

Лабораторная работа №2

Работа с протоколом TCP/IP в ОС семейства Windows

Цель работы: Изучить способы применения основных команд и утилит ОС семейства Windows при работе со стеком протокола TCP/IP.

2.1. Краткие теоретические сведения

TCP/IP (Transmission Control Protocol / Internet Protocol) является самым популярным сетевым протоколом, служащим основой глобальной сети Интернет. Предлагаемые им средства маршрутизации обеспечивают максимальную гибкость функционирования локальных сетей предприятий. В ОС Windows протокол **TCP/IP** устанавливается автоматически.

В сетях протокола **TCP/IP** каждому клиенту должен быть назначен соответствующий **IP**-адрес, представляющее собой 32-разрядное число, разделенное точками (например, 192.168.1.255). Кроме того, клиенту может потребоваться служба имен или алгоритм разрешения имен.

В комплект протокола **TCP/IP** входят служебные программы **FTP** (File Transfer Protocol) и **Telnet**. **FTP** — это приложение с текстовым интерфейсом, позволяющее подключаться к **FTP** — серверам и передавать файлы. **Telnet** обладает графическим интерфейсом и позволяет входить на удаленный компьютер и выполнять команды так же, как если бы пользователь находился за клавиатурой этого компьютера.

2.2. Подготовка к выполнению лабораторной работы

Служебные программы и утилиты протокола **TCP/IP** обеспечивают подключение к различным современным сетям. При этом чтобы использовать эти утилиты, на компьютере должна быть установлена поддержка протокола **TCP/IP**. К числу поддерживаемых протоколом **TCP/IP** служебных команд и утилит относятся следующие: **Finger, Ping, Ftp, Rcp, Hostname, Rexec, Ipconfig, Route, Lpq, Rsh, Lpr, Tftp, Nbtstat, Tracert, Netstat, Getmac**, а также целого ряда команд с приставкой **Net** [**accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view**] и другие. Дополнительные сведения о запуске служб **TCP/IP** из командной строки находятся в разделе **Net start**.

В настоящей лабораторной работе предполагается ознакомление с основным набором команд протокола **TCP/IP** и выполнение нескольких учебных заданий с применением командной оболочки.

Перед началом выполнения лабораторной работы в среде ОС Windows необходимо выполнить следующее:

- загрузить ОС Windows и активировать справочное меню (**Пуск | Справка и поддержка**);
- ознакомиться с описанием и синтаксисом ввода командного интерпретатора **Cmd.exe**;
- ознакомиться с описанием и синтаксисом ввода приведенных команд и служебных утилит.

2.3. Порядок выполнения лабораторной работы

Лабораторная работа выполняется последовательно в соответствии с определенным порядком и включает в себя два учебных задания.

2.3.1. Учебное задание №1. Определение конфигурации и тестирование работоспособности протокола **TCP/IP** в ОС Windows.

Порядок выполнения:

I. Загрузить командную оболочку:

- нажмите **Пуск | Выполнить**,
- наберите в появившемся окне **Cmd.exe** (или **cmd**),
- нажмите **Enter** для ввода.

II. Hostname является одной из основных служебных утилит протокола **TCP/IP**, которая показывает локально настроенное имя узла **TCP/IP** (имя узла может отличаться от локально настроенного имени компьютера).

Задача №2.3.1а. Определить имя локально настроенного узла **TCP/IP**.

В окне командной оболочки выполните следующие действия:

- наберите **Hostname**,
- нажмите **Enter** для ввода.

В соответствии с определенным вариантом задания (см. подраздел 2.5 настоящей лабораторной работы):

- повторите данные действия на разных узлах сети в аудитории,
- запишите имена узлов **TCP/IP** в отчет в табл. 2.1.

Таблица 2.1.

Результаты использования служебной утилиты **Hostname**

№ п/п.	Команда с ключами	Результат и вывод по способу применения команды
1.		
2.		
3.		

III. Команда `Ipconfig`. Эта команда отображает текущие настройки **TCP/IP**, включая адреса серверов **DHCP** и **DNS** имени.

DHCP (Dynamic Host Configuration Protocol) — протокол динамической конфигурации узлов, обеспечивающий динамическое распределение **IP**-адресов и других параметров конфигурации между клиентами сети, поддерживает безопасную, надежную и простую конфигурацию сети **TCP/IP**, препятствует возникновению конфликтов **IP**-адресов и помогает сохранять использование **IP**-адресов клиентов. Протокол **DHCP** использует клиент-серверную модель, в которой сервер **DHCP** осуществляет централизованное управление **IP**-адресами сети.

DNS (Domain Name System) — иерархически распределенная база данных, содержащая сопоставления доменных имен, в частности, с **IP**-адресами сети. **DNS** позволяет находить компьютеры и службы по понятным именам, а также просматривать другие сведения из базы данных.

Синтаксис команды **Ipconfig**:

```
Ipconfig [/all] [/renew [адаптер]] [/release [адаптер]] [/flushdns] [/displaydns]
[/registerdns] [/showclassid адаптер] [/setclassid адаптер [код_класса]],
```

где параметр:

/all — осуществляет вывод полной конфигурации **TCP/IP** для всех адаптеров. Адаптеры представляют собой либо физические интерфейсы (установленные сетевые адаптеры), либо логические интерфейсы удаленного доступа.

/renew *[адаптер]* — обновляет конфигурацию **DHCP** для всех адаптеров (если он не задан) или для заданного адаптера. Этот параметр доступен только на компьютерах с адаптерами, настроенными для автоматического получения **IP**-адресов.

/release *[адаптер]* — отправляет сообщение **DHCPRELEASE** серверу **DHCP** для освобождения текущей конфигурации **DHCP** и удаление конфигурации **IP**-адресов для всех адаптеров (если они не задан) или для заданного адаптера. Адаптер отключает протокол **TCP/IP** для адаптеров, настроенных для автоматического получения **IP**-адресов.

/displaydns — отображает содержимое кэша сопоставления имен **DNS**-клиента. Эта информация используется службой **DNS**-клиента для быстрого сопоставления часто встречаемых имен без обращения к указанным в конфигурации **DNS**-серверам.

/registerdns — осуществляет динамическую регистрацию вручную имен **DNS** и **IP**-адресов.

/showclassid *адаптер* — отображает код класса **DHCP** для указанного адаптера. Этот параметр доступен только на компьютерах с адаптерами, настроенными для автоматического получения **IP**-адресов.

/flushdns — очищает содержимое кэша сопоставления имен **DNS**-клиента.

/setclassid *адаптер* [*код_класса*] — задает код класса **DHCP** для указанного адаптера. Как и предыдущий параметр доступен на компьютерах с адаптерами, настроенными для автоматического получения **IP**-адресов.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Ipconfig /?** и нажав **Enter** для ввода.

Необходимо отметить, что при вызове команды **Ipconfig** без параметров выводится только **IP**-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Задача №2.3.16. Исследовать полную конфигурацию протокола TCP/IP.

В окне командной оболочки выполните следующие действия:

- наберите команду **Ipconfig** с необходимыми ключами,
- нажмите **Enter** для ввода,
- запишите полученную информацию в отчет, заполнив табл. 2.2.

Таблица 2.2. Результаты выполнения команды **Ipconfig**

№ п/п.	Наименование данных	Содержимое Данных
1.	имя узла TCP/IP	
2.	тип узла разрешения имен NetBIOS	
3.	MAC-адрес сетевой платы	
4.	IP-адрес	
5.	маска подсети	
6.	шлюз по умолчанию	
7.	DNS-сервер	



Контрольный вопрос:

Какое количество подсетей можно организовать в сети с IP-адресом 172.16.x.y при одной и той же маске подсети?

Какое количество узлов можно адресовать в сети с IP-адресом 172.16.x.y при одной и той же маске подсети?

IV. Команда **Arp** используется для просмотра, добавления или удаления записей в одной или нескольких таблицах трансляции IP-адресов в физические MAC-адреса сетевых адаптеров, например Ethernet. Эти записи используются при работе протокола ARP (Address Resolution Protocol). Для каждого, установленного в компьютере, сетевого адаптера Ethernet, используется отдельная таблица трансляции IP-адресов.

Синтаксис команды **Arp**:

Arp [-a [инет_адрес] [-N иф_адрес]] [-g [инет_адрес] [-N иф_адрес]] [-d инет_адрес [иф_адрес]] [- инет_адрес е_адрес [иф_адрес]],

где параметр:

-a [инет_адрес] [-N иф_адрес] — выводит таблицу текущего протокола ARP для всех интерфейсов. Для того чтобы вывести записи ARP для определенного IP-адреса, необходимо использовать **Arp -a** с параметром *инет_адрес*, где *инет_адрес* — это IP-адрес. Чтобы вывести таблицы кэша ARP для определенного интерфейса, укажите параметр **-N иф_адрес**, где *иф_адрес* — это назначенный интерфейсу IP-адрес. Параметр **-N** вводится с учетом регистра.

-g [инет_адрес] [-N иф_адрес] — по функционалу совпадает с **-a**.

-d *инет_адрес* [*иф_адрес*] — удаляет запись с определенным **IP**-адресом, где *инет_адрес* — это **IP**-адрес. Чтобы удалить запись таблицы для определенного интерфейса, укажите параметр *иф_адрес*, где *иф_адрес* — это **IP**-адрес, назначенный интерфейсу.

-s *инет_адрес* *е_адрес* [*иф_адрес*] — осуществляет добавление статической записи, которая сопоставляет **IP**-адрес *инет_адрес* с физическим адресом *е_адрес*, в кэше **ARP**.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Arp -?** (или просто **Arp**) и нажав **Enter** для ввода.

Задача №2.3.1в. Исследовать содержимое кэша **ARP**.

В окне командной оболочки выполните следующие действия:

- наберите команду **Arp** с необходимыми ключами,
- нажмите **Enter** для ввода,
- запишите полученную информацию в отчет, заполнив табл. 2.3.

Таблица 2.3. Результаты выполнения команды **Arp**

IP-адрес	MAC-адрес	Тип

- самостоятельно осуществите добавление статической записи в кэш **ARP** в соответствии с вариантом задания (см. подраздел 2.5 настоящей лабораторной работы),
- повторно исследуйте содержимое кэша **ARP**,
- запишите полученную информацию в отчет, заполнив табл. 2.4.

Таблица 2.4. Результаты выполнения команды **Arp**

IP-адрес	MAC-адрес	Тип
тот же		



Контрольный вопрос:

Какое количество записей существует в кэше распознавателя **ARP**?

V. Команда **Route.** Эта команда применяется для редактирования или просмотра таблицы **IP**-маршрутов из командной строки в том случае, когда нужно отыскать путь к удаленному компьютеру с использованием протокола **TCP/IP**.

Синтаксис команды **Route**:

Route [-f] [-p] [*подкоманда* [*конечная_точка*] [mask** *маска_сети*] [*шлюз*] [**metric** *метрика*]] [**if** *интерфейс*]],**

где параметр:

-f — очищает таблицу маршрутизации от всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом замыкания на себя (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) или

маршрутом многоадресной рассылки (маршруты с конечной точкой 224.0.0.0 и маской подсети 240.0.0.0).

-p — при использовании данного параметра с *подкомандой Add* (табл. 2.5) указанный маршрут добавляется в реестр и используется для инициализации таблицы **IP**-маршрутизации каждый раз при запуске протокола **TCP/IP**. При использовании параметра с *подкомандой Print* выводит на экран список постоянных маршрутов. Все другие *подкоманды* игнорируют этот параметр.

Таблица 2.5. Список допустимых *подкоманд*

№ п/п.	Подкоманда	Назначение
1.	Add	Добавление маршрута
2.	Change	Изменение существующего маршрута
3.	Delete	Удаление маршрута или маршрутов
4.	Print	Печать маршрута или маршрутов

Конечная точка — определяет конечную точку маршрута. Конечной точкой может быть сетевой **IP**-адрес (где разряды узла имеют значение 0), **IP**-адрес маршрута к узлу, или значение 0.0.0.0 для маршрута по умолчанию.

Mask маска_сети — указывает маску сети (подсети) в соответствии с точкой назначения. Маска сети может быть маской подсети соответствующей сетевому **IP**-адресу, например, 255.255.255.255 для маршрута к узлу или 0.0.0.0. для маршрута по умолчанию. Если данный параметр пропущен, используется маска подсети 255.255.255.255. Конечная точка не может быть более точной, чем соответствующая маска подсети. Другими словами, значение разряда 1 в адресе конечной точки невозможно, если значение соответствующего разряда в маске подсети равно 0.

Шлюз — указывает **IP**-адрес пересылки или следующего перехода, по которому доступен набор адресов, определенный конечной точкой и маской подсети. Для локально подключенных маршрутов подсети, адрес шлюза — это **IP**-адрес, назначенный интерфейсу, который подключен к подсети. Для удаленных маршрутов, которые доступны через один или несколько маршрутизаторов, адресом шлюза является непосредственно доступный **IP**-адрес ближайшего маршрутизатора.

Metric метрика — задает целочисленную метрику стоимости маршрута (в пределах от 1 до 9999) для маршрута, которая используется при выборе в таблице маршрутизации одного из нескольких маршрутов, наиболее близко соответствующего адресу назначения пересылаемого пакета. Выбирается маршрут с наименьшей метрикой. Метрика отражает количество переходов, скорость прохождения пути, надежность пути, пропускную способность пути и средства администрирования.

If интерфейс — указывает индекс интерфейса, через который доступна точка назначения.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Route -?** (или просто **Route**) и нажав **Enter** для ввода.

Задача №2.3.1г. Вывести список интерфейсов и их индексов.

В окне командной оболочки выполните следующие действия:

- наберите команду **Route** с необходимыми ключами,
- нажмите **Enter** для ввода,
- запишите полученную информацию в отчет, заполнив табл. 2.6.

Таблица 2.6. Результаты выполнения команды **Route**

Физический интерфейс					
MAC-адрес сетевой платы					
Наименование сетевой платы					
№ п/п	Активные маршруты				
	Сетевой Адрес	Маска Сети	Адрес шлюза	Интерфейс	Метрика
1.					
.					
.					
n.					



Контрольный вопрос:

Из скольких и каких именно элементов состоит запись о маршруте?

2.3.2. Учебное задание №2. Использование основных утилит ОС Windows для тестирования работоспособности протокола **TCP/IP**.

Порядок выполнения:

I. Служебная утилита **Ping** используется для отправки **TCP/IP**-пакетов в виде сообщений эхо-запросов протокола **ICMP** по **IP**-адресу и ожиданию эхо-ответов **ICMP**. Утилита **Ping** сообщает количество принятых эхо-ответов и интервал времени между отправкой пакета запроса и приемом ответа; она лежит в основе диагностики сетей, работающих с протоколом **TCP/IP** и используется для проверки получения приемником **TCP/IP**-пакетов. Если с помощью этой команды по сети не удастся «достучаться» до определенного компьютера, вероятнее всего, в сети существует разрыв или связь в сети вовсе отсутствует. Например, чтобы опросить станцию с **IP**-адресом 192.168.1.100, следует набрать **Ping** 192.168.1.100.

ICMP (Internet Control Message Protocol) это обязательный управляющий протокол в наборе протоколов **TCP/IP**, сообщающий об ошибках и обеспечивающий связи между узлами сети.

Синтаксис команды **Ping**:

Ping [-t] [-a] [-n *счетчик*] [-l *размер*] [-f] [-i *TTL*] [-v *тип*] [-r *счетчик*] [-s *счетчик*] [{-j *список_узлов* |-k *список_узлов*}] [-w *интервал*] [*имя_конечного_компьютера*],

где параметр:

-t — задает для команды **Ping** отправку сообщений с эхо-запросом к точке назначения до тех пор, пока команда не будет прервана. Для прерывания команды и вывода статистики нажмите комбинацию клавиш **CTRL+BREAK**. Для прерывания команды **Ping** и выхода из нее нажмите клавиши **CTRL+C**.

-a — задает разрешение обратного имени по **IP**-адресу назначения. В случае успешного выполнения выводится имя соответствующего узла.

-n счетчик — задает число отправляемых сообщений с эхо-запросом.

-l размер — задает в байтах (в диапазоне от 32 до 65527 байт) длину поля данных в отправленных сообщениях с эхо-запросом.

-f — задает отправку сообщений с эхо-запросом с флагом «Don't Fragment» в **IP**-заголовке, установленном в 1. Сообщения с эхо-запросом не фрагментируются маршрутизаторами на пути к месту назначения.

-i TTL — задает значение поля **TTL** (time-to-live, время жизни) в **IP**-заголовке для отправляемых сообщений с эхо-запросом. Для узлов ОС Windows это значение обычно равно 128.

-v тип — задает значение поля типа службы в **IP**-заголовке для отправляемых сообщений с эхо-запросом.

-r счетчик — задает параметр записи маршрута (Record Route) в **IP**-заголовке для записи пути, по которому проходит сообщение с эхо-запросом и соответствующее ему сообщение с эхо-ответом. Каждый переход в пути использует параметр записи маршрута.

-s счетчик — указывает вариант штампа времени Интернета в **IP**-заголовке для записи времени прибытия сообщения с эхо-запросом и соответствующего ему сообщения с эхо-ответом для каждого перехода.

-j список_узлов — указывает для сообщений с эхо-запросом использование параметра свободной маршрутизации в **IP**-заголовке с набором промежуточных точек назначения, указанным в *списке_узлов*. Список узлов — это набор **IP**-адресов (в точечно-десятичной нотации), разделенных пробелами.

-k список_узлов — указывает для сообщений с эхо-запросом использование параметра строгой маршрутизации в **IP**-заголовке с набором промежуточных точек назначения, указанным в *списке_узлов*.

-w интервал — определяет в миллисекундах время ожидания получения сообщения с эхо-ответом, которое соответствует сообщению с эхо-запросом. Если сообщение с эхо-ответом не получено в пределах заданного интервала, то выдается сообщение об ошибке.

имя_конечного_компьютера — задает точку назначения, идентифицированную **IP**-адресом или именем узла.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Ping -?** (или просто **Ping**) и нажав **Enter** для ввода.

Задача №2.3.2а. Проверить наличие соединения с узлом сети по заданному **IP**-адресу или имени узла.

В окне командной оболочки выполните следующие действия:

- убедитесь, что сетевой адаптер для проверяемой конфигурации **TCP/IP** не находится в состоянии «Сеть отключена»,
- наберите команду **Ping** с необходимыми ключами согласно условиям: число отправляемых сообщений с эхо-запросом – 10, длина поля данных – 4096 байт;

- нажав **Enter** для ввода, проверьте наличие соединения с узлом сети, имеющего:
 - IP**-адрес петли обратной связи,
 - IP**-адрес собственного узла пользователя,
 - IP**-адрес основного шлюза (по умолчанию),
 - IP**-адрес шлюза (маршрутизатора) внешнего сетевого интерфейса,
 - IP**-адрес определенного узла локальной сети (см. подраздел 2.5 настоящей лабораторной работы),
 - имя удаленного узла внешней сети (см. подраздел 2.5),
- запишите полученную информацию в отчет, заполнив табл. 2.7.

Необходимо отметить, что в табл. 2.7 понятие «Среднее время» означает среднее приблизительное время приема-передачи, измеряемое в миллисекундах.

Таблица 2.7. Результаты проверки наличия соединения с узлом сети

№ п/п.	Соединение с узлом сети				
	Наименование	Имя Узла	IP-адрес	Среднее время	TTL
1.	Петля обратной связи		127.0.0.1		
2.	Собственный узел пользователя				
3.	Основной шлюз (по умолчанию)				
4.	Шлюз внешнего сетевого интерфейса				
5.	Определенный узел локальной сети				
6.	Удаленный узел внешней сети				



Контрольный вопрос:

Каким образом можно определить **MAC**-адрес сетевой платы определенного локального узла в сети, зная его **IP**-адрес?

Почему изменилось содержимое кэша распознавателя **ARP** по сравнению с тем, что наблюдалось в задаче №2.3.1в?

II. Утилита **Tracert** используется для трассировки маршрута посредством отправки эхо-сообщений протокола **ICMP** по определенному **IP**-адресу, постоянно увеличивая время жизни **TTL** в поле **IP**-заголовка. При этом каждый последующий эхо-запрос проходит по сети дальше на один узел (маршрутизатор), уменьшающий значение **TTL** на единицу до

тех пор, пока оно не достигнет нуля, а последний узел (маршрутизатор), направляющий пакет, возвратит ошибку «время закончилось» протокола **ICMP**.

Одноименная команда **Tracert** отображает на экране путь, упорядоченный список узлов (маршрутизаторов) на пути прохождения пакетов, в случае ошибки, возвращающие соответствующее сообщение. Путь определяется из анализа сообщений протокола **ICMP** об истечении времени, полученных от промежуточных узлов (маршрутизаторов), и эхо-ответов точки назначения. При этом **Tracert** фиксирует число переходов, которые потребовалось совершить на пути к точке назначения. Однако некоторые узлы (маршрутизаторы) не посылают сообщений об истечении времени для пакетов с нулевыми значениями **TTL** и, следовательно, не видны для команды **Tracert**. В этом случае отображается ряд звездочек (*).

Синтаксис команды **Tracert**:

```
Tracert [-d] [-h максимальное_число_переходов] [-j список_узлов] [-w интервал]  
[имя_конечного_компьютера],
```

где параметр:

-d — означает указание не делать поиска **DNS** имен для каждого **IP**-адреса. В отчет заносится **IP**-адрес самого ближнего интерфейса узла (маршрутизатора).

-h *максимальное_число_переходов* — задает максимальное количество переходов на пути при поиске точки назначения. Максимальное количество переходов по умолчанию равно 30, но может быть изменено при необходимости.

-j *список_узлов* — для сообщений с эхо-запросом указывает на использование параметра свободной маршрутизации в **IP**-заголовке с набором промежуточных мест назначения в *списке_узлов*, представляющем собой набор **IP**-адресов (в точечно-десятичной нотации), разделенных пробелами.

-w *интервал* — определяет время ожидания для получения эхо-ответов протокола **ICMP** или **ICMP**-сообщений об истечении времени, соответствующих текущему эхо-запросу.

имя_конечного_компьютера — задает точку назначения, определенную **IP**-адресом или именем узла.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Tracert -?** (или **Tracert**) и нажав **Enter** для ввода.

Задача №2.3.26. Выполнить трассировку маршрута до определенной точки назначения, заданной **IP**-адресом или именем узла.

В окне командной оболочки выполните следующие действия:

- наберите команду **Tracert** с необходимыми ключами,
- нажав **Enter** для ввода, выполните трассировку маршрута, имеющего: **IP**-адрес шлюза (маршрутизатора) внешнего сетевого интерфейса, **IP**-адрес определенного узла локальной сети (см. подраздел 2.5 настоящей лабораторной работы), имя удаленного узла внешней сети (см. подраздел 2.5),
- запишите полученную информацию в отчет, заполнив табл. 2.8.

Необходимо отметить, что в табл. 2.8 понятие «среднее время» означает среднее приблизительное время приема-передачи, измеряемое в миллисекундах.

Таблица 2.8.

Результаты трассировки маршрута к заданному узлу сети

№ п/п.	Точка назначения «Шлюз внешнего сетевого интерфейса»	
	IP-адрес (имя) узла сети	Среднее время
1.		
...		
п.		
№ п/п.	Точка назначения «Узел локальной сети»	
	IP-адрес (имя) узла сети	Среднее время
1.		
...		
п.		
№ п/п.	Точка назначения «Удаленный узел внешней сети»	
	IP-адрес (имя) узла сети	Среднее время
1.		
...		
п.		



Контрольный вопрос:

Какое в каждом из трех случаев задачи №2.3.2б количество пройденных пакетом узлов (маршрутизаторов) сети?

III. Команда **Pathping** является одной из самых полезных новых команд диагностики протокола **TCP/IP**. Позволяет опрашивать каждый промежуточные сетевые узлы (маршрутизаторы) на пути следования сигнала между исходной точкой и точкой назначения, после чего при каждой ретрансляции сигнала фиксирует информацию о задержках и потерях **TCP/IP**-пакетов.

Команда **Pathping** выполняет эквивалентные команде **Tracert** действия, идентифицируя узлы (маршрутизаторы), находящиеся на пути. При этом в течение некоторого периода времени команда **Pathping** отправляет многочисленные сообщения с эхо-запросами каждому узлу (маршрутизатору), находящемуся в сети между исходным и конечным пунктом, а затем на основании **TCP/IP**-пакетов, полученных от каждого из них, вычисляет результаты и обрабатывает статистику приема-передачи. Поскольку **Pathping** показывает коэффициент потери пакетов для каждого узла (маршрутизатора) сети или связи, появляется возможность определить узлы (маршрутизаторы) или подсети, имеющие проблемы.

Синтаксис команды **Pathping**:

Pathping [-n] [-h *максимальное_число_переходов*] [-g *список_узлов*] [-p *период*] [-q *число_запросов*] [-w *интервал*] [-T] [-R] [*имя_конечного_компьютера*],

где параметр:

-n — предотвращает попытки команды **Pathping** сопоставить IP-адреса промежуточных маршрутизаторов с их именами, что позволяет ускорить вывод результатов.

-h *максимальное_число_переходов* — задает максимальное количество переходов на пути при поиске конечного пункта назначения.

-g *список_узлов* — указывает для сообщений с эхо-запросом использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных точек назначения, указанных в *списке_компьютеров*. При свободной маршрутизации последовательные промежуточные точки назначения могут быть разделены одним или несколькими узлами (маршрутизаторами). *Список_адресов* представляет собой набор IP-адресов, разделенных пробелами.

-p *период* — задает в миллисекундах время ожидания между последовательными проверками связи. Значение по умолчанию равно 250 миллисекунд. При этом необходимо помнить, ТСП/IP-пакеты, используемые для проверки связи, отсылаются каждому промежуточному узлу (маршрутизатору) в отдельности. Поэтому интервал времени между двумя пакетами, переданными одному узлу, составляет *период -x* в виде числа узлов.

-q *число_запросов* — задает количество сообщений с эхо-запросом, отправленных каждому узлу (маршрутизатору) на маршруте следования ТСП/IP-пакета.

-w *интервал* — задает в миллисекундах время ожидания каждого отклика. При этом ТСП/IP-пакеты можно отправлять одновременно, а промежуток времени, указанный в параметре *интервал*, не ограничен промежутком времени, указанным в параметре *период*.

-T — присоединяет тег приоритета уровня 2 (например, 802.1p) к сообщениям с эхо-запросом, отправляемым каждому сетевому устройству на маршруте. Это помогает обнаружить сетевые устройства, для которых не настроен приоритет уровня 2. Он предназначен для проверки соединений, использующих спецификации планировщика пакетов QoS.

-R — проверяет, все ли сетевые устройства вдоль маршрута следования ТСП/IP-пакета поддерживают протокол **RSVP** (Resource Reservation Setup Protocol, протокол настройки резервирования ресурсов), который позволяет главному компьютеру резервировать определенную часть пропускной способности для потока данных. Этот параметр предназначен для проверки соединений, использующих спецификации планировщика пакетов QoS.

имя_конечного_компьютера — задает пункт назначения, идентифицированный IP-адресом или именем узла.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Pathping -?** (или **Pathping**) и нажав **Enter** для ввода.

Задача №2.3.2в. Выполнить трассировку маршрута до определенной точки назначения, заданной IP-адресом или именем узла. Исследовать статистику переходов и потерь ТСП/IP-пакетов в процессе трассировки.

В окне командной оболочки выполните следующие действия:

- наберите команду **Ping** с необходимыми ключами согласно условиям:

число отправляемых сообщений с эхо-запросом – 10,
длина поля данных – 8192 байт;

- нажав **Enter** для ввода, выполните запрос узла сети, имеющего:
IP-адрес или имя удаленного узла внешней сети (см. подраздел 2.5 настоящей лабораторной работы),
 - запишите полученную информацию в отчет, заполнив табл. 2.9.
 - наберите команду **Tracert** с необходимыми ключами,
 - нажав **Enter** для ввода, выполните трассировку маршрута, имеющего тот же **IP**-адрес или имя удаленного узла внешней сети,
 - запишите полученную информацию в отчет, заполнив табл. 2.9.
 - наберите команду **Pathping** с необходимыми ключами,
 - нажав **Enter** для ввода, выполните трассировку маршрута, имеющего тот же **IP**-адрес или имя удаленного узла внешней сети,
 - полученную информацию в виде статистики приема-передачи запишите в отчет, заполнив табл. 2.9.

Необходимо отметить, что в табл. 2.9. понятие «среднее время» означает среднее приближительное время приема-передачи, измеряемое в миллисекундах. Понятие «RTT» означает время обмена данными на каждом из узлов (маршрутизаторов).

Таблица 2.9. Результаты трассировки маршрута к узлу сети

Сводная статистика приема-передачи			
Ping	Имя узла		
	IP-адрес узла		
Статистика пакетов	Отправлено		
	Получено		
	Потеряно		
	процент потерь		
Tracert	Имя узла		
	IP-адрес узла		
Статистика прыжков	максимум прыжков		
	прыжков до узла сети		
	среднее время		
Pathping	Имя узла		
	IP-адрес узла		
Статистика приема-передачи			
№ п/п.	Промежуточный IP-адрес узла	RTT	Суммарный процент потерь на узле сети

1.			
...			
n.			



Контрольный вопрос:

Оцените степень потерь пересылаемых по маршруту **TCP/IP**-пакетов для соединений (определяемых вертикальной чертой (|) в столбце **Адрес**) при их перегрузке.

В чем заключается преимущество команды **Pathping** перед альтернативными командами?

IV. Следующей очень важной командой, отображающей текущий статус и статистику подключений по протоколам **TCP/IP** или **UDP** (User Datagram Protocol), является команда **Netstat**. При использовании команды **Netstat** выводятся данные, как о локальных, так и об удаленных именах и портах активных сетевых соединений.

Синтаксис команды **Netstat**:

Netstat [-a] [-e] [-n] [-o] [-p *протокол*] [-r] [-s] [*интервал*],

где параметр:

-a — выводит все активные **TCP/IP**-подключения и прослушиваемые компьютером портов **TCP/IP** и **UDP**.

-e — выводит **Ethernet** статистику, например, количество отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом **-s**.

-n — выводит активные **TCP/IP**-подключения с отображением адресов и номеров портов в числовом формате. Имя локального компьютера (или внешнего адреса), соответствующее **IP**-адресу и имени порта, выводится только в том случае, если не указан параметр **-n**. При этом, если порт не назначен, вместо его номера будет выведена звездочка (*).

-o — выводит все активные **TCP/IP**-подключения и **PID** коды процесса для каждого подключения. Код процесса **PID** позволяет найти приложение на вкладке «Процессы» диспетчера задач Windows. Этот параметр может комбинироваться с ключами **-a**, **-n** и **-p**.

-p *протокол* — выводит подключения 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 — выводит статистику по протоколу. По умолчанию выводится статистика для протоколов **TCP**, **UDP**, **ICMP** и **IP**. Если установлен протокол **IPv6** для ОС Windows, отображается статистика для протоколов **TCP** через **IPv6**, **UDP** через **IPv6**, **ICMPv6** и **IPv6**.

-r — выводит содержимое таблицы маршрутизации **IP**. Эта команда эквивалентна команде **Route print**, рассмотренной ранее.

интервал — указывает на обновление выбранных данных с интервалом, определенным в секундах. Нажатие клавиш **CTRL+C** останавливает обновление.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Netstat -?** (или **Netstat**) и нажав **Enter** для ввода.

Задача №2.3.2г. Исследовать статистические данные **TCP/IP**-подключений с помощью команды **Netstat** на конкретных примерах.

1. Выведите **Ethernet** статистику.
2. Выведите статистику по всем активным протоколам.
3. Выведите статистику только по **TCP**-протоколу
4. Выводите статистику всех активных **TCP/IP**-подключений и **PID**-кодов процессов каждые 10 секунд.

При выполнении задания используйте следующие инструкции:

- по каждому из пунктов задания в окне командной оболочки наберите соответствующую команду с необходимыми ключами,
- нажмите **Enter** для ввода,
- изучите полученный результат и сделайте вывод о проделанной работе,
- запишите полученную информацию в отчет.



Контрольный вопрос:

Каким образом с помощью этой команды можно отобразить локальную таблицу маршрутизации? Сравните локальную таблицу маршрутизации с таблицей, полученной с помощью команды **Route print**. Сделайте вывод и запишите его в отчет.

V. Еще одна диагностическая утилита и одноименная ей служебная команда **Nbtstat** предназначены для отображения статистики протокола и текущих соединений **TCP/IP** с использованием **NetBIOS over TCP/IP (NetBT)**. Кроме того, утилита позволяет отображать таблицы имен **NetBIOS** для локального и удаленного узлов сети, а также кэша имен **NetBIOS** с возможностью его обновления для зарегистрированных имен в службе **WINS** (Windows Internet Name Service).

NetBIOS — сетевая базовая система ввода-вывода, интерфейс программирования (**API**) для использования программами в локальной сети. **NetBIOS** предоставляет программам единый набор команд для запросов к службам нижнего уровня, которые требуются для управления именами, проведения сеансов и передачи данных между узлами сети.

Синтаксис команды **Nbtstat**:

Nbtstat [-a удаленное_имя] [-A IP-адрес] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [интервал],

где параметр:

-a удаленное_имя — выводит таблицу имен **NetBIOS** удаленного узла сети. Таблица имен **NetBIOS** является списком имен **NetBIOS**, соответствующих приложениям **NetBIOS**, работающим на данном компьютере.

-A IP-адрес — выводит таблицу имен **NetBIOS** удаленного узла сети, заданного **IP**-адресом.

-c — выводит содержимое кэша имен **NetBIOS**, таблицы имен **NetBIOS** и их разрешенных **IP**-адресов.

-n — выводит таблицу имен **NetBIOS** локального узла сети. Состояние «Зарегистрирован» означает, что это имя зарегистрировано на сервере **WINS** или в качестве широковещательного адреса.

-r — выводит статистику разрешения имен **NetBIOS**. На компьютере с ОС Windows, настроенном для использования **WINS**, этот параметр возвращает количество имен, разрешенных и зарегистрированных для широковещательной рассылки или **WINS**.

-R — очищает содержимое кэша имен **NetBIOS**.

-RR — обновляет имена **NetBIOS** для локального узла сети, зарегистрированного на серверах **WINS**.

-s — выводит сеансы клиента и сервера **NetBIOS** с попыткой преобразования конечного **IP**-адреса в имя.

-S — выводит сведения о работе сервера и клиента **NetBIOS**. При этом удаленные компьютеры выводятся только по **IP**-адресам.

интервал — определяет обновление выбранной статистики на экране через заданный промежуток времени в секундах. Нажатие клавиш **CTRL+C** останавливает обновление статистики.

Дополнительная информация по данной команде, а также примеры ее использования доступны в справке ОС (**Пуск | Справка и поддержка**) в соответствующем разделе. Справку также можно получить, набрав в окне командной оболочки строку **Nbtstat -?** (или **Nbtstat**) и нажав **Enter** для ввода.

В табл. 2.10 приведены заголовки столбцов, отображаемые утилитой **Nbtstat**. В табл. 2.11 приведены возможные состояния подключения **NetBIOS**.

Таблица 2.10. Заголовки столбцов при работе утилиты **Nbtstat**

Заголовок	Описание
Ввод	Число полученных байт.
Вывод	Число отправленных байт.
Вид	Направление передачи от локального узла (Исх.) или от удаленного узла (Вхд.) сети.
Время жизни	Время, оставшееся до сброса элемента кэша таблицы имен.
Локальное имя	Локальное имя NetBIOS , соответствующее данному подключению.
Удаленный узел	Имя или IP -адрес удаленного узла сети.
<03>	Последний байт имени NetBIOS , преобразованный в шестнадцатеричную форму. Он часто имеет специальное значение, так как одно имя может встречаться несколько раз на одном компьютере, различаясь только последним байтом.
Тип имени	Имя может быть уникальным или именем группы.
Состояние	«Зарегистрирован» (служба NetBIOS работает на удаленном компьютере) или «Конфликт» (в службе уже зарегистрировано такое же имя компьютера).
Состояние	Состояние подключений NetBIOS .

Таблица 2.11. Возможные состояния подключения **NetBIOS**

Состояние	Описание
Подключен	Сеансовое подключение установлено.

Назначен	Конечная точка подключения создана и связана с IP -адресом.
Ожидание	Конечная точка доступна для входящих подключений.
Простаивает	Конечная точка создана, но без подключения.
Прием	Запрос на входящее подключение принят, подключение будет установлено.
Повторное Подключение	Повторная попытка установки подключения (после первой неудачной попытки).
Исходящий	Сеанс находится в процессе подключения, создается подключение TCP .
Входящий	Сеанс находится в процессе подключения.
Отключение	Сеанс находится в процессе отключения.
Отключен	Локальный узел отправил запрос на отключение и ожидает подтверждения от удаленной системы.

Задача №2.3.2д. Изучить статистику протокола и текущих соединений **TCP/IP** с использованием **NetBIOS over TCP/IP** на конкретных примерах.

1. Выведите таблицу имен **NetBIOS** удаленного узла сети, имеющего:
IP-адрес определенного узла локальной сети (см. подраздел 2.5 настоящей лабораторной работы),
IP-адрес удаленного узла внешней сети (см. подраздел 2.5),
имя удаленного узла внешней сети (см. подраздел 2.5),
2. Отобразите содержимое кэша имен **NetBIOS** собственного узла пользователя.
3. Выводите статистику сеанса **NetBIOS** по **IP**-адресам удаленных узлов сети через каждые 15 секунд.

При выполнении задания используйте следующие инструкции:

- по каждому из пунктов задания в окне командной оболочки наберите соответствующую команду с необходимыми ключами,
- нажмите **Enter** для ввода,
- изучите полученный результат и сделайте вывод о проделанной работе,
- запишите полученную информацию в отчет.



Контрольный вопрос:

Проанализируйте конфигурацию протокола **TCP/IP** на Вашей рабочей станции и определите, каким образом разрешаются имена **NetBIOS**?

Если Вам не удалось получить статистику протокола **TCP/IP** с использованием **NetBIOS over TCP/IP**, ответьте на вопрос почему? Что в данном случае необходимо сделать, чтобы получить требуемую статистику?

В настоящей лабораторной работе были рассмотрены команды и служебные утилиты, позволяющие посредством командного интерпретатора иметь доступ к основным функциям протокола **TCP/IP** с целью тестирования сетевого оборудования, взаимодействия узлов (маршрутизаторов) в сети, а также настройки программного обеспечения для обеспечения коммутации компьютеров в глобальной сети Интернет. Основным преимуществом данного набора команд является их универсальность в применении, а их принадлежность к

протоколу **TCP/IP** обеспечит возможность взаимной связи различного сетевого оборудования и компьютеров с разными операционными системами.

Изученные команды и утилиты являются базовыми инструментами системного администратора и специалиста в области информационных технологий. Эти знания являются необходимыми в развивающихся условиях современного информационного пространства. Они создают основу для дальнейшего изучения принципов сетевого взаимодействия и развития навыков в области обеспечения сетевой безопасности.

2.4. Содержание отчета по лабораторной работе

Отчет по лабораторной работе оформляется в соответствии с требованиями государственного стандарта и должен содержать:

- 1) титульный лист (**Приложение 6**);
- 2) описание и цель работы;
- 3) краткое описание протокола **TCP/IP**;
- 4) краткое описание служебных команд и утилит, поддерживаемых протоколом **TCP/IP** (см. подраздел 2.1);
- 5) результаты исследований работы служебных команд и утилит в соответствии с учебными заданиями лабораторной работы;
- 6) заполненные таблицы учебных заданий лабораторной работы;
- 7) письменные ответы на контрольные вопросы, размещенные в соответствующих учебных заданиях лабораторной работы.
- 8) выводы о проделанной работе.

2.5. Варианты заданий к лабораторной работе

Варианты заданий для выполнения лабораторной работы представлены в табл. 2.12 и 2.13, имеющие столбцы с заглавиями, указывающими на их причастность к определенной задаче (например, «Задача №2.3.1а»). Для того чтобы выбрать требуемый вариант для выполнения задания лабораторной работы, необходимо из столбца с номером текущего задания выбрать строку номера варианта, определяемую порядковым номером обучающегося в списке группы.

Таблица 2.12. Варианты заданий к лабораторной работе

Учебное задание №1				
Вар №	Задача №2.3.1а			Задача №2.3.1в
	Номер узла сети в аудитории			Физический MAC-адрес
1.	1	2	13	00-AA-00-4F-2A-9C
2.	2	3	1	00-AB-01-F5-3A-9D
3.	3	4	2	00-BA-02-FA-AA-1A
4.	4	5	3	00-CC-30-BB-A1-DC
5.	5	6	4	00-CD-35-AB-5A-AA
6.	6	7	5	00-BB-03-DD-B1-31
7.	7	8	6	00-FA-45-C1-D4-55
8.	8	9	7	00-FD-DC-34-D1-FA
9.	9	10	8	00-F3-D9-C1-AA-22
10.	10	11	9	00-FA-C1-F1-66-DA
11.	11	12	10	00-FD-11-A1-1A-DA
12.	12	13	11	00-16-D1-C2-A3-AA
13.	13	1	12	00-1A-AB-5C-59-AC
14.	1	2	13	01-F1-8A-BA-23-FE
15.	2	3	1	01-D2-7A-CD-22-EE
16.	3	4	2	01-E3-6B-FF-12-AB
17.	4	5	3	01-C4-1E-BA-56-EF
18.	5	6	4	01-95-2D-CB-43-E3
19.	6	7	5	01-A6-5F-43-1A-EA
20.	7	8	6	01-B7-6E-DD-CD-F1
21.	8	9	7	01-78-6F-AB-21-CA
22.	9	10	8	01-49-8C-21-AD-F4

Таблица 2.13. Варианты заданий к лабораторной работе

Учебное задание №2			
Вар. №	Задачи №2.3.2а и №2.3.2б		
		Задача №2.3.2в	
	Задача №2.3.2д		
	Локальный IP-адрес	Имя удаленного узла	Удаленный IP-адрес
1.	Приложение 3	www.rambler.ru	212.98.161.252
2.	Приложение 3	www.mail.ru	66.29.53.20
3.	Приложение 3	www.yandex.ru	63.246.158.4
4.	Приложение 3	www.altavista.com	62.213.76.150
5.	Приложение 3	www.gmail.com	124.83.139.192
6.	Приложение 3	www.google.com	193.111.247.70
7.	Приложение 3	www.ag.ru	143.166.83.38
8.	Приложение 3	www.render.ru	89.31.143.1
9.	Приложение 3	www.kaspersky.ru	86.57.253.203
10.	Приложение 3	www.ixbt.com	62.149.13.65
11.	Приложение 3	www.thg.com	77.221.131.22
12.	Приложение 3	www.opera.com	216.118.117.101
13.	Приложение 3	www.microsoft.ru	64.131.71.23
14.	Приложение 3	www.ati.ru	69.65.118.47
15.	Приложение 3	www.intercon.ru	194.169.192.144
16.	Приложение 3	www.asus.com	91.194.10.50
17.	Приложение 3	www.samsung.com	83.222.23.134
18.	Приложение 3	www.logitech.com	84.204.96.147
19.	Приложение 3	www.ferra.ru	193.178.144.154
20.	Приложение 3	www.3dnews.ru	81.3.137.196