**Практическая работа №5 Работа с диагностическими утилитами протокола**

### ТСР/IР

**Цель работы:** обобщение и систематизация знаний по теме «Межсетевое взаимо- действие»

### ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

#### Диагностические утилиты TCP/IP

В состав TCP/IP входят диагностические утилиты, предназначенные для провер- ки конфигурации стека и тестирования сетевого соединения.

|  |  |
| --- | --- |
| **Утилита:** | **Применение:** |
| arp | Выводит для просмотра и изменения таблицу трансляции адресов, ис- пользуемую 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, установ- ленному поверх TCP/IP. Используется для проверки состояния теку- щих соединений NetBIOS. |
| netstat | Выводит статистику и текущую информацию по соединению TCP/IP. |
| nslookup | Осуществляет проверку записей и доменных псевдонимов хостов, до- менных 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 ком- пьютер. |

#### Проверка правильности конфигурации TCP/IP

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

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая кон- фигурация 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 сете- вого 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 кон- фигурация 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 .

#### Тестирование связи с использованием утилиты ping

Утилита ping (Packet Internet Grouper) используется для проверки конфигуриро- вания TCP/IP и диагностики ошибок соединения. Она определяет доступность и функ- ционирование конкретного хоста. 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 путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый послан- ный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая после- довательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использу- ет, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать па- кет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекун- дах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как зна- чение 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 откли- ка, 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 – неудач- но, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Использование утилиты ping:

− 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

− 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*

− Чтобы проверить, что шлюз по умолчанию функционирует и что можно уста- новить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

*ping IP-адрес\_шлюза*

− Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

*ping IP-адрес\_удаленного хоста*

*list] |*

Синтаксис утилиты ping:

*ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [ [-j host-*

*[-k host-list] ] [-w timeout] destination-list*

Параметры:

*-t* - выполняет команду ping до прерывания. Control- Break - посмотреть стати- стику 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 пара- метром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хо- стов в списке, позволенное IP, равно 9;

*-k host-list* - направляет пакеты через список хостов, определенный в host-list. По- следовательные 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:\Documents and Set-

tings\user>ping [www.ya.ru](http://www.ya.ru/)

Обмен пакетами с ya.ru [213.180.204.8] по 32 байт:

Ответ от 213.180.204.8: число байт=32 время=1887мс TTL=53 Ответ от 213.180.204.8: число байт=32 время=1475мс TTL=53 Ответ от 213.180.204.8: число байт=32 время=1094мс TTL=53 Ответ от 213.180.204.8: число байт=32 время=736мс TTL=53 Статистика Ping для 213.180.204.8:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс:

Минимальное = 736мсек, Максимальное = 1887 мсек, Среднее = 1298 мсек

#### Изучение маршрута между сетевыми соединениями с помощью утилиты tracert

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to- live, время жизни) пакета IP и сообщения об ошибках 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 хо- ста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (\*), либо сообщения типа «Destination net unreacha- ble», «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 жиз- ни. 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 определяется 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 ис- текшим 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 соответ-

ствии с host-list;

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

Пример использования утилиты tracert: C:\Documents and Settings\user>tracert [www.ya.ru](http://www.ya.ru/) Трассировка маршрута к ya.ru

[213.180.204.8]

с максимальным числом прыжков 30:

1 <1 мс <1 мс <1 мс mygateway1.ar7 [192.168.1.1]

2 16 ms 15 ms 23 ms 192.168.229.9

3 16 ms 16 ms 16 ms 192.168.224.46

1. \* \* \* Превышен интервал ожидания для запроса.
2. \* \* \* Превышен интервал ожидания для запроса.

6 24 ms 24 ms 25 ms 18.224.168.192.in-addr.arpa

[192.168.224.18]

7 23 ms 23 ms 23 ms 17.224.168.192.in-addr.arpa

[192.168.224.17]

8 2542 ms 2577 ms 2928 ms

18.13.22.172.in-addr.arpa [172.22.13.18]

9 2189 ms 1811 ms 2016 ms

225.126.18.84.in-addr.arpa [84.18.126.225]

10 2354 ms 2193 ms 1653 ms

87.226.230.253

11 1442 ms 1361 ms 1105 ms

87.226.133.38

12 56 ms 55 ms68 ms 87.226.233.198

13 1715 ms 2206 ms 2579 ms [www.ya.ru](http://www.ya.ru/)

[213.180.204.8]

Трассировка завершена

#### Утилита ARP

Основная задача протокола ARP –трансляция IP-адресов в соответствующие ло- кальные адреса (MAC-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 запи- сей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения ши- роковещательных запросов. Для них существует понятие времени жизни. Если в тече- ние определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Синтаксис: адреса;

*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-

*-a* - просмотр содержимого кэша для всех сетевых адаптеров локального компьютера; *inet\_addr* - IP-адрес;

*eth\_addr -* MAC-адрес.

Пример использования утилиты ARP: C:\Documents and Set- tings\user>arp -a 169.254.15.2 Интерфейс: 169.254.15.1 --- 0x2

Адрес IP Физический адрес Тип 169.254.15.2 00-19-5b-82-fb- d0 динамический

#### Утилита netstat

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.

Синтаксис:

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

Параметры:

*-a* - выводит перечень всех сетевых соединений и прослушивающихся портов ло- кального компьютера;

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

*-n* - выводит информацию по всем текущим 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.

### ПРАКТИЧЕСКАЯ ЧАСТЬ

**Задание 1.** Получение справочной информации по командам

− Выведите на экран справочную информацию по утилитам *ipconfig*, *ping*, *tracert*, *hostname*. Для этого в командной строке введите имя утилиты без параметров или с /?.

− Изучите ключи, используемые при запуске утилит.

**Получение имеени хоста**

− Выведите на экран имя локального хоста с помощью команды *hostname*.

#### Изучение утилиты ipconfig

|  |  |  |  |
| --- | --- | --- | --- |
| − Проверьте конфигурацию TCP/IP с помощью утилиты *ipconfig*. Заполните таб-  лицу: | | | |
|  | 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 |  |
| **Тестирование связи с помощью утилиты ping**  − Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.  − Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублиру- ется ли IP-адрес. | | | |

− Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.

− Проверьте возможность установления соединения с удаленным хостом (например [www.yandex.ru](http://www.yandex.ru/))

**Определение пути IP-пакета**

− С помощью команды *tracert* проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их:

192.168.0.1:

10.70.0.3:

10.70.1.1:

[www.ineka.ru](http://www.ineka.ru/)

#### Просмотр ARP-кэша

− С помощью утилиты *arp* просмотрите ARP-таблицу локального компьютера.

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

− С помощью утилиты *netstat* выведите перечень сетевых соединений и стати- стическую информацию для протоколов UDP, TCP, ICMP, IP.