

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. Сетевые утилиты

Утилита hostname

Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды *hostname*:

```
C:\Documents and Settings\Администратор>hostname
```

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). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров;

/release [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров. 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.

Пример использования *ipconfig* без параметров:

C:\Documents and Settings\Администратор>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

```
DNS-суффикс этого подключения . . . :
IP-адрес . . . . . : 10.10.11.70
Маска подсети . . . . . : 255.255.252.0
Основной шлюз . . . . . : 10.10.10.1
```

Утилита *net view*

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

net view [\\компьютер /domain[:домен]]; *net view /network:nw [\\компьютер]* - используется в сетях Novell NetWare,

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;

/network:nw - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети NetWare. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.

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

с параметром *\\компьютер*:

```
C:\Documents and Settings\Администратор>net view \\- /Domain:Lab-261
Общие ресурсы на \\-
```

Имя общего ресурса	Тип	Используется как	Комментарий

NONE (H)	Диск		

Команда выполнена успешно.

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 мин] [-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); *-v tun* - устанавливает тип службы (Type Of Service) пакетов; *-r счетчик* - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;

-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;

Пример использования утилиты *ping* с параметром *список назн*:

```
C:\Documents and Settings\Администратор>ping 10.10.10.1
```

Обмен пакетами с 10.10.10.1 по 32 байт:

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128

Статистика Ping для 10.10.10.1:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),

Приблизительное время приема-передачи в мс:

Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

Утилита netstat

Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола 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.

Утилита tracert

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью послышки 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 послышки 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_узел] [-j список компьютеров] [-w интервал] точка назн,
 где *-d* - отменяет разрешение имен компьютеров в их адреса;

-h макс_узел - 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 компьютера.

Пример использования утилиты *tracert*:

```
C:\Documents and Settings\Администратор>tracert 10.10.10.1
```

Трассировка маршрута к 10.10.10.1 с максимальным числом прыжков 30

```
1  <1 мс  <1 мс  <1 мс  10.10.10.1
```

Трассировка завершена.

Команда telnet

Команда *telnet* предназначена для соединения с другим хостом по протоколу TELNET. Приведенные ниже примеры использования *telnet* относятся к проверке работоспособности почтовых ящиков и возможности соединения с почтовым сервером по протоколам POP3 и SMTP.

Для того, чтобы выполнить команду *telnet*, надо:

Войти в командную строку".

Набрать имя программы *telnet*, имя хоста и номер порта:

```
telnet mail.ИМЯ_ДОМЕНА 110
```

```
или telnet mail.ИМЯ_ДОМЕНА 25,
```

где ИМЯ_ДОМЕНА - имя Вашего домена, например, domain.ru

Пример 1. Доступ к почтовому серверу по протоколу POP3 (проверка работоспособности почтового ящика)

Введите:

```
C:\> telnet mail.ИМЯ_ДОМЕНА 110
```

Ответ сервера:

+OK

В качестве имени пользователя введите свой адрес электронной почты:

```
user test@domain.ru
```

Ответ сервера:

+OK

Введите пароль для этого почтового ящика:

pass пароль

Ответ сервера:

+OK

Для выхода введите:

quit

+OK

Connection closed by foreign host.

Пример 2. Проверка доступа к smtp-серверу

Введите:

telnet mail.ИМЯ_ДОМЕНА 25

Если в результате Вы получите сообщение, начинающееся с цифры 2, то у Вас есть доступ к smtp-серверу, в противном случае можно судить об ошибке. Возможно у Вашего провайдера закрыт 25 порт, тогда стоит проверить 10025 порт. Если он открыт, тогда стоит для отправки почты использовать его.

Команда nslookup

Команда nslookup предназначена для поиска информации на DNS сервере.

По умолчанию, nslookup ищет на тех серверах, которые указаны в настройках сети компьютера.

Пример:

C:\>nslookup

*** Can't find server name for address 10.5.150.1: Non-existent domain DNS request timed out.
timeout was 2 seconds.

*** Can't find server name for address 62.33.11.252: Timed out

Default Server: ns2.flex.ru

Address: 80.252.130.254

> mail.ru

Server: ns2.flex.ru

Address: 80.252.130.254

Non-authoritative answer:

Name: mail.ru

Addresses: 194.67.57.20, 194.67.57.26, 194.67.57.126, 194.67.57.226

> exit

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 (" "). Имя компьютера может иметь длину от 1 до 15 символов; *том* - задает имя тома системы Novell NetWare. Для подключения к серверам Novell NetWare должна быть запущена служба клиента сети Novell NetWare (для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server);

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.

Пример вызова команды *net use*:

C:\Documents and Settings\Администратор>net use

net share

Управление общими ресурсами. При вызове команды *net share* без параметров выводятся сведения обо всех общих ресурсах локального компьютера.

Синтаксис

```
net share [имя_ресурса] net share [имя_ресурса=диск:путь [{/users:число|unlimited}] [/remark:"текст"] [/cache:
{manual|automatic|no}]] net share [имя_ресурса [{/users:число|unlimited}] [/remark:"текст"] [/cache: {manual|automatic|no}]] net
share [{имя_ресурса|диск:путь} /delete]
```

Параметры

имя_ресурса

Сетевое имя общего ресурса. Команда *net share имя_ресурса* выводит сведения об отдельном ресурсе.

диск:путь

Абсолютный путь к папке, которую требуется сделать общей.

/users:число

Максимальное количество пользователей, которым разрешен одновременный доступ к общему ресурсу.

/unlimited

Отмена ограничения на число пользователей, которым разрешен одновременный доступ к общему ресурсу.

/remark:"текст"

Добавление описательного комментария к ресурсу. Текст следует заключать в кавычки.

/cache:automatic

Включение автономного кэширования клиентов с автоматической реинтеграцией.

/cache>manual

Включение автономного кэширования клиентов с реинтеграцией вручную.

/cache:no

Оповещение клиента о невозможности автономного кэширования.

/delete

Отмена общего доступа к ресурсу.

net help команда

Отображение справки для указанной команды **net**.

Заметки

- Чтобы предоставить общий доступ к папке, имя которой содержит пробелы, заключите диск и путь к папке в кавычки (например "**С:\Новая папка**").
 - При запросе списка всех общих ресурсов компьютера выводятся: имя общего ресурса, имена устройств или путь, связанный с устройством, а также комментарий к этому ресурсу. Вывод будет иметь следующий вид:
- | Общее имя | Ресурс | Заметки |
|-----------|-----------------------|--------------------------|
| ADMIN\$ | C:\WINNT | Удаленный Admin |
| C\$ | C:\ | Стандартный общий ресурс |
| print\$ | C:\WINNT\SYSTEM\SPool | |
| IPC\$ | | Удаленный IPC |
| LASER | LPT1 | Очередь Лазерный принтер |
- Когда общий ресурс создается на сервере, его конфигурация сохраняется. После остановки службы «Сервер» все общие ресурсы отключаются, но после следующего запуска службы «Сервер» они будут восстановлены. Дополнительные сведения о службах содержатся в разделе Службы.
 - Имена общих ресурсов, заканчивающиеся знаком \$, не отображаются при обзоре локального компьютера с удаленного компьютера.

Примеры

Чтобы вывести сведения об общих ресурсах компьютера, введите:

net share

Чтобы сделать папку «С:\Данные» общим ресурсом Данные и включить примечание к нему, введите:

net share ОбщиеДанные=c:\Данные /remark:"Для отдела 123"

Чтобы отменить общий доступ к ресурсу ОбщиеДанные, созданному в предыдущем примере, введите:

net share ОбщиеДанные /delete

Чтобы сделать папку «С:\Список рисунков» общим ресурсом Список, введите:

net share Список="c:\Список рисунков"

1.4. Рекомендации и замечания

На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику локальных сетей. Они позволяют минимизировать усилия по поиску и исправлению ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество программ этого направления: Monitor It, Nautilus NetRanger, CiscoWorks 2000, ServiceSentinel и д.р. Они распространяются через Internet на условиях freeware. Windows NT Server обладает встроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

1.5 Задания и вопросы для выполнения лабораторной работы

1. Самостоятельно освоить на практике сетевые утилиты с разными параметрами;
2. Выполнить задания (при выполнении заданий использовать только консольные утилиты):
 - 2.1. Получить имя своего компьютера;
 - 2.2. Вывести список доступных сетевых ресурсов своего компьютера;
 - 2.3. Спросив у соседа слева имя компьютера, просмотреть его общие ресурсы;
 - 2.4. Получив свой IP адрес, пропинговать его, количество пакетов - номер варианта, сначала с минимальным размером пакета, затем с максимально возможным;
 - 2.5. Используя ранее полученное от соседа слева имя компьютера, определить его IP адрес;
 - 2.6. 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;
 - 2.7. Просмотреть список всех сетевых портов на вашем компьютере и сосчитать количество открытых (прослушиваемых);
 - 2.8. Определить маршрут до сайта по вариантам, с максимальным числом прыжков, равным значению полученному в предыдущем пункте + номер варианта;
 - 2.9. Очистите текущую конфигурацию DHCP, затем обновите;
 - 2.10. Изучив утилиту **netsh**, измените с ее помощью свой IP адрес на статический – 192.168.1.(номер варианта), маска подсети – 255.255.255.0;
 - 2.11. Проверьте подключение к IP адресу из п.2.5;
 - 2.12. Используя **netsh**, верните свой IP адрес на получение по DHCP;
 - 2.13. Сделайте диск D:\ общим сетевым ресурсом, используя в качестве имени Фамилию, а в качестве комментария строку «Моя первая Шара. Вариант + номер варианта»;
 - 2.14. Выведите список общих сетевых ресурсов соседа слева;
 - 2.15. Подключите созданный соседом ресурс в качестве сетевого диска «Z:»;
 - 2.16. Выведите список подключений вашего компьютера;
 - 2.17. Отключите сетевой диск «Z:» ;
3. Ответьте на вопросы:
 - 3.1. Какой протокол необходим для работы с утилитой **ping**? Найти описание и характеристики протокола.
 - 3.2. Можно ли утилитой **tracert** задать максимальное число ретрансляций?
 - 3.3. Какой результат выдаст утилита **netstat** с параметрами **-a -s -r**? Поясните полученный результат.
4. Что такое localhost?
5. Найти самостоятельно любую стандартную сетевую утилиту Windows.
6. В отчете предоставить: ФИО, группу, результаты выполнения всех заданий и ответы на вопросы.