Лабораторная работа №8
Тема: «Использование диагностических утилит протокола TCP/IP»

Цель работы: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Целью устранения неисправностей в настройке TCP/IP является восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения

Практическое задание

Задание 1. Получение справочной информации по командам.

1. Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу п.1). Для этого в командной строке (значок Windows + R, затем ввести cmd, затем Enter) введите имя утилиты без параметров и дополните **/?**

arp	*Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)*
hostname	*Выводит имя локального хоста. Используется без параметров.*
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)*
nbtstat	*Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.*
netstat	*Выводит статистику и текущую информацию по соединению TCP/IP.*
nslookup	*Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.*
ping	*Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.*
route	*Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.*
tracert	*Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.*

2. Сохраните справочную информацию в отдельном файле.
3. Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

1. Выведите на экран имя локального хоста с помощью команды hostname.
2. Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

1. Проверьте конфигурацию TCP/IP с помощью утилиты ***ipconfig***. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование 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, посылая к этому хосту несколько IP-пакетов 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, то может служить субъективной оценкой «качества связи» между узлами. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

Утилита использует протокол ICMP. 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.

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.

4.1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.

4.2. Проверьте возможность установления соединения с удаленным хостом.

4.3. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика.

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

Если тест успешно пройден, то вы получите следующий ответ:

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, 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 локальным 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 удаленного хоста:

ping IP-адрес_удаленного 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 удаленный хост, к которому надо направить пакеты ping.

Пример использования утилиты ping.

C:\WINDOWS>ping –n 10
Обмен пакетами с [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

Задание 5. Определение пути IP-пакета.

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).

С помощью команды **tracert** проверьте для адреса yarus.aspu.ru, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

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.

Задание 6. Просмотр ARP-кэша.

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса. 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.

6.1. С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.
6.2. Внести в кэш локального компьютера любую статическую запись.
Утилита arp выводит для просмотра и изменения таблицу трансляции адресов.

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.
Задание 7. Просмотр локальной таблицы маршрутизации.
С помощью утилиты route просмотреть локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.
Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.
С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.
Синтаксис:
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]
Параметры:
-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;
-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.

Контрольные вопросы
1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут,
маска сети, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности
конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным
хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert?
(превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни
при передаче пакета).

Содержание отчета
1. Наименование и цель лабораторной работы
2. Таблицу с полученными результатами задания 3.
3. Скриншоты выполнения лабораторной работы.
4. Выводы по лабораторной работе.
5. Ответы на контрольные вопросы.