Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

Кафедра электронных приборов

ГЛОБАЛЬНЫЕ И ЛОКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным работам
для студентов направлений «Фотоника и оптоэлектроника» и «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

2012

Шандаров Евгений Станиславович

Глобальные и локальные компьютерные сети: методические указания к лабораторным работам для студентов направлений «Фотоника и оптоэлектроника» и «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства»/ Е.С. Шандаров; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Томский государственный университет систем управления и радиоэлектроники, Кафедра электронных приборов. - Томск : ТУСУР, 2012. - 38 с.

Данный курс лабораторных работ посвящен дисциплине «Глобальные и локальные компьютерные сети» и включает в себя описание 8 лабораторных работ.

Лабораторные работы по курсу проводятся с использованием программного обеспечения операционной системы Linux, бесплатно распространяемого пакета OpenOffice.org и программного продукта PHP, также бесплатно-распространяемого.

В рамках данного курса студенты изучают различные аспекты сетевого взаимодействия компьютеров, работу сетевых протоколов прикладного уровня.

Предназначено для студентов очной и заочной форм, обучающихся по направлению «Фотоника и оптоэлектроника» и по направлению «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства») по курсу «Глобальные и локальные компьютерные сети»

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и
радиоэлектроники»

Кафедра электронных приборов

УТВЕРЖДАЮ
Зав.кафедрой ЭП
_____С.М. Шандаров
«___» _____ 2012 г.

ГЛОБАЛЬНЫЕ И ЛОКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторной работе для студентов направлений
«Фотоника и оптоэлектроника» и «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

Разработчик

_____Е.С. Шандаров
_____2012 г

2012

СОДЕРЖАНИЕ

Введение

Данный курс лабораторных работ посвящен дисциплине «Глобальные и локальные компьютерные сети» и включает в себя описание 8 лабораторных работ.

Лабораторные работы по курсу проводятся с использованием программного обеспечения операционной системы Linux, бесплатно распространяемого пакета OpenOffice.org и программного продукта PHP, также бесплатно-распространяемого.

В рамках данного курса студенты изучают различные аспекты сетевого взаимодействия компьютеров, работу сетевых протоколов прикладного уровня.

Лабораторная работа №1. Определение параметров сетевого соединения компьютера

1.1 Введение

Сейчас любая локальная сеть, как правило, имеет подключение к глобальной сети Интернет. В Интернет передача данных осуществляется с помощью протоколов TCP/IP(Transmission Control Protocol/Internet Protocol) и в локальной сети эти протоколы оказываются также необходимы. Но использование протоколов стека TCP/IP позволяет решать и задачи обмена информацией между локальными компьютерами. Применение в локальных сетях протоколов TCP/IP сближает их с глобальными компьютерными сетями в смысле использования подобных способов адресации и методов администрирования.

1.2 Теоретическая часть

1.2.1 IP-адресация

Передача сообщений в Интернет основана на том, что каждый компьютер сети имеет индивидуальный адрес – IP-адрес. Этот адрес выражается одним 32-разрядным числом, имеющим две смысловые части. Одна часть IP-адреса определяет номер сети, вторая – номер узла(компьютера) в сети. Так как оперировать длинными двоичными числами достаточно сложно, число, определяющее IP-адрес, разбивают на 4 октета – восьмиразрядных двоичных числа, а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса, 10000000 00001010 00000010 00011110 – двоичная форма представления этого же

адреса.

В сети Интернет различные глобальные сети, в зависимости от размера, делятся по классам:

– сети класса A: большие сети общего пользования, первый октет определяет номер сети, три последующие октета – номер узла;

– сети класса B: сети среднего размера. Два первых октета определяют номер сети, два оставшихся – номер узла;

– сети класса C: сети малого размера. В этих сетях три первых октета определяют номер сети и последний октет – номер узла.

В таблице 1.1 представлена общая характеристика схемы Интернет-адресации.

Таблица 1.1 – Общая характеристика схемы Интернет-адресации.

Класс	Диапазон значений первого октета	Общее количество сетей	Максимальное количество узлов в каждой сети
A	1 – 126	126	16 777 214
B	128 – 191	16 382	65 534
C	192 – 223	2 097 150	254

Некоторые IP-адреса имеют специальное назначение, например, адрес:

– представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети;

– 127.любое число (часто 127.0.0.1) – адрес «петли». Данные, переданные по этому адресу, поступают на вход компьютера, как полученные по сети. Такой адрес необходим при отладке сетевых программ;

– 255.255.255.255 – широковещательный адрес. Сообщения, переданные по этому адресу, получают все узлы локальной сети, содержащей компьютер-источник сообщения (в другие локальные сети оно не передается);

– номер сети . все нули – адрес сети;

– все нули . номер узла – узел в данной сети. Может использоваться для передачи сообщений конкретному узлу внутри локальной сети;

– номер сети . все единицы (двоичные) – все узлы указанной сети.

В локальных сетях используются специальные, так называемые «серые» IP-адреса. Они определены документом RFC 1918 (RFC – Requests For Comments, предлагаемый проект стандарта, большинство документов, регламентирующих Интернет, описано в RFC) и приведены в табл. 1.2:

Таблица 1.2 – Диапазоны IP-адресов, используемых в локальных сетях

Диапазоны IP-адресов, используемых в локальных сетях
10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

В небольших по размеру локальных сетях обычно применяется последний диапазон адресов. Сетевые маршрутизаторы не передают информацию для узлов с этими адресами, поэтому она оказывается «запертой» внутри локальной сети. Такая схема позволяет в разных локальных сетях использовать одни и те же IP-адреса и не приводит к конфликтам.

Для повышения гибкости использования IP-адресов деление адреса на части с использованием классов дополняется технологией CIDR (Classless Inter-Domain Routing) – бесклассовой междоменной маршрутизации. В этом случае адрес сети формируется с помощью двух чисел: адреса и **маски**. Маска это тоже 32-разрядное двоичное число, с помощью которого из IP-адреса выделяется адрес сети. Схема формирования адреса сети с использованием маски проста, ее можно пояснить на примере, допустим, адрес представлен двоичным числом 110101, маска числом 111100. Маска накладывается на адрес, как трафарет, в котором единицы соответствуют прорезям, в которых мы «увидим» адрес сети, в нашем примере адрес сети соответствует числу 110100. Маска всегда содержит такое двоичное число, старшие разряды которого подряд единицы, а младшие – нули, единицы представляют «прозрачную» часть трафарета, а нули – «непрозрачную». Маска так же, как и адрес, записывается в виде четырех десятичных чисел, разделенных точками и представляющих двоичные октеты. Для компактной записи пары чисел: IP-адрес-маска, используется также другая форма, например: 10.0.0.8/30. Число до слеша представляет собой IP-адрес, а число после слеша – количество разрядов в IP-адресе, отводимых для адресации сети. Число 30 после слеша соответствует маске 255.255.255.252. После определения адреса сети, оставшаяся часть IP-адреса используется для адресации узлов в сети.

1.2.2 Символьное представление имени компьютера в сети

Каждый компьютер в сети имеет уникальный адрес. При использовании IP-адресации это IP-адрес. Однако человеку достаточно трудно оперировать длинными наборами цифр, не несущих смысловой нагрузки, поэтому всегда применяются системы преобразования имен,

ставящие в соответствие цифровому адресу компьютера его символьное имя. В глобальных сетях и сети Интернет это служба DNS (Domain Name System)~ распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Определенные~ части базы данных доменных имен хранятся на специальных серверах~ DNS-серверах, обрабатывающих запросы любого компьютера и определяющие имя, соответствующее IP-адресу или наоборот. В каждой локальной сети, подключенной к Интернет, работает по крайней мере один DNS-сервер. База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, а точки в имени отделяют части, соответствующие узлам домена, например, www.tusur.ru.

Для именования компьютеров в локальных сетях используются плоские (не имеющие иерархии) символьные имена, так называемые NetBIOS-имена. Протокол NetBIOS (Network Basic Input/Output System), как расширение стандартных функций базовой системы ввода-вывода, был разработан в 1984г. компанией IBM и широко применяется в ее продуктах, а также продуктах компании Microsoft. В протоколе NetBIOS реализован механизм широковещательного разрешения имен, когда все компьютеры в локальной сети получают запрос на разрешение имени, соответствующего некоторому IP-адресу. Кроме того, компания Microsoft для своей сетевой операционной системы Windows NT разработала централизованную службу разрешения имен WINS(Windows Internet Name Service). WINS-сервер, работающий в локальной сети, централизованно обрабатывает все запросы, касающиеся разрешения имен в сетях Windows. При большом числе компьютеров в локальной сети WINS-сервер необходим. Однако в малых сетях, содержащих менее 10 компьютеров, часто используется широковещательный механизм разрешения имен протокола NetBIOS, упрощающий административное обслуживание таких сетей.

1.2.3 Автоматизация процесса назначения IP-адресов узлам сети

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора достаточно сложную и длительную процедуру, если количество компьютеров в локальной сети достаточно велико. Если происходят изменения в сети, например, появляются новые компьютеры, процедуру необходимо выполнить и для них, а в некоторых случаях и выполнить коррекцию предыдущих настроек на уже работающих компьютерах. Протокол DHCP (Dynamic Host Configuration Protocol) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое

назначение IP-адресов. В локальной сети, содержащей DHCP-сервер, каждый компьютер при включении посылает запрос этому серверу на получение IP-адреса. Способы выдачи адресов могут быть различными.

При автоматическом статическом способе выделения адреса DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IP-адресов. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом в этом случае, как и при ручном назначении, существует постоянное соответствие.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время (время подключения к сети), что дает возможность впоследствии повторно использовать этот же IP-адрес другими компьютерами (пользователями).

1.2.4 Адресация компьютеров на канальном уровне

Каждый компьютер, подключенный к сети, имеет сетевой адаптер (сетевую карту) с присвоенным ему адресом. Этот адрес носит название MAC-адреса, он задается при изготовлении сетевого адаптера и впоследствии не изменяется. Длина и другие особенности MAC-адреса зависят от используемой в локальной сети технологии. В сетях Ethernet MAC-адрес имеет длину 6 байт, записанных в шестнадцатеричном формате и разделенных дефисами (например 00-AA-00-4F-2A-9C). Для определения локального адреса по IP-адресу используется протокол разрешения адреса ARP (Address Resolution Protocol). Существует также протокол, решающий обратную задачу ~ нахождение IP-адреса по известному локальному адресу. Он называется RARP ~ реверсивный ARP, и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения. Работа протокола ARP начинается с просмотра так называемой АКР-таблицы (рис.). Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Поле «Тип записи» может содержать одно из двух значений ~ «динамический» или «статический». Статические записи создаются вручную с помощью утилиты **arp** и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор не будут выключены. Динамические же записи создаются модулем протокола ARP, использующим широковещательные возможности локальных сетевых технологий. Динамические записи должны периодически обновляться.

Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш. после того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес, а затем отправляет его уже по адресу компьютера, сформировавшего запрос, так как в адрес отправителя указан в самом запросе.

1.2.5 Сетевые утилиты

В операционной системе Linux существует большое число утилит (специальных программ), предназначенных для управления и анализа сетевых соединений, рассмотрим три из них: IFCONFIG, ARP, NETSTAT.

Утилита IFCONFIG

Позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений, с ее помощью можно определить IP-адрес данного компьютера. Запущенная без параметров, адаптеров и коммутируемых соединений:

```
eth0      Link encap:Ethernet  HWaddr 00:1d:60:38:94:4f
          inet addr:192.168.0.130  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::21d:60ff:fe38:944f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:246109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:211095 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:224796147 (224.7 MB)  TX bytes:40813580 (40.8 MB)
          Interrupt:27 Base address:0xa000

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

```
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:12 errors:0 dropped:0 overruns:0 frame:0
        TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:720 (720.0 B)  TX bytes:720 (720.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:1b:77:72:2d:6e
        inet6 addr: fe80::21b:77ff:fe72:2d6e/64 Scope:Link
        UP BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:1075 errors:0 dropped:0 overruns:0 frame:0
        TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:86321 (86.3 KB)  TX bytes:26876 (26.8 KB)
```

Команду ifconfig следует первой использовать для диагностирования возможных проблем с соединением TCP/IP. С ее помощью можно определить, был ли вообще назначен IP-адрес сетевому адаптеру, а также узнать адрес шлюза.

Утилита NETSTAT

Команда позволяет получить подробную информацию о соединениях, активных в настоящее время. Дополнительные ключи позволяют также получить информацию о сетевых портах, об IP-адресах компьютеров, участвующих в подключении, а также о других сетевых параметрах.

Параметры:

-a

Вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP (рис.).

-e

Вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом **-s**.

-n

Вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.

netstat -a

Активные соединения с интернетом (servers and established)

```
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp       0      0 localhost:ipp    *:*                 LISTEN
tcp       0      0 *:17500          *:*                 LISTEN
tcp       0      0 u5f.local:33799   sjc-not19.sjc.dropb:www ESTABLISHED
tcp      38      0 u5f.local:60223   75.126.110.108-st:https CLOSE_WAIT
```

```
tcp      38      0 u5f.local:34882   v-client-2b.sjc.d:https CLOSE_WAIT
tcp      38      0 u5f.local:40990   v-client-1b.sjc.d:https CLOSE_WAIT
tcp      38      0 u5f.local:34500   ec2-50-16-225-86.:https CLOSE_WAIT
tcp      38      0 u5f.local:38920   v-d-1a.sjc.dropbo:https CLOSE_WAIT
tcp      38      0 u5f.local:57300   ec2-50-16-213-132:https CLOSE_WAIT
tcp6      0      0 localhost:ipp     [::]:*                  LISTEN
udp       0      0 *:bootpc          *:*
udp       0      0 *:17500           *:*
udp       0      0 *:mdns            *:*
udp       0      0 *:41844           *:*
```

-o

вывод активных подключений TCP и включение кода процесса (PID) для каждого подключения. Код процесса позволяет найти приложение на вкладке **Процессы** диспетчера задач Windows. Этот параметр может комбинироваться с ключами **-a**, **-n** и **-p**.

-p *протокол*

Вывод подключений для протокола, указанного параметром *протокол*. В этом случае параметр *протокол* может принимать значения **tcp**, **udp**, **tcpv6** или **udpv6**. Если данный параметр используется с ключом **-s** для вывода статистики по протоколу, параметр *протокол* может иметь значение **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6** или **ipv6**.

-s

Вывод статистики по протоколу. По умолчанию выводится статистика для протоколов TCP, UDP, ICMP и IP. Если установлен протокол IPv6 для Windows XP, отображается статистика для протоколов TCP через IPv6, UDP через IPv6, ICMPv6 и IPv6. Параметр **-p** может использоваться для указания набора протоколов.

-r

Вывод содержимого таблицы маршрутизации IP:

netstat -r

Таблица маршутизации ядра протокола IP

```
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.0.0  *              255.255.255.0  U        0 0        0 eth0
link-local   *              255.255.0.0    U        0 0        0 eth0
default      192.168.0.1    0.0.0.0        UG       0 0        0 eth0
```

Интервал

Обновление выбранных данных с интервалом, определенным параметром *интервал* (в секундах). Нажатие клавиш CTRL+C останавливает обновление. Если этот параметр пропущен, **netstat** выводит выбранные данные только один раз. **/?** Отображение справки в командной строке.

Утилита ARP

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица. Запущенная без параметров, команда arp выводит справку.

Параметры

-a

Вывод таблиц текущего протокола ARP для всех интерфейсов

Чтобы вывести записи ARP для определенного IP-адреса, следует указать его после ключа через пробел:

Arp -a *IP-адрес*

Чтобы вывести таблицы кэша ARP для определенного интерфейса, следует указать параметр **-N**

Arp -a -N *иф_адрес*

иф_адрес, где *иф_адрес* ˜ это IP-адрес, назначенный интерфейсу. Параметр **-N** вводится с учетом регистра.

-g Выполняет те же функции, что и **-a**.

-d *IP-адрес* [*иф_адрес*]

Выполняет удаление записи с определенным IP-адресом. Чтобы удалить запись таблицы для определенного интерфейса, следует указать этот интерфейс после IP-адреса. Чтобы удалить все записи, нужно ввести звездочку (*) вместо параметра *IP-адрес*.

-s *IP-адрес Ethernet_адрес* [*иф_адрес*]

Добавление статической записи, которая сопоставляет IP-адрес с физическим адресом в кэш ARP. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, следует указать параметр *иф_адрес*, где *иф_адрес* - это IP-адрес, назначенный интерфейсу.

1.3 Экспериментальная часть

1.3.1 Задание на лабораторную работу

1. Определить символьное имя компьютера, адрес локальной сети, IP-адрес компьютера, MAC-адрес компьютера.
2. Определить используемую в локальной сети технологию.
3. Определить сетевой адрес, маску подсети, адрес шлюза, интерфейс, метрику.
4. Определить IP-адрес, MAC-адрес, тип

1.3.2 Методические указания по выполнению работы

Работа выполняется индивидуально. С помощью утилит IFCONFIG,

ARP, NETSTAT необходимо получить информацию для заполнения таблиц 1.3 - 1.5.

Таблица 1.3

Символьное имя компьютера	Адрес локальной сети	IP-адрес компьютера	MAC-адрес компьютера	Используемая в локальной сети технология

Таблица 1.4 – Таблица маршрутизации. Активные маршруты

Таблица маршрутизации. Активные маршруты:				
Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика

Таблица 1.5 - Таблица ARP-кэша

Таблица ARP-кэша:		
IP-адрес	MAC-адрес	Тип

Кроме этого, необходимо определить используются ли в локальной сети серверы DNS, WINS, DHCP и если используются, указать их IP-адреса.

1.3.3 Содержание отчета

Отчет по проделанной работе готовится в текстовом редакторе OpenOffice.org Write и предоставляется для проверки в электронном виде в формате электронных документов PDF.

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №2. Использование сетевых утилит операционной системы

2.1 Теоретическая часть

Команда PING

Команда PING является едва ли не самой используемой в локальных сетях командой. Она позволяет тестировать сетевое соединение, получая иформацию о различных его аспектах. Неудачная попытка соединения с каким-либо компьютером, или ошибка получения доступа к общим файлам и папкам, находящимся на других компьютерах локальной сети, может быть вызвана тем, что другие компьютеры просто не получают отправленных им по сети запросов. После введения в командной строке имени команды, в качестве параметра для нее, указывается адрес по которому будут направляться специальные эхо-пакеты, это может быть IP-адрес (рис. 1), или символьное имя компьютера. Получив эхо-запрос, удаленный компьютер сразу же отправляет его обратно по тому адресу, откуда он пришел, команда ping позволяет узнать, пришли ли обратно посланные запросы, проверяя таким образом не только целостность физической среды передачи данных, но и корректную обработку информации на всех остальных семи уровнях модели OSI.

```
ping -c 3 www.tusur.ru
PING www.tusur.ru (88.204.75.138) 56(84) bytes of data.
64 bytes from portal.tusur.ru (88.204.75.138): icmp_seq=1 ttl=60 time=0.860 ms
64 bytes from portal.tusur.ru (88.204.75.138): icmp_seq=2 ttl=60 time=0.909 ms
64 bytes from portal.tusur.ru (88.204.75.138): icmp_seq=3 ttl=60 time=0.873 ms
--- www.tusur.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.860/0.880/0.909/0.040 ms
```

При успешном возвращении запросов можно быть уверенным в том, что среда передачи данных, программное обеспечение TCP/IP, а также все устройства (маршрутизаторы, повторители и др.), встретившиеся на пути между двумя компьютерами, работают нормально. Необходимо отметить, что даже при отсутствии каких-либо неисправностей на пути между двумя компьютерами, один или сразу несколько пакетов могут быть утеряны, как правило, это бывает в случае перегруженности сети, а также с тем, что диагностирующие пакеты имеют очень низкий приоритет и могут быть отброшены в процессе передачи. Если хотя бы один из посланных пакетов вернется, это уже будет означать исправность работы сети. По-умолчанию размер эхо-пакета составляет 32 байта, по указанному адресу направляются эхо-пакеты и после выполнения команды выводится статистика прохождения эхо-пакетов по сети.

Команда TRACEROUTE

Эта команда подобна команде PING, обе посылают в точку назначения эхо-пакеты и затем ожидают их возвращения. Отличие пакетов команды TRACEROUTE от пакетов PING заключается в том, что они имеют различный срок жизни (Time to Live, TTL). Каждый маршрутизатор при прохождении через него пакета уменьшает значение поля TTL в нем на единицу. Первые пакеты, отправляемые командой TRACEROUTE имеют TTL=1, поэтому первый маршрутизатор, получив такой пакет и уменьшив на единицу поле TTL, обнаруживает, что пакет не может быть доставлен по адресу (пакет с TTL=0 не передается маршрутизатором) и возвращает сообщение об ошибке, содержащее IP-адрес маршрутизатора. Получив это сообщение, команда выводит на экран информацию об IP-адресе маршрутизатора и отправляет по прежнему адресу эхо-пакет с TTL=2. Количество маршрутизаторов, через которые может пройти пакет, будет каждый раз увеличиваться на единицу до тех пор, пока пакет не достигнет точки назначения. Таким образом, с помощью команды traceroute можно получить подробный маршрут прохождения пакетов данных между компьютером, на котором была запущена traceroute, и любым удаленным компьютером сети. Это делает traceroute весьма ценным средством обнаружения неисправностей в сетевом соединении: в случае возникновения проблемы с подключением к Web-узлу или к какой-нибудь другой службе Internet можно определить участок, на котором она возникла.

```
traceroute ed.tusur.ru
traceroute to ed.tusur.ru (88.204.77.199), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.404 ms  0.586 ms  0.706 ms
 2  fet-internal.fet.tusur.ru (212.192.122.225)  5.500 ms  5.664 ms  5.878 ms
 3  cl-ft.SUR.net.ru (88.204.72.249)  3.658 ms  3.631 ms  3.718 ms
 4  dl-rk-4.SUR.net.ru (88.204.72.218)  3.688 ms  3.912 ms  4.001 ms
 5  ed.tusur.ru (88.204.77.199)  3.731 ms  3.698 ms  3.856 ms
```

Утилита NSLOOKUP

Утилита nslookup (англ. name server lookup поиск на сервере имён) — утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS (проще говоря, DNS-клиент). Позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера.

```
nslookup www.tusur.ru
Server:         212.192.122.17
Address:    212.192.122.17#53
Name:       www.tusur.ru
Address: 88.204.75.138
```

2.2 Экспериментальная часть

2.2.1 Цель работы

Изучить работу сетевых утилит операционной системы Linux.

2.2.2 Задание на лабораторную работу

Используя сетевые утилиты PING, TRACEROUTE и NSLOOKUP исследовать свойства сетевых соединений компьютера.

2.2.3 Методические указания по выполнению работы

С помощью утилиты PING протестировать соединения с серверами находящимися на разном "расстоянии" от нас: в локальной сети ТУСУР, в городской томской сети, в российском сегменте Интернет, в "мировом" интернете.

С помощью утилиты TRACEROUTE протестировать соединения с серверами находящимися на разном "расстоянии" от нас: в локальной сети ТУСУР, в городской томской сети, в российском сегменте Интернет, в "мировом" интернете.

С помощью утилиты NSLOOKUP определить IP-адреса нескольких интернет ресурсов.

По итогам выполнения работы подготовить отчет. В отчете необходимо представить результаты работы утилит.

2.2.4 Содержание отчета

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №3. Исследование протокола HTTP

3.1 Введение

HTTP (HyperText Transfer Protocol - протокол передачи гипертекста) был разработан как основа World Wide Web.

Работа по протоколу HTTP происходит следующим образом: программа-клиент устанавливает TCP-соединение с сервером (стандартный номер порта-80) и выдает ему HTTP-запрос. Сервер обрабатывает этот запрос и выдает HTTP-ответ клиенту.

3.2 Теоретическая часть

3.2.1 Структура HTTP-запроса

HTTP-запрос состоит из заголовка запроса и тела запроса, разделенных пустой строкой. Тело запроса может отсутствовать.

Заголовок запроса состоит из главной (первой) строки запроса и последующих строк, уточняющих запрос в главной строке. Последующие строки также могут отсутствовать.

Запрос в главной строке состоит из трех частей, разделенных пробелами:

Метод (иначе говоря, команда HTTP):

– GET - запрос документа. Наиболее часто употребляемый метод;

– HEAD - запрос заголовка документа. Отличается от GET тем, что выдается только заголовок запроса с информацией о документе. Сам документ не выдается;.

– POST - этот метод применяется для передачи данных CGI-скриптам. Сами данные следуют в последующих строках запроса в виде параметров;

– PUT - разместить документ на сервере.

Ресурс - это путь к определенному файлу на сервере, который клиент хочет получить (или разместить - для метода PUT). Если ресурс - просто какой-либо файл для считывания, сервер должен по этому запросу выдать его в теле ответа. Если же это путь к какому-либо CGI-скрипту, то сервер запускает скрипт и возвращает результат его выполнения.

Версия протокола - версия протокола HTTP, с которой работает клиентская программа.

Таким образом, простейший HTTP-запрос может выглядеть следующим образом:

GET / HTTP/1.0

Здесь запрашивается корневой файл из корневой директории web-сервера.

Строки после главной строки запроса имеют следующий формат:

Параметр: значение

Таким образом задаются параметры запроса. Это является необязательным, все строки после главной строки запроса могут отсутствовать; в этом случае сервер принимает их значение по умолчанию или по результатам предыдущего запроса (при работе в режиме Keep-Alive).

3.2.2 Наиболее употребительные параметры HTTP-запроса

Connection (соединение)- может принимать значения Keep-Alive и close. Keep-Alive ("оставить в живых") означает, что после выдачи данного документа соединение с сервером не разрывается, и можно выдавать еще запросы. Большинство браузеров работают именно в режиме Keep-Alive, так как он позволяет за одно соединение с сервером "скачать" html-страницу и рисунки к ней. Будучи однажды установленным, режим Keep-Alive сохраняется до первой ошибки или до явного указания в очередном запросе Connection: close.

close ("закрыть") - соединение закрывается после ответа на данный запрос.

User-Agent - значением является "кодовое обозначение" браузера, например:

Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)

Accept - список поддерживаемых браузером типов содержимого в порядке их предпочтения данным браузером, например:

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, */*

Referer - URL, с которого перешли на этот ресурс.

Host - имя хоста, с которого запрашивается ресурс. Необходимо, если на сервере имеется несколько виртуальных серверов под одним IP-адресом. В этом случае имя виртуального сервера определяется по этому полю.

Accept-Language - поддерживаемый язык. Имеет значение для сервера, который может выдавать один и тот же документ в разных языковых версиях.

3.2.3 Формат HTTP-ответа

Формат ответа очень похож на формат запроса: он также имеет заголовок и тело, разделенное пустой строкой.

Заголовок также состоит из основной строки и строк параметров, но формат основной строки отличается от таковой в заголовке запроса.

Основная строка запроса состоит из 3-х полей, разделенных пробелами:

- **версия протокола** - аналогичен соответствующему параметру

запроса;.

– **код ошибки** - кодовое обозначение "успешности" выполнения запроса. Код 200 означает "все нормально" (OK);

– **словесное описание ошибки** - "расшифровка" предыдущего кода. Например для 200 это OK, для 500 - Internal Server Error.

3.2.4 Наиболее употребительные параметры http-ответа

Connection - аналогичен соответствующему параметру запроса. Если сервер не поддерживает Keep-Alive (есть и такие), то значение Connection в ответе всегда close.

Content-Type ("тип содержимого") - содержит обозначение типа содержимого ответа. В зависимости от значения Content-Type браузер воспринимает ответ как HTML-страницу, картинку gif или jpeg, как файл, который надо сохранить на диске, или как что-либо еще и предпринимает соответствующие действия. Значение Content-Type для браузера аналогично значению расширения файла для такой системы как Windows.

Некоторые типы содержимого:

– text/html - текст в формате HTML (веб-страница);

– text/plain - простой текст (аналогичен "блокнотовскому");

– image/jpeg - картинка в формате JPEG;

– image/gif - то же, в формате GIF;

– application/octet-stream - поток "октетов" (т.е. просто байт) для записи на диск.

Content-Length ("длина содержимого") - длина содержимого ответа в байтах.

Last-Modified ("Модифицирован в последний раз") - дата последнего изменения документа.

3.3. Экспериментальная часть

3.3.1 Цель работы

Изучить основы работы с протоколом HTTP.

3.3.2 Задание на лабораторную работу

С помощью программы TELNET осуществить взаимодействие по протоколу HTTP с несколькими web-ресурсами, находящимися на разном "расстоянии" от нас: в локальной сети ТУСУР, в городской томской сети, в российском сегменте Интернет, в "мировом" интернете. В форме запроса клиента применить следующие опции:

– запрос обычного html документа;

– запрос изображения с сервера;

– запрос с передачей параметров по методу GET (например запрос на поисковый сервер);

– запрос с передачей параметров по методу POST (например запрос на авторизацию).

3.3.3 Методические указания по выполнению работы

Для связи с сервером по протоколу HTTP с помощью программы TELNET вам, возможно пригодится следующая конструкция:

telnet www.tusur.ru 80

По окончании работы необходимо подготовить отчет. В отчете привести тексты запросов клиента и ответов сервера.

3.3.4 Содержание отчета

Отчет по проделанной работе готовится в текстовом редакторе OpenOffice.org Write и предоставляется для проверки в электронном виде в формате электронных документов PDF.

Отчет должен состоять из следующих частей:

– введение;
– постановка задачи;
– основная часть;
– заключение;
– приложение.

Лабораторная работа №4. Исследование технологии CGI

4.1 Введение

Common Gateway Interface - средство расширения возможностей технологии World Wide Web
Спецификация CGI была разработана в Центре Суперкомпьютерных Приложений Университета штата Иллинойс (NCSA). Работы над ней велись параллельно с Mosaic. С точки зрения общей архитектуры программного обеспечения World Wide Web, CGI определила все дальнейшее развитие системных средств.

До появления этой спецификации все новые возможности реализовывались в виде модулей, включенных в библиотеку общих кодов ЦЕРН. Разработчики серверов должны были использовать эти коды для реализации программ или заменять их своими собственными аналогами. Это означало, что после компиляции сервера добавить в него новые возможности будет невозможно. CGI в корне изменила эту практику.

Главное назначение Common Gateway Interface - обеспечение единообразного потока данных между сервером и прикладной программой, которая запускается из-под сервера. CGI определяет протокол обмена данными между сервером и программой. Для тех, кто знаком с протоколом HTTP, может показаться, что CGI - это просто подмножество этого протокола. Однако это не так. Во-первых, CGI определяет порядок взаимодействия сервера с прикладной программой, в котором сервер выступает инициирующей стороной, во-вторых, CGI определяет механизм реального обмена данными и управляющими командами в этом взаимодействии, что не определено в HTTP. Естественно, что такие понятия, как метод доступа, переменные заголовка, MIME, типы данных, заимствованы из HTTP и делают спецификацию прозрачной для тех, кто знаком с самим протоколом.

4.2 Теоретическая часть

При описании различных программ, которые вызываются сервером HTTP и реализованы в стандарте CGI, используют следующую терминологию:

- CGI-скрипт - программа, написанная в соответствии со спецификацией Common Gateway Interface. CGI-скрипты могут быть написаны на любом языке программирования (C, C++, PASCAL, FORTRAN и т.п.) или командном языке (shell, cshell, командный язык MS-DOS, Perl и т.п.);

- Шлюз - это CGI-скрипт, который используется для обмена данными с другими информационными ресурсами Internet или приложениями-демонами.

Обычная CGI-программа запускается сервером HTTP для выполнения некоторой работы, возвращает результаты серверу и завершает свое выполнение.

Шлюз выполняется точно также, только, фактически, он инициирует взаимодействие в качестве клиента с третьей программой. Если эта третья программа является сервисом Internet, например, сервер Gopher, то шлюз становится клиентом Gopher, который посылает запрос по порту Gopher, а после получения ответа пересылает его серверу HTTP.

Механизмы обмена данными

Собственно спецификация CGI описывает четыре набора механизмов обмена данными:

- через переменные окружения;
- через командную строку;
- через стандартный ввод;
- через стандартный вывод.

Переменные окружения

При запуске внешней программы сервер создает специфические переменные окружения, через которые передает приложению как служебную информацию, так и данные. Все переменные можно разделить на общие переменные окружения, которые генерируются при любой форме запроса, и запрос-ориентированные переменные.

К общим переменным окружения относятся:
ERVER_SOFTWARE - определяет имя и версию сервера.
SERVER_NAME - определяет доменное имя сервера.
GATEWAY_INTERFACE - определяет версию интерфейса.

К запрос-ориентированным относятся:
SERVER_PROTOCOL - протокол сервера. Вообще говоря, CGI разрабатывалась не только для применения в World Wide Web с протоколом HTTP, но и для других протоколов также, но широкое применение получила только в WWW;

SERVER_PORT - определяет порт TCP, по которому осуществляется взаимодействие. По умолчанию для работы по HTTP используется 80 порт, но он может быть и переназначен при конфигурировании сервера;

REQUEST_METHOD - определяет метод доступа к информационному ресурсу. Это важнейшая переменная в CGI. Разные методы доступа используют различные механизмы передачи данных. Данная переменная может принимать значения GET, POST, HEAD и т. п.;

PATH_INFO - передает программе путь, часть спецификации URL, в

том виде, в котором она указана в клиентом. Реально это означает, что передается путь (адрес скрипта) в виде, указанном в HTML-документе;

PATH_TRANSLATED - то же самое, что и PATH_INFO, но только после подстановки сервером определенных в его конфигурации вставок. Дело в том, что при конфигурировании сервера некоторым элементам (ветвям) дерева файловой системы можно назначить синонимы. Типичным примером такого сорта является назначение типа:

cgi-bin ----------> /usr/local/etc/httpd/cgi-bin

В данном случае справа указано стандартное место CGI скриптов для сервера NCSA, а слева - его синоним. При получении скриптом test управления, в переменной окружения PATH_INFO будет значение:

"/cgi-bin/test", а в PATH_TRANSLATED -

"/usr/local/etc/httpd/cgi-bin/test".

SCRIPT_NAME - определяет адрес скрипта так, как он указан клиентом.

Если не указаны параметры, то значение этой переменной будут совпадать с PATH_INFO, но если переменные указаны, то все, что следует за знаком "?" будет отброшено.

PATH_INFO ----------> "/cgi-bin/search?nuclear+isotop"

SCRIPT+NAME --------> "/cgi-bin/search"

QUERY_STRING - переменная определяет содержание запроса к скрипту. Чрезвычайно важна при использовании метода доступа GET. Возвращаясь к примеру с адресами скрипта укажем, что в QUERY_STRING помещается все, что записано после символа "?".

QUERY_STRING -------> "nuclear+isotop"

При этом никакого преобразования строки запроса сервером не производится. Все манипулирования с содержанием QUERY_STRING возложены на скрипт.

Следующий набор переменных связан с идентификацией пользователя и его машины:

REMOTE_HOST - доменный адрес машины, с которой осуществляется запрос.

REMOTE_ADDR - IP-адрес запрашивающей машины.

AUTH_TYPE - тип идентификации пользователя. Используется в случае если скрипт защищен от несанкционированного использования.

REMOTE_USER - используется для идентификации пользователя.

REMOTE_IDENT - данная переменная порождается сервером, если он поддерживает идентификацию пользователя по протоколу RFC-931. Рекомендовано использование этой переменной для первоначального использования скрипта.

Следующие две переменные определяют тип и длину передаваемой информации от клиента к серверу.

CONTENT_TYPE - определяет MIME-тип данных, передаваемых скрипту. Используя эту переменную можно одним скриптом обрабатывать различные форматы данных.

CONTENT_LENGTH - определяет размер данных в байтах, которые передаются скрипту. Данная переменная чрезвычайно важна при обмене данными по методу POST, т.к. нет другого способа определить размер данных, которые надо прочитать со стандартного ввода.

Возможна передача и других переменных окружения. В этом случае перед именем указывается префикс "HTTP_". Отдельный случай представляют переменные, порожденные в заголовке HTML-документа в тагах META. Они передаются в заголовке сообщения и некоторые серверы могут порождать переменные окружения из этих полей заголовка.

Опции командной строки

Командная строка используется только при запросах типа ISINDEX. При HTML FORMS или любых других запросах неопределенного типа командная строка не используется. Если сервер определил, что к скрипту обращаются через ISINDEX-документ, то поисковый критерий выделяется из URL и преобразуется в параметры командной строки. При этом знаком разделения параметров является символ "+". Тип запроса определяется по наличию или отсутствию символа "=" в запросе. Если этот символ есть, то запрос не является запросом ISINDEX, если символа нет, то запрос принадлежит к типу ISINDEX. Параметры, выделенные из запроса, помещаются в массив параметров командной строки argv. При этом после из выделения происходит преобразование всех шестнадцатеричных символов в их ASCII коды. Если число параметров превышает ограничения, установленные в командном языке, например в shell, то формирования командной строки не происходит и данные передаются только через QUERY_STRING. Вообще говоря, следует заранее подумать об объеме данных, передаваемом скрипту и выбрать соответствующий метод доступа. Размер переменных окружения тоже ограничен, и если

необходимо передавать много данных, то лучше сразу выбрать метод POST, т.е. передачу данных через стандартный ввод.

Формат стандартного ввода

Стандартный ввод используется при передаче данных в скрипт по методу POST. Объем передаваемых данных задается переменной окружения CONTENT_LENGTH, а тип данных – переменной CONTENT_TYPE.

Если из HTML-формы надо передать запрос типа: a=b&b=c,

то

CONTENT_LENGTH=7,

CONTENT_TYPE=application/x-www-form-urlencoded, а первым символом в стандартном вводе будет символ "a". Следует всегда помнить, что конец файла сервером в скрипт не передается, а поэтому завершать чтение следует по числу прочитанных символов.

Формат стандартного вывода

Стандартный вывод используется скриптом для возврата данных серверу. При этом вывод состоит из заголовка и собственно данных. Результат работы скрипта может передаваться клиенту без каких-либо преобразований со стороны сервера, если скрипт обеспечивает построение полного HTTP-заголовка, в противном случае сервер заголовок модифицирует в соответствии со спецификацией HTTP. Заголовок сообщения должен отделяться от тела сообщения пустой строкой. Обычно в скриптах указывают только три поля HTTP-заголовка:

Content-type, Location, Status.

Content-type указывается в том случае, когда скрипт сам генерирует документ "на лету" и возвращает его клиенту. В этом случае реального документа в файловой системе сервера не остается. При использовании такого сорта скриптов следует учитывать, что не все серверы и клиенты отрабатывают так, как представляется разработчику скрипта. Так, при указании Content-type: text/html, некоторые клиенты не реализуют сканирования полученного текста на предмет

наличия в нем встроенной графики. Обычно в Content-type указывают текстовые типы text/plain и text/html.

Location используется для переадресации. Иногда переадресация помогает преодолеть ограничения сервера или клиента на обработку встроенной графики или серверной предобработки. В этом случае скрипт создает файл на диске и указывает его адрес в Location. Сервер, таким образом, передает реально существующий файл.

4.3 Экспериментальная часть

4.3.1 Цель работы

Познакомиться с технологией CGI и языком PHP. Написать простейшие CGI-скрипты.

4.3.2 Задание на лабораторную работу

На языке PHP написать скрипт, который выводит на странице имена и значения переменных окружения, текущее время и дату на сервере.

4.3.3 Методические указания по выполнению работы

Написать скрипт.

По итогам выполнения работы подготовить отчет. В отчете привести исходный код скрипта и результат его работы.

4.3.4 Содержание отчета

Отчет по проделанной работе готовится в текстовом редакторе OpenOffice.org Write и предоставляется для проверки в электронном виде в формате электронных документов PDF.

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №5. Изучение механизма Cookies

5.1 Введение

Cookie является решением одной из наследственных проблем HTTP спецификации. Эта проблема заключается в непостоянстве соединения между клиентом и сервером, как при FTP или Telnet сессии, т.е. для каждого документа (или файла) при передаче по HTTP протоколу посылается отдельный запрос.
Включение cookie в HTTP протокол дало частичное решение этой проблемы.

Cookie это небольшая порция информации, которую сервер передает клиенту. Клиент (броузер) будет хранить эту информацию и передавать ее серверу с каждым запросом как часть HTTP заголовка. Некоторые cookie хранятся только в течение одной сессии, они удаляются после закрытия броузера. Другие, установленные на некоторый период времени, записываются в файл.

Сами по себе cookies не могут делать ничего, это только лишь некоторая информация. Однако, сервер может реагировать на содержащуюся в cookies информацию. Например, в случае авторизованного доступа к чему либо через WWW, в cookies сохраняется login и password в течение сессии, что позволяет не вводить их при запросе каждого запаролированного документа. Другой пример: cookies могут использоваться для построения персонализированных страниц.

Полное описание поля Set-Cookie HTTP заголовка:

Set-Cookie: NAME=VALUE; expires=DATE; path=PATH;
domain=DOMAIN_NAME; secure

Минимальное описание поля Set-Cookie HTTP заголовка:

Set-Cookie: NAME=VALUE;

NAME=VALUE - строка символов, исключая перевод строки, запятые и пробелы. NAME-имя cookie, VALUE - значение.

expires=DATE - время хранения cookie, т.е. вместо DATE должна стоять дата в формате Wdy, DD-Mon-YYYY HH:MM:SS GMT, после которой истекает время хранения cookie. Если этот атрибут не указан, то cookie хранится в течение одного сеанса, до закрытия броузера.

domain=DOMAIN_NAME - домен, для которого значение cookie действительно. Например, domain=cit-forum.com. В этом случае значение cookie будет действительно и для сервера cit-forum.com, и для www.cit-forum.com. Если этот атрибут опущен, то по умолчанию используется доменное имя сервера, с которого было выставлено значение cookie.

path=PATH - этот атрибут устанавливает подмножество документов, для которых действительно значание cookie. Например, указание path=/win приведет к тому, что значение cookie будет действительно для множества документов в директории /win/, в директории /wings/ и файлов в текущей директории с именами типа wind.html и windows.shtml.

Если этот атрибут не указан, то значение cookie распространяется только на документы в той же директории, что и документ, в котором было установлено cookie.

secure - если стоит такой маркер, то информация cookie пересылается только через HTTPS (HTTP с использованием SSL). Если этот маркер не указан, то информация пересылается обычным способом.

5.3 Экспериментальная часть

5.3.1 Цель лабораторной работы

Познакомиться с механизмом использования Cookies

5.3.2 Задание на лабораторную работу

Создать систему авторизации пользователя с помощью механизма Cookies.

5.3.3 Методические указания по выполнению работы

Создать скрипт с формой авторизации пользователя. Обеспечить доступ к внутренней странице только авторизованным пользователям.

По окончании работы подготовить отчет с исходными текстами скриптов и внешним видом страниц сайта.

5.3.4 Содержание отчета

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №6. Исследование протокола SMTP

6.1 Введение

Основная задача протокола SMTP (Simple Mail Transfer Protocol) заключается в том, чтобы обеспечивать передачу электронных сообщений (почту). Для работы через протокол SMTP клиент создаёт TCP соединение с сервером через порт 25. Затем клиент и SMTP сервер обмениваются информацией пока соединение не будет закрыто или прервано. Основной процедурой в SMTP является передача почты (Mail Procedure). Далее идут процедуры форвардинга почты (Mail Forwarding), проверка имён почтового ящика и вывод списков почтовых групп. Самой первой процедурой является открытие канала передачи, а последней - его закрытие.

Команды SMTP указывают серверу, какую операцию хочет произвести клиент. Команды состоят из ключевых слов, за которыми следует один или более параметров. Ключевое слово состот из 4-х символов и разделено от аргумента одним или несколькими пробелами. Каждая командная строка заканчивается символами CRLF. Вот синтаксис всех команд протокола SMTP (SP - пробел):

HELO <SP> <domain> <CRLF>
MAIL <SP> FROM:<reverse-path> <CRLF>
RCPT <SP> TO:<forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM:<reverse-path> <CRLF>
SOML <SP> FROM:<reverse-path> <CRLF>
SAML <SP> FROM:<reverse-path> <CRLF>
VRFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP <SP> <string> <CRLF>
NOOP <CRLF>
QUIT <CRLF>

Обычный ответ SMTP сервера состоит из номера ответа, за которым через пробел следует дополнительный текст. Номер ответа служит индикатором состояния сервера.

Отправка почты

Первым делом подключаемся к SMTP серверу через порт 25. Теперь надо передать серверу команду HELLO и наш IP адрес:

C: HELLO 88.204.75.135
S: 250 ms.tusur.ru is ready

При отправке почты передаём некоторые нужные данные (отправитель, получатель и само письмо):

C: MAIL FROM:<shandarov> 'указываем отправителя

S: 250 OK

C: RCPT TO:<shandarov@mail.ru> 'указываем получателя
S: 250 OK
указываем серверу, что будем передавать содержание письма (заголовок и тело письма)
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
передачу письма необходимо завершить символами CRLF.CRLF
S: 250 OK

C: From: Shandarov <shandarov@mail.ru>
C: To: support <support@mail.ru>
C: Subject: Hello
между заголовком письма и его текстом не одна пара CRLF, а две.
C: Hello Drol!
C: You will be die on next week!
заканчиваем передачу символами CRLF.CRLF
S: 250 OK
Теперь завершаем работу, отправляем команду QUIT:
S: QUIT
C: 221 ms.tusur.ru is closing transmission channel

Другие команды

– SEND - используется вместо команды MAIL и указыает, что почта должна быть доставлена на терминал пользователя.

– SOML, SAML - комбинации команд SEND или MAIL, SEND и MAIL соответственно.

– RSET - указвает серверу прервать выполнение текущего процесса. Все сохранённые данные (отправитель, получатель и др) удаляются. Сервер должен отправить положительный ответ.

– VRFY - просит сервер проверить, является ли переданный аргумент именем пользователя. В случае успеха сервер возвращает полное имя пользователя.

– EXPN - просит сервер подтвердить, что переданный аргумент - это список почтовой группы, и если так, то сервер выводит членов этой группы.

– HELP - запрашивает у сервера полезную помощь о переданной в качестве аргумента команде.

– NOOP - на вызов этой команды сервер должен положительно ответить. NOOP ничего не делает и никак не влияет на указанные до этого данные.

6.3 Экспериментальная часть

6.3.1 Цель лабораторной работы

Познакомиться с протоколом SMTP

6.3.2 Задание на лабораторную работу

Освоить основные команды протокола SMTP, написать web-приложение для отправки почты.

6.3.3 Методические указания по выполнению работы

С помощью программы TELNET отправить электронное письмо.

Создать скрипт с формой подготовки и отправки электронного письма.

По окончании работы подготовить отчет с исходными текстами скриптов и внешним видом страниц сайта.

6.3.4 Содержание отчета

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №7. Исследованиие протокола FTP

7.1 Теоретическая часть

FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Исходящий порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

7.2. Экпериментальная часть

7.2.1 Цель лабораторной работы

Познакомиться с протоколом FTP.

7.2.2 Задание на лабораторную работу

Освоить основные команды протокола FTP, загрузить файл с FTP-сервера, отправить файл на FTP-сервер.

7.2.3 Методические указания по выполнению работы

Изучить команды протокола FTP с помощью системы man.

С помощью программы FTP подключиться к ftp-серверу ed.tusur.ru.

Загрузить с сервера на клиентский компьютер файл текстовый и файл бинарный.

Отправить на сервер небольшой файл.

Протестировать функцию докачки при обрыве соединения

По окончании работы подготовить отчет со скриншотами, списком и описанием команд протокола.

7.2.4 Содержание отчета

Отчет по проделанной работе готовится в текстовом редакторе OpenOffice.org Write и предоставляется для проверки в электронном виде в формате электронных документов PDF.

Отчет должен состоять из следующих частей:

- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Лабораторная работа №8. Знакомство с MIME-типами

8.1 Экспериментальная часть
8.1.1 Цель лабораторной работы

Познакомиться с MIME-типами.

8.1.2 Задание на лабораторную работу

Создать web-приложение с помощью которого представить данные в различных MIME-типах.

8.1.3 Методические указания по выполнению работы

Изучить набор стандартных MIME-типов.
На сервере в своей папке подготовить следующий набор файлов:
- текстовый файл;
- html-документ;
- xml-документ;
- изображение в формате JPEG;
- файл PDF.

Создать web-приложение с помощью которого можно указанные файлы представить в следующих MIME-типах:
- text/plain;
- text/html;
- text/xml;
- image/jpeg;
- application/pdf;
- application/octet-stream.

По окончании работы подготовить отчет со скриншотами, исходным текстом программ и собственными выводами по работе.

8.3.4 Содержание отчета

Отчет должен состоять из следующих частей:
- введение;
- постановка задачи;
- основная часть;
- заключение;
- приложение.

Приложение А

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и
радиоэлектроники»

Кафедра электронных приборов

дисциплина «Глобальные и локальные компьютерные сети»

ОТЧЕТ
по лабораторной работе
«_____»

Выполнил
Студент гр. _____
_____И.О. Фамилия
_____ 2012 г

Проверил преподаватель
_____ И.О. Фамилия
_____2012 г

2012

Учебное пособие

Шандаров Е.С.

Глобальные и локальные компьютерные сети
Методические указания по самостоятельной работе

Усл. печ. л. _____. Препринт
Томский государственный университет
систем управления и радиоэлектроники
634050, г.Томск, пр.Ленина, 40