**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ**

**ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В. Г. ШУХОВА»**

**(БГТУ им. В.Г. Шухова)**



ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

**Лабораторная работа №7**

по дисциплине: Компьютерные сети

тема: «Протоколы POP3 и SMTP»

Выполнил: ст. группы ПВ-223

Пахомов Владислав Андреевич

Проверили:

Рубцов Константин Анатольевич

Белгород 2025 г.

**Лабораторная работа №6  
Протоколы POP3 и SMTP**

**Цель работы:** изучить принципы и характеристику протоколов POP3 и SMTP и составить программу для приема/отправки электронной почты.

**Краткие теоретические сведения**

**Протокол POP3**

POP3 (англ. Post Office Protocol Version 3) - стандартный Интернет-протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению.

В некоторых небольших узлах Интернет бывает непрактично поддерживать систему передачи сообщений (MTS - Message Transport System). Рабочая станция может не иметь достаточных ресурсов для обеспечения непрерывной работы SMTP-сервера [RFC-821]. Для “домашних ЭВМ” слишком дорого поддерживать связь с Интернет круглые сутки.

Но доступ к электронной почте необходим как для таких малых узлов, так и индивидуальных ЭВМ. Для решения этой проблемы разработан протокол POP3 (Post Office Protocol - Version 3, STD- 53. M. Rose, RFC-1939). Этот протокол обеспечивает доступ узла к базовому почтовому серверу.

POP3 не ставит целью предоставление широкого списка манипуляций с почтой. Почтовые сообщения принимаются почтовым сервером и сохраняются там, пока на рабочей станции клиента не будет запущено приложение POP3. Это приложение устанавливает соединение с сервером и забирает сообщения оттуда. Почтовые сообщения на сервере стираются. POP3 поддерживает простые требования «загрузи-и-удали» для доступа к удаленным почтовым ящикам. Хотя большая часть POP-клиентов предоставляют возможность оставить почту на сервере после загрузки, использующие POP клиенты обычно соединяются, извлекают все письма, сохраняют их на пользовательском компьютере как новые сообщения, удаляют их с сервера, после чего разъединяются.

Другие протоколы, в частности IMAP, предоставляют более полный и комплексный удаленный доступ к типичным операциям с почтовым ящиком. Многие клиенты электронной почты поддерживают как POP, так и IMAP; однако, гораздо меньше интернет-провайдеров поддерживают IMAP.

POP3-сервер прослушивает порт 110. Шифрование связи для POP3 запрашивается после запуска протокола, с помощью либо команды STLS (если она поддерживается), либо POP3S, которая соединяется с сервером используя TLS или SSL по TCP-порту 995.

Доступные сообщения клиента фиксируются при открытии почтового ящика POP-сессией и определяются количеством сообщений для сессии, или, по желанию, с помощью уникального идентификатора, присваиваемого сообщению POP-сервером. Этот уникальный идентификатор является постоянным и уникальным для почтового ящика и позволяет клиенту получить доступ к одному и тому же сообщению в разных POP-сессиях. Почта извлекается и помечается для удаления с помощью номера сообщения. При выходе клиента из сессии помеченные сообщения удаляются из почтового ящика.

Обычно РОРЗ-сервис устанавливается на 110-й ТСР -порт сервера, который будет находиться в режиме ожидания входящего соединения. Когда клиент хочет воспользоваться РОРЗ-сервисом, он просто устанавливает TCP-соединение с портом 110 этого хоста. После установления соединения сервис РОРЗ отправляет подсоединившемуся клиенту приветственное сообщение. После этого клиент и сервер начинают обмен командами и данными. По окончании обмена РОРЗ-канал закрывается.

Команды РОРЗ состоят из ключевых слов, состоящих из ASCIIсимволов, и одним или несколькими параметрами, отделяемыми друг от друга символом "пробела" - . Все команды заканчиваются символами "возврата каретки" и "перевода строки" - . Длина ключевых слов не превышает четырех символов, а каждого из аргументов может быть до 40 символов.

Ответы РОРЗ-сервера на команды состоят из строки статусиндикатора, ключевого слова, строки дополнительной информации и символов завершения строки. Длина строки ответа может достигать 512 символов. Строка статус-индикатора принимает два значения: положительное ("+ОК") и отрицательное ("-ERR"). Любой сервер РОРЗ обязан отправлять строки статус-индикатора в верхнем регистре, тогда как другие команды и данные могут приниматься или отправляться как в нижнем, так и в верхнем регистрах. Ответы РОРЗ-сервера на отдельные команды могут составлять несколько строк. В этом случае строки разделены символами . Последнюю строку информационной группы завершает строка, состоящая из символа "." (код — 046) и , т. е. последовательность "CRLF.CRLF".

РОРЗ-сессия состоит из нескольких частей. Как только открывается TCP-соединение и РОРЗ-сервер отправляет приветствие, сессия должна быть зарегистрирована - состояние аутентификации (AUTHORIZATION state). Клиент должен зарегистрироваться в РОРЗсервере, т. е. ввести свой идентификатор и пароль.

После этого сервер предоставляет клиенту его почтовый ящик и открывает для данного клиента транзакцию - состояние начала транзакции обмена (TRANSACTION state). На этой стадии клиент может считать и удалить почту своего почтового ящика. После того как клиент заканчивает работу (передает команду QUIT), сессия переходит в состояние UPDATE - завершение транзакции. В этом состоянии РОРЗ-сервер закрывает транзакцию данного клиента (на языке баз данных - операция COMMIT) и закрывает TCP-соединение. В случае получения неизвестной, неиспользуемой или неправильной команды, РОРЗ-сервер должен ответить отрицательным состоянием индикатора.

РОРЗ-сервер может использовать в своей работе таймер контроля времени соединения. Этот таймер отсчитывает время "бездействия" ("idle") клиента в сессии от последней переданной команды. Если время сессии истекло, сервер закрывает TCP-соединение, не переходя в состояние UPDATE (иными словами, откатывает транзакцию или на языке баз данных — выполняет ROLLBACK). РОРЗ-сервер может 64 обслуживать группу клиентов, которые, возможно, присоединяются по коммутируемой линии, и, следовательно, необходимо иметь средство автоматического регулирования времени соединения. По спецификации РОРЗ-таймер контроля состояния "idle" должен быть установлен на промежуток времени не менее 10 минут.

Команды протокола POP3:

* USER - идентифицирует пользователя с указанным именем;
* PASS - указывает пароль для пары клиент-сервер;
* QUIT - закрывает TCP-соединение;
* STAT - сервер возвращает количество сообщений в почтовом ящике плюс размер почтового ящика;
* LIST - сервер возвращает идентификаторы сообщений вместе с размерами сообщений;
* RETR - извлекает сообщение из почтового ящика;
* DELE - отмечает сообщение для удаления;
* NOOP - Сервер возвращает положительный ответ, но не совершает никаких действий;
* LAST - Сервер возвращает наибольший номер сообщения из тех, к которым ранее уже обращались;
* RSET - Отменяет удаление сообщения, отмеченного ранее командой DELE.

**Протокол SMTP**

SMTP (Simple Mail Transfer Protocol) - широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. SMTP впервые был описан в RFC 821 (1982 год); последнее обновление в RFC 5321 (2008) включает масштабируемое расширение - ESMTP (Extended SMTP). В настоящее время под «протоколом SMTP», как правило, подразумевают и его расширения. Протокол SMTP предназначен для передачи исходящей почты, используя для этого порт TCP 25.

Упрощенно схема взаимодействия представлена на рис. 7.1 (объемными стрелками показано направление движения почтовых сообщений).



Со стороны пользователя обычно одна и та же программа выступает в роли и POP3 клиента, и SMTP клиента отправителя. Наиболее распространенными на данный момент являются MS Outlook, The Bat, Netscape Messenger, Eudora, Pegasus mail, Mutt, Pine и др. При нажатии в них на кнопочку "отправить" происходит формирование очереди сообщений, и установление двустороннего сеанса общения с SMTP сервером провайдера. На схеме у пользователя есть клиентское ПО, а у провайдера – серверная часть приложения. На самом деле это немного не так. Протокол SMTP делает возможным смену сторон даже в ходе одного сеанса. Условно принято считать клиентом ту сторону, которая начинает взаимодействие и хочет отослать почту, а сервером ту, что принимает запросы. После того, как клиент посылает серверу несколько служебных команд и получает положительные ответы на них, он отправляет SMTP серверу собственно тело сообщения. SMTP сервер получает сообщение, вносит в него дополнительные заголовки, указывающие на то, что он обработал данное послание, устанавливает связь со следующим SMTP сервером по пути следования письма. Общение между любыми SMTP серверами происходит по той же схеме. Инициирует переговоры клиент, сервер на них отвечает, а затем получает корреспонденцию и "ставит штампик" в теле письма (в его заголовочной части). Все это очень напоминает обычную бумажную почту, где работу по сортировке и отправке почты выполняют люди.

Если на каком-нибудь этапе передачи SMTP клиент обнаружит невозможность подключиться к следующему серверу (например, компьютер отправили на профилактику или аппаратура связи вышла из строя), он будет пытаться отправить сообщение через некоторое время – 1 час, 4 часа, день и т.д. до 4 суток в общем случае. Причем временные отрезки между попытками, как правило, зависят от настроек программы-пересыльщика почты. Одновременно, такой сервер должен уведомить отправителя сообщения о невозможности доставить почту, послав ему стандартное письмо "Failed delivery" (доставка невозможна) и рассказав о графике дальнейших попыток по продвижению исходного сообщения. Если канал связи не восстановится за указанный большой промежуток времени (например, 4 дня), посланная информация будет считаться утерянной.

Как только почта достигнет конечного пункта (SMTP сервера адресата сообщения), она будет сложена в почтовый ящик абонента, который всегда сможет в удобное для него время изъять ее по протоколам POP3 или IMAP, в зависимости от того, какой из них поддерживается провайдером.

Анализируя заголовок письма, можно узнать какими путями оно путешествовало, как долго длился сам путь, как называлась почтовая программа отправителя и многое другое. Получить эту информацию можно в "Свойствах письма", кликнув правой кнопкой мыши на самом письме в MS Outlook, нажав Ctrl+Shift+H в The Bat или совершить нечто подобное в других почтовых клиентах.

Рассмотрим клиент-серверное взаимодействие по протоколу SMTP. Программа пользователя, выбрав для связи соответствующий почтовый сервер, устанавливает с ним контакт на транспортном и сеансовом уровнях эталонной модели взаимодействия открытых систем OSI/RM (в терминах TCP/IP (transmission control protocol / internet protocol) это – TCP уровень). Взаимодействие на более низких уровнях (канальном, сетевом) происходит прозрачно для обеих сторон. Протокол SMTP – протокол прикладного уровня и базируется поверх TCP. В его рамках не оговаривается ни размер сегментов данных, ни правила квитирования, ни отслеживание ошибок, возникающих при передаче информации.

По уже установленному соединению клиентское ПО передает команды SMTP серверу, ожидая тут же получить ответы. В арсенал SMTP клиента, равно как и сервера, входит около 10 команд, но, воспользовавшись только пятью из них, уже можно легально послать почтовое сообщение. Это HELO, MAIL, RCPT, DATA, QUIT. Их использование подразумевается именно в такой последовательности. HELO предназначена для идентификации отправителя, MAIL указывает адрес отправителя, RCPT – адрес назначения. После команды DATA и ответа на нее, клиент посылает серверу тело сообщения, которое должно заканчиваться строкой, содержащей лишь одну точку.

Непосредственно после установления соединения сервер выдает строчку с кодом ответа 220. В ответ на нее клиент может инициировать сеанс связи по протоколу SMTP, послав команду HELO и указав у нее в аргументах имя своего компьютера. По принятии команды HELO сервер обязан сделать запрос в DNS и, если это возможно, по IP адресу определить доменное имя компьютера клиента. (IP адрес уже известен на момент установления соединения по TCP протоколу).

Далее в команде "MAIL FROM:" клиент сообщает обратный адрес отправителя, который проверяется обычно только на корректность. После слов "RCPT TO:" следует набрать адрес электронной почты абонента на данном сервере. Клиент отсылает команду DATA и ждет приглашения начать пересылку тела письма (код 354).

Сообщение может быть достаточно длинным, но обязательно должно заканчиваться строкой, в которой есть одна-единственная точка. Это служит сигналом SMTP серверу о том, что тело письма закончилось. Он присваивает этому письму определенный идентификатор, и ждет команды QUIT, после чего сеанс считается завершенным.

Если клиент посылает сообщение, у которого в заголовочной части в поле CC указаны несколько e-mail адресов, первый по пути следования SMTP сервер должен будет в общем случае установить сеанс продвижения почты с каждым из серверов данного списка и отослать точную копию письма каждому. В случае использования поля BCC клиент, формирующий сообщение, уничтожит запись BCC в теле сообщения и по количеству адресатов отошлет первому SMTP серверу команду "RCPT TO:" каждый раз с новым адресом в качестве аргумента. Таким образом, сервер получит указание разослать почту по многим адресатам. Причем, в этом случае получатели писем ничего не будут знать друг о друге, т.к. рассылка осуществляется посредством команд SMTP протокола.

**Используемые функции**

* Перевод сокета в состояние “прослушивания” (для TCP) осуществляется функцией listen (SOCKET s, int backlog), где s – дескриптор сокета; backlog – максимальный размер очереди входящих сообщений на соединение. Используется сервером, чтобы информировать ОС, что он ожидает (“слушает”) запросы связи на данном сокете. Без этой функции всякое требование связи с сокетом будет отвергнуто.
* Функция connect (SOCKET s, const struct sockaddr FAR\* name, int namelen) нужна для соединения с сокетом, находящимся в состоянии “прослушивания” (для TCP). Она ипользуется процессомклиентом для установления связи с сервером. В случае успешного установления соединения connect возвращает 0, иначе SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError.
* Функция accept (SOCKET s, struct sockaddr FAR\* addr, int FAR\* addrlen) служит для подтверждения запроса на соединение (для TCP). Функция используется для принятия связи на сокет. Сокет должен быть уже слушающим в момент вызова функции. Если сервер устанавливает связь с клиентом, то данная функция возвращает новый сокет-дескриптор, через который и производит общение клиента с сервером. Пока устанавливается связь клиента с сервером, функция блокирует другие запросы связи с данным сервером, а после установления связи “прослушивание” запросов возобновляется.
* В случае автоматического распределения адресов и портов узнать какой адрес и порт присвоен сокету можно при помощи функции getsockname (SOCKET s, struct sockaddr FAR\* name, int FAR\* namelen). Если операция выполнена успешно, возвращает 0, иначе возвращает SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError.
* Для передачи данных по протоколу UDP используется функция sendto (SOCKET s, const char FAR \* buf, int len, int flags, const struct sockaddr FAR \* to, int tolen). Если операция выполнена успешно, возвращает количество переданных байт, иначе возвращает SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError.
* Для передачи данных по протоколу TCP используется функция send (SOCKET s, const char FAR \* buf, int len, int flags), где s - дескриптор сокета; buf - указатель на буфер с данными, которые необходимо переслать; len - размер (в байтах) данных, которые содержатся по указателю buf; flags - совокупность флагов, определяющих, каким образом будет произведена передача данных. Если операция выполнена успешно, возвращает количество переданных байт, иначе возвращает SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError.
* Для приема данных по протоколу UDP используется функция recvfrom (SOCKET s, char FAR\* buf, int len, int flags, struct sockaddr FAR\* from, int FAR\* fromlen). Если операция выполнена успешно, возвращает количество полученных байт, иначе возвращает SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError.
* Для приема данных по протоколу TCP используется функция recv (SOCKET s, char FAR\* buf, int len, int flags). Если операция выполнена успешно, возвращает количество полученных байт, иначе возвращает SOCKET\_ERROR и номер ошибки можно получить при помощи функции WSAGetLastError

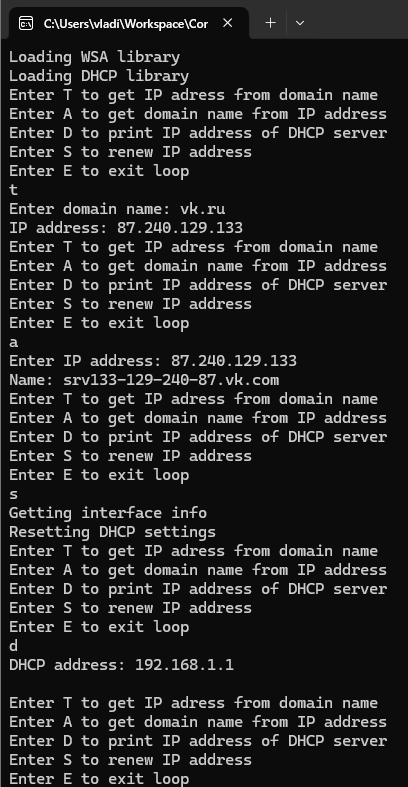
**Разработка программы. Блок-схемы программы.**

**Анализ функционирования программ**

**Вывод:** в ходе лабораторной изучили принципы и характеристику протоколов POP3 и SMTP и составить программу для приема/отправки электронной почты.

**Текст программ. Скриншоты программ.**

Ссылка на репозиторий с кодом: <https://github.com/IAmProgrammist/comp_net/tree/lab7>



#include <iostream>

#include <algorithm>

#include <ws2tcpip.h>

#include <webstur/dhcp.h>

int main() {

    try {

        DHCPHelper::init();

        std::string input;

        // Считытваем команду пользователя

        while (true)

        {

            std::cout

                << "Enter T to get IP adress from domain name\n"

                << "Enter A to get domain name from IP address\n"

                << "Enter D to print IP address of DHCP server\n"

                << "Enter S to renew IP address\n"

                << "Enter E to exit loop"

                << std::endl;

            std::cin >> input;

            std::cin.get();

            std::transform(input.begin(), input.end(), input.begin(), toupper);

            if (input == "T") {

                // Ввести имя домена

                std::cout << "Enter domain name: ";

                std::cout.flush();

                std::string name;

                std::getline(std::cin, name);

                // Получить IP адрес

                auto result = DHCPHelper::getAddrInfo(name);

                char buf[64];

                InetNtopA(AF\_INET, &((sockaddr\_in \*) result->ai\_addr)->sin\_addr, buf, sizeof(buf));

                std::cout << "IP address: " << std::string(buf, buf + strlen(buf)) << std::endl;

            }

            else if (input == "A") {

                // Ввести IP адрес

                sockaddr\_in info;

                info.sin\_family = AF\_INET;

                std::cout << "Enter IP address: ";

                std::cout.flush();

                std::string name;

                std::getline(std::cin, name);

                char buf[64] = {};

                memcpy(buf, name.c\_str(), name.size());

                InetPtonA(AF\_INET, buf, &info.sin\_addr);

                std::cout << "Name: " << DHCPHelper::getNameInfo(info) << std::endl;

            }

            else if (input == "D") {

                // Вывести информацию о сервере

                DHCPHelper::printDHCPServerInfo(std::cout << "DHCP address: ") << std::endl;

            }

            else if (input == "S") {

                // Обновить информацию об IP

                DHCPHelper::renewIP();

            }

            else if (input == "E") {

                // Выход из цикла

                break;

            }

        }

    }

    catch (const std::runtime\_error& error) {

        std::cerr << "Failed while running server. Caused by: '" << error.what() << "'" << std::endl;

        return -1;

    }

    // Выгрузка библиотеки WSA

    DHCPHelper::detach();

    return 0;

}

#include "pch.h"

#include <iostream>

#include <dhcpcsdk.h>

#include <iphlpapi.h>

#include <ws2tcpip.h>

#include <webstur/dhcp.h>

void DHCPHelper::init() {

    std::clog << "Loading WSA library" << std::endl;

    loadWSA();

    std::clog << "Loading DHCP library" << std::endl;

    DWORD dwVersion;

    if (DhcpCApiInitialize(&dwVersion) != 0) {

        throw std::invalid\_argument(getErrorTextWithWSAErrorCode("Unable to load DHCP library"));

    }

}

void DHCPHelper::detach() {

    std::clog << "Unloading WSA library" << std::endl;

    unloadWSA();

    std::clog << "Unloading DHCP library" << std::endl;

    DhcpCApiCleanup();

}

addrinfo\* DHCPHelper::getAddrInfo(std::string name) {

    addrinfo\* res = nullptr;

    if (getaddrinfo(name.c\_str(), nullptr, nullptr, &res) != 0)

        throw std::invalid\_argument(getErrorTextWithWSAErrorCode("Unable to get addr info"));

    return res;

}

std::string DHCPHelper::getNameInfo(sockaddr\_in ip) {

    char host[512];

    if (getnameinfo((sockaddr\*) &ip, sizeof(ip), host, sizeof(host), nullptr, 0, 0) != 0)

        throw std::invalid\_argument(getErrorTextWithWSAErrorCode("Unable to get name info"));

    return std::string(host, host + strlen(host));

}

std::ostream& DHCPHelper::printDHCPServerInfo(std::ostream& out) {

    ULONG ulOutBufLen = 0;

    PIP\_ADAPTER\_INFO pInfo = (PIP\_ADAPTER\_INFO) malloc(sizeof(IP\_ADAPTER\_INFO));

    PIP\_ADAPTER\_INFO pAdapter;

    if (GetAdaptersInfo(NULL, &ulOutBufLen) != NO\_ERROR) {

        free(pInfo);

        pInfo = (PIP\_ADAPTER\_INFO) malloc(ulOutBufLen);

    }

    if (GetAdaptersInfo(pInfo, &ulOutBufLen) != NO\_ERROR) {

        free(pInfo);

        throw std::invalid\_argument(getErrorTextWithWSAErrorCode("Can't get interface info"));

    }

    for (pAdapter = pInfo; pAdapter != NULL; pAdapter = pAdapter->Next) {

        if (pAdapter->DhcpEnabled) {

            out << pAdapter->DhcpServer.IpAddress.String << std::endl;

            free(pInfo);

            return out;

        }

    }

    free(pInfo);

    return out;

}

void DHCPHelper::renewIP() {

    std::clog << "Getting interface info" << std::endl;

    ULONG ulOutBufLen = 0;

    PIP\_INTERFACE\_INFO pInfo;

    pInfo = (IP\_INTERFACE\_INFO\*) malloc(sizeof(IP\_INTERFACE\_INFO));

    if (GetInterfaceInfo(NULL, &ulOutBufLen) != NO\_ERROR) {

        free(pInfo);

        pInfo = (IP\_INTERFACE\_INFO\*) malloc(ulOutBufLen);

    }

    if (GetInterfaceInfo(pInfo, &ulOutBufLen) != NO\_ERROR) {

        free(pInfo);

        throw std::invalid\_argument(getErrorTextWithWSAErrorCode("Can't get interface info"));

    }

    std::clog << "Resetting DHCP settings" << std::endl;

    if (IpReleaseAddress(&pInfo->Adapter[0]) != NO\_ERROR)

        std::cerr << getErrorTextWithWSAErrorCode("Can't reset ip address") << std::endl;

    if (IpRenewAddress(&pInfo->Adapter[0]) != NO\_ERROR)

        std::cerr << getErrorTextWithWSAErrorCode("Can't reset ip address") << std::endl;

    if (pInfo != NULL)

        free(pInfo);

    return;

}

#pragma once

#include <ostream>

#include <webstur/utils.h>

class DLLEXPORT DHCPHelper {

public:

    // Возвращает информацию об IP адресе по доменному имени

    //   name             доменное имя

    static addrinfo\* getAddrInfo(std::string name);

    // Возвращает информацию о доменном имени по IP адресу

    //   addrinfo         информация об адресе

    static std::string getNameInfo(sockaddr\_in ip);

    // Выводит информацию о DHCP-сервере

    static std::ostream& printDHCPServerInfo(std::ostream& out);

    // Обновить IP адрес при помощи DHCP

    static void renewIP();

    // Загружает библиотеку DHCP

    static void init();

    // Выгружает библиотеку DHCP

    static void detach();

};