Лабораторна робота № 12.

Укладач: Денищук Павло Миколайович.

Тема. Використання утиліт командного рядка для діагностики мережі.

Мета. Формування вмінь і навиків діагностики локальної мережі за допомогою штатних засобів ОС Windows. Закріплення знань, щодо проведення діагностики мережі, вмінь і навичок використання можливостей штатних утиліт операційної системи Windows.

Теоретична частина

1. Ping

Команда ping вже давно є вірним другом багатьох досвідчених користувачів і мережевих адміністраторів. За допомогою команди ping можна швидко переконатися, що:

• є зв'язок між двома системами

• працює служба перетворення імен DNS

Крім цього, команда ping дозволяє провести додаткові тести над мережевим середовищем між двома системами, що легко помітити з опису синтаксису команди:

ping <ім'я_призначення або адреса_IP> [-a] [-f] [-i <TTL>] [-j <список_узлів>] [-k < список_узлів>] [-l <розмір>] [-n <лічильник>] [-r <лічильник>] [-s <лічильник>] [-t] [-v <TOS>]

Параметри команди ping представлені в наступній таблиці.

Параметр	Використання
<ім'я_призначення або адреса_IP>	Вказує ім'я призначення та адресу IP
-a	Визначення адрес по іменах вузлів
-f	Корисно при з'ясуванні розміру Maximum Transmission Unit (MTU); тестові пакети відправляються з прапором, заборонним фрагментацію пакету IP, що не дає фрагментувати пакети тестових запитів на маршрутизаторах по шляху проходження.
-i <TTL>	Вказує час життя (TTL) тестового запиту; за умовчанням використовується значення 128; цей параметр дозволяє встановити значення до 255, що дозволяє тестового пакету пройти 255 маршрутизаторів і бути віддаленим 256 маршрутизатором.
-j <список_вузлів>	Дозволяє вказати проміжні вузли у вигляді адрес IP, розділених пробілами (список_вузлів). Цей аргумент використовує параметр Loose Source Routing, що дозволяє включати між елементами списку один або кілька маршрутизаторів. Ця команда дозволяє вказати не більше дев'яти вузлів.
-k <список_вузлів>	Дозволяє вказати проміжні вузли у вигляді адрес IP, розділених пробілами (список_вузлів). Цей аргумент використовує параметр Strict Source Routing, що не дозволяє включати між елементами списку один або кілька маршрутизаторів. Ця команда дозволяє вказати не більше дев'яти вузлів.
-l <розмір>	Дозволяє вказати завантаження поля Data пакета в байтах. За замовчуванням використовується значення 32, але можна вказати завантаження до 65527 байт. Це один із способів перевірки наявності обмеженої пропускної здатності або затору в мережі.
-n <лічильник>	Використовується для вказівки кількості тестових запитів, які відправляються командою ping.
-r <лічильник>	Дозволяє вказати кількість (1-9) переходів, які записуються в повідомленнях Echo Request і Echo Reply. Вказане значення повинно бути більшим або рівним кількості маршрутизаторів на маршруті.
-s <лічильник>	Дозволяє вказати кількість переходів (1-4), для яких записує час прибуття запиту і відповіді. Це можливо, коли маршрутизатори підтримують Internet Timestamp для заголовка пакета IP.
-t	Змушує команду ping безперервно відправляти тестові запити, поки виконання команди не буде перервано комбінацією клавіш <Ctrl+C>.
-v <TOS>	Дозволяє вказати значення типу обслуговування (Type of Service - TOS) в заголовку пакета IP, яке буде підставляти команда ping в тестові запити. За замовчуванням використовується значення 0. Можна вказати будь-яке значення з діапазону від 1 до 255.

Ось кілька прикладів типового використання команди ping.

Перевірка перетворення імен та зв'язку для системи www.microsoft.com:

ping www.microsoft.com

Перевірка зв'язку з віддаленим вузлом за адресою IP:

ping 175.55.9.73

Перевірка пропускної здатності мережі за допомогою відправки пакетів розміром 32KB при кожному запиті:

ping 15.39.81.54-l 32768

2. Pathping

Команда (вона ж утиліта) pathping дозволяє виявити певні проблеми, яка виникають при передачі пакетів між двома мережами.

Для перевірки маршрутизаторів між двома точками зв'язку команда pathping відправляє кілька тестових луна-пакетів кожному маршрутизатору і відображає відсоток пакетів, які були втрачені на кожному з маршрутизаторів на протязі маршруту.

Велика кількість втрачених пакетів може вказувати на неправильну настройку маршрутизатора або на затор в сегменті мережі, які можуть бути причиною виникнення проблем в роботі глобальних мереж.

Команда pathping має наступний синтаксис:

pathping <ім'я_призначення або адреса_IP> [-n] [-h <максимальна_кількість_переходів>] [-g <список_вузлів>] [-p <період>] [-q <кількість_запитів>] [-w <timeout>] [-T] [-R]

Далі представлено опис параметрів команди pathping.

Параметр	Використання
<ім'я_призначення або адреса IP>	Вказує ім'я або адресу IP вузла призначення
-n	Прискорює виконання команди за рахунок відмови від перетворення адрес IP в імена
-h <максимальна_кількість_переходів>	Вказує максимальну кількість маршрутизаторів до точки призначення (за замовчуванням 30)
-g <список_вузлів>	Поміщає в заголовки тестових пакетів ICMP параметр Loose Source Router
-p <період>	Дозволяє вказати час у мілісекундах (ms), яке команда буде очікувати між послідовними запитами (за замовчуванням 250). Занадто часті послідовні пакети можуть привести до неточного виявленню заторів у мережі
-q <кількість_запросов>	Дозволяє вказати кількість тестових запитів до кожного маршрутизатора в мережі (за замовчуванням 100)
-w <очікування відповіді>	Дозволяє встановити час (в мілісекундах) очікування відповіді від кожного маршрутизатора (за замовчуванням 3000 мс або 3 с)
-T	Використовується для перевірки наявності Quality of Service (QoS) у вигляді виявлення пристроїв, що не підтримують пріоритети рівня 2
-R	Так само використовується для виявлення QoS; визначає підтримку Resource Reservation Protocol (RSVP) кожним пристроєм на маршруті

Припустимо, є підозри, що в мережі між сайтами Москви і Пітера є проблеми з доставкою пакетів. Можна скористатися командою pathping для перевірки своїх підозр. Для перевірки наявності затору або проблеми на маршрутизаторі уздовж шляху проходження пакета в Москві можна запустити команду:

pathping адрес_сайта

Якщо маршрутизатор має великий відсоток втрачених пакетів, то можна вважати, що джерело проблеми в роботі мережі знайдений.

3. Ipconfig

ipconfig - утиліта командного рядка для управління мережевими інтерфейсами.

В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти з назвами winipcfg і wntipcfg (остання передувала ipconfig). Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурування або задані адміністратором вручну.

Обмеження:

• Якщо ім'я мережевого адаптера містить пробіли, його слід брати в лапки "ім'я адаптера"

• В іменах адаптерів допускається використовувати знак *.

ipconfig про якщо у властивостях мережевого адаптера встановлений протокол TCP / IP.

Доступні ключі командного рядка в Windows:

ключ	опис
/ all	Відображення повної інформації по всім адаптерам.
/ release [адаптер]	Надсилання повідомлення DHCPRELEASE сервера DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Цей ключ відключає протокол TCP / IP для адаптерів, настроєних для автоматичного отримання IP-адрес.
/ renew [адаптер]	Оновлення IP-адреси для певного адаптера або якщо адаптер не заданий, то для всіх. Доступно тільки при налагодженому автоматичному одержанні IP-адрес.
/ flushdns	Очищення DNS кеша.
/ registerdns	Оновлення всіх зарезервованих адрес DHCP та перереєстрація імен DNS.
/ displaydns	Відображення вмісту кеша DNS.
/ showclassid адаптер	Відображення коду класу DHCP для зазначеного адаптера. Доступно тільки при налагодженому автоматичним отриманням IP-адрес.
/ setclassid адаптер [код_класса]	Зміна коду класу DHCP. Доступно тільки при налагодженому автоматичним отриманням IP-адрес.
/?	Довідка.

Приклади виведення для Windows

Друк статусу з'єднання:

C: \> ipconfig / all
Windows 2000 IP Configuration
Host Name. . . . . : wikipedia
Primary DNS Suffix. . . . . :
Node Type. . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : wikipedia.org
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix. : wikipedia.org
Description. . . . . : Intel (R) PRO/100 VE Netwon # 3
Physical Address. . . . . : 00-D0-B7-A6-F1-11
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled. . . . : Yes
IP Address. . . . . : 192.168.0.100
Subnet Mask. . . . . : 255.255.0.0

Default Gateway. . . . . : 192.168.0.3
DHCP Server. . . . . : 192.168.0.1
DNS Servers. . . . . : 192.168.0.1
Primary WINS Server. . . . . : 192.168.0.75
Lease Obtained. . . . . : 27 May 2004 9:04:06
Lease Expires. . . . . : 30 May 2004 9:04:06

Перерезервірованіе і оновлення DHCP:

C: \> ipconfig / release
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 2"
C: \> ipconfig / renew
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix. : wikipedia.org
IP Address. . . . . : 192.168.0.100
Subnet Mask. . . . . : 255.255.0.0
Default Gateway. . . . . : 192.168.0.1
Скидання кеша DNS:
C: \> ipconfig / flushdns
Windows 2000 IP Configuration
Successfully flushed the DNS Resolver Cache.
Реєстрація записів ресурсу DNS
C: \> ipconfig / registerdns
Windows 2000 IP Configuration
Registration of the DNS resource records for all adapters of this computer has been initiated.
Any errors will be reported in the Event Viewer in 15 minutes.

4. Arp

Команда arp створена на основі протоколу Address Resolution Protocol (ARP), який необхідний для функціонування протоколу TCP / IP. Кожен фрагмент апаратного забезпечення, підключений до мережі, має унікальну 48-ми розрядний ідентифікатор Media Access Control (MAC), який зазвичай виражається в шістнадцятковій формі. Протокол ARP використовується для зв'язування адрес MAC мережевих інтерфейсів, наприклад, 00-60-56-50-1B-DE, з відповідними адресами IP, наприклад, 20.0.0.100.

Коли одній системі потрібно зв'язатися із іншою системою в локальній підмережі, вона видає широкомовний запит ARP в локальну підмережу, який містить в собі питання "Гей, який MAC адресу у системи з адресою IP 20.0.0.100?". Як тільки адресу MAC для цієї адреси IP буде отриманий, він записується в системний кеш ARP. Кешування зв'язків адресу IP-MAC адреса дозволяє відмовитися від широкомовного запиту при наступній відправці пакета до цієї системи.

Команда arp може виявитися корисною в ситуації, коли одна система не може зв'язатися з іншою системою в тій же підмережі. Прикладом ситуації, коли в кеші ARP виникають неправильні записи, є ситуація, коли обидва комп'ютера випадково отримують однакову адресу IP. Коли це відбувається комп'ютер кешує неправильний MAC адресу у відповідності з певною адресою IP. Саме в цьому випадку виявляється корисною команда arp. Ось синтаксис цієї команди:

arp-a [адреса IP] [-N <адрес_інтерфейса>]

arp-d <адреса IP> [адрес_інтерфейса]

arp-s <адреса IP> <адресу MAC> [адрес_інтерфейса]

Параметри команди arp розглядаються в наступній таблиці.

Параметр	Використання
-a	Відображає відповідність Адреса IP-Адреса MAC, яке зберігається в локальному кеші ARP
-d	Видаляє запис кешу ARP для вказаної адреси IP
-s	Додає статичну (постійну) запис у Кеш ARP

<адреса IP>	Призводить до відображення інформації тільки для цієї адреси IP
<адрес_інтерфейса>	Для систем з декількома мережевими адаптерами цей параметр використовується для вказівки адреси MAC локального мережного адаптера, для якого виконується команда arp, в іншому випадку команда arp виконується по відношенню до першого ж мережевому адаптеру в порядку прив'язки до мережі
<адрес_MAC>	Використовується для вказівки адреси MAC, для якого створюється статична запис у кеші ARP

Ось деякі приклади використання команди arp в цілях вирішення виникаючих проблем:
• Показати весь вміст кешу ARP на комп'ютері з одним мережевим адаптером: arp-a
• Видалити некоректну запис з кешу ARP: arp-d 10.98.7.205
• Додати статичну запис в кеш ARP: arp-s 10.98.7.205 00-bb-73-51-b8-4c

Хоча утиліта arp є відмінним інструментом, в деяких ситуаціях необхідно отримати адресу MAC віддаленого мережевого інтерфейсу. Саме в цьому випадку стає корисною утиліта getmac, про яку розповідається в наступній статті, посилання на яку представлена нижче.

5. getmac

Утиліта getmac дозволяє визначити адресу MAC віддаленої системи.
Ось синтаксис команди getmac:

getmac [/ s <система> [/ u <ім'я_користувача> [/ p <пароль>]]] [/ fo <формат>] [/ nh] [/ v]

Параметри команди getmac представлені в наступній таблиці.

Параметр	Використання
/ s <система>	Використовується для вказівки імені сайту або адреси IP віддаленої системи, адреси MAC якої необхідно отримати
/ u <ім'я_користувача>	Вказує ім'я користувача домену, від імені якого виконується команда
/ p <пароль>	При використанні параметра / u дозволяє задати пароль користувача
/ fo <формат>	Вказує формат виводу даних. Доступні варіанти: table (за замовчуванням), list або csv
/ nh	Для форматів виводу table і csv пригнічує відображення заголовка стовпця
/ v	Докладний режим - змушує утиліту відображати більш детальну інформацію

6. hostname

Команда hostname надає швидкий спосіб отримати ім'я вузла локальної системи. Ця команда не підтримує віддалене визначення імені.

Команда має простий синтаксис: hostname. Відразу ж після виконання команди, ім'я комп'ютера буде відображено на екрані.

7. nbtstat

Утиліта nbtstat використовується для відображення інформації протоколу NetBIOS over TCP / IP (NetBT) і в основному застосовується при вирішенні проблем, що виникають при наявності в мережі на основі Windows 2000 і більш старих систем.

Починаючи з Windows 2000 протокол NetBT більше не є обов'язковим при використанні протоколу TCP / IP, тому ця утиліта в основному виявляється корисною при роботі з робочими станціями під керуванням Windows NT.

Ось синтаксис команди nbtstat:

nbtstat [-a <ім'я_комп'ютера>] [-A <адреса_IP>] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Інтервал_обновленія]

Параметри команди nbtstat розглядаються далі.

Параметр	Використання
-a <ім'я_комп'ютера>	Використовується для відображення таблиці імен NetBIOS зазначеного віддаленого комп'ютера
-A <адреса_IP>	Використовується для відображення таблиці імен NetBIOS для комп'ютера з вказаною адресою IP
-c	Відображає таблицю кеша NetBIOS
-n	Відображає таблицю імен NetBIOS локального комп'ютера
-r	Використовується для відображення статистики перетворення імен NetBIOS, включаючи перетворення імен, виконані через широкомовні запити і за допомогою сервера WINS.
-R	Очищає вміст кеша NetBIOS. Всі статичні відображення Имя NetBIOS - Адреса IP з файлу LMHosts з префіксами # PRE переносяться в кеш NetBIOS
-RR	Використовується для звільнення імен NetBIOS клієнта на відповідному сервері WINS з наступним оновленням імен NetBIOS за допомогою відповідного сервера WINS. Ця команда виявляється корисною при оновленні сервера WINS, коли адресу IP клієнта змінився
-s	Використовується для відображення таблиці сеансів NetBIOS з перерахуванням віддалених вузлів по іменах NetBIOS
-S	Використовується для відображення таблиці сеансів NetBIOS з перерахуванням віддалених вузлів за адресами IP
період_обновленія	Якщо вказати період оновлення (в секундах), то команда постійно буде оновлювати свій висновок, поки не буде перервана комбінацією клавіш <Ctrl+C>

Зверніть увагу, що багато параметрів командного рядка чутливі до регістра. Будьте уважні і не напишіть-r, коли маєте на увазі-R.

Ось деякі з варіантів використання команди nbtstat при вирішенні проблем з перетворенням імен NetBIOS:

• Для очищення та перереєстрації динамічної реєстрації WINS: nbtstat-RR

• Після зміни адреси IP сервера можна скористатися цією командою, якщо клієнт все ще намагається зв'язатися з сервером за старою адресою IP: nbtstat-R

9. net start stop pause continue

Команди net start, net stop, net pause та net continue використовуються для адміністрування служб за допомогою командного рядка.

Наприклад, якщо на локальній системі необхідно запустити службу DNS, в командному рядку можна ввести таку команду:

net start DNS

Для зупинки служби DNS необхідно ввести наступну команду:

net stop DNS

Відповідно, команди net pause та net continue використовуються для тимчасової зупинки виконання служби і її повторного запуску, відповідно.

У наступній таблиці перераховані значення атрибуту служба.

Значення	Опис	Нотатки
alerter	Запуск служби «Оповіщувач».	• Служба Оповіщувач дозволяє відправляти повідомлення окремому користувачеві або користувачам, підключеним до даного сервера. Ці повідомлення служать для оповіщення користувачів про проблеми безпеки, доступу і користувальницьких сеансів.
browser	Запуск служби «Оглядач комп'ютерів».	• Використовуйте диспетчер серверів (сістемний_корневой_каталог \ System32 \ Srvmgr.exe) для вказівки адміністраторів, які будуть отримувати адміністративні сповіщення. Диспетчер серверів входить до складу тільки Windows Server 2000.
"Клієнт для мереж NetWare"	Запуск служби «Клієнт для мереж NetWare».	• Сповіщення відправляються з сервера на комп'ютер користувача як повідомлення. Для прийому сповіщень на комп'ютері користувача має бути запущена служба повідомлень.
"Сервер папки обміну"	Запуск служби «Сервер папки обміну».	• Служба «Оглядач комп'ютерів» підтримує поточний список комп'ютерів в локальній мережі і надає цей список запитуючою його додаткам.
dhcp client	Запуск служби «DHCP-клієнт».	• Ця команда доступна, тільки якщо встановлена служба «Клієнт для мереж NetWare».
eventlog	Запуск служби «Журнал подій».	• Служба «Сервер папки обміну» дозволяє копіювати і вставляти текстові та графічні дані по мережі.
file replication	Запуск служби реплікації файлів.	• Служба «Сервер папки обміну» підтримує вікно папки обміну, за допомогою якої можна переглядати сторінки видалених тек обміну.
messenger	Запуск служби повідомлень.	• Ця команда доступна, тільки якщо встановлений протокол TCP / IP.
netlogon	Запуск служби «Мережевий вхід в систему».	• Служба «DHCP-клієнт» підтримує мережеву конфігурацію, запитуючи і оновлюючи IP-адреси та імена DNS. Служба «DHCP-клієнт» підтримує отримання IP-адреси від DHCP-сервера.
"Постачальник підтримки безпеки NT LM"	Запуск служби «Постачальник підтримки безпеки NT LM».	• Служба «DHCP-клієнт» не може бути припинена або зупинена.
"plug and play"	Запуск служби «Plug and Play».	• Служба «Журнал подій» заносить в журнал повідомлення про події, одержувані від програм і Windows XP. Звіти журналу подій містять відомості, які можуть бути корисні при пошуку причини неполадок. Ці звіти можна переглядати у вікні «Перегляд подій». Перегляд цих подій можливий тільки після запуску служби «Журнал подій».
"Диспетчер підключень віддаленого доступу"	Запуск служби диспетчера підключень віддаленого доступу.	• Цю службу не можна зупинити або призупинити.
"Маршрутизація	Запуск служби	

та віддалений доступ"	«Маршрутизація та віддалений доступ».	
rpclocator	Запуск служби «Локатор віддаленого виклику процедур (RPC)».	• Ця служба дозволяє комп'ютеру отримувати повідомлення.
rpcss	Запуск служби «Віддалений виклик процедур (RPC)».	• Повідомлення відправляються комп'ютера з використанням ідентифікаційного імені комп'ютера.
schedule	Запуск служби «Планувальник завдань».	• Служба «Мережевий вхід в систему» перевіряє запити на підключення і управляє реплікацією облікових записів користувачів у домені.
server	Запуск служби «Сервер».	• Служба «Мережевий вхід в систему» повинна бути запущена на всіх серверах домену, де зберігаються копії облікових даних користувачів.
spooler	Запуск служби «Диспетчер черги друку».	• Ця команда доступна після установки системи забезпечення захисту NT LM.
"Модуль підтримки NetBIOS через TCP / IP"	Запуск служби підтримки NetBIOS через TCP, що дозволяє працювати службам NetBIOS через TCP / IP (NetBT).	
ups	Запуск служби «Джерело безперебійного живлення».	• Ця команда доступна, тільки якщо встановлена служба віддаленого доступу.
workstation	Запуск служби «Робоча станція».	

net help команда

Відображення довідки для вказаної команди net.
Примітки:
• Набір відображуваних служб і додатків може змінюватися в залежності від параметрів, вибраних при установці або настройці.
• Додаткові відомості про служби англійською мовою можна знайти у посібнику «System Essentials Guide» на веб-сайті корпорації Майкрософт.
• Деякі служби можуть залежати від інших служб.
• Крім того, для налаштування автоматичного запуску або зупинки служб можна використовувати оснастку «Служби». Це оснащення дозволяє запускати, зупиняти, припиняти і відновлювати роботу мережевих служб.
• Команду Net start можна використовувати і для запуску служб, які не входять до складу Windows XP.
• Якщо ім'я служби містить пробіли, його слід брати в лапки (наприклад "ім'я служби").
Приклади: Щоб отримати список поточних запущених служб, введіть:

net start

Щоб запустити службу клієнта для мереж Netware, введіть:

net start "Клієнт для мереж NetWare".

10. net statistics

Команда net statistics виявляється корисною для отримання статистики роботи в мережі для служб Сервер (Server) і Робоча станція (Workstation).

Ця команда корисна для ідентифікації проблем, що виникають при неправильній роботі протоколу TCP / IP, наприклад:
• Помилки в роботі мережі
• Завислі сеанси
• Невдалі сеанси
• Операції, що завершилися невдало

Хоча команда повідомляє тільки про помилки, вона допомагає підтвердити або відхилити підозри про наявність проблеми. Ось синтаксис команди net statistics:

net statistics [server | workstation]

При використанні без параметрів команда net statistics повідомляє доступну статистику. В іншому випадку, можна розглянути статистику окремо по службі Сервер (Server) або Робоча станція (Workstation).

11. net session

Припустимо, що за допомогою команди net statistics вдалося ідентифікувати наявність завислого сеансу. Як припинити цей сеанс? Для цієї мети в Windows представлена чудова команда net session. Ця команда, яка може використовуватися тільки на сервері, дозволяє переглядати активні сеанси і відключати вибрані сеанси. Команда net session має наступний синтаксис:

net session [\ \ ім'я_комп'ютера] [/ delete]

Параметри цієї команди представлені в наступній таблиці.

Параметр	Використання
\\ім'я_комп'ютера	Відображає інформацію сеансу для зазначеного комп'ютера
/delete	Якщо цей параметр використовується окремо, всі сеанси сервера завершуються і всі відкриті файли закриваються. Якщо вказується ім'я комп'ютера, то закриваються тільки сеанси для цього комп'ютера

Якщо команду запустити без параметрів, відображається список сеансів, встановлених на сервері. Ось пара варіантів використання команди net session.

Перегляд інформації по всім встановленим сеансам:

net session

Завершення всіх сеансів з комп'ютером compik:

net session \ \ compik / delete

12. Net view

Остання команда з групи мережевих служб, яка буває корисна при вирішенні виникаючих проблем, називається net view.

При включенні режиму NetBIOS over TCP / IP багато хто починає використовувати Провідник Windows (Windows Explorer) в якості способу перегляду доступних ресурсів в мережі.

Команда net view надає таку ж функціональність для командного рядка. Якщо необхідно переглянути список доступних ресурсів на певному сервері, команда net view надає швидкий спосіб отримати список всіх загальних папок і принтерів на цьому комп'ютері.

Команда net view має наступний синтаксис:

net view [\ \ ім'я_комп'ютера] [/ domain: <ім'я>]

net view / Network: NW [\ \ ім'я_комп'ютера]

Далі представлено опис параметрів команди net view.
Параметри команди net view

параметр	Використання
\ \ ім'я_комп'ютера	Ім'я комп'ютера, загальні ресурси якого необхідно переглянути
/ domain: <ім'я>	Використовується для перегляду комп'ютерів у вказаному домені
/ Network: NW	Використовується для відображення всіх доступних серверів в мережі NetWare

Прикладом використання команди net view може бути перевірка, чи застосовується користувачем правильне ім'я або шлях для отримання доступу до спільної папки.
Для перегляду списку всіх загальних ресурсів в системі, яка називається Dempsey, необхідно ввести таку команду:

net view \ \ Dempsey

13. Netstat

Корисна команда і утиліта одночасно, яка називається netstat, дозволяє переглядати інформацію про з'єднання системи по протоколах UDP і TCP.

Команду можна запустити так, щоб вона виконувалася кожні n секунд і дозволяла отримувати таку інформацію в табличному форматі:
• Назва протоколу (TCP або UDP)
• Локальний адресу IP і номер порту, які використовуються з'єднанням через сокет
• Віддалений адресу IP (адреса призначення) і номер порту, який використовується з'єднанням через сокет
• Стан з'єднання (що очікує (Listening)), Встановлене (Established)) і т.д.)

Вивчення стану портів з'єднання між двома системами дозволяє виключити протокол TCP / IP, як одну з причин проблеми. Для повного розуміння інформації, що надається цією командою, необхідно зрозуміти принципи встановлення з'єднання в протоколі TCP / IP. Ось основні етапи процесу установки з'єднання TCP / IP:
1. При спробі встановити з'єднання клієнт відправляє повідомлення SYN серверу.
2. Сервер відповідає власним повідомленням SYN і підтвердженням (ACK).
3. Після цього клієнт відправляє повідомлення ACK назад на сервер, завершуючи процес установки з'єднання.

Процес розриву з'єднання складається з наступних етапів:
1. Клієнт повідомляє "Я закінчив", відправляючи повідомлення FIN серверу. На цьому етапі клієнт тільки приймає дані від сервера, але сам нічого не відправляє.
2. Після цього сервер відправляє повідомлення ACK і відправляє власне повідомлення FIN клієнтові.
3. Після цього клієнт відправляє повідомлення ACK серверу, підтверджуючи запит сервера FIN.
4. При отриманні повідомлення ACK від клієнта сервер закриває з'єднання.

Розуміння етапів процесу установки і розриву з'єднання дозволяє більш прозоро інтерпретувати стану з'єднань у виводі команди netstat. З'єднання в списку можуть знаходитися в наступних станах.
• CLOSE_WAIT - вказує на пасивну фазу закриття з'єднання, яка починається після отримання сервером повідомлення FIN від клієнта.
• CLOSED - сполучення перервано і закрито сервером.
• ESTABLISHED - клієнт встановив з'єднання з сервером, отримавши від сервера повідомлення SYN.
• FIN_WAIT_1 - клієнт ініціював закриття з'єднання (відправив повідомлення FIN).
• FIN_WAIT_2 - клієнт отримав повідомлення ACK і FIN від сервера.
• LAST_ACK - сервер відправив повідомлення FIN клієнтові.
• LISTEN - сервер готовий приймати вхідні з'єднання.
• SYN_RECEIVED - сервер отримав повідомлення SYN від клієнта і відправив йому відповідь.
• TIMED_WAIT - клієнт відправив повідомлення FIN серверу й очікує відповіді на це повідомлення.
• YN_SEND - зазначене з'єднання активно і відкрито.
Тепер все, що необхідно знати про команду netstat, це синтаксис її виклику:

netstat [-a] [-e] [-n] [-o] [-p <протокол>] [-r] [-s] [інтервал]

Параметри команди netstat наводяться далі.

Параметр	Використання

-a	Відображає всі з'єднання і очікують порти
-e	Відображає статистику Ethernet
-n	Показує адреси і порти в цифровому форматі (адреси IP замість імен інтерфейсів
-o	Відображає ідентифікатор процесу-власника для кожного з'єднання
-p <протокол>	Показує з'єднання для вказаного протоколу. Можна вибрати один із таких протоколів: TCP, TCPv6, UDP і UDPv6. При вказівці параметра-s можна вказувати IP, IPv6, ICMP і ICMPv6.
-r	Відображає таблицю маршрутизації системи
-s	Відображає статистику для кожного протоколу окремо; за замовчуванням статистика відображається для протоколів TCP, TCPv6, UDP і UDPv6, IP, IPv6, ICMP і ICMPv6. Підмножина протоколів може бути вказано за допомогою параметра-p.
інтервал	Інтервал в секундах, за який команда оновлює свій висновок. При вказівці інтервалу команду можна перервати комбінацією клавіш <Ctrl+C>.

Відображення активних підключень TCP, портів, що прослуховуються комп'ютером, статистики Ethernet, таблиці маршрутизації IP, статистики IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP через IPv6 і UDP через IPv6). Запущена без параметрів, команда nbtstat відображає підключення TCP.

Синтаксис

netstat [-a] [-e] [-n] [-o] [-p протокол] [-r] [-s] [інтервал]

/? Відображення довідки в командному рядку.

Примітки

• Параметри, які використовуються з даною командою, повинен передувати дефіс (-), а не коса риска (/).

• Команда Netstat виводить статистику для наступних об'єктів.

• Протокол Ім'я протоколу (TCP або UDP).

• Локальні адреси IP-адреса локального комп'ютера і номер використовуваного порту. Ім'я локального комп'ютера, відповідне IP-адресою і імені порту, виводиться тільки в тому випадку, якщо не вказано параметр-n. Якщо порт не призначений, замість номера порту буде виведена зірочка (*).

• Зовнішні адреси IP-адресу та номер порту віддаленого комп'ютера, підключеного до даного сокета. Імена, відповідні IP-адресою і порту, виводяться тільки в тому випадку, якщо не вказано параметр-n. Якщо порт не призначений, замість номера порту буде виведена зірочка (*).

• (Стан) Вказівка стану підключення TCP. Можливі значення: CLOSE_WAIT CLOSED ESTABLISHED FIN_WAIT_1 FIN_WAIT_2 LAST_ACK LISTEN SYN_RECEIVED SYN_SEND TIMED_WAIT Для отримання додаткових відомостей про стани підключення TCP див. документ RFC 793.

• Ця команда доступна, тільки якщо у властивостях мережевого адаптера в об'єкті Мережеві підключення в якості компонента встановлений протокол Інтернету (TCP / IP).

Приклади

Для виведення статистики Ethernet і статистики по всіх протоколах введіть наступну команду: netstat-e-s Для виведення статистики тільки за протоколами TCP і UDP введіть наступну команду: netstat-s-p tcp udp Для виведення активних підключень TCP і кодів процесів кожні 5 секунд введіть наступну команду: nbtstat-o 5 Для виведення активних підключень TCP і кодів процесів кожні з використанням числового формату введіть наступну команду:

nbtstat-n-o

Деякі адміністратори Windows Server користуються командою netstat регулярно, деякі - тільки для діагностики. Для команди netstat передбачено десять параметрів, що дозволяють отримати докладну інформацію для вирішення найрізноманітніших завдань. Втім, не менш корисні відомості можна отримати і без жодних параметрів.

Найчастіше netstat застосовують з параметром-a, щоб отримати список всіх підключень і прослуховує портів. Нижче перераховані кілька інших параметрів, які можуть стати в нагоді при використанні цієї утиліти.

Повністю певне ім'я домену. Параметр-f дозволяє дізнатися FQDN для зовнішнього адреси. При використанні netstat з цим параметром імена дозволяються як у внутрішній, так і в зовнішній мережі. На рис. 1 показаний висновок команди.

Рисунок 1

Який процес використовує той чи інший порт. Поєднання параметрів-a-n-o дозволяє з'ясувати, якому ідентифікатору процесу (PID) відповідає той чи інший порт. (Як дізнатися, яким процесом використовується порт TCP в Windows Server 2008) Висновок команди показаний на рис. 2.

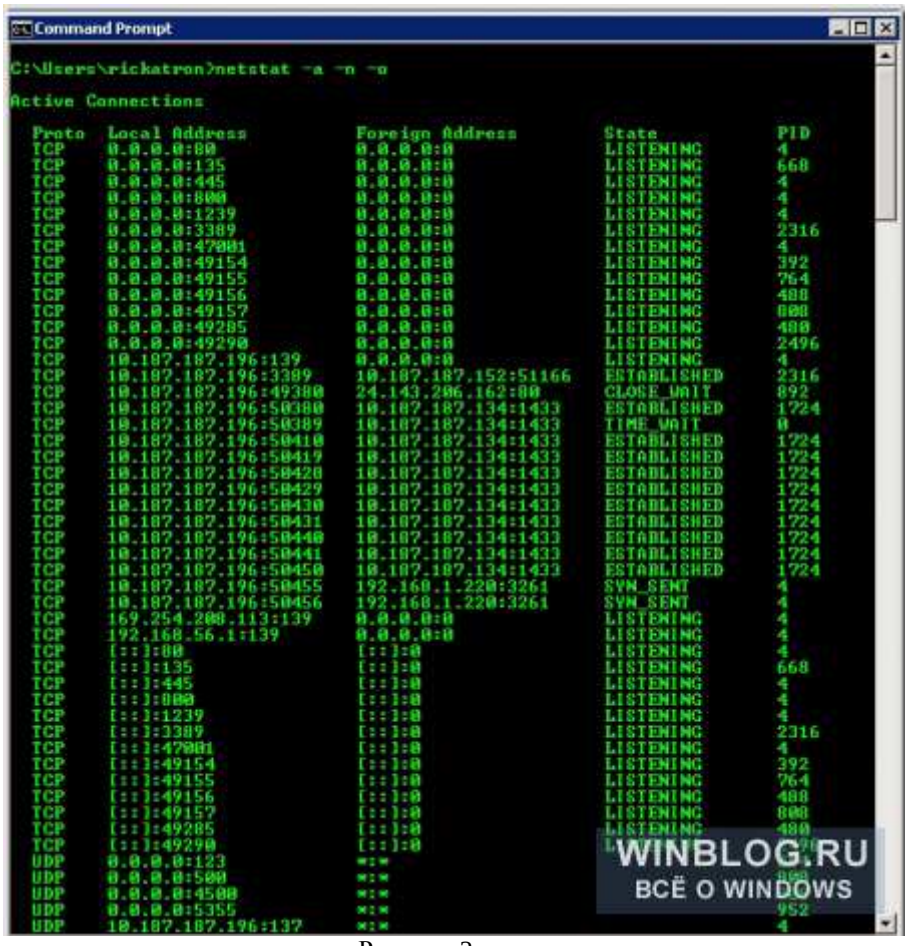

Рисунок 2

А якщо додати до цієї комбінації параметр-b, для кожного процесу будуть використовуватися дружні імена, як показано на рис. 3. Правда, для цього будуть потрібні права адміністратора.

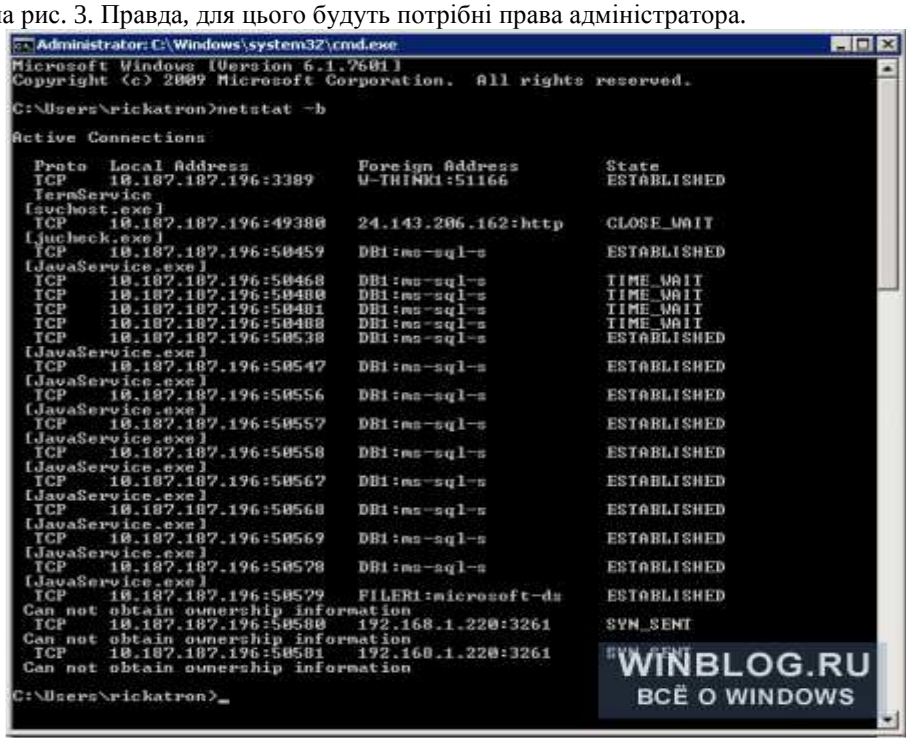

Рисунок 3

Зверніть увагу: видалені адреси, які вказують на 192.168.1.220:3261, належать службі ініціатора Windows iSCSI і позначаються інакше, ніж адреси інших служб.

Висновок таблиці маршрутизації. Коли потрібно з'ясувати, чому на одному комп'ютері мережеве з'єднання працює інакше, ніж на інших у тій же мережі, можна використовувати параметр-r, який виводить маршрут для даної системи, як показано на рис. 4. Зверніть увагу на розділ «Постійні маршрути» (Persistent routes): в ньому вказуються всі статичні маршрути, налаштовані для Windows Server).

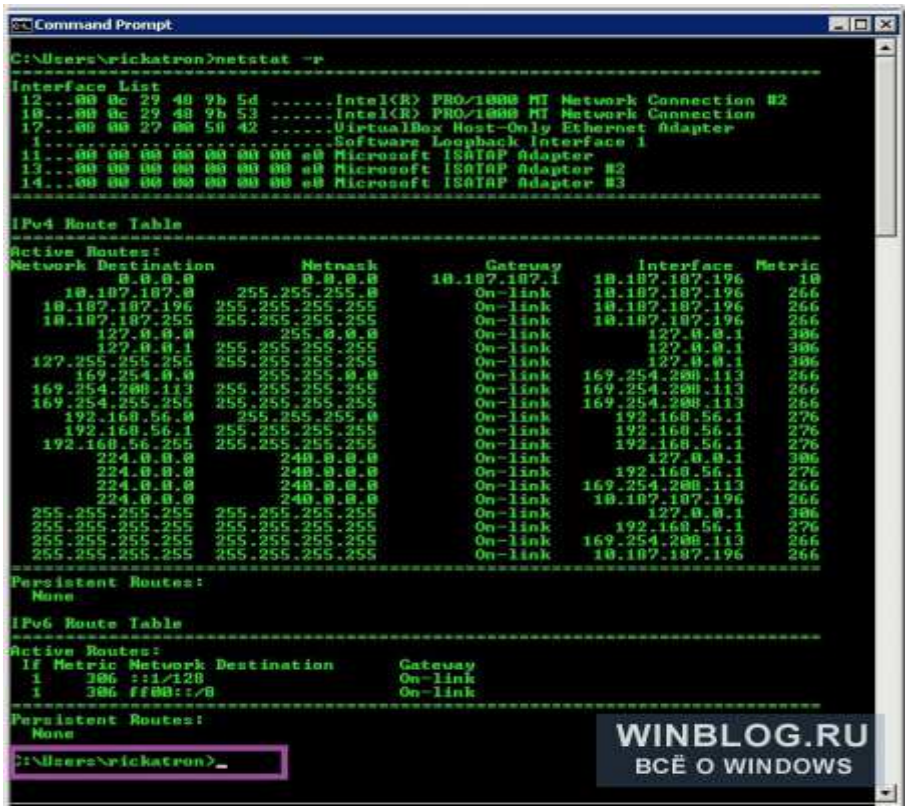

Рисунок 4

14. Telnet

Історично Telnet служив для віддаленого доступу до інтерфейсу командного рядка операційних систем. Згодом його стали використовувати для інших текстових інтерфейсів, аж до ігор MUD і анімованого ASCII-art. Теоретично, навіть обидві сторони протоколу можуть бути програмами, а не людиною.

Іноді клієнти telnet використовуються для доступу до інших протоколах на основі транспорту TCP, див. # Telnet і інші протоколи.

Протокол telnet використовується в керуючому з'єднанні FTP, тобто заходити на сервер командою telnet ftp.example.net ftp для виконання налагодження і експериментів не тільки можливо, але і правильно (на відміну від застосування клієнтів telnet для доступу до HTTP, IRC і більшості інших протоколів).

Утиліта Telnet бродить по світу UNIX багато років і дозволяє віддалено адмініструвати сервери. Починаючи з Windows 2000, операційна система Windows теж надає власну службу Telnet.

Команда telnet дозволяє швидко отримати доступ до командного рядка віддаленого комп'ютера і виконати такі дії, як:

• Запуск і зупинка служб

• Управління файлами і каталогами

• Запуск сценаріїв

Хоча в підключенні за допомогою telnet до іншої системи бувають ньюанси, наступний базовий синтаксис дозволяє встановити зв'язок і ініціювати управління віддаленої системою:

telnet <IP_компютера_до_якого_необхідний_доступ> [port: <номер_порта>]

После завершения удаленного администрирования можно завершить сеанс работы с программой telnet, введя команду **exit** в строке приглашения командной строки сеанса Telnet.

По соображениям безопасности, служба Telnet останавливается и настраивается на ручной режим запуска по умолчанию. Эта политика относится к серверам под управлением Windows 2000 и более поздних версий операционной системы Windows.

Дополнительную безопасность удаленного администрирования можно обеспечить с помощью Службы Терминалов.

15. Tracert

Команда tracert трохи нагадує команду pathping, дозволяючи перевіряти шлях між двома маршрутизуються мережами, але ця утиліта не перевіряє маршрутизатори на шляху проходження пакетів так ретельно, як це робить утиліта pathping.

Як і утиліти pathping і ping, утиліта tracert відображає кожен перехід (маршрутизатор) між джерелом, на якому була виконана команда, і точкою призначення, але при цьому не відображається статистична інформація, наприклад, співвідношення загублених пакетів, яке відображається утилітою pathping.

Ось синтаксис команди tracert:

tracert <ім'я_призначення або адреса_IP> [-d] [-h <максимальна_кількість_переходів>] [-j <список_вузлів>] [-w <таймаут>]

Параметри команди tracert представлені в наступній таблиці.

Параметр	Використання
<ім'я_призначення або адреса_IP>	Вкажіть доменне ім'я точки призначення або адресу IP
-d	Прискорює виконання команди tracert за рахунок відмови від перетворення адрес IP маршрутизаторів в доменні імена
-h <максимальна_кількість_переходів>	Використовується для вказівки максимальної кількості переходів по шляху до точки призначення. За замовчуванням використовується значення 30.
-j <список_вузлів>	Дозволяє вказати проміжні точки призначення у вигляді списку адрес IP, розділених пробілами (список_вузлів). Цей параметр використовує Loose Source Routing, що дозволяє вставляти один або кілька маршрутизаторів між проміжними пунктами. Ця команда дозволяє вказати до дев'яти проміжних вузлів.
-w <таймаут>	Використовується для вказівки часу (у мілісекундах) очікування відповіді ICMP Time Exceeded або відповіді Echo Reply на тестовий запит. Якщо відповідь не була отримана за вказаний час, відображається символ (*). За замовчуванням використовується значення 4000 (4 секунди).

16. Route

Виводить на екран і змінює записи в локальній таблиці IP-маршрутизації. Запущена без параметрів, команда route виводить довідку.

Синтаксис:

route [-f] [-p] [команда [конечная_точка] [mask маска_сеті] [шлюз] [metric метрика]] [if інтерфейс]]

Параметри:

-F Очищує таблицю маршрутизації від всіх записів, які не є вузловими маршрутами (маршрути з маскою підмережі 255.255.255.255), мережевим маршрутом замикання на себе (маршрути з кінцевою точкою 127.0.0.0 і маскою підмережі 255.0.0.0) або маршрутом багатоадресної розсилки (маршрути з кінцевою точкою 224.0.0.0 і маскою підмережі 240.0.0.0). При використанні даного параметра спільно з однією з команд (таких, як add, change або delete) таблиця очищається перед виконанням команди.

-P При використанні даного параметра з командою add вказаний маршрут додається до реєстру та використовується для ініціалізації таблиці IP-маршрутизації кожен раз при запуску протоколу TCP / IP. За замовчуванням додані маршрути не зберігаються при запуску протоколу TCP / IP. При використанні параметра з командою print виводить на екран список постійних маршрутів. Всі інші команди ігнорують цей параметр. Постійні маршрути зберігаються в реєстрі за адресою HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Tcpip \ Parameters \ PersistentRoutes.

команда Вказує команду, яка буде запущена на віддаленій системі. У наступній таблиці представлений список допустимих параметрів:

Команда	Призначення
add	Додавання маршруту
change	Зміна існуючого маршруту
delete	Видалення маршруту чи маршрутів
print	Друк маршруту чи маршрутів

кінцева_точка Визначає кінцеву точку маршруту. Кінцевою точкою може бути мережева IP-адреса (де розряди вузла в мережевому адресу мають значення 0), IP-адресу маршруту до вузла, або значення 0.0.0.0 для маршруту за замовчуванням.
mask маска_мережі Вказує маску мережі (також відомої як маска підмережі) відповідно до точкою призначення. Маска мережі може бути маскою підмережі відповідної мережевого IP-адресою, наприклад 255.255.255.255 для маршруту до вузла або 0.0.0.0. для маршруту за замовчуванням. Якщо даний параметр пропущено, використовується маска підмережі 255.255.255.255. Кінцева точка не може бути більш точною, ніж відповідна маска підмережі. Іншими словами, значення розряду 1 в адресі кінцевої точки неможливо, якщо значення відповідного розряду в масці підмережі дорівнює 0. шлюз Вказує IP-адресу пересилання або наступного переходу, по якому доступний набір адрес, визначений кінцевою точкою і маскою підмережі. Для локально підключених маршрутів підмережі, адресу шлюзу - це IP-адреса, призначений інтерфейсу, який підключений до підмережі. Для віддалених маршрутів, які доступні через один або кілька маршрутизаторів, адреса шлюзу - безпосередньо доступний IP-адресу найближчого маршрутизатора.
metric метрика Задає цілочисельну метрику вартості маршруту (в межах від 1 до 9999) для маршруту, яка використовується при виборі в таблиці маршрутизації одного з декількох маршрутів, найбільш близько відповідного адресою призначення пересилається пакета. Вибирається маршрут з найменшою метрикою. Метрика відображає кількість переходів, швидкість проходження шляху, надійність шляху, пропускну здатність шляхи і засоби адміністрування.
if інтерфейс Вказує індекс інтерфейсу, через який доступна точка призначення. Для виведення списку інтерфейсів і їх відповідних індексів використовуйте команду route print. Значення індексів інтерфейсів можуть бути як десяткові, так і шістнадцяткові. Перед шістнадцятиричними номерами вводиться 0x. У випадку, коли параметр if пропущений, інтерфейс визначається з адреси шлюзу.
/? Відображає довідку в командному рядку.

Примітки
• Великі значення в стовпці metric таблиці маршрутизації - результат можливості протоколу TCP / IP автоматично визначати метрики маршрутів таблиці маршрутизації на підставі конфігурації IP-адреси, маски підмережі та стандартного шлюзу для кожного інтерфейсу ЛВС. Автоматичне визначення метрики інтерфейсу, включене за замовчуванням, встановлює швидкість кожного інтерфейсу і метрики маршрутів для кожного інтерфейсу так, що найшвидший інтерфейс створює маршрути з найменшою метрикою. Щоб видалити великі метрики, відключіть автоматичне визначення метрики інтерфейсу в додаткових властивостях протоколу TCP / IP для кожного підключення по локальній мережі.
• Імена можуть використовуватися для параметра конечная_точка, якщо існує відповідний запис у файлі бази даних Networks, що знаходиться в папці сістемний_корневой_каталог \ System32 \ Drivers \ Etc. У параметрі шлюз можна вказувати імена до тих пір, поки вони вирішуються в IP-адреси за допомогою стандартних способів вирішення вузлів, таких як запит служби DNS, використання локального файлу Hosts, що знаходиться в папці сістемний_корневой_каталог \ system32 \ drivers \ etc, або дозвіл імен NetBIOS .
• Якщо команда - print або delete, параметр шлюз опускається і використовуються знаки підстановки для вказівки точки призначення та шлюзу. Значення конечной_точкі може бути підстановки значенням, яке вказується зірочкою (*). При наявності зірочки (*) або знаку (?) В описі кінцевої точки, вони розглядаються як підстановки, тоді друкуються або видаляються тільки маршрути, відповідні точки призначення. Зірочка відповідає будь-якій послідовності символів, а знак питання - будь одному символу. 10. * .1, 192.168. *, 127. * I * 224 * є допустимими прикладами використання зірочки в якості підстановки.
• При використанні неприпустимою комбінації значень кінцевої точки і маски підмережі (маски мережі) виводиться таке повідомлення про помилку: «Маршрут: невірна маска підмережі адреси шлюзу». Помилка з'являється, коли одне або декілька значень розрядів в адресі кінцевої точки дорівнює 1, а значення відповідних розрядів маски підмережі - 1. Для перевірки цього стану висловіть кінцеву точку та маску підмережі в двійковому форматі. Маска підмережі в двійковому форматі складається з послідовності одиничних бітів, яка представляє частину мережевої адреси кінцевої точки, і послідовності нульових бітів, що позначає частину

адреси вузла кінцевої точки. Перевірте наявність поодиноких бітів в частині адреси точки призначення, яка є адресою вузла (як визначено маскою підмережі).
• Параметр-p підтримується в команді route тільки в операційних системах Windows NT 4.0, Windows 2000, Windows Millennium Edition і Windows XP. Цей параметр не підтримується командою route в системах Windows 95 і Windows 98.
• Ця команда доступна, тільки якщо у властивостях мережевого адаптера в об'єкті Мережеві підключення в якості компонента встановлений протокол Інтернету (TCP / IP).

Приклади:
Щоб вивести на екран весь вміст таблиці IP-маршрутизації, введіть команду:

route print

Щоб вивести на екран маршрути з таблиці IP-маршрутизації, які починаються з 10., Введіть команду:

route print 10.*

Щоб додати маршрут за умовчанням з адресою стандартного шлюзу 192.168.12.1, введіть команду:

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

Щоб додати маршрут до кінцевої точки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступним адресою переходу 10.27.0.1, введіть команду:

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1

Щоб додати постійний маршрут до кінцевої точки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступним адресою переходу 10.27.0.1, введіть команду:

route-p add 10.41.0.0 mask 255.255.0.0 10.27.0.1

Щоб додати маршрут до кінцевої точки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступним адресою переходу 10.27.0.1 і метрикою вартості 7, введіть команду:

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7

Щоб додати маршрут до кінцевої точки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступним адресою переходу 10.27.0.1 і використанням індексу інтерфейсу 0x3, введіть команду:

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 if 0x3

Щоб видалити маршрут до кінцевої точки 10.41.0.0 з маскою підмережі 255.255.0.0, введіть команду:

route delete 10.41.0.0 mask 255.255.0.0

Щоб видалити всі маршрути з таблиці IP-маршрутизації, які починаються з 10., Введіть команду:

route delete 10. *

Щоб змінити таку адресу переходу для маршруту з кінцевою точкою 10.41.0.0 і маскою підмережі 255.255.0.0 з 10.27.0.1 на 10.27.0.25, введіть команду:

route change 10.41.0.0 mask 255.255.0.0 10.27.0.25

17. nsloockup

nslookup (англ. name server lookup пошук на сервері імен) - утиліта, яка надає користувачеві інтерфейс командного рядка для звернення до системи DNS (простіше кажучи, DNS-клієнт). Дозволяє задавати різні типи запитів і запитувати довільно вказувані сервера. Її аналогом є утиліти host і dig. Розроблена в складі пакету BIND (для UNIX-систем).

Утиліта портована на Windows безпосередньо фірмою Microsoft і поставляється разом з операційною системою. Приклад:

nslookup wikipedia.org

Server: 127.0.0.1
Address: 127.0.0.1#53
Non-authoritative answer
Name: wikipedia.org
Address: 208.80.152.201

Хід роботи

1. Відкрийте вікно з підтримкою командного рядка за допомогою підпункту головного меню *Пуск – Программы – Стандартные – Командная строка* та виконайте у ньому наведені вище команди (не менше двох прикладів для кожної команди). Скопіюйте образи вікон зрозумілих вам команд та їх результатів (не менше п'яти) у звіт по лабораторній роботі.
2. Створіть електронний лист у своїй поштовій скриньці на сайті *gmail.com*. Приєднайте до цього листа документ з скопійованими образами вікон. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР12_Величко Володимир*. Надішліть створений лист на адресу LRCompNet@gmail.com.