Лабораторная работа № 1
УТИЛИТЫ TCP/IP

Цель работы

Познакомиться со средствами диагностики сети и поиска неисправностей стека TCP/IP.

Постановка задачи

1. Используя материалы лекций, рекомендуемую литературу и методические указания к лабораторной работе, изучить основные теоретические вопросы:
- понятие и основные компоненты компьютерной сети;
- диагностические утилиты TCP/IP и их возможности;
- функции протокола ARP;
- функции протокола ICMP;
- понятие общего ресурса.
2. Выполнить упражнения к лабораторной работе.
3. Подготовить отчет.
4. Устно ответить на контрольные вопросы.

Методические указания

1. Диагностические утилиты TCP/IP.

Для диагностики и поиска неисправностей работы сети можно использовать специальные утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения. Список некоторых утилит приведен в таблице 1.

Таблица 1 – Диагностические утилиты TCP/IP.

Утилита	Применение
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу).
hostname	Отображает имя локального хоста. Используется без параметров.
getmac	Отображает MAC-адреса сетевых адаптеров компьютера
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
ping	Осуществляет тестирование сетевых подключений.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.
pathping	Аналогична утилите tracert, предназначена для определения потерь данных на промежуточных узлах.
route	Просмотр и редактирование таблицы маршрутищации
nslookup	Определение ip-адреса по доменному имени и имен-псевдонимов

Синтаксис использования для всех утилит одинаков. В окне работы с командной строкой после приглашения операционной системы указывается имя утилиты, пробел, параметры. Команды нечувствительны к регистру.

C:\WINDOWS>ping –n 10 www.gmail.com

Справочную информацию по любой из утилит можно получить, используя /? после имени утилиты.

C:\WINDOWS>ipconfig /?

2. Файлы конфигурации

При установке стека TCP/IP создается несколько системных файлов и файлов разрешения имен в каталогах System32\Drivers и System32\Drivers\Etc

Файл конфигурации	Описание
Hosts	Обеспечивает разрешение имен узлов в IP адреса
LMHosts	Обеспечивает разрешение имен NetBIOS в IP адреса
NETWorks	Обеспечивает разрешение имен сетей в идентификаторы сетей
PROTOCOL	Обеспечивает преобразование имени протокола в идентификатор протокола, заданный в RFC. Номер протокола – это значение поля в заголовке IP-пакета, идентифицирующего, какому протоколу верхнего уровня принадлежат данные в IP пакете.
SERVICES	Обеспечивает преобразование имени сервиса в номер порта и имя протокола транспортного уровня.

3. Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

С помощью утилиты ipconfig можно получить сведения обо всех сетевых интерфейсах данного узла, в частности, всю адресную информацию (имя узла, все IP-адреса узла, маски, адреса шлюзов, адреса DNS-серверов, все физические адреса узла).

Эта команда особенно полезна на компьютерах, работающих с **DHCP (Dynamic Host Configuration Protocol) – протокол динамического конфигурирования хоста.** Утилита позволяет определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] освобождает выделенный DHCP IP-адрес;

adapter – имя сетевого адаптера;

displaydns выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация TCP/IP и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;

- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

4. Тестирование связи с использованием утилиты ping.

Утилита ping (Packet Internet Grouper) используется для тестирования сетевого соединения с удаленным узлом, сервером, маршрутизатором, диагностики ошибок соединения, а также для проверки конфигурирования TCP/IP. Она определяет доступность указанного узла и позволяет измерить время прохождения пакетов от данного узла до любого другого узла сети. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. **Хостом** называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом. Она посылает к указанному пользователем хосту несколько IP-пакетов (по умолчанию 4) и ожидая ответы на них. При этом она измеряет интервал времени, в течение которого пакет вернулся, а также показывает соотношение количества отосланных пакетов к количеству принятых, что может служить субъективной оценкой «качества связи» между узлами. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Утилита ping используется следующими способами:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address): ping 127.0.0.1

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, в утилите ping используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес или имя удаленного хоста:

ping IP-адрес_удаленного хоста

либо ping имя хоста

Синтаксис утилиты ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

Параметры:

-t выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count посылает количество пакетов ECHO, указанное параметром count;

-l length посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;
-i ttl устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);
-v tos устанавливает тип поля «сервис» в величину tos;
-r count записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;
-s count позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;
-j host-list направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;
-k host-list направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;
-w timeout указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);
destination-list указывает IP-адрес или имя удаленного хоста, к которому надо направить пакеты ping.

Пример использования утилиты ping.

```
C:\WINDOWS>ping –n 10 www.netscape.com
Обмен пакетами с www.netscape.com [205.188.247.65] по 32 байт:
    Ответ от 205.188.247.65: число байт=32 время=194мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=240мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=173мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=250мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=187мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=239мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=263мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=230мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=185мс TTL=48
    Ответ от 205.188.247.65: число байт=32 время=406мс TTL=48
    Статистика Ping для 205.188.247.65:
    Пакетов: послано = 10, получено = 10, потеряно = 0 (0% потерь)
    Приблизительное время передачи и приема:
    Наименьшее = 173мс, наибольшее = 406мс, среднее =236мс
```

Утилита ping, а также утилиты Tracert и PathPing, используют **протокол сетевого уровня ICMP (Internet Control Message Protocol) – Протокол межсетевых управляющих сообщений и сообщений об ошибках.** Посылаемые и получаемые IP-пакеты – это эхо-запросы и эхо-ответы протокола ICMP.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли

фрагментировать пакет и т. д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

По умолчанию протокол ICMP блокируется брандмауэром Windows Vista и Windows Server 2008, а также некоторыми маршрутизаторами и функционально независимыми брандмауэрами. Соответственно, для устранения неполадок сетевых подключений нужно отменить блокирование ICMP удаленным узлом. Для этого в Центре управления сетями и общим доступом (Network And Sharing Center) необходимо включить Общий доступ к файлам (File Sharing).

5. Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert - это утилита трассировки маршрута. Она позволяет проследить путь от данного узла до любого другого узла сети Internet. Хост за хостом показывается прохождение IP-пакетов, при этом выводится название и IP-адрес каждого пройденного хота, а также значение интервала времени, в течение которого был получен ответ.

Утилита использует поле TTL (time-to-live, время жизни) из заголовка IP-пакета и сообщения об ошибках протокола ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут исследуется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

ПРИМЕЧАНИЕ: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops указывает максимальное число хопов для того, чтобы искать цель;

-j host-list указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

6. Определение потерь данных с помощью утилиты PathPing.

Эта утилита аналогична утилите Tracert, за исключением того, что PathPing предназначена для определения потерь данных на промежуточных узлах. Утилита PathPing отправляет пакеты на каждый маршрутизатор на пути к конечной точке и вычисляет процентное соотношение пакетов, возвращаемых в каждом прыжке. Поскольку утилита PathPing показывает степень потери пакетов на каждом маршрутизаторе или узле, с ее помощью можно точно определить маршрутизаторы и узлы, на которых возникают сетевые проблемы.

Для определения потерь данных в командную строку надо ввести команду PathPing и указать имя или адрес конечного компьютера, сервера или маршрутизатора, путь к которому необходимо отследить.

7. Утилита arp.

ARP – это имя утилиты и протокола.

Основная задача протокола разрешения адресов ARP (Address Resolution Protocol) – трансляция IPv4-адресов в соответствующий MAC-адрес (аппаратный, локальный) сетевого интерфейса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилиту arp можно использовать для отображения и редактирования ARP-кэша компьютера и для определения MAC-адресов узлов подсети.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

Например, отобразив кэш с помощью команды arp -a, можно обнаружить проблему, связанную с тем, что соседние виртуальные машины назначили себе один и тот же виртуальный MAC-адрес (довольно распространенная ситуация).

С помощью команды arp /-d можно удалить запись в ARP-кэше компьютера или виртуальной машины с недействительным MAC-адресом.

В редких случаях с помощью утилиты Arp можно определить попытки локального хакера связать в ARP-кэше локальные IPv4-адреса с MAC-адресом самого хакера. Эта

технология позволяет хакеру тайно выполнять маршрутизацию сетевых подключений через свой компьютер.

ПРИМЕЧАНИЕ 1. Каждый IPv4-адрес в ARP-кэше должен быть связан с уникальным физическим адресом.

ПРИМЕЧАНИЕ 2. Для разрешения преобразований IP в MAC в версии IPv6 используется протокол ND (Neighbor Discovery), а не протокол ARP, применяемый в IPv4. Потому у всех сетей IPv6 есть преимущество - невозможность инфицирования ARP-кэша.

8. Утилита netstat.

Утилита netstat производит отображение активных подключений TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6). Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера. Если порт содержится в перечне файла services из каталога <Windir>\system32\drivers\etc, то утилита netstat вместо номера порта отобразит имя протокола;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n выводит информацию по всем активным соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r выводит содержимое таблицы маршрутизации.

9. Утилита route

Утилита route предназначена для просмотра и редактирования таблицы маршрутизации (добавление маршрута, удаление маршрута, редактирование маршрута). Вывод таблицы маршрутизации на экран:

route print

10. Команды сетевых служб net view и net use.

Ресурс, к которому разрешён доступ с других компьютеров сети, называется **общим**. Совместно использовать можно практически все сетевые ресурсы: файлы, папки, жесткие диски, принтеры, приложения, физически находящиеся на различных узлах. Для реализации этого преимущества с компьютера, на котором установлен ресурс, необходимо разрешить к нему доступ, а на компьютере-клиенте необходимо подключить этот ресурс. Нельзя выделить в общий доступ отдельный файл. Необходимо поместить этот файл в общую папку, чтобы он стал доступен с других узлов сети.

Для просмотра удалённых компьютеров и доступных на них ресурсов в командной строке используется команда NET VIEW. Например, следующая команда показывает символьные имена всех доступных в данный момент компьютеров локальной сети или домена

> NET VIEW

Для отображения всех доступных ресурсов компьютера с именем, например PC1, используется команда

> NET VIEW \\PC1

Для подключения ресурсов через командную строку используется команда

>NET USE ДИСК: \\ ИМЯ_КОМПЬЮТЕРА\ РЕСУРС

где ДИСК – буква диска, к которой подключается удалённый ресурс,

ИМЯ_КОМПЬЮТЕРА – имя удалённого компьютера (либо символьное, либо IP-адрес),

РЕСУРС – подключаемый ресурс удалённого компьютера.

Например, следующая команда позволит подключить ресурс Inform сервера Serv1 (рисунок 1), используя букву диска H

>NET USE H: \\Serv1\Inform

Следующая команда отображает все подключенные к данному компьютеру удалённые ресурсы.

> NET USE

Отключение подключенного ранее ресурса производится при помощи команды

> NET USE ДИСК: /D

Подключение сетевого принтера производится аналогичным образом, только вместо буквы диска пишется порт (например, LPT1):

>NET USE LPT1 \\ ИМЯ_КОМПЬЮТЕРА\ ИМЯ_ПРИНТЕРА

Порядок выполнения работы

Упражнение 1. Получение справочной информации по командам TCP/IP, командам ОС MS Windows, сетевым командам

1. Вывести на экран справочную информацию по утилитам TCP/IP. Для этого в командной строке ввести имя утилиты без параметров или с /?. Изучить ключи, используемые при запуске утилит.

Например: ipconfig /? (выводит справочную информацию по команде ipconfig)

2. Вывести на экран справочную информацию по командам ОС MS Windows. Для этого используется: help [команда].

Например: help dir (выводит справочную информацию по команде dir)

help (выводит перечень команд MS Windows)

3. Вывести на экран справочную информацию по командам сетевых служб. Для этого используется: net help [имя команды].

Например: net help use (выводит справочную информацию по команде net use)

net help (выводит перечень команд сетевых служб и правила получения справки по ним)

Упражнение 2. Сбор информации о системе

С помощью команды ОС MS Windows systeminfo вывести на экран справочную информацию о системе.

Упражнение 3. Получение имени хоста

Вывести на экран имя локального хоста с помощью команды hostname.

Упражнение 4. Получение MAC-адресов сетевых адаптеров

Вывести на экран MAC-адреса сетевых адаптеров с помощью утилиты getmac.

Упражнение 5. Чтение результатов ipconfig

Изучить конфигурацию TCP/IP локального хоста с помощью утилиты ipconfig. Использовать утилиту без параметров и с параметром /all

1. Определить символьное имя узла.
2. Сколько физических сетевых интерфейсов у данного узла? Перечислите их. Укажите их адреса.
3. Сколько программных сетевых интерфейсов назначено узлу? Перечислите их. (* возле подключения по локальной сети означает, что это туннельный интерфейс)
4. Сколько IPv4 и IPv6-адресов назначено узлу? Перечислите их. Укажите для каждого IP-адреса основные настройки TCP/IP – маску и адрес шлюза по умолчанию.

Упражнение 6. Тестирование связи с помощью утилиты ping

1. Проверить правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверить, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
3. Проверить функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.
4. Проверить с помощью ping, можно ли обратиться к компьютерам в своей локальной сети по имени компьютера, по IPv4-адресу, по IPv6-адресу (указав идентификатор зоны %n своей машины).
5. Указать в ping адрес компьютера, который отключен, несуществующий адрес. Сравнить полученные результаты?
6. Проверить возможность установления соединения с различными удаленными хостами, используя DNS-имена. Определить IP-адреса этих узлов. Отметить время отклика (время кругового обращения пакета). Попробовать увеличить время отклика. Как влияет размер пакета на время кругового обращения?

Упражнение 7. Определение пути IP-пакета

1. Воспользоваться командой tracert для определения числа участков маршрута от вашего компьютера к различным хостам (локальному хосту, шлюзу по умолчанию, удаленному хосту). Отметьте, через какие промежуточные узлы проходят эхо-пакеты.
2. Сравнить значения времени кругового обращения, полученные при выполнении программы ping, с числом участков маршрута, полученным при выполнении программы tracert, для ряда адресов назначения. Существует ли зависимость между продолжительностью задержки и числом участков маршрута?

Упражнение 8. Утилита PathPing

Используя утилиту PathPing, определить потери данных на промежуточных узлах при тестировании маршрута к различным хостам. Прокомментировать полученные результаты.

Упражнение 9. Утилита arp

С помощью утилиты arp просмотреть ARP-таблицу локального узла. Какая информация в ней хранится? Для чего она нужна?

Упражнение 10. Просмотр файлов конфигурации

Просмотреть содержимое файлов конфигурации hosts, lmhosts, protocol, services.

Упражнение 11. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP

1) С помощью утилиты netstat вывести на экран перечень сетевых соединений и используемых в данный момент портов локального узла. Просмотреть информацию о состоянии соединения. Выяснить, находится ли соединение в состоянии прослушивания или уже установлено.

2) Получить статистическую информацию для протоколов UDP, TCP, ICMP, IP.

3) Вывести на экран локальную таблицу маршрутизации. Изучить ее содержимое.

Упражнение 12. Просмотр списка компьютеров домена или сети. Просмотр списка общих ресурсов данного компьютера.

1) Просмотреть через командную строку список всех доступных компьютеров в локальной сети.

2) Просмотреть через командную строку список всех доступных ресурсов сервера.

3) Подключить ресурс сервера (папку) к локальному узлу в качестве сетевого диска.

4) Просмотреть через командную строку список всех подключенных к данному компьютеру ресурсов.

5) Отключить все подключенные ранее ресурсы.

Контрольные вопросы

1. Дайте определение компьютерной сети. Из каких компонентов состоит компьютерная сеть? Что такое хост?
2. Как определить имя компьютера?
3. Как определить, сколько у данного компьютера физических сетевых интерфейсов, виртуальных сетевых интерфейсов? Как определить физический адрес компьютера?
4. Как узнать, в какое количество подсетей в данный момент подключен компьютер?
5. Каким образом команда ping проверяет сетевые соединения? Какой протокол использует утилита ping? Отметьте возможные причины, по которым ping не может связаться с удаленным хостом.
6. Если утилита ping с IP-адресом выполнилась успешно, а с именем хоста неудачно, что это означает?
7. Что такое «петля обратной связи»?
8. Для чего предназначена и как работает утилита tracert? Чем отличается использование утилит tracert и PathPing?
9. Каково назначение протокола ARP? Что такое ARP-кэш? Для чего используется утилита arp?
10. Как просмотреть перечень всех используемых в данный момент портов?
11. Как просмотреть список компьютеров домена или сети?
12. Что такое общий ресурс? Как просмотреть список общих ресурсов данного компьютера? Какие ресурсы можно выделить в общий доступ?