Лабораторная работа № 1. Основы диагностики сети консольным средствами ОС Windows

1.1 Постановка задачи

Используя стандартные сетевые утилиты, проанализировать конфигурацию сети на платформе ОС Windows, т.е. получить свой IP-адрес, узнать имя рабочей группы, имена компьютеров, входящих в группу, просмотреть и при необходимости подключить общие ресурсы, определить причину возможных неполадок, так же получить информацию об использовании портов и т.д. Выполнить задания, ответить на вопросы и предоставить отчет.

1.2 Краткая теоретическая справка

Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, который дает базу для измерения реакции сети на изменения и перегрузки. Чтобы осуществить сетевую передачу, нужно проверить корректность подключения клиента к сети, наличие у клиента хотя бы одного протокола сервера, знать IP-адрес компьютеров сети и т. д. Поэтому в сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок. Утилиты запускаются из сеанса интерпретатора команд Windows XP (Пуск → Выполнить → cmd).

1.3 Свойства командной строки

Стандартный вид командной строки представляет собой чёрное окно с белым текстом. Если этот вариант не устраивает пользователя, он может изменить цвета в зависимости от своих предпочтений.

Для этого следует кликнуть правой кнопкой мыши по верхней части окна и перейти к свойствам CMD. В открывающемся окне можно выбрать и расположение строки, и цвета текста или окна, и даже размеры шрифта. Здесь же есть возможность расширить интерфейс практически на весь экран, повысив уровень удобства работы с ним.

Ещё больше упростить использование командной строки помогают горячие клавиши – хотя они и не совпадают с привычными комбинациями Windows. Вместо нажатия стандартных наборов Ctrl + C и Ctrl + V, копирование и вставка текста выполняются следующим образом:

1. Кликнуть по выбранной строке в открытом окне CMD правой кнопкой мыши;
2. Выбрать пункт «Пометить»;

3. Выделить текст с помощью левой кнопки;
4. Ещё раз кликнуть правой кнопкой. После этого вся информация оказывается в буфере обмена операционной системы.

Для того чтобы вставить скопированную информацию нажимают ту же правую кнопку и выбирают пункт «Вставить». Упростить копирование данных можно, поставив галочку на пункте «Выделение мышью» в свойствах командной строки.

После этого текст можно сразу выделять левой кнопкой. Если же снять галочку на пункте быстрой вставки, данные вставляются поверх уже написанных команд.

После выполнения нескольких команд окно заполняется текстом, который может оказаться помехой для дальнейшей работы. Избавиться от лишних данных можно с помощью команды CLS (Clear Screen). После её запуска экран полностью очищается, оставляя место для дальнейших действий пользователя.

Все команды выполняющиеся в окне командной строки могут дублироваться с помощью пакетного файла. Пример работы с пакетным файлом:

- Создать текстовый документ;
- Ввести утилиту для выполнения и файл, куда выводить результат. Например, *ipconfig > 1.txt*
- Сохранить текстовый документ с расширением .bat (например, script.bat).
- По двойному нажатию на bat-файл с той же директории создастся текстовый документ 1.txt. Данные в документе находятся в кодировке OEM 866, данный файл можно просмотреть, указав соответствующую кодировку, например, используя утилиту Notepad.

1.4 Сетевые утилиты

1.4.1 Утилита hostname

Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP.

1.4.2 Утилита ipconfig

Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую конфигурацию IP-адресов компьютеров сети. Синтаксис утилиты *ipconfig:*

ipconfig [/all | */renew* [адаптер] | */release* [адаптер]],

где *all* - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда *ipconfig* выводит только IP-адреса, маску подсети и основной шлюз;

/renew [адаптер] – обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol – автоматическая настройка IP-адресов).

/release [адаптер] – очищает текущую конфигурацию DHCP. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты *ipconfig /release,* IP-адрес становится доступен для назначения другому компьютеру.

Запущенная без параметров, команда *ipconfig* выводит полную конфигурацию TCP/IP, включая IP адреса и маску подсети.

1.4.3 Утилита net view

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты *net view:*

*net view [**компьютер* | */domain[:*домен]];

где *компьютер* – задает имя компьютера для просмотра общих ресурсов;

*/domain[:*домен] – задает домен (рабочую группу), для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;

Вызванная без параметров, утилита выводит список компьютеров в текущем домене (рабочей группе).

1.4.4 Утилита ping

Проверяет соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *ping:*

ping [-t] [-a] [-n счетчик] [-l *длина] [-f]* [-i *ttl]* [-v *тип] [-r счетчик]* [*-s число] [[-j список комп] | [-k список комп]] [-w интервал] список назн,*

где *-t* – повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;

-a – разрешает имя компьютера в адрес;

-n счетчик – передается число пакетов ECHO, заданное параметром. По умолчанию – 4;

-l *длина* – отправляются пакеты типа ECHO, содержащие порцию данных заданной длины. По умолчанию – 32 байта, максимум – 65500;

-f – отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;

-i *ttl* – устанавливает время жизни пакетов TTL (Time To Live);

-*s число* – задает число ретрансляций на маршруте, где делается отметка времени;

-*j список комп* – направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;

-*k список комп* – направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;

-*список назн* – указывает список компьютеров, которым направляются запросы;

1.4.5 Утилита netstat

Выводит статистику протокола и текущих подключений сети TCP/IP. Синтаксис утилиты *netstat:*

netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал],

где -*a* – выводит все подключения и сетевые порты. Подключения сервера обычно не выводятся;

-*e* – выводит статистику Ethernet. Возможна комбинация с ключом -*s;*

-*n* – выводит адреса и номера портов в шестнадцатеричном формате (а не имена);

s – выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (Internet Control Message Protocol) и IP. Ключ -*p* может быть использован для указания подмножества стандартных протоколов;

-*p протокол* – выводит соединения для протокола, заданного параметром. Параметр может иметь значения *tcp* или *udp.* Если используется

с ключом -*s* для вывода статистики по отдельным протоколам, то параметр может принимать значения *tcp, udp, icmp* или *ip; -r* – выводит таблицу маршрутизации;

интервал – обновляет выведенную статистику с заданным в секундах интервалом. Нажатие клавиш CTRL+C останавливает обновление статистики. Если этот параметр пропущен, *netstat* выводит сведения о текущей конфигурации один раз.

1.4.6 Утилита tracert

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью посылки эхо-пакетов протокола ICMP с различными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета. Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе–источнику сообщение ICMP «Time Exceeded». Утилита *tracert* определяет маршрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное допустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «Time Exceeded», полученных от промежуточных маршрутизаторов. Однако, некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты *tracert.* Синтаксис утилиты *tracert:*

tracert [-d] [-h макс_узл] [-j список компьютеров] [-w интервал] точка назн,

где - *d* – отменяет разрешение имен компьютеров в их адреса;

-*h макс_узл* – задает максимальное количество ретрансляций, используемых при поиске точки назначения;

-*j список компьютеров* – задает список_компьютеров для свободной маршрутизации;

-*w интервал* – задает интервал в миллисекундах, в течение которого будет ожидаться ответ;

точка назн – указывает имя конечного хоста.

1.4.7 Утилита net use

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты *net use:*

net use [устройство | *] [\\компьютер\ресурс[\том]] [пароль* | *]] [/user:[домен\]имя пользователя] [[/delete]* | *[/persistent:{yes* | *no}]] net use устройство [/home[пароль* | *]] [/delete: {yes* | *no}] net use [/persistent:{yes* | *no}],*

где *устройство* – задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

компьютер\ *ресурс* – указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" ").

пароль – задает пароль, необходимый для подключения к общему ресурсу;

* – выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;

/user – задает другое имя пользователя для подключения к общему ресурсу;

домен – задает имя другого домена. Если домен не указан, используется текущий домен;

имя пользователя – указывает имя пользователя для подключения; */delete* – отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения; */home* – подключает пользователя к его основному каталогу; */persistent* – управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными;

yes – сохраняет все существующие соединения и восстанавливает их при следующем подключении;

no – не сохраняет выполняемые и последующие подключения. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ */delete.*

Вызванная без параметров утилита *net use* извлекает список сетевых подключений.

1.4.8 Утилита ARP

Команда *ARP* позволяет просматривать и изменять записи в кэш ARP (Address Resolution Protocol – протокол разрешения адресов), который представляет собой таблицу соответствия IP-адресов аппаратным адресам сетевых устройств.

Аппаратный адрес - это уникальный, присвоенный при изготовлении, 6-байтный адрес сетевого устройства, например, сетевой карты. Этот адрес также часто называют MAC-адресом (Media Access Control – управление доступом к среде) или Ethernet-адресом.

Отображение IP-адресов (формируемых программным путем), в аппаратные адреса, выполняется с помощью следующих действий:

- в сеть отправляется широковещательный запрос (ARP-request), принимаемый всеми сетевыми устройствами. Он содержит IP и Ethernet адреса отправителя, а также, целевой IP-адрес, для которого выполняется определение MAC-адреса.
- каждое устройство, принявшее запрос проверяет соответствие целевого IP-адреса, указанного в запросе, своему собственному IP-адресу. При совпадении, отправителю передается ARP-ответ (ARP-Reply), в котором содержатся IP и MAC адреса ответившего узла. Кадр с ARP-ответом содержит IP и MAC адреса как отправителя, так и получателя-составителя запроса.
- информация, полученная в ARP-ответе, заносится в ARP-кэш и может использоваться для обмена данными по IP-протоколу для данного узла. ARP-кэш представляет собой таблицу в оперативной памяти, каждая запись в которой содержит IP, MAC и возраст их разрешения. Возраст записи учитывается для того, чтобы обеспечить возможность повторного выполнения процедуры ARP при каком-либо изменении соответствия адресов.

Синтаксис *ARP*:

arp[-a [InetAddr] [-NIfaceAddr]] [-g [InetAddr] [-NIfaceAddr]] [-dInetAddr [IfaceAddr]] [-sInetAddr EtherAddr [IfaceAddr]]

где *a* – отображает текущую таблицу ARP для всех интерфейсов. Для отображения записи конкретного IP-адреса используется ключ -a с параметром InetAdd, в качестве которого указывается IP-адрес.

g[InetAddr] [-NIfaceAddr] ключ -g идентичен ключу -a.

d InetAddr [IfaceAddr] - используется для удаления записей из ARP-кэш. Возможно удаление по выбранному IP или полная очистка ARP

кэш. Для удаления всех записей, вместо адреса используется символ * Если имеется несколько сетевых интерфейсов, то очистку можно выполнить для одного из них, указав в поле IfaceAddr его IP.

s InetAddr EtherAddr [IfaceAddr] - используется для добавления статических записей в таблицу ARP. Статические записи хранятся в ARP-кэш постоянно. Обычно, добавление статических записей используется для сетевых устройств, не поддерживающих протокол ARP или не имеющих возможности ответить на ARP- запрос.

/? - получение справки по использованию arp.exe. Аналогично - запуск arp.exe без параметров.

1.4.9 Анализатор протоколов Wireshark

Wireshark – программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.

Это приложение, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Окно Wireshark включает в себя 3 области просмотра с различными уровнями детализации. Область 1 содержит список всех захваченных кадров, организованный в виде таблицы с заголовками. Если выделить строку, то более подробная информация о кадре и ее расшифровка будут отображены в области 2. Область 3 содержит код кадра в шестнадцатеричном или текстовом представлении. Чтобы начать перехват трафика, необходимо выбрать правильный сетевой интерфейс, с которого будет выполняться перехват. В данном случае это будет проводное подключение по локальной сети.

1.5 Задания и вопросы для выполнения лабораторной работы 1

1. Самостоятельно освоить на практике сетевые утилиты с разными параметрами. Предварительная настройка:

1. Установить цвет фона командной строки на белый;
2. Сохранить полную диагностическую информацию о подключении в текстовый файл (при помощи bat-файла).

2. Выполнить задания (при выполнении заданий использовать только консольные утилиты):

1. Получить имя своего компьютера;
2. Вывести список доступных сетевых подключений своего компьютера;

3. Спросив у соседа символьное имя компьютера, просмотреть общие с ним ресурсы;
4. Запустить на ПК анализатор протоколов Wireshark. Получив символьное имя соседа пропинговать его. Количество пакетов – номер компьютера; сначала с минимальным размером пакета, затем с максимально возможным, запустить бесконечный ping;
5. Используя IP-адрес полученный в предыдущем пункте, проверить подключение к нему, используя число ретрансляций на маршруте, где делается отметка времени, равное количеству его общих сетевых ресурсов;
6. Просмотреть список всех сетевых портов на вашем компьютере и сосчитать количество открытых (прослушиваемых);
7. Определить маршрут до сайта (сайт выбрать самостоятельно), указав максимальное число прыжков, равное значению, полученному в предыдущем пункте + номер компьютера. Дальнейшая информация в анализаторе протоколов Wireshark. Посмотреть, как меняется параметр TTL у протокола ICMP при трассировке. Запустить ping, посмотреть, что происходит с TTL у протокола ICMP при ping.
8. Очистите текущую конфигурацию DHCP, затем обновите (Посмотрите в Wireshark, какие сообщения там есть и что они означают);
9. Отобразите все записи таблицы ARP;
10. Добавьте в таблицу ARP статическую запись, задающую соответствие IP-адреса 192.168.0.1 и MAC-адреса 00-22-33-44-55-X (где X – номер компьютера);
11. Полностью очистить таблицу ARP.

3. Ответьте на вопросы (ответить дома, используя интернет и голову):

3.1. Какой протокол необходим для работы с утилитой ping? Найти описание и характеристики протокола.
3.2. Что такое localhost?
3.3. Найти самостоятельно любую стандартную сетевую утилиту Windows (из тех, что не описаны в лабораторной работе).
3.4. Что такое TTL? Изменение параметра TTL при трассировке и ping. Какие протоколы фигурируют в обоих утилитах?
3.5. Определить всем встречающимся в лабораторной работе протоколам уровни модели OSI.
3.6. Почитайте про число ретрансляций. Зачем оно, что означает и в каком формате записывается

В конце лабораторной работы поменять параметры окна командной строки на исходные.

В отчете предоставить результаты выполнения **всех** заданий и ответы на вопросы, отчет оформлять согласно **СТО**.