Лабораторная работа №1

Сетевые сервисы: DHCP, DNS, HTTP, FTP, EMAIL

Цель: получить начальные навыки настройки в Cisco Packet Tracer служб динамического назначения IP-адресов, поддержки доменных имен, предоставления гипертекстовой информации, обмена файлами и сообщениями электронной почты

1. Теоретические сведения

Адресация узлов в IP сетях

Каждый сетевой узел в IP сетях может иметь три типа адресов:

- **Локальный адрес**. Определяется сетевой технологией канального уровня. В технологии Ethernet локальным адресом узла является MAC-адрес сетевого адаптера или порта маршрутизатора. Например, 11-A0-17-3D-BC-01. MAC-адрес является уникальным для каждого сетевого интерфейса и хранится в памяти контроллера сетевого адаптера. Присвоение MAC-адреса адаптеру выполняется производителем сетевого оборудования из диапазона, который был назначен ему координирующим комитетом IEEE Registration Authority. Наибольшее распространение получили адреса MAC-48. Они используются в таких технологиях, как Ethernet, Token Ring, FDDI, WiMAX и других. Их размер равен 48 бит, а адресное пространство MAC-48 насчитывает 2^{48} (281 474 976 710 656) адресов. Старшие 3 байта MAC-адреса – это идентификатор фирмы производителя, а младшие 3 байта определяются уникальным образом самим производителем.

- **IP-адрес (IP_v4)**. Такой адрес состоит из 4 байт. Для удобства записи адреса каждый байт отделяется точкой. Например, 109.26.17.100. IP-адрес введен для идентификации узлов в составных сетях, работающих на основе стека TCP/IP. Поэтому он содержит две части: номер подсети и номер узла. Назначение IP-адреса выполняется администратором во время конфигурирования компьютеров и маршрутизаторов. В локальных сетях IP-адрес может быть выбран администратором произвольно, а в Интернет он назначается по рекомендации специального подразделения – Network Information Center (NIC). Обычно провайдеры услуг Интернет получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла (MAC-адреса).

  В настоящее время для выделения из IP-адреса номера подсети применяется метод бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR). Метод CIDR использует маску подсети. Ее наложение на IP-адрес с помощью операции AND (логическое И) обнуляет биты номера узла и выделяет номер подсети. Например, IP-адрес: 192.168.3.83 с маской 255.255.255.224 (другая запись 192.168.3.83/27; 27 – количество единичных бит в маске, определяющих номер подсети) задает подсеть с номером: 192.168.3.64, и номер узла: 19.

Октеты IP-адреса	192								168								3								83							
Биты IP-адреса	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	0	1	1
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
Октеты маски	255								255								255								224							

Подсеть 192.168.3.64/27 включает диапазон из 32 адресов (0 – 31). Однако начальный адрес из диапазона используется для обозначение самой посети, а конечный (в примере он равен 31) применяется в качестве адреса для широковещательной рассылки. Поэтому начальный и конечный адреса не могут использоваться для адресации сетевых узлов. Следовательно, если в IP-адресе под адресацию узлов отводится n бит, то количество узлов в посети не превышает значения 2^n-2. Маска посети должна соответствовать правилу: граница между нулевыми и единичными битами в маске должна быть единственной; единичные биты маски должны находится в старших разрядах по отношению к нулевым; возможна маска 0.0.0.0.

Узел может входить в несколько IP-сетей (например, маршрутизатор). В этом случае он должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

- **Доменное имя**. Например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени рабочей станции, имени организации, имени домена. Такой адрес называемый DNS-именем. Доменное имя важно для работы Интернета (**Интранета** – локальная сеть, использующая технологию Интернет), в котором для соединения с узлом необходима информация о его IP-адресе. Однако для людей проще запоминать буквенные (осмысленные) адреса, чем последовательность цифр IP-адреса. DNS-серверы в IP сетях поддерживают соответствие доменных имен и IP-адресов сетевых узлов. Поэтому, когда выполняется обращение к сетевому узлу по доменному имени, сначала задействуется протокол DNS, по которому в запросе к серверу передается доменное имя, а в ответе возвращается IP-адрес.

Сервис DHCP

DHCP (Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых DHCP-сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- **Ручное распределение**. При этом способе сетевой администратор сопоставляет локальному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
- **Автоматическое распределение**. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- **Динамическое распределение**. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок – **срок аренды**. По истечении половины срока клиент должен отправить запрос на продление аренды. Если такой запрос не поступает на DHCP-сервер до конца срока аренды, то IP-адрес вновь считается свободным.

Служба DHCP состоит из трех основных компонент:

1. **Серверы DHCP.** В состав сервера DHCP входит инструмент, который позволяет администратору настраивать пул адресов и режимы их назначения. В работе сервер DHCP использует собственную базу данных IP-адресов и других параметров настройки. Сервер DHCP поддерживает более 30 опций DHCP согласно RFC 2132. Параметры конфигурации TCP/IP, которые могут быть назначены сервером DHCP по умолчанию, включают: IP-адрес для каждого сетевого адаптера на клиентском компьютере, маску подсети, шлюз по умолчанию, IP-адрес DNS или WINS сервера.
2. **Клиенты DHCP.** Клиентами сервера DHCP могут быть компьютеры, работающие на любой платформе.

3. **Агенты ретрансляции DHCP**. Работа протокола DHCP основана на механизме широковещания. Маршрутизаторы не ретранслируют широковещательные посылки, поэтому передача таких посылок выполняется агентом ретрансляции. Агент ретрансляции DHCP, как правило, работает на маршрутизаторе, либо хосте, который слушает широковещательные сообщения DHCP и переадресовывает их на заданный сервер (серверы) DHCP. Использование агентов ретрансляции избавляет от необходимости устанавливать сервер DHCP в каждом физическом сегменте сети. Агент не только обслуживает прямые локальные запросы клиента DHCP и перенаправляет их на удаленные серверы DHCP, но также возвращает ответы удаленных серверов DHCP клиентам DHCP.

Сервис DNS

DNS (Domain Name System – система доменных имен) – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене. Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу. Основой DNS имеет представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения – другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла **hosts**, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS-служба.

Ключевыми понятиями DNS являются:

- **Домен** (domain, область) – узел в дереве имён, вместе со всеми подчинёнными ему узлами, то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вверху находится корневой домен (не имеющий идентификатора), ниже идут домены первого уровня (доменные зоны), затем – домены второго уровня, третьего и т. д. (например, для адреса ru.wikipedia.org. домен первого уровня – org, второго wikipedia, третьего ru). На практике точку перед корневым доменом часто опускают («ru.wikipedia.org»вместо «ru.wikipedia.org.»), но она бывает важна в случаях разделения между относительными доменами и FQDN (англ. Fully Qualified Domain Name, полностью определённое имя домена).

- **Поддомен** (subdomain) – подчинённый домен (например, wikipedia.org – поддомен домена org, а ru.wikipedia.org – домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения. Например, если у вас есть домен вида mydomain.ru, вы можете создать для него различные поддомены вида mysite1.mydomain.ru, mysite2.mydomain.ru и т. д.

- **Ресурсная запись** – единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному Доменному имени,

узлу в дереве имен), тип и поле данных, формат и содержание которого зависит от типа.

- **Зона** – часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен (DNS-сервере), а чаще – одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за какой-либо домен другому лицу или организации. Это называется делегированием. Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имен DNS как структуру из зон, а не отдельных узлов/имен, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчиненных. На практике большинство зон 0-го и 1-го уровня ('.', ru, com, …) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны. В больших корпоративных доменах (2-го и более уровней) иногда встречается образование дополнительных подчиненных уровней без выделения их в дочерние зоны.
- **DNS-сервер** – специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.
- **DNS-клиент** – специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

Сервис HTTP

HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста) – протокол передачи данных (изначально – в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

HTTP в настоящее время повсеместно используется в Интернете для получения информации с веб-сайтов. Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т.д. (В частности для этого используется HTTP-заголовок). Именно благодаря возможности указания способа кодирования сообщения клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает, что не сохраняется промежуточное состояние между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять хранение данных о состоянии, связанного с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

Сервис FTP

FTP (File Transfer Protocol, протокол передачи файлов) - протокол передачи файлов по сети. FTP используется для передачи файлов. В отличие от TFTP (Trivial FTP), гарантирует передачу (либо выдачу ошибки) за счёт применения квитирования. Протокол использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно. Можно использовать протокол SSH для безопасной передачи, скрывающей (шифрующей) логин и пароль, а также шифрующей содержимое.

Особенность протокола FTP в том, что он использует множественное (как минимум — двойное) подключение. При этом один канал является управляющим, через который поступают команды серверу и возвращаются его ответы (обычно через TCP-порт 21), а через остальные происходит собственно передача данных, по одному каналу на каждую передачу. Поэтому в рамках одной сессии по протоколу FTP можно передавать одновременно несколько файлов, причём в обоих направлениях. Для каждого канала данных открывается свой TCP порт, номер которого выбирается либо сервером, либо клиентом, в зависимости от режима передачи. Для этого должен быть запущен FTP-сервер, ожидающий входящих запросов. Компьютер-клиент может связаться с сервером по порту 21. Это соединение (поток управления) остаётся открытым на время сессии. Второе соединение (поток данных), может быть открыт как сервером из порта 20 к порту соответствующего клиента (активный режим), или же клиентом из любого порта к порту соответствующего сервера (пассивный режим), что необходимо для передачи файла данных. Поток управления используется для работы с сессией — например, обмен между клиентом и сервером командами и паролями с помощью telnet-подобного протокола. Например, «RETR имя файла» передаст указанный файл от сервера клиенту.

Сервис электронной почты

Электронная почта (e-mail) — технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему бумажной почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, задержки передачи сообщений, достаточную надёжность и, в то же время, отсутствие гарантии доставки.

В терминологии электронной почты выделяются следующие компоненты (рис. 1):

- **MTA** (Mail Transfer Agent — агент пересылки почты) — отвечает за пересылку почты между почтовыми серверами; как правило, первый MTA в цепочке получает сообщение от MUA, последний передаёт сообщение к MDA.
- **MDA** (Mail Delivery Agent — агент доставки почты) — отвечает за доставку почты конечному пользователю.
- **MUA** (Mail user agent — почтовый агент пользователя; в русской нотации закрепился термин почтовый клиент) — программа, обеспечивающая пользовательский интерфейс, отображающая полученные письма и предоставляющая возможность отвечать, создавать, перенаправлять письма.
- **MRA** (Mail retrieve agent) — почтовый сервер, забирающий почту с другого сервера по протоколам, предназначенным для MDA.

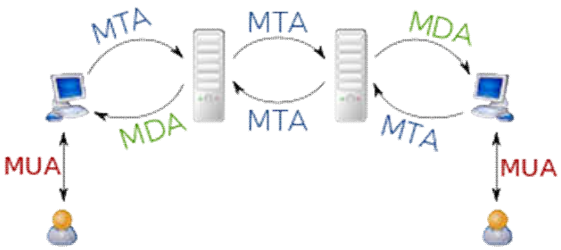

Рис. 1. Взаимоотношения между MTA, MDA и MUA при передаче электронной почты

В мире наиболее известным протоколом обмена электронной почтой является **SMTP** (simple mail transfer protocol — простой протокол передачи почты). Он использует DNS для определения правил пересылки почты. В различных доменах настроены свои, независимые друг от друга почтовые системы. У каждого почтового домена может быть несколько пользователей. Почта передаётся между узлами с использованием программ пересылки почты **MTA** (такими, как, например: sendmail, exim4, postfix, Microsoft Exchange Server, Lotus Domino и т. д.). Взаимодействие почтовой системы и пользователей, в общем случае, никак не регламентируется и может быть произвольным, хотя существуют как открытые, так и закрытые протоколы взаимодействия между пользователями и почтовой системой. В некоторых почтовых системах MDA и MTA могут быть объединены в одну программу, а в других системах представлены в виде разных программ или вообще выполняться на различных серверах. Программа, с помощью которой пользователь осуществляет доступ, называется **MUA**. В случае использования веб-интерфейса для работы с почтой, её роль выполняет приложение веб-интерфейса, запускаемое на сервере.

В концепции почтового хранилища почта на сервере хранится временно, в ограниченном объёме, а пользователь периодически обращается к ящику и «забирает» письма. На основании этой концепции действует протокол **POP3**.

Концепция почтового терминала подразумевает, что вся корреспонденция, связанная с почтовым ящиком (включая копии отправленных писем), хранится на сервере, а пользователь обращается к хранилищу для просмотра корреспонденции и написания новых писем. На этом принципе действует протокол **IMAP** и большинство веб-интерфейсов бесплатных почтовых служб. Подобное хранение почтовой переписки требует значительно больших мощностей от почтовых серверов. Поэтому во многих случаях происходит разделение между почтовыми серверами, пересылающими почту, и серверами хранения писем.

Утилита ipcofig

Утилита **ipconfig** отображает параметры протокола TCP/IP для заданного сетевого соединения, обновляет эти параметры с помощью DHCP, поддерживает работу с системой доменных имен. При использовании без параметров утилита отображает IP-адреса версии 4 (IPv4) и IPv6, маску подсети и шлюз по умолчанию для всех адаптеров. Синтаксис:

ifconfig [/? | /all | /release [адаптер] | /renew [адаптер] | /flushdns | /registerdns | /showclassid адаптер | /setclassid адаптер [устанавливаемый_код_класса_dhcp]]

адаптер: полное имя или имя, содержащие подстановочные знаки "*" и "?" из допустимого множества: * - любое количество символов, ? - один любой символ.

ключи:

/?	Отобразить справочное сообщение.
/all	Отобразить полную информацию о настройке параметров.
/release	Освободить IP-адрес для указанного адаптера.
/renew	Обновить IP-адрес для указанного адаптера.
/flushdns	Очистить кэш разрешений DNS.

/registerdns	Обновить все DHCP-аренды и перерегистрировать DNS-имена
/displaydns	Отобразить содержимое кэша разрешений DNS.
/showclassid	Отобразить все допустимые для этого адаптера коды (ID) классов DHCP.
/setclassid	Изменить код класса DHCP (ID).

Утилита ping

Утилита **ping** используется для проверки подключения к другому компьютеру на уровне протокола IP. Принцип работы: команда *ping IP-адрес* отправляет серию небольших пакетов данных на указанное устройство, а затем показывает время ответа. Утилита ping является основным средством стека TCP/IP для обнаружения неполадок подключения, доступности и разрешения имени. Она также позволяет определить имя и IP-адрес сетевого узла. Синтаксис и справка по утилите ping приведены на рисунке 2.

```
Использование: ping [-t] [-a] [-n <число>] [-l <размер>] [-f] [-i <TTL>]
                   [-v <TOS>] [-r <число>] [-s <число>]
                   [[-j <список_узлов>] | [-k <список_узлов>]]
                   [-w <время_ожидания>] [-R] [-S <адрес_источника>]
                   [-c секция] [-p] [-4] [-6] конечный_узел

Параметры:
  -t                 Проверяет связь с указанным узлом до прекращения.
                     Для отображения статистики и продолжения проверки
                     нажмите клавиши CTRL+BREAK;
                     для прекращения нажмите CTRL+C.
  -a                 Разрешает адреса в имена узлов.
  -n <число>         Число отправляемых запросов проверки связи.
  -l <размер>        Размер буфера отправки.
  -f                 Устанавливает флаг, запрещающий фрагментацию,
                     в пакете (только IPv4).
  -i <TTL>           Срок жизни пакетов.
  -v <TOS>           Тип службы (только IPv4; этот параметр
                     использовать не рекомендуется, и он не влияет на поле
                     TOS в заголовке IP).
  -r <число>         Записывает маршрут для указанного числа прыжков
                     (только IPv4).
  -s <число>         Задает метку времени для указанного числа прыжков
                     (только IPv4).
  -j <список_узлов>  Задает свободный выбор маршрута по списку узлов
                     (только IPv4).
  -k <список_узлов>  Задает жесткий выбор маршрута по списку узлов
                     (только IPv4).
  -w <время_ожидания> Задает время ожидания каждого ответа (в миллисекундах).
  -R                 Использует заголовок маршрута для проверки и обратного
                     маршрута (только IPv6). В соответствии с RFC 5095,
                     использование этого заголовка маршрута не рекомендуется.
                     В некоторых системах запросы проверки связи могут быть
                     сброшены, если используется этот заголовок.
  -S <адрес_источника> Задает адрес источника.
  -c секция          Идентификатор секции маршрутизации.
  -p                 Проверяет связь с сетевым адресом поставщика
                     виртуализации Hyper-V.
  -4                 Задает принудительное использование протокола IPv4.
  -6                 Задает принудительное использование протокола IPv6.
```

Рис. 2. Справочные данные по утилите ping

2. Задание

2.1. Обучающая часть

1. Постойте в Cisco Packet Tracer (CPT) схему сети, показанную на рисунке 3.

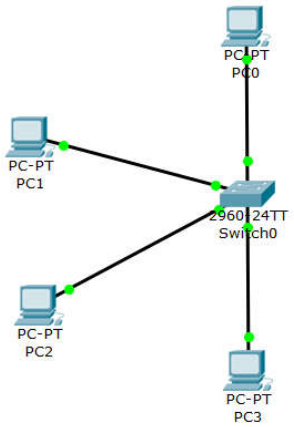

Рис. 3. Начальная топология сети

Для этого в левом нижнем углу главном окна приложения щелкните пиктограмму (Switches – Коммуникаторы), находящуюся в панели типов сетевых устройств, в панели моделей устройств выбранного типа, которая расположена рядом, выберите коммутатор любой модели (рис. 4). При этом символ выбранной модели измениться на . Поместите курсор в рабочую область окна приложения и щелкните. Экземпляр выбранной модели коммуникатора появиться в рабочей области. Если при выборе модели коммуникатора удерживать клавишу *Ctrl*, то можно будет добавить в рабочую область несколько экземпляров. Чтобы выйти из режима множественного добавлений выбранного элемента сети в рабочую область приложения, нажмите кнопку *Esc*.

Рис. 4. Выбор типа и модели сетевого устройства

В панели типов сетевых устройств щелкните по пиктограмме (End Devices – Конечные устройства), а в панели моделей выберите (PC – Персональный компьютер), зажав кнопку *Ctrl*. Добавьте четыре ПК в рабочую область CPT. Нажмите кнопку *Esc*. Для соединения рабочих станций с коммутатором в панели типов устройств щелкните пиктограмму , а в панели моделей - (прямой кабель витой пары). Теперь поместите курсор над одним из ПК в рабочей области приложения и щелкните левой кнопкой мыши. Появиться плавающее меню со списком портов интерфейсов ПК. Выберите порт FastEthernet0. Появиться линия, протянутая от устройства до курсора. Поместите курсор над коммуникатором и щелкните левой кнопкой мыши. Во всплывающем меню щелкните по любому порту типа FastEthernet левой кнопкой мыши. Должна образоваться линия связи между ПК и коммутатором. Цветные метки на линии около устройств показывают состояние портов сетевых адаптеров. Оранжевый цвет сигнализирует о том, что в настоящий момент идет настройка порта и передача по нему данных пользователя невозможна. Красный цвет маркера показывает, что порт отключен, а зеленый – порт готов к работе. CTP симулирует работу сети во времени. Поэтому при загрузке проекта или установления новой связи порт некоторое время (примерно равное времени настройки порта реального сетевого устройства) находится в состоянии конфигурирования (оранжевый цвет маркера). Чтобы пропустить этот период симуляции

сети нажмите надпись «Fast Forward Time», которая находится над панелью моделей сетевых устройств. Аналогичным образом подключите остальные ПК к коммутатору.

2. Для каждого компьютера настройте статический IP-адрес так, чтобы они все принадлежали подсети: 192.168.0.0/24. Левой кнопкой мыши щелкните по любому ПК. В появившемся диалоговом окне выберите закладку «Desktop» и щелкните по элементу «IP Configuration». В окне «IP Configuration» выберите режим назначения IP-адреса «Static», в поле «IP address» введите уникальное значение из диапазона 192.168.0.1 – 192.168.0.254. В поле маски подсети укажите значение 255.255.255.0. Остальные поля диалогового окна пока можно оставить пустыми. Закройте окно «IP Configuration», нажав на крестик в его верхнем правом углу. Диалоговое окно ПК также можно закрыть. Аналогичным образом настройте IP-адреса на остальных ПК симулируемой сети.
3. С помощью утилиты ping проверьте прохождение пакетов между узлами сети. Например, нужно проверить соединение PC1 (IP-адрес: 192.168.0.1/24) с PC3 (IP-адрес: 192.168.0.3/24). Левой кнопкой мыши щелкаем по PC1 и в появившемся диалоговом окне выбираем закладку «Desktop». Щелкаем по элементу «Command Prompt». В командной строке вводим: *ping 192.168.0.3* и нажимаем *Enter*. В консоли появятся результаты посылки 4 тестовых пакетов. Если узел назначения смог принять ICMP-пакет, который отправляет утилита ping, то он формирует ответный ICMP-пакет и направляет его источнику. Консоль источника показывает сколько байт содержал тестовый пакет, за какое время был получен ответ и время жизни пакета в маршрутизируемой сети (параметр TTL). Если за время тайм-аута ответный пакет не возвращается к источнику, то консоль выводит соответствующее сообщение, а пакет считается потерянным, что характеризует связь между сетевыми устройствами.
4. Добавьте в Вашу сеть сервер и назовите его в CPT: DHCP. В панели типов сетевых устройств выберите «End Devices», а в панели моделей щелкните по пиктограмме  (Server). Поместите в рабочей области CPT один сервер. Чтобы изменить название сервера левой кнопкой мыши щелкните по нему в рабочей области CPT, откройте закладку «Config» и в поле «Display name» укажите требуемое имя. Соедините сервер с коммутатором и назначьте ему статический IP-адрес, не принадлежащий сети, в которую входят рабочие станции. Например, 192.168.1.254/24.
5. Проверьте прохождение пакетов между сервером и рабочими станциями. Каков результат?
6. Отключите на сервере все сетевые службы кроме сервиса DHCP. Левой кнопкой мыши щелкните по серверу и в диалоговом окне выберите закладку «Services». Затем последовательно выбираете в списке «SERVIECS» отключаемые службы и останавливаете их работу с помощью радиокнопки «Off». Служба EMAIL использует два протокола и для ее полного отключения нужно выключить оба протокола: SMTP и POP3.
7. В диалоговом окне сервера откройте закладку для настройки службы DHCP. Настройте начальный адрес пула адресов, маску сети и максимальное число пользователей так, чтобы IP-адрес сервера и начальный адрес пула принадлежали одной сети, но адрес сервера не входил в пул арендуемых адресов (рис. 5). Нажмите кнопку *Save* и закройте окно конфигурирования сервера.
8. У всех рабочих станций включите протокол DHCP либо с помощью закладки «IP Configuration», либо на каждой рабочей станции с помощью консоли выполните команду: *ipconfig /renew*.
9. В консоли рабочих станций с помощью утилиты ipconfig узнайте их IP-адреса.
10. Проверьте прохождение пакетов между станциями и сервером. Каков результат?

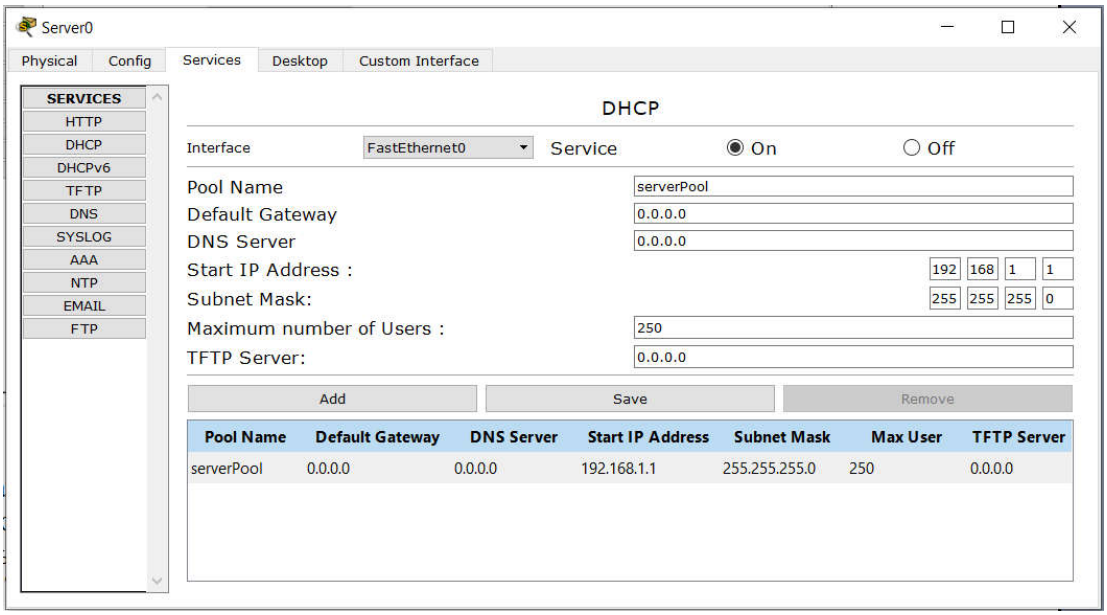

Рис. 5. Настройка сервера DHCP

11. Добавьте в Вашу сеть еще один сервер и настройте ему статический IP-адрес так, чтобы он оказался в одной сети с DHCP-сервером, но не входил в пул адресов, назначаемых им.
12. Назовите новый сервер именем NetServ и отключите на нем все службы, кроме служб DNS, HTTP, FTP, EMAIL.
13. Настройте службу DNS на NetServ. Пусть все компьютеры нашей сети входят в домен **ugrasu.ru**, тогда полное доменное имя сервера NetServ будет **netserv.ugrasu.ru**. Для этого в конфигурации NetServ необходимо перейти на вкладку Services, выбрать DNS и создать запить типа A Record, тем самым связав доменное имя с IP-адресом (рис. 6). Для добавления записи нажать кнопку ADD.

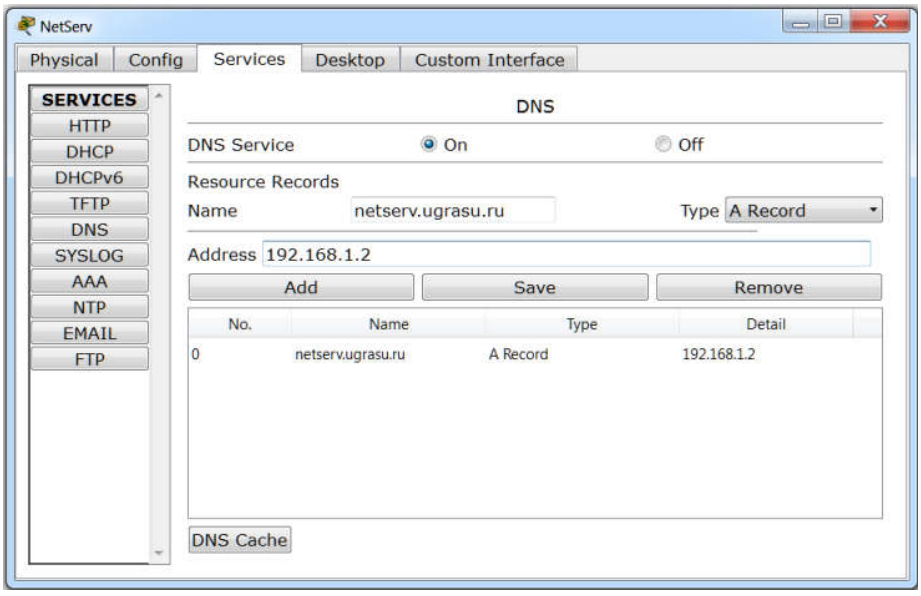

Рис. 6. Окно конфигурации DNS-службы в CPT

14. Иногда вместо полного доменного имени удобно использовать короткое имя узла сети. Для этого в DNS-сервере настраивают псевдонимы узлов. Создайте в настройках DNS-сервера ресурсную запись типа CNAME (позволяет присваивать хосту мнемонические имена или псевдонимы, используемые для связывания с узлом какой-либо функции, либо просто для сокращения имени), чтобы связать псевдоним с доменным именем (рис. 7).

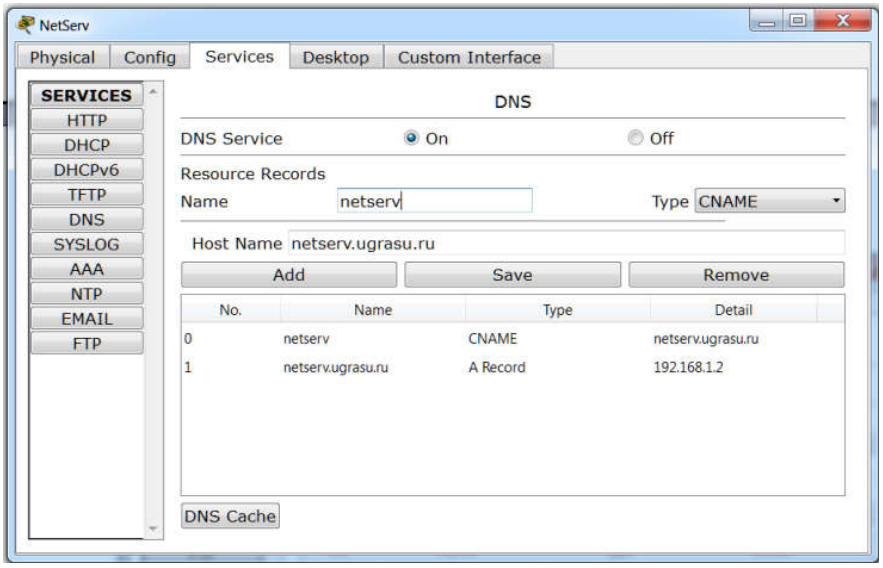

Рис. 7. Задание псевдонима узла netserv.ugrasu.ru

15. Самостоятельно задайте полное доменное имя и псевдоним для DHCP-сервера.
16. Чтобы рабочие станции в сети могли воспользоваться DNS-сервисом им необходимо в настройках протокола IP сообщить IP-адрес DNS-сервера в качестве параметра. Подкорректируйте настройки DHCP-сервера, указав в поле "DNS Server" IP-адрес NetServ (рис. 5).
17. Обновите настройки протокола IP на рабочих станциях. Для этого в окне командной строки вызовите утилиту ipconfig /renew. Ключ renew заставляет клиента DHCP (рабочую станцию) запросить новый IP-адрес и обновить параметры протокола IP раньше, чем истечет срок аренды.
18. В окне командной строки рабочей станции введите ping netserv.ugrasu.ru. Каков результат? С помощью утилиты ping по доменному имени проверьте связь рабочих станций с DHCP-сервером.
19. Настройте службу HTTP. На сервере NetSevr зайдите на вкладку Services. Слева в списке выберите кнопку HTTP. В File Manager удалите все файлы, если они там будут присутствовать (рис. 8).
20. Создайте новый файл. Назовите его index.html. Вставьте в него следующий текст:

```
<html>
<center><font size='+2' color='blue'>Laboratory work #1</font></center>
<hr>Network services: DHCP, DNS, HTTP.
</html>
```

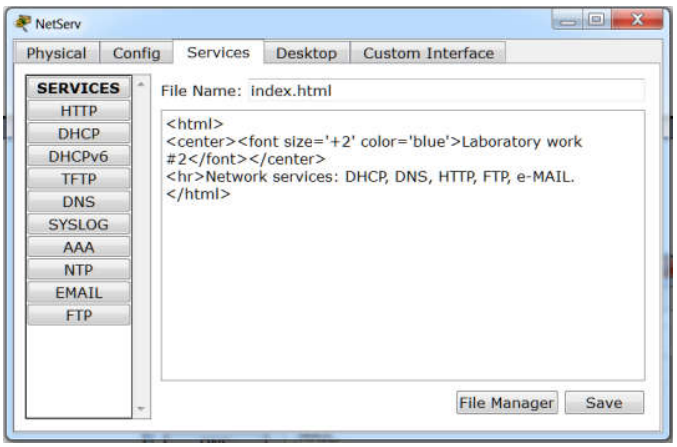

Рис. 8. Создание начальной гипертекстовой странице на сервере

21. Нажмите кнопку Save. Закройте окно настройки сервера NetServ.
22. На любой рабочей станции запустите Web-браузер и введите адрес: netserv.ugrasu.ru. Должно появиться окно, показанное на рисунке 9.

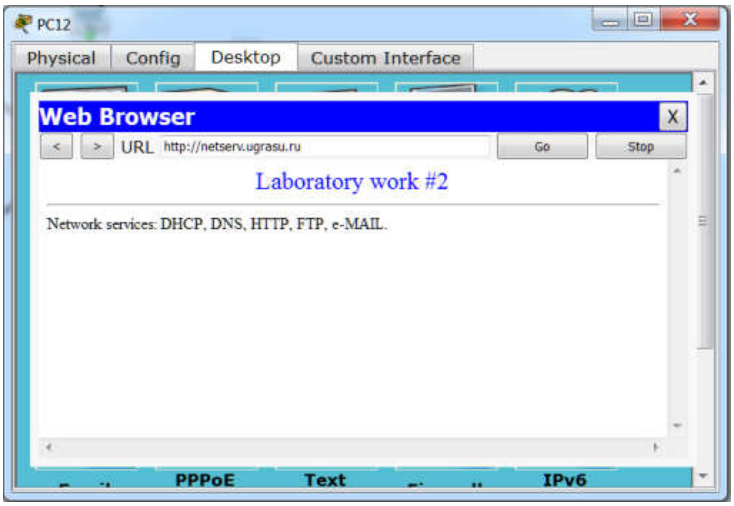

Рис. 9. Отображение гипертекстовой странице в Web-браузере рабочей станции PC12

23. На любой рабочей станции запустите Web-браузер и введите адрес: netserv. Каков результат? Заставьте появляться эту страницу в Web-браузере по адресу: **www.ugrasu.ru**.
24. Для настройки работы FTP-сервера создайте несколько учетных записей пользователей и установите им различные права доступа к файлам. Указанные действия можно произвести на закладке "Services - FTP" (рис. 10). Чтобы добавить нового пользователя, в поля "Username" и "Password" введите имя пользователя и его пароль соответственно. Затем установите его права доступа флажками: "Write", "Read", "Delete", "Rename", "List" и нажмите кнопку "Add".

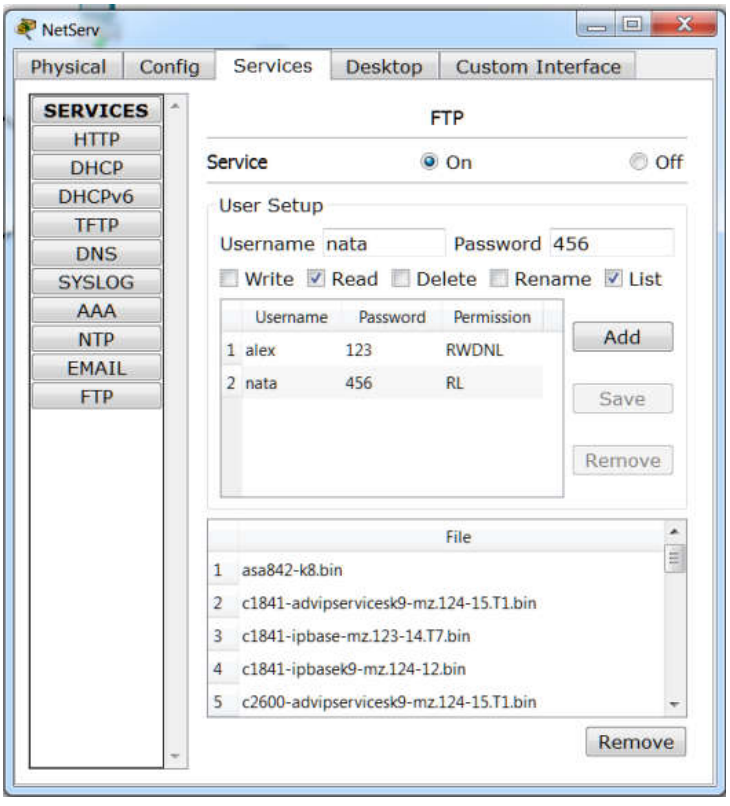

Рис. 10. Панель настройки FTP-сервера

25. Для тестирования работы FTP-сервера откройте командное окно на любой рабочей станции и выполните команду:

ftp <доменное имя сервера или его IP-адрес>

В результате выполнения команды должно появиться приглашение для ввода имени пользователя, а затем его пароля. Если логин и пароль введены корректно, то появиться приглашение FTP-сервера для ввода его внутренних команд (рис. 11).

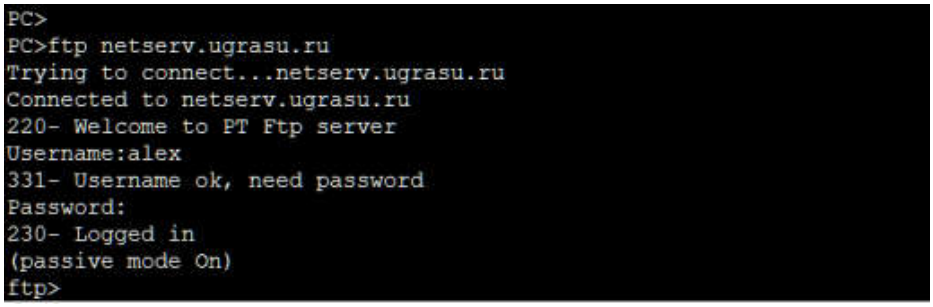

Рис. 11. Подключение к FTP-серверу

Для вывода списка доступных FTP-команд в CPT укажите символ "?" и нажмите Enter. Например, команда *dir* отобразит список файлов и папок корневого каталога, а команда *quit* завершит сеанс работы с FTP-сервером (рис. 12).

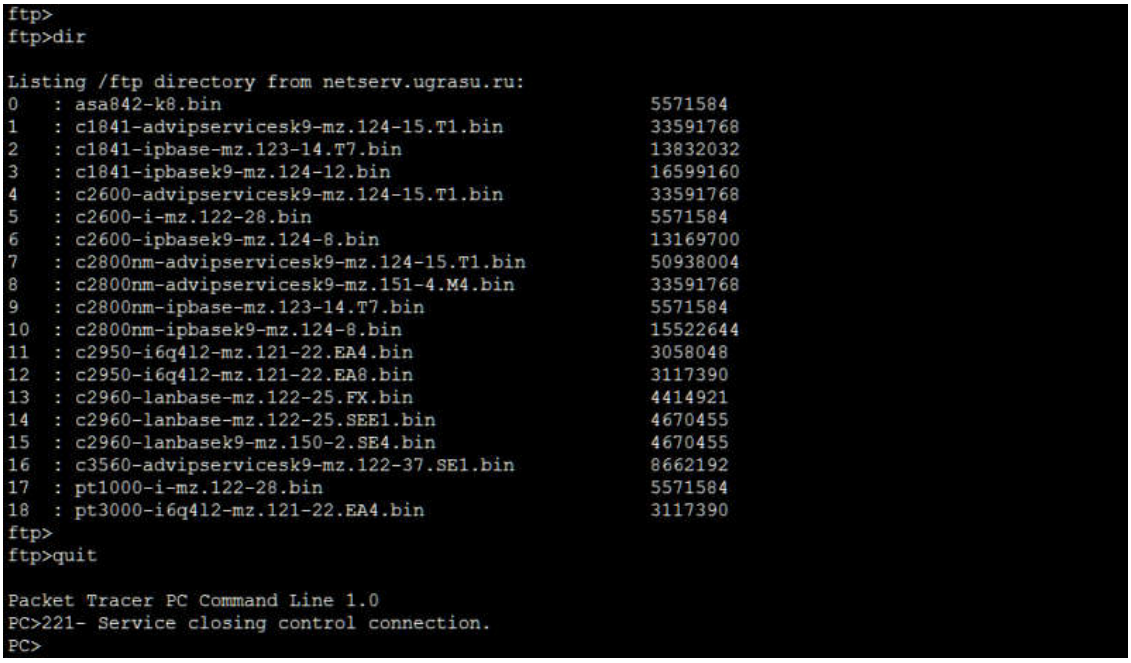

Рис. 12. Результаты выполнения команд FTP-сервера

26. Настройку EMAIL-сервиса можно произвести на закладке "Services - EMAIL" (рис. 13). Сначала включите работу протоколов SMTP и POP3. Затем создайте имя домена электронной почты. Для этого введите в поле "Domain Name" название Вашего домена и нажмите кнопку "Set". Затем создайте почтовые ящики нескольких пользователей, указав их имя и пароль в полях "User", "Password" и нажав кнопку "+". Зарегистрированным на сервере пользователям будут соответствовать адреса почтовых ящиков: <имя пользователя>@<имя домена>. Например, на рисунке 13 пользователю *alex* на EMAIL-сервере будет соответствовать почтовый ящик с адресом: *alex@ugrasu.ru*

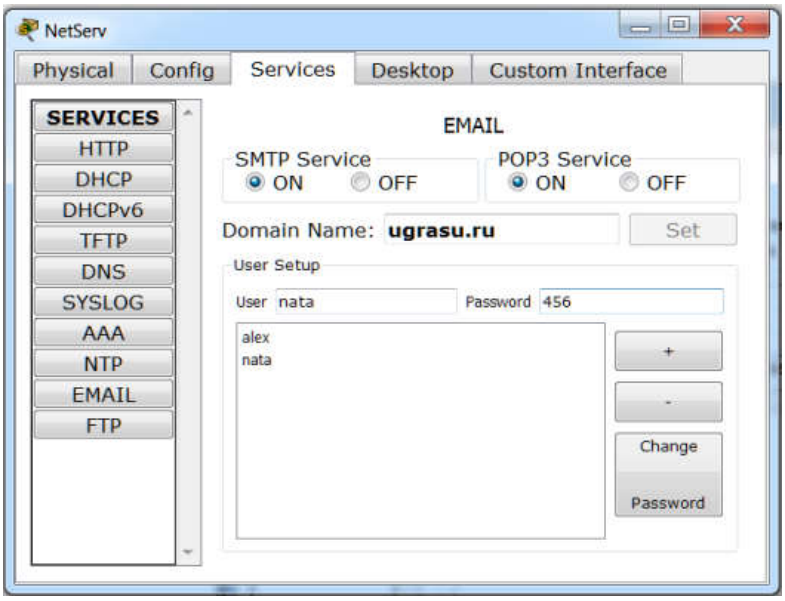

Рис. 13. Панель настройки EMAIL-сервера

27. Для тестирования работы EMAIL-сервера щелкните по значку "Email" на вкладке "Desktop" любой рабочей станции сети. В появившемся диалоге произведите настройку EMAIL-клиента следующим образом. В поле "Your Name" введите на латинице вашу Фамилию и Имя. В поле "Email Address" необходимо указать адрес почтового ящика, к которому вы собираетесь подключиться. Например: alex@ugrasu.ru . В полях "Incoming Mail Server" и "Outgoing Mail Server" укажите доменное имя вашего сервера, на котором работает EMAIL-сервис. В поля "User Name" и "Password" введите соответственно логин и пароль пользователя почтового ящика. Нажмите кнопку "Save" (рис. 14).

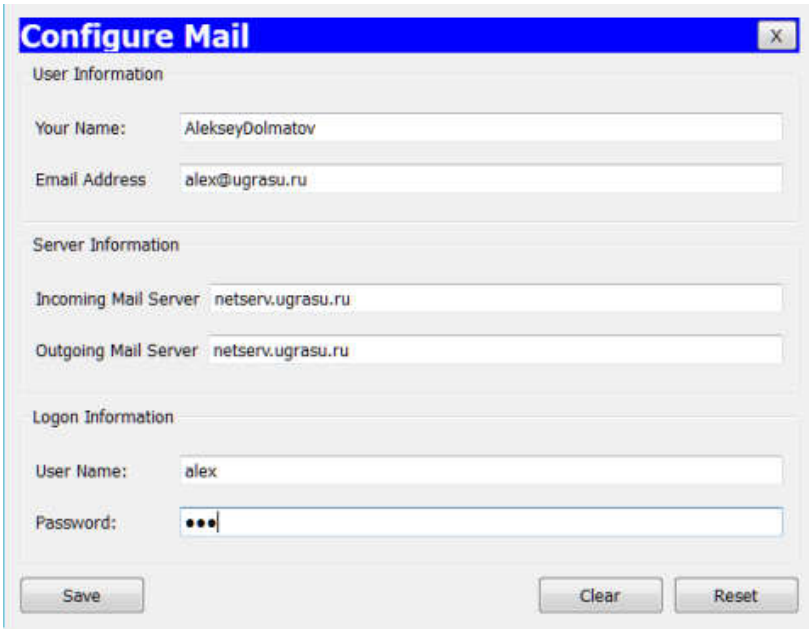

Рис. 14. Диалог настройки EMAIL-клиента

Для создания нового письма в MAIL BROWSER нажмите кнопку "Compose". В поле "To" введите почтовый адрес, а в поле "Subject" тему сообщения. Ниже введите текст письма (на английском языке). Для начала отправьте письмо самому себе. После ввода текста сообщения нажмите кнопку "Send". При этом внизу появившегося основного окна MAIL BROWSER появиться информация об отправке письма. Если она оканчивается текстом "Send Success", то письмо успешно доставлено в почтовый ящик получателя. Т.к. отправителем были Вы сами, то письмо оказалось в Вашем почтовом ящике на EMAIL-

сервере. Для доставки письма из почтового ящика нажмите кнопку "Receive". При успешной доставке письмо появиться в списке MAIL BROWSER. Чтобы прочитать текст письма щелкните по нему мышкой.

Создайте еще одно письмо и отправьте его другому адресату, почтовый ящик которого создан на почтовом сервере. Откройте MAIL BROWSER на другой рабочей станции сети, настройте клиентскую почтовую программу от имени адресата Вашего письма и доставьте письмо из его почтового ящика в MAIL BROWSER. В нижней части окна MAIL BROWSER отразятся стадии получения письма с почтового сервера (рис. 15).

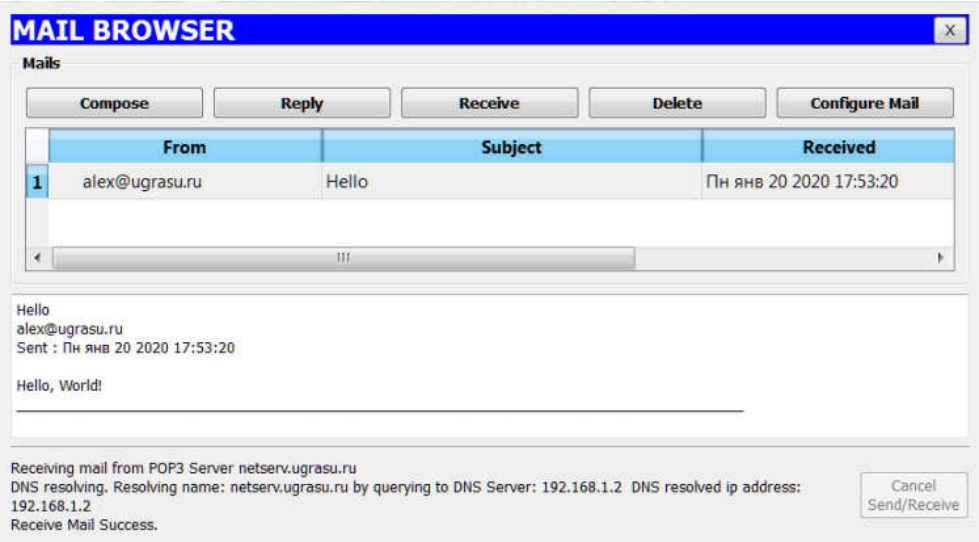

Рис. 15. Результат получения письма электронной почтой

Кнопка "Reply" позволяет ответить на письмо выделенное в списке, а кнопка "Delete" удалить такое письмо.

28. Сохраните проект CPT с именем LabNet-1-task-1(Фамилия_группа).pkt.
29. Продемонстрируйте его работоспособность преподавателю и загрузите на сайт eluniver.ugrasu.ru.

2.2. Индивидуальное задание

1. Создайте сеть с физической топологией "звезда" на основе нескольких концентраторов типа Hub-PT, чтобы в нее входило не менее 12 рабочих станций и 5 отдельных серверов: DHCP-, DNS- и HTTP-, FTP- и EMAIL-сервер. IP-адреса серверам назначить статически, а рабочим станциям с помощью протокола DHCP.
2. Настройте доменные имена Ваших серверов так: корневой домен - Ваша фамилия (на латинице); домен 1 уровня - Ваше имя; домен 2 уровня - название сервера. Например, dns.alex.ivanov. Для каждого сервера настройте псевдонимы. Проверьте работу сети с помощью утилиты ping, используя IP-адреса, доменные имена и псевдонимы.
3. В HTTP-службе создайте собственную HTML-страницу с указанием следующих сведений:
   - Названия лабораторной работы;
   - Перечисление доменных имен серверов и их IP-адресов;
   - группа и ФИО студента, выполнившего лабораторную работу.
4. Настройте и протестируйте работу FTP-сервера в Вашей сети.
5. Настройте и протестируйте работу EMAIL-службы в Вашей сети.
6. Сохраните проект CPT с именем LabNet-1-task-2(Фамилия_группа).pkt.
7. Продемонстрируйте его работоспособность преподавателю и загрузите на сайт eluniver.ugrasu.ru.

3. Защита лабораторной работы

1. Изучить теоретический материал на основе лекций, настоящего методического указания, дополнительной литературы.
2. Приготовиться к ответу на контрольные вопросы.
3. В процессе защиты быть готовым к выполнению дополнительных задач на основе построенных Вами Проектов СРТ.

4. Контрольные вопросы

1. Для чего предназначен протокол DHCP?
2. На каком уровне модели OSI работает протокол DHCP?
3. Какие способы назначения IP-адресом с помощью DHCP существуют?
4. Какие параметры, кроме IP-адреса, может получить DHCP-клиент?
5. Какой запрос позволяет DHCP-клиенты получить дополнительные параметры без назначения IP-адреса?
6. Может ли DHCP-клиент получить IP-адрес, если DHCP-сервер отсутствует в рамках физической сети?
7. Какие компоненты службы DHCP Вам известны?
8. Что понимается под арендой в протоколе DHCP?
9. Какая утилита позволяет узнать текущий IP-адрес узла сети?
10. В каком случае DHCP-сервер продлевает срок аренды IP-адреса?
11. Какие запросы используются при получении IP-адреса по протоколу DHCP?
12. Какая утилита позволяет сбросить текущие настройки стека TCP/IP или обновить их с DHCP-сервера?
13. Для чего предназначена служба DNS?
14. Какие типы доменных имен существуют?
15. Как создать соответствие "доменное имя - IP-адрес" в базе DNS-сервера?
16. Что понимается под псевдонимами доменных имен и как создаются соответствующие записи в БД DNS-сервера?
17. Можно ли назначать IP-адрес DNS-серверов динамически с помощью DHCP?
18. Можно ли с помощью утилиты ping по доменному имени проверить прохождение пакетов между узлами?
19. Какими функциональными возможностями обладает протокол HTTP?
20. Как происходит настройка HTTP-службы в Cisco Packet Tracer?
21. Назовите достоинства и недостатки HTTP?
22. Каким образом можно защитить гипертекстовые данные, передаваемые от Web-сервера клиенту?