|  |
| --- |
| *Министерство образование и науки*  *Российской федерации*  Федеральное агентство по образованию  Курганский государственный университет |
| Кафедра «Безопасность информационных и автоматизированных систем» |
| Лабораторная работа № 1:  **«СЕТЕВЫЕ УТИЛИТЫ OC wINDOWS»** |
| Выполнил \_\_\_\_ Бутенко А.Ю.  Принял \_\_\_\_\_\_ Дубровских В.А. |
|  |
| Курган 2016 |

Цель работы:

* ознакомиться с утилитами ос windows предназначенными для работы с сетью;
* научится применять утилиты для решения проблем возникающих при настройке сетевого оборудования.

**Ход работы:**

**ARP**

- разрешение адресов по протоколу ARP выполняется только при операциях передачи данных по протоколу IP .   
- время жизни записей в таблице ARP ограничено, поэтому, перед просмотром ее содержимого для конкретного адреса нужно выполнить ping на этот адрес.  
- если ответ на ping не приходит, а запись для данного IP-адреса присутствует в таблице ARP, то этот факт можно интерпретировать как блокировку ICMP-пакетов брандмауэром пингуемого узла.   
- невозможность подключения к удаленному узлу по протоколам TCP или UDP при наличии записей в таблице ARP для целевого IP, может служить признаком отсутствия служб обрабатывающих входящие подключения, или их блокировки брандмауэром (закрытые порты).  
- ARP протокол работает в пределах локального сегмента сети. Поэтому, если выполнить ping на внешний узел ( например ping yandex.ru ), то в таблице ARP будет присутствовать запись для IP - адреса маршрутизатора, через который выполняется отправка пакета во внешнюю сеть.

**IPCONFIG**

Утилита командной строки IPCONFIG присутствует во всех версиях Windows. Некоторые параметры командной строки не поддерживаются в версиях предшествующих Windows Vista/Windows 7. Команда IPCONFIG используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).

**GETMAC**

Утилита командной строки GETMAC присутствует в версиях Windows XP и старше. Используется для получения аппаратных адресов сетевых адаптеров (MAC-адресов) как на локальном, так и на удаленном компьютере.

**NBTSTAT**

Команда NBTSTAT позволяет получить статистику протокола NetBIOS over TCP/IP (NetBT), таблицу имен локальных и удаленных компьютеров и содержимое кэш NetBIOS имен. Применение NBTSTAT позволяет принудительно обновить кэш NetBIOS-имен компьютеров и имена, зарегистрированные с помощью серверов Windows Internet Name Service (WINS).

**NETSH**

Утилита сетевой оболочки NETSH (NETwork SHell) - наиболее полное и функциональное стандартное средство управления сетью с использованием командной строки в среде Windows XP и старше. Набор внутренних команд сетевой оболочки пополняется с появлением новых версий операционной системы, что необходимо учитывать при работе в локальной сети с различными ОС. Так, например, команда уровня wlan ( netsh wlan - управление беспроводной сетью) может использоваться на компьютерах под управлением Windows Vista и старше и отсутствует в Widows XP. Синтаксис используемых команд и параметров также может различаться в разных операционных системах семейства Windows.

**NETSTAT**

Утилита netstat.exe присутствует во всех версиях Windows, однако, существуют некоторые отличия используемых параметров командной строки и результатов ее выполнения, в зависимости от операционной системы. Используется для отображения TCP и UDP -соединений, слушаемых портов, таблицы маршрутизации, статистических данных для различных протоколов.

**NET**

Утилита NET.EXE существует во всех версиях Windows и является одной из самых используемых в практической работе с сетевыми ресурсами. Позволяет подключать и отключать сетевые диски, запускать и останавливать системные службы, добавлять и удалять пользователей, управлять совместно используемыми ресурсами, устанавливать системное время, отображать статистические и справочные данные об использовании ресурсов и многое другое.

**NSLOOKUP**

Утилита NSLOOKUP присутствует во всех версиях операционных систем Windows и является классическим средством диагностики сетевых проблем, связанных с разрешением доменных имен в IP-адреса. NSLOOKUP предоставляет пользователю возможность просмотра базы данных DNS-сервера и построения определенные запросов, для поиска нужных ресурсов DNS. Практически, утилита выполняет функции службы DNS-клиент в командной строке Windows.   
  
После запуска, утилита переходит в режим ожидания ввода. Ввод символа ? или команды help позволяет получить подсказку по использованию утилиты.

**PATHPING**

Команда PATHPING выполняет трассировку маршрута к конечному узлу аналогично команде TRACERT , но дополнительно, выполняет отправку ICMP-эхо запросов на промежуточные узлы маршрута для сбора информации о задержках и потерях пакетов на каждом из них.

**PING**

Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений ICMP(Internet Control Message Protocol). Команда ping позволяет выполнить отправку управляющего сообщения типа Echo Request (тип равен 8 и указывается в заголовке сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел дожжен отправить icmp-пакет с теми же данными, которые были приняты, и типом сообщения Echo Reply (код типа в заголовке равен 0) . Если при обмене icmp-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

**ROUTE**

Утилита ROUTE.EXE используется для просмотра и модификации таблицы маршрутов на локальном компьютере. При запуске без параметров, на экран выводится подсказка по использованию route.

**TELNET**

**TRACERT**

Не смотря на появление утилиты PATHPIG, классическая утилита трассировки маршрута до заданного узла TRACERT , по-прежнему остается наиболее часто используемым инструментом сетевой диагностики. Утилита позволяет получить цепочку узлов, через которые проходит IP-пакет, адресованный конечному узлу. В основе трассировки заложен метод анализа ответов при последовательной отправке ICMP-пакетов на указанный адрес с увеличивающимся на 1 полем TTL. ("Время жизни" - Time To Live). На самом деле это поле не имеет отношения к времени, а является счетчиком числа возможных переходов при передаче маршрутизируемого пакета. Каждый маршрутизатор, получив пакет, вычитает из этого поля 1 и проверяет значение счетчика TTL. Если значение стало равным нулю, такой пакет отбрасывается и отправителю посылается ICMP-сообщение о превышении времени жизни ("Time Exceeded" - значение 11 в заголовке ICMP).

**Вывод**:

С утилитами ознакомился. Применять для диагностики проблем связанных с сетью научился.