h** *максимальноеЧислоПереходов*] [**-j** *списокУзлов*] [**-w** *интервал*] *имяКонечногоКомпьютера*

Параметры утилиты **tracert**

Параметр	Назначение
-d	Запрещает разрешение IP-адресов промежуточных маршрутизаторов в имена.
-h *максимальноеЧислоПереходов*	Задает максимальное число переходов на пути при поиске конечного узла. Значение по умолчанию – 30.
-j *списокУзлов*	Указывает для сообщений с эхо-запросом использование параметра свободной маршрутизации в заголовке IP с набором промежуточных шлюзов, указанных в *спискеУзлов*.
-w *интервал*	Определяет в миллисекундах время ожидания эхо-ответов протокола ICMP, соответствующих данному эхо-запросу. Если эхо-ответ не получен в течении заданного времени, протокол утилиты **tracert** выводит (*). Таймаут по умолчанию – 4000 (4 сек.)
имяКонечногоКомпьютера	Задает узел назначения, указанный IP-адресом или именем узла.

Выходная информация представляет собой список машин, начиная с первого шлюза и кончая пунктом назначения. Кроме того, фиксируется полное время прохождения каждого шлюза.

В следующем примере пакет должен пройти два маршрутизатора (10.0.0.1 и 192.168.0.1), чтобы достигнуть узла 172.16.0.99. Шлюз по умолчанию для

узла имеет адрес 10.0.0.1, а IP-адресом маршрутизатора в сети 192.168.0.0 является адрес 192.168.0.1.

C:\>tracert 172.16.0.99 -d

Трассировка маршрута к 172.16.0.99 с максимальным числом прыжков 30:
1 2 мс 3 мс 2 мс 10.0.0.1
2 75 мс 83 мс 88 мс 192.168.0.1
3 73 мс 79 мс 93 мс 172.16.0.99
Трассировка завершена.

Каждый маршрутизатор, через который проходит путь, обязан перед дальнейшей пересылкой пакета уменьшить значение его поля TTL по меньшей мере на 1. Фактически, TTL — счетчик узлов. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP об истечении времени.

Команда tracert определяет маршрут, посылая **первый** эхо-запрос с полем TTL, равным 1, и увеличивая значение этого поля на единицу для каждого последующего отправляемого эхо-пакета до тех пор, пока конечный узел не ответит или пока не будет достигнуто максимальное значение поля TTL. Максимальное количество переходов по умолчанию равно 30 и может быть изменено с помощью параметра **-h**. Путь определяется из анализа сообщений ICMP об истечении времени, полученных от промежуточных маршрутизаторов, и эхо-ответов точки назначения. Однако некоторые маршрутизаторы не посылают сообщений об истечении времени для пакетов с нулевыми значениями TTL и не видны для команды tracert. В этом случае для перехода отображается ряд звездочек (*). Таким образом, каждое приращение поля времени жизни позволяет пакету пройти на один шлюз дальше.

Команда **tracert** посылает для каждого значения поля времени жизни **три** пакета. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разными машинами. В этом случае на печать выводятся они все. Даже если конкретный шлюз определить нельзя, **tracert** чаще всего сможет увидеть следующие за ним узлы маршрута.

Утилита pathping

Pathping - это средство трассировки маршрута, сочетающее функции программ **ping** и **tracert** и обладающее дополнительными возможностями, которых не имеют две эти программы.. Команда **pathping** в течение некоторого периода времени отправляет многочисленные сообщения с эхо-запросом каждому маршрутизатору, находящемуся между исходным пунктом и пунктом назначения, а затем на основании пакетов, полученных от каждого из них, вычисляет результаты. Поскольку **pathping** показывает степень потери пакетов для каждого маршрутизатора или связи, можно определить маршрутизаторы или подсети, имеющие проблемы с сетью. Команда **pathping** выполняет эквивалентное команде **tracert** действие, идентифицируя маршрутизаторы, находящиеся на пути. Затем она периодически в течение заданного времени обменивается пакетами со всеми маршрутизаторами и на основании числа пакетов, полученных от каждого из них, обрабатывает статистику.

Запущенная без параметров, команда **pathping** выводит справку.

Формат команды:

pathping [**-n**] [**-h** *максимальноеЧислоПереходов*] [**-g** *списокУзлов*] [**-p** *период*] [**-q** *числоЗапросов* [**-w** *интервал*] [**-T**] [**-R**] [*имяКонечногоКомпьютера*]

Параметры утилиты **pathping**

Параметр	Назначение
-n	Предотвращает попытки команды **pathping** сопоставить IP-адреса **промежуточных** маршрутизаторов их именам. Это позволяет ускорить вывод результатов команды **pathping.**
-h *максимальноеЧислоПереходов*	Задает максимальное число переходов на пути при поиске конечного узла. Значение по умолчанию – **30.**
-g *списокУзлов*	Указывает для сообщений с эхо-запросом использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных мест назначения, указанным в параметре *списокУзлов*. При свободной маршрутизации последовательные промежуточные места назначения могут быть разделены одним или несколькими маршрутизаторами. Максимальное число адресов или имен в списке равно **9.** *списокУзлов* представляет собой набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами.
-p *период*	Задает время ожидания между последовательными проверками связи (в миллисекундах). Значение по умолчанию равно **250** миллисекунд (**1/4** секунды).
-q *числоЗапросов*	Задает количество сообщений с эхо-запросом, отправленных каждому маршрутизатору пути. По умолчанию - **100.**
-w *интервал*	Задает время ожидания каждого отклика (в миллисекундах). Значение по умолчанию равно **3000** миллисекунд (**3** секунды)
-T	Присоединяет тег приоритета уровня 2 (например, 802.1p) к сообщениям с эхо-

	запросом, отправляемым каждому сетевому устройству на маршруте. Это помогает обнаружить сетевые устройства, для которых не настроен приоритет уровня 2. Он предназначен для проверки соединений, использующих спецификации **QoS**.
-R	Проверяет, все ли сетевые устройства вдоль маршрута поддерживают протокол **RSVP** (Resource Reservation Setup Protocol, протокол настройки резервирования ресурсов), который позволяет главному компьютеру резервировать определенную часть пропускной способности для потока данных. Этот параметр предназначен для проверки соединений, использующих спецификации QoS.
имя Конечного Компьютера	Задает узел назначения, идентифицированный IP-адресом или именем узла.

Примечания

- Параметры команды **pathping** вводятся с учетом регистра.
  - Во избежание перегрузки сети пакеты должны передаваться через достаточно большие интервалы времени.
  - Чтобы минимизировать эффект потери пакетов, не нужно слишком часто выполнять проверку связи.
  - При использовании параметра **-p** пакеты для проверки связи отсылаются каждому промежуточному узлу отдельно. Поэтому интервал времени между двумя пакетами, переданными одному узлу, составляет: (*период*) x (число узлов).
  - С помощью параметра **-w** пакеты можно отправлять одновременно. Поэтому промежуток времени, указанный в параметре *интервал*, не ограничен промежутком времени, указанным в параметре *период*.
- Использование параметра **-T**

Включение приоритета уровня 2 на узловом компьютере позволяет передавать пакеты с тегом приоритета уровня 2, который используется устройствами уровня 2 для назначения пакету приоритета. Устройства старого типа, которые не распознают приоритет уровня 2, будут отвергать пакеты с тегами, так как они будут выглядеть неправильно сформированными. Данный параметр помогает определить компьютер сети, который отвергает эти пакеты.

- Использование параметра **-R**

Каждому сетевому устройству на маршруте передается сообщение резервирования RSVP для несуществующего сеанса. Если устройство не настроено на поддержку протокола RSVP, оно возвращает сообщение о недоступности протокола ICMP. Если устройство поддерживает протокол

RSVP, оно возвращает ошибку резервирования. Некоторые устройства не могут возвращать ни одно из этих сообщений. В этом случае выводится сообщение о таймауте.

Приведенный ниже пример содержит результаты работы команды **pathping**

```
D:\>pathping -n corp1
Трассировка маршрута к corp1
[10.54.1.196] с максимальным
числом прыжков 30:
  1  172.16.87.35
  2  172.16.87.218
  3  192.168.52.1
  4  192.168.80.1
  5  10.54.247.14
  6  10.54.1.196
Подсчет статистики за: 125 сек. ...
          Исходный узел  Маршрутный узел
Нор RTT   Утер./Отпр.     Утер./Отпр.
Адрес
                          0/ 100 = 0%  |
 1  41мс    0/ 100 = 0%   0/ 100 = 0% 172.16.87.2
                         13/ 100 =    18 |
 2  22мс   16/ 100 = 16%  3/ 100 = 3% 192.68.52.
                          0/ 100 = 0% 1 |
 3  24мс   13/ 100 = 13%  0/ 100 = 0% 192.68.80.
                          0/ 100 = 0% 1 |
 4  21мс   14/ 100 = 14%  1/ 100 = 1% 10.54.247.1
                          0/ 100 = 0% 4 |
 5  24мс   13/ 100 = 13%  0/ 100 = 0% 10.540.10.1
Трассировка завершена.
```

После запуска **pathping** сначала выводится путь. Это тот же путь, который выводится командой **tracert**. Далее команда выдает сообщение о том, что она в течение 125 секунд занята (это время варьируется в зависимости от числа переходов). В течение этого времени происходит сбор сведений со всех маршрутизаторов, перечисленных выше, и со всех соединений между ними. По завершении этого периода выводятся результаты проверки.

В отчете, приведенном выше, столбцы **Маршрутный узел**/ **Утер./Отпр.** и **Адрес** показывают, что при переходе от адреса 172.16.87.218 к 192.168.52.1 теряется 13 процентов пакетов. Остальные соединения работают нормально. Маршрутизаторы в узлах 2 и 4 также пропускают пакеты, адресованные им, но эти потери не оказывают влияние на их способность пересылать пакеты, которые им не адресованы.

Оценки потерь **для соединений** (задаваемых вертикальной чертой | в столбце **Адрес**) показывают перегрузку, вызывающую потерю пакетов, пересылаемых по маршруту. Она свидетельствует о заторах **в каналах связи**. Степень потерь пакетов **на маршрутизаторах** (в правом столбце таких строк указан IP-адрес маршрутизатора) показывает, что процессоры этих маршрутизаторов перегружены.

Задание

►Сформировать **собственное** рабочее пространство доменных имен узлов (не менее шести узлов) для проведения экспериментов с утилитами **ping, tracert, pathping**. Например, mstuca.ru (МГТУ ГА), www.spb.ru (С-Петербург), www.mail.ru (Москва), www.romeguide.it (Италия), www.novol.pl (Польша), www.newslink.org (США).

►С помощью команды **ping** проверить состояние связи с выбранными узлами. Число отправляемых запросов рекомендуется взять равным 20. Сделать экранные копии листингов, выводимых утилитой в каждом эксперименте (для формирования отчета по лабораторной работе).

►Результаты исследований представить в таблице:

Доменное имя	IP-адрес	Страна	Число потерянных запросов, %	Среднее время прохождения запроса, мс	TTL

►Построить диаграммы, графически представляющие статистические данные в последних трех столбцах таблицы .

►С помощью команды **tracert** произвести трассировку узлов из сформированного рабочего пространства доменных имен узлов. Результаты протоколировать в файл отчета по лабораторной работе.

►Представить графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указать наиболее узкие места в сети.

►Описать маршрут прохождения пакета **для двух** из ранее выбранных узлов (страна, город, сеть). Для этого можно использовать графические утилиты трассировки, например, **NeoTrace**, **VisualRoute** и т.п.

►Сравнить статистические данные, полученные в предыдущем эксперименте (для выбранной пары узлов) **с соответствующими** данными для выбранной пары узлов, выводимыми используемой графической утилитой.

►Оценить состояние маршрутов передачи пакетов в сети с помощью утилиты **pathping**.

►Определить перегруженные маршрутизаторы, перегруженные линии связи, процент потерь передаваемых пакетов на перегруженных участках сети. ►Сравнить результаты с **соответствующими** им в предыдущих экспериментах на основе работы утилит **ping** и **tracert**.

Практическая работа № 8.

Тема: Работа с протоколами транспортного уровня

Подготовительная часть

Для проведения данной лабораторной работы необходим компьютер под управлением операционной системы Microsoft Windows XP или более старшей версии.

Все команды будут выполняться в командном интерпретаторе. Для его запуска необходимо нажать кнопку «Пуск» и выбрать раздел «Выполнить…». В строке ввода указать имя команды:

cmd

и нажать кнопку “Ok”. Откроется окно интерпретатора. Команды вводятся с клавиатуры, завершаются вводом “Enter”. Предыдущие команды можно вызвать для редактирования и последующего выполнения с помощью курсорной клавиши «Вверх».

Утилита ipconfig

Данная программа предназначена для получения информации о настройках протокола TCP/IP сетевых интерфейсов ОС Windows. Для получения краткой информации о настройках необходимо выполнить команду ipconfig без параметров.

Задание 1.

Выполните команду **ipconfig** и запишите информацию об IP-адресе, маске сети и шлюзе по умолчанию для сетевого адаптера.

Для получения подробной информации о настройках TCP/IP необходимо выполнить команду ipconfig с ключом /all, т.е. ipconfig /all

Задание 2.

Выполните команду **ipcofig /all** и запишите информацию об аппаратном адресе сетевой карты, списке DNS-серверов сетевого подключения.

1. Утилита route

Утилита route позволяет получить/изменять таблицу маршрутизации локального компьютера. Для того чтобы получить таблицу маршрутизации, необходимо выполнить команду route с параметром print, т.е. **route print**

Задание 3.

Получите таблицу маршрутизации локального компьютера.

Для внесения изменений в таблицу маршрутизации используются параметры **add** и **delete**.

2. Утилита arp

Данная утилита позволяет получить таблицу соответствия IP-адресов и MAC-адресов. В связи с тем, что сетевой уровень вводит свою систему адресов, уникальных в пределах все составной сети, то необходим механизм, с помощью которого можно преобразовывать IP-адреса в аппаратные адреса канального уровня, используемой транспортной сети.

В случае если IP-адрес назначения находится в подсети, подключенной напрямую к одному из сетевых интерфейсов компьютера (т.е. не используя шлюз), то отправитель может отправить пакет данных «напрямую. Для этого

отправитель посылает в соответствующий сетевой интерфейс (согласно таблице маршрутизации) широковещательный запрос по протоколу ARP, содержащий следующие данные:

- MAC-адрес источника
- IP-адрес источника
- искомый IP-адрес

Тот компьютер, который владеет искомым IP-адресом, отвечает на запрос. При этом результат опроса, т.е. MAC-адрес конечного компьютера, сохраняется в таблице ARP отправителя в течение некоторого времени, после которого запись удаляется. Конечный компьютер так же сохраняет в своей таблице ARP соответствие IP-адреса и MAC-адресе отправителя.

Если же удаленный узел достижим через шлюз, то пакет передается ему, и он принимает решение о методе доставке конечному узлу. В этом случае ARP запрос будет послан для выяснения аппаратного адреса шлюза.

Для получения таблицы ARP, необходимо запустить команду arp с ключом -a, т.е. **arp -a**

Задание 4.
Получите таблицу ARP локального компьютера.

Команда arp также позволяет выполнять модификацию таблицы маршрутизации с помощью ключей -s и -d (добавление и удаление соответственно).

3. Утилита netstat

Если запустить команду netstat без параметров, то можно получить список активных TCP соединений между локальным и удаленными компьютерами. В колонке "состояние" отображается статус TCP-соединения.

Задание 5.
Получите список активных TCP-соединений локального компьютера.

По умолчанию netstat выполняет преобразование полученных IP-адресов в символьные имена DNS и номера портов в название сетевых служб. Это замедляет работу netstat, поэтому если преобразование не требуется, то можно указать ключ **–n**

Задание 6.
Получите список активных TCP-соединений локального компьютера без преобразования IP-адресов в символьные имена DNS.

Если указать ключ **-a**, то в списке соединений будут указаны также и прослушиваемые компьютером порты TCP и UDP.

Задание 7.
Получите список прослушиваемых компьютером портов TCP и UDP с и без преобразования IP-адресов в символьные имена DNS.

Утилита netstat в операционной системе Windows XP и старше поддерживает ключ **-o**, с помощью которого можно получить название/идентификатор процесса, создавшего/прослушивающего соединение.

4. Утилита telnet

Данная программа изначально была предназначена для реализации сеансов удаленного терминала с компьютером по сети по протоколу telnet. В качестве «побочного» эффекта утилиты можно отметить ее способность проверять прослушиваемые порту протокола TCP. Формат выполнения команды следующий:

telnet *хост порт*

Хост – это удаленный компьютер, порт – это номер TCP-порта.

Вот значения номеров портов широко известных сетевых служб:

Порт	Служба	Протокол
25	Почтовый сервис	SMTP
110	Почтовый сервис	POP
143	Почтовый сервис	IMAP
80	Веб-сервер	HTTP
443	Веб-сервер поверх SSL	HTTPS
21	Передача файлов	FTP

Если соединение установилось, то, чтобы прервать сессию связи, необходимо перейти в режим команд, для этого нажать **Ctrl** + **]** и набрать команду quit.

Практическая работа №9.

Тема: Настройка протокола TCP/IP в операционных системах.

Цель работы: изучить принципы работы протоколов TCP/IP и научиться их настраивать для работы в сети Интернет.

Теоретическая справка

Хотя Windows поддерживает большое количество сетевых протоколов, TCP/IP используется чаще всего по целому ряду причин:

- обеспечивает межсетевое взаимодействие компьютеров с разной аппаратной архитектурой и операционными системами;
- является основным протоколом, используемым в сети Интернет;
- необходим для функционирования Active Directory.

TCP/IP - это аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet). В терминологии вычислительных сетей протокол - это заранее согласованный стандарт, который позволяет двум компьютерам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому вы часто слышите, как его называют набором, или комплектом протоколов, среди которых TCP и IP - два основных.

В Windows параметры протокола TCP/IP являются частью параметров настройки сетевого адаптера, поэтому все изменения, связанные с этим протоколом, осуществляются через ***Панель управления.***

Для настройки сетевых адаптеров и протоколов дважды щелкните значок ***Сеть и удаленный доступ к сети*** в ***Панели управления.*** Вы также можете выбрать пункт ***Свойства*** в контекстном меню папки Мое

В появившемся окне представлены различные соединения вашего компьютера с внешним миром. После успешной установки сетевого адаптера (во время установки или позже) в окне должен присутствовать как минимум один значок с именем *Подключение по*

локальной сети.

Двойной щелчок значка выводит окно с информацией о состоянии соединения. Можно узнать длительность соединения, его скорость, количество отправленных и принятых пакетов данных.

Кнопка ***Отключить*** позволяет выключить сетевой адаптер, прекратив тем самым обмен данными через него. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения. Отключенные соединения отображаются в виде "серых" значков.

Кнопка *Свойства* вызывает окно настройки свойств соединения, в том числе и параметров используемых протоколов. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения

В этом окне можно получить информацию о сетевом адаптере, через который осуществляется соединение. Щелкнув кнопку *Настроить,* вы откроете окно свойств сетевого адаптера и сможете их изменить.

Установив флажок *Вывести значок подключения на панель задач,* вы включите отображение значка, представляющего соединение, на панели задач Windows. Это позволит наблюдать за активностью соединения и быстро осуществлять его настройку, не используя *Панель управления.*

В центральной части окна в списке представлены все клиенты, службы и протоколы, связанные соединением Для нормального функционирования домена или рабочей группы Windows необходимо наличие следующих компонентов

Компонент	Описание
Клиент для сетей Microsoft	Обеспечивает компьютеру доступ к ресурсам сети Microsoft
Служба доступа к файлам и принтерам сетей Microsoft	Позволяет предоставлять папки и принтеры компьютера в совместный доступ в сетях Microsoft
Протокол Интернета (TCP/IP)	Обеспечивает связь компьютеров в локальных и глобальных сетях

Настройка основных параметров TCP/IP

Стек протоколов TCP/IP, входящий в состав Windows, поддерживает два режима настройки: с использованием статического или динамического IP-адреса. Каждый из этих режимов имеет свои преимущества и недостатки и должен использоваться в зависимости от конфигурации вашей локальной сети:

Преимущества:

Статический IP-адрес	Динамический IP-адрес
Не требуются дополнительные серверы и дополнительная подготовка администратора сети. Соответствие имени компьютера и IP-адреса практически	Все параметры настройки TCP/IP определяются один раз на сервере и автоматически используются рабочими станциями. Нет необходимости вести учет

никогда не изменяется.	используемых IP-адресов. Изменение одного или нескольких глобальных параметров IP-сети требует изменения параметров настройки только на сервере. Общее количество компьютеров может превышать количество выделенных IP-адресов, так как адрес выделяется на время работы компьютера в сети. Удобство настройки TCP/IP на компьютерах временных пользователей.

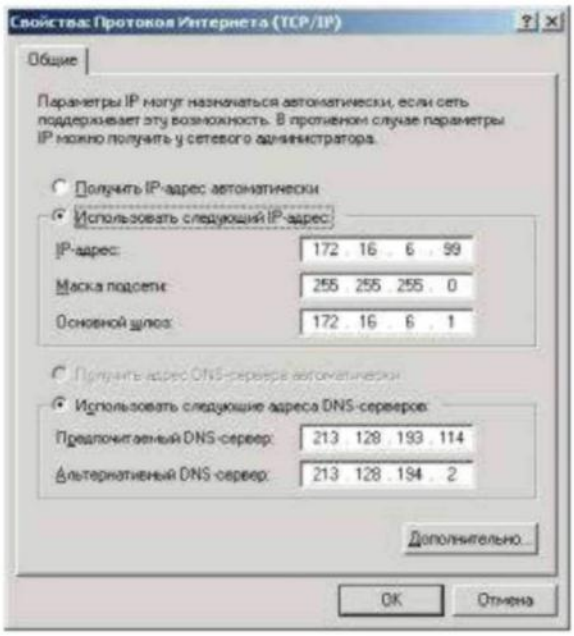
Статический IP-адрес	Динамический IP-адрес
Параметры необходимо изменять вручную на каждом компьютере в сети. Администратор должен вести учет используемых IP-адресов во избежание конфликтов. Изменение одного или нескольких глобальных параметров IP-сети (например адреса DNS-сервера) требует перенастройки TCP/IP на каждом компьютере.	Необходимо наличие сервера, осуществляющего выделение IP-адресов и передачу параметров настройки протокола TCP/IP. DHCP-сервер, входящий в состав Windows Server, обеспечивающий механизм динамического распределения адресов, требует наличия Active Directory и своей авторизации в домене, что существенно усложняет администрирование сети. Постоянное закрепление за компьютером одного и того же адреса не гарантируется. Существуют определенные трудности при использовании DHCP в сложных маршрутизируемых сетях. Работоспособность рабочих станций с динамическими IP-адресами может быть нарушена при выходе из строя или недоступности DHCP-сервера.

Недостатки:

В общем случае статическая адресация удобна в небольших (10-20 компьютеров) одноранговых сетях, состав которых редко изменяется. Если количество компьютеров в сети превышает 20, а компьютеры входят в домен Windows, гораздо проще и удобнее использовать динамическое выделение адресов.

Использование статического IP-адреса

По умолчанию Windows настраивает стек TCP/IP на использование динамически выделяемого IP-адреса. Чтобы использовать статический адрес, это необходимо указать в свойствах протокола TCP/IP. После этого вы должны задать следующие параметры.



IP-адрес - 32-разрядный адрес, представленный в формате W.X.Y.Z. Адрес должен быть уникальным не только в пределах локальной, но и в пределах всего Интернета. Обычно используется один из IP-адресов, выделенный провайдером.

Маска подсети - 32-разрядное число, представленное в формате W.X.Y.Z, которое используется для разделение крупных сетей на несколько более мелких.

Основной шлюз - IP-адрес маршрутизатора, используемого для выхода в глобальные сети и взаимодействия с другими сетями.

Предпочтительный и альтернативный *DNS-серверы* - IP-адреса основного и резервного DNS-серверов, которые будут использоваться стеком TCP/IP для разрешения символьных имен компьютеров в их IP-адреса.

Настроив параметры протокола, щелкните кнопку *ОК.* Для применения новых параметров TCP/IP щелкните кнопку *(Ж* в окне свойств соединения.

Использование динамически выделяемого IP-адреса

Для использование динамически выделяемого IP-адреса необходимо в настройках протокола TCP/IP указать автоматическое получение IP-адреса. Также рекомендуется указать автоматическое получение адресов DNS-серверов, хотя можно указать эту информацию вручную.

Для динамического выделения IP-адреса в локальной сети должен быть установлен и настроен DHCP-сервер.

При недоступности DHCP-сервера используется служба APIPA (автоматическая настройка частных LP-адресов), которая генерирует IP-адрес вида 169.254.Y.Z и маску подсети 255.255.0.0. Если выбранный адрес уже используется, служба генерирует следующий адрес.

Отключение автоматической адресации

По умолчанию функция автоматической настройки частных IP-адресов включена, но можно ее отключить, добавив в системный реестр соответствующий параметр.

Дерево реестра	HKEY_LOCAL_MACHINE
Раздел реестра	SYSTEM\CurrentControlSet\Services\Tcpip \Parameters\Interfaces\{GUID_адаптера}
Имя параметра	IPAutoConfigurationEnabled
Тип параметра	REG_DWORD
Значение	0 - отключить автоматическую адресацию; 1 - включить автоматическую адресацию

Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

Настройка дополнительных параметров TCP/IP

Стек протоколов TCP/IP в Windows достаточно сложен и позволяет настраивать множество дополнительных параметров. Доступ к ним можно получить, щелкнув кнопку *Дополнительно* в окне свойств протокола **TCP/IP.**

На вкладке ***Параметры IP*** можно связать с сетевым адаптером несколько LP-адресов и задать несколько основных шлюзов.

Стек TCP/IP Windows позволяет связать с любым сетевым адаптером несколько IP-адресов. Для каждого из адресов может быть задана своя маска подсети.

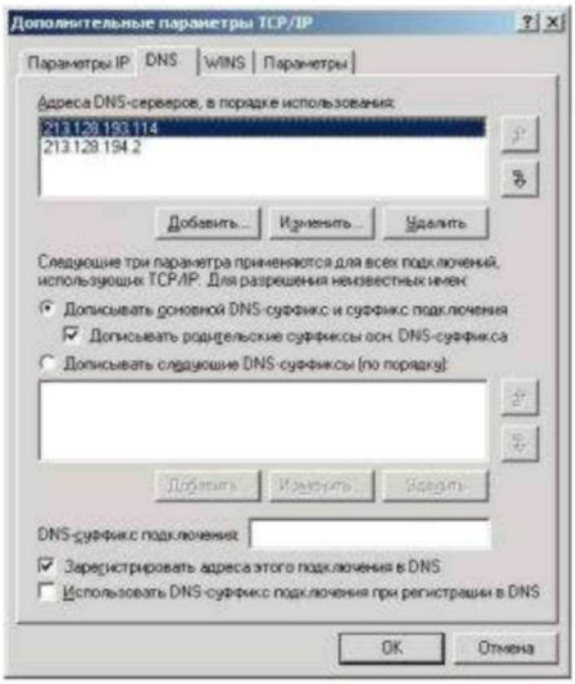
Несколько IP-адресов для одного сетевого адаптера принято использовать в следующих случаях:

- на web и ftp-серверах, обслуживающих большое количество сайтов, каждому из которых должен быть выделен отдельный ЕР-адрес;
- при подключении компьютера к локальной сети с несколькими наложенными IP-сетями; при постоянном перемещении компьютера из одной сети в другую.

Добавить адрес можно, щелкнув кнопку *Добавить.* Первый адрес из списка будет считаться основным и отображаться в окне основных свойств протокола TCP/IP. При использовании нескольких IP-адресов, особенно из разных сетей, необходимо указать несколько основных шлюзов, чтобы обеспечить возможность связи с компьютером извне

по любому из связанных с ним адресов. Кроме того, для повышения надежности можно использовать несколько маршрутизаторов, соединяющих вашу сеть с другими. В этом случае имеет смысл указать в параметрах адреса нескольких основных шлюзов. Для каждого шлюза кроме его адреса задается метрика - целое число от 1 до 9999. Метрики служат для определения приоритета шлюзов. В любой момент времени используется первый доступный шлюз с минимальной метрикой. Таким образом, альтернативный шлюз с метрикой 2 будет использован только при недоступности основного с метрикой I.

Кроме того, можно задать метрику и самого интерфейса. Метрики интерфейсов служат для определения интерфейса, используемого для установления нового соединения. При использовании нескольких сетевых адаптеров метрики применяются для определения приоритета этих адаптеров.



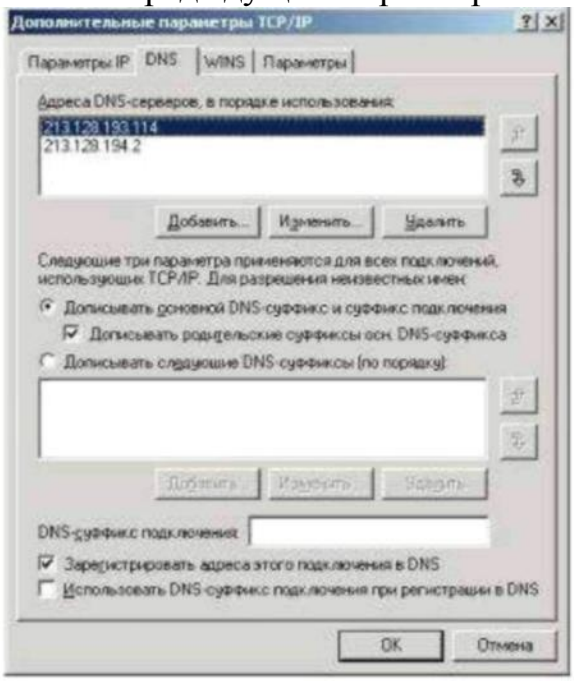
На вкладке *DNS* можно настроить все параметры, связанные со службой DNS. По аналогии с IP-адресами можно задать несколько (более двух) адресов DNS-серверов и определить порядок их использования. Метрики для определения порядка здесь не используются, т. к. при недоступности первого сервера будет использован второй, при недоступности второго - третий и т. д.

В работе DNS используются два параметра, отвечающие за разрешение неполных имен. Первый - основной суффикс DNS - задается на вкладке *Сетевая идентификация* свойств системы и обычно является полным DNS-именем домена, в который входит компьютер. При работе в рабочей группе этот суффикс может быть произвольным и задается при настройке Windows. Второй - DNS-суффикс подключения - задается на вкладке DNS свойств каждого подключения.

Если в параметрах настройки DNS указано *Дописывать основной DNS-суффикс и суффикс подключения,* то при разрешении неполных имен будет использованы соответствующие суффиксы. Например, при использовании основного суффикса msk.net.fio.ru и суффикса подключения lab.msk.net.fio.ru при вводе команды **ping xyz** будет предпринята попытка разрешения имен xyz.msk.net.fio.ru и xyz.lab.msk.net.fio.ru Кроме того, если включен параметр *Дописывать родительские суффиксы,* то при разрешении будут

проверены еще и имена xyz.net.fio.ru, xyz.fio.ru и xyz.ru.

Если в параметрах настройки DNS указано *Дописывать следующие DNS-суффиксы,* то основной суффикс и суффикс подключения использованы не будут, а будет использован (последовательно) указанный список суффиксов. При разрешении неполных имен этот список будет использован аналогично приведенному примеру. Параметр *Зарегистрировать адреса **этого** подключения в DNS* использует основной DNS-суффикс для определения DNS-сервера, обеспечивающего функционирование соответствующей зоны, и автоматически регистрирует на нем запись A со своим именем и IP-адресом соединения. Если для соединения задано несколько IP-адресов или используется несколько соединений, то в DNS будут зарегистрированы несколько записей A с одним и тем же именем, но разными IP-адресами ■*■. Параметр *Использовать DNS-суффикс подключения при регистрации в DNS* позволяет осуществить регистрацию соответствующей записи A на DNS-сервере по аналогии с предыдущим параметром.

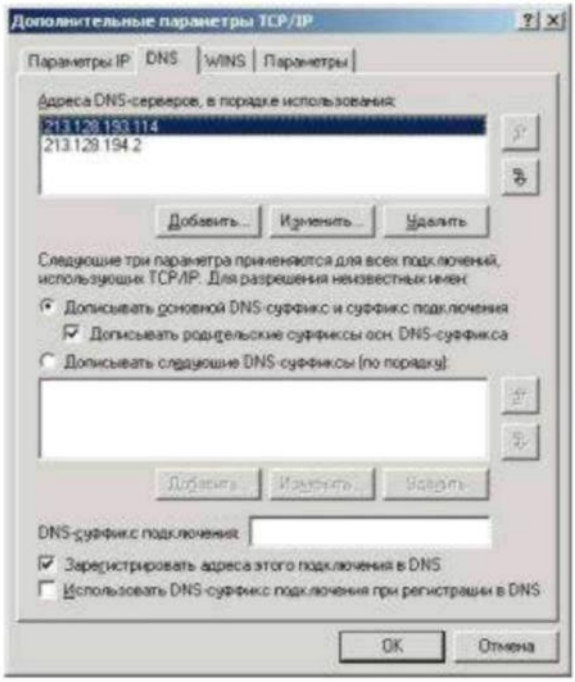


служба предназначена для разрешения имен NetBIOS в IP-адреса. При использовании домена и клиентов Windows использование этой службы не требуется - все ее функции выполняются службой DNS.

Для работы этой службы требуется WINS-сервер, адрес (адреса) которого добавляется в соответствующий список.

Помимо использования WINS-сервера Windows поддерживает устаревший способ разрешения имен NetBIOS- файл LMHOSTS. Можно включить использование этого файла и при необходимости импортировать уже существующий файл. Файл LMHOSTS можно редактировать самостоятельно в любом текстовом редакторе. Этот файл расположен в папке **%systemroot%\ system32\drivers\etc**

Кроме того, на этой вкладке осуществляется управление поддержкой NetBIOS поверх TCP/IP. Такая поддержка требуется для обеспечения совместной работы со старыми NetBIOS-клиентами (Windows 9x, NT). При использовании в локальной сети только Windows, NetBIOS поверх TCP/IP может быть отключен. При использовании динамически выделяемого IP-адреса можно задавать этот параметр через DHCP.



На вкладке ***Параметры*** можно настроить ряд необязательных параметров стека TCP/IP. Windows поддерживает настройку IP-безопасности (протокол IPSec) и фильтрации TCP/IP. Для настройки необходимо выбрать параметр из списка и щелкнуть кнопку *Свойства*.

Порядок выполнения работы

1. Изучить состав и назначение протоколов стека TCP/IP.
2. В системе Windows выполнить настройку стека протоколов TCP/IP для организации работы в сети Интернет. Для этого получить необходимые данные у преподавателя.
3. Создать группу в сети. Добавить в эту группу несколько компьютеров.
4. Поэкспериментировать с настройками Firewall, (пропускание/блокирование ping, HTTP и др.)

Контрольные вопросы.

1. Сколько протоколов образуют стек TCP/IP?
2. Какие уровни протоколов содержит стек TCP/IP?
3. что такое IP - адресация?
4. На каком уровне применяется IP - адресация?
5. Является ли IP - адресация абсолютной или относительной?
6. Поясните понятия статический и динамический IP - адрес.
7. Что такое шлюз?
8. Что такое маршрутизатор?
9. 9
   Для чего применяется маска подсети
10. 7
    Какие службы, устройства, клиенты необходимы для работы в сетях
11. Какие три основных вида угроз безопасности при работе в сети Internet?
12. Рассказать о каждой угрозе при работе в сети Internet.
13. 9
    Виды программ-паразитов (и в чем их различие)
14. Адресация в сети Internet.
15. Основные сетевые протоколы (TCP, IP, UDP, POP, SMTP, DNS, WINS, 1CMP, HTTP,

FTP,). Рассказать о любом по выбору преподавателя.

16. Какие средства сетевой защиты существуют?

Практическая работа 10.

Тема: Работа с диагностическими утилитами протокола TCP/IP

Цель: обобщить и систематизировать знания по теме «Работа с диагностическими утилитами протокола TCP/IP»

Ход работы.

Задание 1. Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам. Для этого в командной строке введите имя утилиты без параметров и дополните **/?**.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname. Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5. Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи

команды.

a) aspu.ru

b) mathmod.aspu.ru

c) yarus.aspu.ru

Задание 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотрите локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
7. Всегда ли можно узнать символьное имя узла по его ip-адресу?
8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Практическая работа № 11
Тема: «Решение проблем с TCP/IP»

Цель: обобщение и систематизация знаний по теме «Организация межсетевого взаимодействия»

Задания к работе

1. Открыть окно командной строки, ввести команду ping с IP адресом машины, при взаимодействии с которой возникают проблемы. Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого доступа.
2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола. Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).
3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:
    1. Использует ли машина статичную или динамичную конфигурацию?
    2. Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?
    3. Получает ли машина адрес DNS сервера автоматически?
    4. Если адрес DNS сервера вводится вручную, то какой адрес используется?
4. Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.
5. Проверьте тип адаптера.
6. Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: IPCONFIG /ALL.
7. Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.
8. Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: *PING LOCALHOST.*
9. Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP адрес.

11. Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО,

сбросьте DNS кэш путем ввода следующей команды: *IPCONFIG /FLUSHDNS.*

Контрольные вопросы

1. Поясните, что может означать, если время TTL закончилось до получения ответа.
2. Как подтвердить наличие сетевого соединения?
3. Что показывает команда IPCONFIG /ALL?
4. Что означает наличие IP адрес со значением 0.0.0.0.?
5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает корректно, и что отсутствуют проблемы с стеком локального протокола TCP/IP?
6. Как производится опрос основного шлюза?
7. Как производится опрос DNS сервера?

Практическая работа № 12

Тема: «Настройка удаленного доступа к компьютеру с помощью модема»

Цель: обобщение и систематизация знаний по теме «Организация межсетевого взаимодействия»

Задания к работе

1. Описать цепи и назначение сигналов интерфейса RS-232.
2. Составить краткую сравнительную характеристику протоколов обмена данными X-modemиZ-modem.
3. Составить блок-схемы следующих алгоритмов:

- алгоритм организации соединения и ведения диалога с удаленным абонентом;
- алгоритм организации соединения и передачи файлов;
- алгоритм организации соединения и приема файлов.

Контрольные вопросы:

1. Протоколы X-modemиZ-modem.
2. Цепи и назначение сигналов интерфейса RS-232.
3. Методы управления потоком в модеме и режимы обмена данными между модемом и компьютером.

Практическая работа № 13

Тема: «Работа с модемом на коммутируемых аналоговых линиях»

Цель: обобщение и систематизация знаний по теме «**Компьютерные глобальные сети с коммуникацией пакетов**»

Задания к работе

1. Составить таблицу стандартов на модемы. В таблицу должны быть внесены следующие стандарты: V.22,V.22bis,V.32,V.32bis,V.34,V.42,V.42bis,V.90,V.92. Таблица должна содержать следующие сведения:

Название стандарта	Стандарт определяет	Основные технические характеристики
…	…	…

2. Составить схему подключения модема. При составлении схемы принять следующие исходные данные. Имеются два ПК. Первый ПК укомплектован внешним модемом, второй – внутренним модемом. На обоих ПК предусмотреть использование телефонов. Телефонная сеть двухпроводная.
3. Пояснить назначение световых индикаторов на лицевой панели внешнего модема.
4. Составить перечень команд, обеспечивающих следующую инициализацию модема:

- разрешить эхо-вывод команд, передаваемых модему;
- разрешить ответ модема на АТ-команды в символьном виде;
- выводить сообщения модема об установлении связи в полном виде;
- номер набирается модемом после паузы при наличии гудка на линии;
- состояние «занято» определяется;
- сигнал DCDустанавливается только тогда, когда модем обнаруживает несущую частоту от удаленного модема;
- режим автоответа выключен;
- при тональном наборе длительность передачи одной цифры номера должна быть 55 миллисекунд.

5. Составить схему и описать локальный аналоговый тест с самотестированием

Контрольные вопросы

1. Назначение модемов.
2. Взаимодействие модемов с оконечным оборудованием и каналом связи.
3. Описать световые индикаторы на лицевой панели внешнего модема и их назначение.

Практическая работа № 14

Тема: «Работа с программой Outlook Express»

Цель: обобщение и систематизация знаний по теме «Информационные ресурсы сети Интернет»

Задания к работе

1. Откройте пункт меню Сервис – Учетные записи (Tools–Accounts).
2. Выберите вкладку Почта (Mail).
3. В поле со списком вы увидите все зарегистрированные учетные записи. Если таковых не имеется, список пуст. Если имеются, очистите список выделив находящиеся в нем учетные записи и нажав кнопку Удалить (Delete).
4. Для создания собственной учетной записи нажмите кнопку Добавить (Add).
5. Выберите значение Почта (Mail).
6. Начинает работать мастер настройки. Следуйте его указаниям.
7. Закончив работу с мастером создания учетной записи вновь войдите в меню Сервис – Учетные записи. Вы должны увидеть только что созданную вами учетную запись. Возможно, она искажена. Выделите запись и нажмите кнопку Свойства (Properties).
8. Здесь имеется несколько вкладок. На вкладке Общие (General) уточните еще раз ваш почтовый адрес.
9. На вкладке Серверы проверьте еще раз подключение вашей машины к почтовому серверу. На прием сообщений это должен быть протокол POP3, на передачу – SMTP.
10. На вкладке Подключение задайте тип подключения вашей станции к почтовому серверу: Локальная сеть.
11. На вкладке Дополнительно задайте режим, когда прочитанные вами сообщения остаются лежать на сервере. Это нужно для того, чтобы потом вы их могли прочитать вручную при подключении к почтовому серверу по протоколу telnet.
12. Для проверки действия почты отправьте первое письмо самому себе. Для этого щелкните мышкой на значке Создать сообщение в левой части панели инструментов. В адресе раскрывшегося окна сообщения наберите student_i@meu.rsuh.ru, затем наберите понятную тему сообщения и в основной части окна наберите нужный текст. Затем щелкните на значке Отправить сообщение на панели инструментов.
13. Проверьте содержимое папки Отправленные. Если в нем содержится отправленное вами письмо, получите его. Для этого надо щелкнуть на значке Доставить почту панели управления.
14. Если письмо получено правильно, покажите его преподавателю.
15. Удалите полученное вами письмо из папки Входящие (для этого выделите это письмо и нажмите клавишу Deleteили щелкните на значке Удалить панели инструментов.

16. Выберите пункт меню Сервер – учетные записи. Выделите вашу учетную запись и удалите ее. Это нужно для работы других групп. На следующем занятии вам вновь надо будет создать собственную учетную запись.

Контрольные вопросы

1. Расскажите устройство адресной книги почтовой программы.
2. Опишите возможность создания новых папок хранения сообщений.
3. Опишите возможность создания псевдонимов почтовых адресатов
4. Опишите возможность добавления стандартной подписи в конце сообщения.
5. Поясните разницу между возможностями ответа на сообщения, ответа всем и пересылки сообщения.

Практическая работа № 15

Тема «Настройка свойств web-браузера»

Цель: обобщение и систематизация знаний по теме «**Информационные ресурсы сети Интернет**»

Задания к работе

1. Выберите [Настройки] пункта [Сервис] строки меню и нажмите кнопку ×.
2. Отрегулируйте или введите информацию о настройках, если это необходимо, нажмите [OK], а затем нажмите кнопку . Для получения дополнительной информации см. пояснения по каждому элементу.
3. Настройки домашней страницы. Можно задать отображение страницы при запуске web-браузера или при выборе меню [Домой].

Адрес	Установка адреса, вводимого в качестве адреса домашней страницы
Использовать пустую страницу	Установка пустой страницы в качестве домашней страницы
Использовать текущую страницу	Установка текущей страницы в качестве домашней страницы

4. Настройки просмотра. Можно задать условия отображения содержания страницы при ее открытии.

Изображения	**Вкл.:** изображения отображаются. **Выкл.:** изображения не отображаются.
Анимация	**Вкл.:** анимация отображается. **Выкл.:** анимация не отображается.
JavaScript	**Вкл.:** JavaScript включен. **Выкл.:** JavaScript выключен.
Flash	**Вкл.:** данные Flash® отображается. **Выкл.:** данные Flash® не отображается.
Сбережение памяти	**Вкл.:** уменьшение объема используемой памяти при отображении веб-страниц. **Выкл.:** использование обычного объема памяти для отображения веб-страниц.

5. Настройки подключения. Можно задать метод выбора подключения для использования при подключении к Интернету.

Автоматический выбор	Последнее используемое подключение выбирается автоматически.
Выбрать вручную	Подключение выбирается вручную при каждом запуске веб-браузера.

6. Настройки прокси-сервера. Можно ввести информацию о настройках прокси-сервера.

Использовать настройки подключения	Перенести в настройки подключения режима инфраструктуры, сохраненные в системе PSP™.
Использовать	Использовать прокси-сервер. Потребуется заполнить поле «Адрес» и «Номер порта».
Не использовать	Не использовать прокси-сервер.

7. Настройки cookie. Можно указать способ работы с файлами cookies.

Разрешить все	Разрешаются все файлы cookie.
Блокировать все	Блокируются все файлы cookie.
Запрашивать подтверждение	Каждый раз при запросе файла cookie запрашивается разрешение или блокировка.

8. Настройки временных файлов. Можно установить размер памяти для временных файлов.

Не использовать	Не использовать временные файлы.
512 Кб	Сохранение временных файлов до 512 Кб.
1024 Кб	Сохранение временных файлов до 1024 Кб.
2048 Кб	Сохранение временных файлов до 2048 Кб.

9. Отказаться от услуги безопасности браузера. Отказ от используемой услуги безопасности браузера. Для настройки этого параметра нужно ввести пароль из 4 символов.
10. Стандартная конфигурация.

Настройки просмотра	**Изображения:** Вкл. **Анимация:** Вкл.**JavaScript:** Вкл. **Flash:** Вы кл. **Сбережение памяти:** Выкл.
Настройки подключения	Автоматический выбор
Настройки прокси-сервера	Использовать настройки подключения
Настройки cookie	Разрешить все
Настройки временных файлов	512 Кб

Контрольные вопросы:

1. Что называется браузером, Web-страницей, Web-сервером , HTML? Приведите примеры браузеров?
2. Какие настройки можно сделать в обозревателе Internet Explorer и для чего?

3. Как настроить обозреватель Internet Explorer, чтоб Web-страницы загружались быстрее?

5. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452574 (дата обращения: 07.12.2020).
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. —
3. Ковган, Н.М. Компьютерные сети : учебное пособие : [16+] / Н.М. Ковган. – Минск : РИПО, 2019. – 180 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599948 (дата обращения: 07.12.2020). – Библиогр. в кн. – ISBN 978-985-503-947-2. – Текст : электронный.
4. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2020. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456799 (дата обращения: 07.12.2020).

Дополнительные источники:

1. Ковган Н.М. Компьютерные сети [Электронный ресурс] : учебное пособие / Н.М. Ковган. — Электрон. текстовые данные. — Минск: Республиканский институт профессионального образования (РИПО), 2020. — 180 с. — 978-985-503-374-6. — Режим доступа: http://www.iprbookshop.ru/67638.html
2. Компьютерные сети [Электронный ресурс] : учебник / В.Г. Карташевский [и др.]. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2020. — 267 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/71846.html
3. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. — Электрон. текстовые данные. — Саратов: Профобразование, 2020. — 333 с. — 978-5-4488-0054-2. — Режим доступа: http://www.iprbookshop.ru/63577.html

Интернет-ресурсы:

1. Федеральный портал «Российское образование», предметный раздел: Компьютерные сети и телекоммуникации: www.edu.ru/
2. Лекции по дисциплине: http://zarabotait.narod.ru/kompyuternie_seti/

Онлайн учебник по дисциплине: http://www.lessons-tva.info/edu/telecom.html