Бекас Б. О.

# *Лабораторна робота .*
# ДОСЛІДЖЕННЯ КОНФІГУРУВАННЯ І КЕРУВАННЯ УБУДОВАНИМИ ЗАСОБАМИ МОНІТОРИНГУ ОС WINDOWS 2000 PRO

**Мета роботи** — ознайомлення студентів з основними принципами роботи системи моніторингу мереж. Дослідження цілей використання убудованих засобів моніторингу мереж, їхніх достоїнств і недоліків. Одержання практичних навичок використання і дослідження роботи убудованих засобів моніторингу мереж (**ЗММ**).

**Рекомендації щодо підготовки до виконання** лабораторної роботи. Необхідно вивчити основні типи убудованих засобів моніторингу мереж, принципи і логіку їхньої роботи в мережі, основні параметри і характеристики, а також можливості інтерактивної роботи в мережі. Навчитися аналізувати отримані дані про мережні настроювання. Вивчити вимоги до апаратного, мережного й програмного забезпечення ОС.

## *Суть роботи*

Використання убудованих ЗММ здійснюється шляхом запуску відповідних програм з командного рядка в режимі емуляції DOS. Виклик убудованої довідкової системи можна здійснити, набравши наступний рядок "ім'я_профами /?". Задаючи різні ключі в рядку параметрів кожної убудованої програми, можна визначити практично вагу інформацію про мережі. Отримані в такий спосіб параметри характеристики необхідно класифікувати і записати належним образом у звіті по роботі, за якими в результаті зробити загальний висновок.

Розглянемо деякі описи і приклади роботи розповсюджених убудованих засобів ЗММ.

**PING** — посилка пакетів на зазначений вузол і чекання відповідей (час у мілісекундах). Без установок 4 рази.

Використання:

**ping** [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j список Вузлів] | [-k список Вузлів]] [-w інтервал] список Розсилання

Параметри:

| | |
|---|---|
| -t | Відправка пакетів на вказаний вузол до команди переривання. Для виведення статистики і продовження натисніть <Ctrl>+<Break>, для припинення - <Ctrl>+<C>. |
| -a | Визначення адрес по іменах вузлів. |
| -n число | Число запитів, що відправляються. |
| -l розмір | Розмір буфера відправки. |
| -f | Установка прапора, що забороняє фрагментацію пакету. |
| -i TTL | Завдання терміну життю пакету (поле "Time To Live"). |
| -v TOS | Завдання типу служби (поле "Type Of Service"). |
| -r число | Запис маршруту для вказаного числа переходів. |
| -s число | Штамп часу для вказаного числа переходів. |
| -j список Вузлів | Вільний вибір маршруту за списком вузлів. |
| -k список Вузлів | Жорсткий вибір маршруту за списком вузлів. |
| -w інтервал | Інтервал кожної відповіді в мілісекундах. |

**********

Бекас Б. О.

```
C:\>ping -t -a -n 5 -l 100 –f -i 15  -v 1 -r 2 -s 3 -w 20 zevs
Обмін пакетами з zevs.kn.local [172.16.1.2] по 100 байт:

Відповідь від 172.16.1.2: число байт=100 время<10мс TTL=128
   Маршрут: a50.kn.local [172.16.1.2]
   Штамп часу: a50.kn.local [172.16.1.2] : 2993309444
Відповідь від 172.16.1.2: число байт=100 время<10мс TTL=128
   Маршрут: a50.kn.local [172.16.1.2]
   Штамп часу: a50.kn.local [172.16.1.2] : 2590918404
Відповідь від 172.16.1.2: число байт=100 время<10мс TTL=128
   Маршрут: a50.kn.local [172.16.1.2]
   Штамп часу: a50.kn.local [172.16.1.2] : 2188527364
Відповідь від 172.16.1.2: число байт=100 время<10мс TTL=128
   Маршрут: a50.kn.local [172.16.1.2]
   Штамп часу: a50.kn.local [172.16.1.2] : 1786136324
Відповідь від 172.16.1.2: число байт=100 время<10мс TTL=128
   Маршрут: a50.kn.local [172.16.1.2]
   Штамп часу: a50.kn.local [172.16.1.2] : 1383745284

Статистика Ping для 172.16.1.2:
   Пакетів: відправлено = 5, отримано = 5, втрачений = 0 (0% втрат)
   Приблизний час передачі і прийому:
   найменше = 0мс, найбільше =  0мс, середнє =  0мс
**********************************************************************************************
```

**NETSTAT** — трасування маршруту до зазначеного вузла.

Відображення статистики протоколу і поточних мережних підключень TCP/IP.

NETSTAT [-a] [-e] [-n] [-s] [-p ім'я] [-r] [інтервал]

-a Відображення всіх підключень і портів, що очікують, (підключення з боку сервера не відображаються).

-e Відображення статистики Ethernet. Цей ключ може використовуватися разом із ключем -s.

-n Відображення адреси і номерів портів у числовому форматі.

-p [ім'я] Відображення підключень для протоколу "ім'я": tcp або udp. Використовується разом із ключем -s для відображення статистики по протоколах. Припустимі значення "ім'я": tcp, udp або ip.

-r Відображення вмісту таблиці маршрутів,

-s Відображення статистики за протоколами. За замовчуванням виводяться дані для TCP, UDP і IP. Ключ -p дозволяє вказати підмножина даних, що вводиться.

[інтервал] Повторне введення статистичних даних через зазначений інтервал у секундах. Для зупинки висновку даних натиснути клавіші CTRL+C. Якщо параметр не заданий, зведення про поточну конфігурацію виводяться один раз.

**********************************************************************************************

Бекас Б. О.

```
C:\>netstat -a

Активні підключення

  Ім'я   Локальна адреса       Зовнішня адреса        Стан
  TCP    A4748-09:epmap         A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:microsoft-ds  A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:1068          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:1076          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:2222          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:2223          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:2224          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:2846          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:gds_db        A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:3306          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:3580          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:8888          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:1097          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:1100          A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:30606         A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:netbios-ssn   A4748-09.kn.local:0    LISTENING
  TCP    A4748-09:1105          a50.kn.local:microsoft-ds  TIME_WAIT
  TCP    A4748-09:1107          a50.kn.local:microsoft-ds  TIME_WAIT
  TCP    A4748-09:kpop          a50.kn.local:microsoft-ds  TIME_WAIT
  TCP    A4748-09:1110          a50.kn.local:netbios-ssn   TIME_WAIT
  TCP    A4748-09:1111          a50.kn.local:microsoft-ds  TIME_WAIT
  TCP    A4748-09:1113          a50.kn.local:microsoft-ds  TIME_WAIT
  TCP    A4748-09:1114          a50.kn.local:netbios-ssn   TIME_WAIT
  UDP    A4748-09:microsoft-ds  *:*
  UDP    A4748-09:1027          *:*
  UDP    A4748-09:1045          *:*
  UDP    A4748-09:2343          *:*
  UDP    A4748-09:5000          *:*
  UDP    A4748-09:5001          *:*
  UDP    A4748-09:5002          *:*
  UDP    A4748-09:5003          *:*
  UDP    A4748-09:6000          *:*
  UDP    A4748-09:6001          *:*
  UDP    A4748-09:6002          *:*
  UDP    A4748-09:6003          *:*
  UDP    A4748-09:6004          *:*
  UDP    A4748-09:6005          *:*
  UDP    A4748-09:6006          *:*
  UDP    A4748-09:netbios-ns    *:*
  UDP    A4748-09:netbios-dgm   *:*
  UDP    A4748-09:isakmp        *:*
*****************************************************************************************************
```

Бекас Б. О.

```
C:\>netstat -n
Активні підключення
  Ім'я      Локальна адреса        Зовнішня адреса        Стан
  TCP       172.16.1.40:1105       172.16.1.2:445         TIME_WAIT
  TCP       172.16.1.40:1107       172.16.1.2:445         TIME_WAIT
  TCP       172.16.1.40:1109       172.16.1.2:445         TIME_WAIT
  TCP       172.16.1.40:1110       172.16.1.2:139         TIME_WAIT
  TCP       172.16.1.40:1111       172.16.1.2:445         TIME_WAIT
  TCP       172.16.1.40:1113       172.16.1.2:445         TIME_WAIT
  TCP       172.16.1.40:1114       172.16.1.2:139         TIME_WAIT
*******************************************************************************************

C:\>netstat -e -s -p udp
Статистика інтерфейсу
                                   Отримано        Відправлено
Байт                                864319             779399
Одноадресні пакети                    1723               1785
Багатоадресні пакети                  1709                 74
Відкинуте                                0                  0
Помилки                                  0                  0
Невідомий протокол                       0
Статистика UDP
  Отримано датаграм      = 1505
  Відсутність портів     = 10
  Помилки при отриманні  = 0
  Відправлено датаграм   = 126
Активні підключення
Ім'я     Локальна адреса       Зовнішня адреса        Стан
*******************************************************************************************

C:\>netstat -r Таблиця маршрутів
Список інтерфейсів
0x1 ........................... MS TCP Loopback interface
0x1000003 ..00 18 f3 90 51 c2 .. Realtek RTL8169/8110 Family Gigabit Ethernet NIC
===========================================================
Активні маршрути:
Мережева адреса     Маска мережі    Адреса шлюзу    Інтерфейс    Метрика
          0.0.0.0          0.0.0.0       172.16.1.2  172.16.1.40      1
        127.0.0.0        255.0.0.0        127.0.0.1    127.0.0.1      1
        172.16.1.0    255.255.255.0      172.16.1.40  172.16.1.40      1
      172.16.1.40  255.255.255.255        127.0.0.1    127.0.0.1      1
   172.16.255.255  255.255.255.255      172.16.1.40  172.16.1.40      1
        224.0.0.0        224.0.0.0      172.16.1.40  172.16.1.40      1
  255.255.255.255  255.255.255.255      172.16.1.40  172.16.1.40      1
Основний шлюз:        172.16.1.2
===========================================================
Постійні маршрути:  Відсутній
*******************************************************************************************
```

Бекас Б. О.

**TRACERT**

Використання:

tracert [-d] [-h макс. число] [-j список вузлів] [-w інтервал] ім'я

Параметри:

| | |
|---|---|
| -d | Без визначення адреси за іменами вузлів. |
| -h макс. число | Максимальне число переходів при пошуку вузла. |
| -j список вузлів | Вільний вибір маршруту за списком вузлів. |
| -w інтервал | Інтервал чекання кожної відповіді в мілісекундах. |

**********

C:\>tracert google.com.ua -h 10

Трасування маршруту до google.com.ua [74.125.77.104]
з максимальним числом стрибків 10:

| | | | | |
|---|---|---|---|---|
| 1 | <1 мс | <1 мс | <1 мс | 172.16.0.1 |
| 2 | 3 ms | 1 ms | 1 ms | 194.44.236.60 |
| 3 | 3 ms | 2 ms | 2 ms | 194.44.237.233 |
| 4 | 3 ms | 2 ms | 2 ms | 194.44.212.105 |
| 5 | 12 ms | 11 ms | * | 194.44.212.35 |
| 6 | 12 ms | 11 ms | 11 ms | 194.44.35.254 |
| 7 | 36 ms | 35 ms | 36 ms | 72.14.239.14 |
| 8 | 52 ms | 51 ms | 51 ms | 72.14.232.102 |
| 9 | 58 ms | 58 ms | 58 ms | 209.85.248.182 |
| 10 | 59 ms | 58 ms | 58 ms | 64.233.175.246 |

Трасування завершене.

**********

**NET CONFIG** — висновок поточних параметрів робочої групи.

NET CONFIG [SERVER / WORKSTATION]

C:\>net config workstation

| | |
|---|---|
| Ім'я комп'ютера | \A4748-09 |
| Повне ім'я комп'ютера | A4748-09.kn.local |
| Ім'я користувача | test |
| Активна робоча станція на | |
| NetbiosSmb (000000000000) | |
| NetBT_Tcpip_{79087AB3-5F2F-4A7A-A2C5-D960BE3FF3DF} (0018F39051C2) | |
| Версія програми | Windows 2000 |
| Домен робочої станції | KN |
| DNS-ім'я домена робочої станції | kn.local |
| Домен входу | A4748-09 |
| | |
| Інтервал очікування відкриття COM-порту (с) | 0 |
| Відлік передачі COM-порту (байт) | 16 |
| Таймаут передачі COM-порту (мс) | 250 |

Команда виконана успішно.

**********

**NET** (NET /?)

З метою одержання додаткових зведень про конкретну команду Microsoft NET розташуєте слідом за ім'ям команди ключ /? (наприклад NET VIEW /?).

| Опція | Опис |
|---|---|
| NET CONFIG | Висновок зведень про робочу групу |
| NET DIAG | Запуск програми Microsoft Network Diagnostics для одержання даних про мережі |
| NET HELP | Висновок зведень про команди і повідомлення про помилки |
| NETINIT | Завантаження протоколу і драйверів мережної плати без прив'язки їх до диспетчера протоколів |
| NET LOGOFF | Відключення всіх загальних ресурсів, використовуваних комп'ютером |
| NET LOGON | Ідентифікація користувача як члена робочої групи |
| NET PASSWORD | Зміна пароля для входу в мережу |
| NET PRINT | Висновок зведень про черги печатки і керування завданнями висновку на печатку |
| NET START | Запуск служб |
| NET STOP | Зупинка роботи служб |
| NET TIME | Висновок часу з іншого комп'ютера або синхронізація годин з годинником на серверу часу Microsoft Windows для робочих груп, Windows NT, Windows 95 або NetWare |
| NET USE | Підключення і відключення мережних ресурсів і висновок повідомлень про підключення |
| NETVER | Висновок типу і версії використовуваної системи переадресації |
| NET VIEW | Висновок списку комп'ютерів, що забезпечують спільний доступ до ресурсів або загальних ресурсів конкретного комп'ютера |

**NET DIAG** — запуск програми Microsoft Network Diagnostics для перевірки апаратного з'єднання між комп'ютерами і висновку зведень про комп'ютер,

NET DIAGNOSTICS [/NAME | /STATUS]

/NAME Ім'я сервера діагностики, необхідне для усунення конфліктів при використанні NET DIAG одночасно декількома користувачами. Цей параметр можна використовувати лише при використанні протоколу NetBIOS.

/STATUS Комп'ютер, про який необхідно одержати повідомлення.

**********

C:\>net name
Ім'я
---
A4748-09
A4748-09$
TEST
Команда виконана успішно.

**********

**NET HELP** — Висновок зведень про команди і повідомлення NET.

команда /?

NET HELP [суфікс]

NET HELP код помилки

Команда визначає команду Microsoft NET, зведення про яку необхідно одержати.

Суфікс дає інше слово команди, що цікавить, наприклад, суфікс команди NET VIEW — слово VIEW.

Код помилки — задає номер повідомлення про помилку, яка цікавить.

Щоб одержати короткий опис усіх команд Microsoft NET, уведіть команду NET HELP без параметрів.

**********

C:\>net help computer

Синтаксис даної команди:

**NET COMPUTER** — ця команда додає /видаляє комп'ютери з бази даних домену і використовується тільки на серверах Windows NT Server.

NET COMPUTER \\ім'я_комп'ютера {/ADD | /DEL}

Ім'я комп'ютера Вказує комп'ютер, якому необхідно додати до домену або видалити з домену.

/ADD — додає зазначений комп'ютер до домену.

/DEL — видаляє зазначений комп'ютер з домену.

**********

**NET INIT** — завантаження протоколу і драйверів мережної плати без їхньої прив'язки до диспетчера протоколів. Ця команда може знадобитися при використанні драйверів сторонніх виготовлювачів. Прив'язка драйверів виконується командою NET START NETBIND.

NET INITIALIZE [/DYNAMIC]

/DYNAMIC Динамічне завантаження диспетчера протоколів. Вона зручна при роботі з мережами сторонніх виготовлювачів, наприклад Banyan(R) VINES, і служить для усунення неполадок з пам'яттю.

## *Завдання*

Вивчите алгоритми роботи вбудованих засобів моніторингу мережі за описом, викладеним у внутрішній допомозі цих засобів. Сконфігуруйте використовувані засоби моніторингу мережі для повноцінного використання і видачі повного звіту про параметри і характеристики мережі. Використовуючи убудовані засоби моніторингу мережі, досліджуйте можливості керування мережею. Одержите перелік параметрів і характеристик мережі за заданим варіантом, використовуючи вбудовані засоби моніторингу мережі.

Список використовуваних убудованих засобів моніторингу: **netstat, nbtstat, arp, ping, tracert, net, netsh, nslookup, ntdsutil, route, winmsd, at, finger, hostname, ipconfig, lpr, mmc, mrinfo, rcp, rsh.**

Використання убудованих засобів моніторингу регламентується індивідуальним завданням, у якому визначений набір засобів. Крім того, для кожного студента **обов'язковим** є дослідження наступних засобів: **ntdsutil, route, winmsd, at, finger, hostname, ipseccmd, lpr, mmc, mrinfo, rcp, rsh.**

Бекас Б. О.

*Варіанти рішення завдання*

| Команда / № варіанта | ping | netstat | tracert | ipconfig | net config | net print | nslookup | nbtstat | arp | netsh |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | + | + | + | + | + | | | | | |
| 2 | + | + | + | + | | + | | | | |
| 3 | + | + | + | + | | | + | | | |
| 4 | + | + | + | + | | | | + | | |
| 5 | + | + | + | + | | | | | + | |
| 6 | + | + | + | + | | | | | | + |
| 7 | + | + | + | + | + | | | | | |
| 8 | + | + | + | + | | + | | | | |
| 9 | + | + | + | + | | | + | | | |
| 10 | + | + | + | + | | | | + | | |
| 11 | + | + | + | + | | | | | + | |
| 12 | + | + | + | + | | | | | | + |
| 13 | + | + | + | + | + | | | | | |
| 14 | + | + | + | + | | + | | | | |
| 15 | + | + | + | + | | | + | | | |
| 16 | + | + | + | + | | | | + | | |
| 17 | + | + | + | + | | | | | + | |
| 18 | + | + | + | + | | | | | | + |
| 19 | + | + | + | + | + | | | | | |
| 20 | + | + | + | + | | + | | | | |
| 21 | + | + | + | + | | | + | | | |
| 22 | + | + | + | + | | | | + | | |
| 23 | + | + | + | + | | | | | + | |
| 24 | + | + | + | + | | | | | | + |
| 25 | + | + | + | + | + | | | | | |
| 26 | + | + | + | + | | + | | | | |
| 27 | + | + | + | + | | | + | | | |
| 28 | + | + | + | + | | | | + | | |
| 29 | + | + | + | + | | | | | + | |
| 30 | + | + | + | + | | | | | | + |

## *Контрольні запитання*

1.Визначите мету використання убудованих засобів моніторингу мережі.
2.Опишіть процес використання убудованих ЗММ.
3.Дайте визначення моніторингу мережі.
4.У чому полягають принципові відмінності убудованих засобів моніторингу мережі.
5.Області використання убудованих ЗММ.
6.Назвіть основні принципи побудови убудованих ЗММ.
7.Приведіть класифікацію убудованих ЗММ.