ЛАБОРАТОРНА РОБОТА №1

Тема: “Вивчення роботи мережевих утиліт операційної системи”

Мета: Вивчити синтаксис та принципи використання основних мережевих утиліт, які застосовуються в операційних системах Windows та Linux для управління, контролю та зміни мережевих ресурсів та оточення.

В операційних системах для визначення мережевої конфігурації вузла (персонального комп’ютера, сервера, комутаційного обладнання тощо), його інтерфейсів, а також для налаштування та зміну параметрів мережі використовують програмне забезпечення — утиліти. З розвитком операційних систем змінювалась і функціональність утиліт, стало можливим отримати деякі параметри або виконати одні і ті самі налаштування за допомогою різних утиліт, з’явились утиліти з гіпернабором можливостей, наприклад, ip-пакет в Unix системах. Спектр можливостей утиліт та їх різноманіття у різних версіях та клонах операційних систем потребує інтенсивного самостійного вивчення як для тих, хто буде адмініструвати комп’ютерні мережі, так і для тих, хто буде створювати програмне забезпечення, що їх використовує. Тому в лабораторній роботі розглядається певний базовий набір утиліт та деякі приклади їх використання, що дозволяють отримати інформацію про наявну мережеву конфігурацію вузла та його оточення у мережі.

Утиліта ifconfig (операційні системи Linux та UNIX) використовується для отримання інформації по мережевим інтерфейсам комп’ютера та конфігурування їх параметрів. Також вона може використовуватись для перевизначення адреси мережевого інтерфейсу. В операційних системах Windows подібну функцію має утиліта ipconfig.

Якщо не вказуються опції, то утиліта ifconfig виводить поточну конфігурацію мережевих інтерфейсів. Якщо необхідно вивести мережеву конфігурацію певного інтерфейсу, то в команді вказується його ім’я. Наприклад, для wi-fi адаптеру за командою ifconfig wlo1 було отримано:

```
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.165  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::667f:65e2:8ebb:5fcb  prefixlen 64  scopeid 0x20<link>
        ether 24:77:03:51:bd:e8  txqueuelen 1000  (Ethernet)
        RX packets 12832  bytes 9166196 (9.1 MB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 6060  bytes 807819 (807.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

де wlo1 вказує на інтерфейс; flags вказує на прапорці, що встановлені для інтерфейсу — UP (увімкнено) BROADCAST (може приймати пакети широкомовлення) RUNNING (має підключення до мережі) MULTICAST (може приймати групові пакети) PROMISC (працює у нерозбірливому режимі); mtu —

розмір максимального блоку; inet — IP-адреса інтерфейсу; netmask — мережева маска або маска підмережі; broadcast — IP-адреса для пакетів широкомовлення; inet6 — IP-адреса версії 6; prefixlen — довжина префіксу для IP версії 6; scopeid — вказує на зв'язок із пристроєм; ether — MAC-адреса пристрою; txqueuelen — максимальна довжина черги; RX — вказує на кількість прийнятих пакетів та байт; TX — вказує на кількість переданих пакетів та байт.

Утиліту ping призначено для тестування зв'язку у комп'ютерній мережі. Утиліта генерує, так званні, пакети відлуння та відправляє їх до вузла призначення. Якщо вузол в мережі існує, він у робочому стані та його налаштування працездатні, то у відповідь прийде відповідь на відлуння. Утиліта ping має певну кількість різних аргументів та опцій, що також дозволяє її використовувати до діагностики зв'язку. Корисно застосовувати опцію `-c` для задавання кількості пакетів відлуння, що генерується (за замовчуванням, пакети генеруються безперервно, поки не буде натиснуто одночасно клавіші Ctrl-C). Опція `-i` дозволяє задавати інтервал часу між пакетами (за замовчуванням 1 секунда). Опція `-I` дозволяє задати конкретний інтерфейс, із якого будуть відправлятись пакети (має сенс, якщо в системі декілька мережевих інтерфейсів). `-S` дозволяє задати деяку конкретну IP адресу джерела пакетів відлуння. Опція `-f` використовується системними адміністраторами для одночасного відправлення множини пакетів для перевірки стабільності рроботи інтерфейсу (як правило використовується разом з опцією `-c`). Нижче наведено простий приклад використання утиліти ping:

```
vgorbenko@vgorbenko-HP-EliteBook-8460p:~$ ping 10.1.100.31
PING 10.1.100.31 (10.1.100.31) 56(84) bytes of data.
64 bytes from 10.1.100.31: icmp_seq=1 ttl=62 time=12.8 ms
64 bytes from 10.1.100.31: icmp_seq=2 ttl=62 time=9.30 ms
64 bytes from 10.1.100.31: icmp_seq=3 ttl=62 time=3.06 ms
^C
--- 10.1.100.31 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.060/8.411/12.871/4.055 ms
```

У команді використано певну IP-адресу 10.1.100.31 локальної мережі. Кожний рядок відлуння вказує на довжину пакету відлуння — 64 байти, номер пакету у послідовності, значення TTL для прийнятого пакету та час, що пройшов між відправленням та прийняттям пакету.

Утиліта route використовується для управління таблицею маршрутизації. Таблиця маршрутизації дозволяє встановлювати шляхи відправлення пакетів як до сегментів локальної мережі, так і до певних мереж глобальної мережі Інтернет, а також встановлювати пріоритетність використання інтерфейсів та шляхів при пересиланні пакетів. У найпростішому випадку утиліта route використовується без опцій і дозволяє отримати наявну таблицю маршрутизації:

```
vgorbenko@vgorbenko-HP-EliteBook-8460p:~$ route
Таблица маршутизации ядра протокола IP
Destination Gateway Genmask Flags Metric Ref Use Iface
default         router.asus.com 0.0.0.0         UG    600    0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```

Усю інформацію розбито на декілька стовпчиків, що залежить від використаних опцій. Стовпчик Destination вміщує певні елементи мережі — вузли, мережеві сегменти, інтерфейси. Стовпчик Gateway вміщує адресу шлюзу для пересилання пакетів (0.0.0.0 — за замовчуванням). Стовпчик Genmask — маски підмереж, що вказують на об’єм елементу мережі. У стовпчику Flags прапорець U вказує, що шлях активний, а прапорець G, що цей елемент мережі є основним шлюзом. Metric вказує на пріоритетність маршруту — найменше значення вказує на найвищий пріоритет. Ref вказує на кількість посилань на певний маршрут, а Use — на інтенсивність його використання. Iface вказує на зв’язок з певним інтерфейсом.

Утиліту traceroute часто використовують для визначення маршруту від одного вузла комп’ютерної мережі до іншого. Для цього створюються ICMP-пакети з адресою вузла призначення. Суттєвим є те, що створювані пакети мають послідовно збільшуваний за значенням параметр TTL (time to live). Цей параметр зазвичай вказує на максимальну кількість візлув-маршрутизаторів, що дозволяється пройти пакету. Будь який вузол мережі, коли отримує пакет, що має бути переправлений на інший вузол, обов’язково зменшує значення TTL на 1. Якщо TTL стає рівним 0, то такий пакет далі не пересилається, а на вузол, що його відправив, повертається ICMP-повідомлення «time exceeded in transit». Утиліта traceroute фіксує адрес цього маршрутизатора, а також проміжок часу між відправленням пакету та отриманням відповіді. Саме ця інформація і виводиться на термінал. Після цього traceroute повторює створення і відправлення пакетів, але значення TTL збільшується на 1, що дозволяє “проскочити” вузли-маршрутизатори, які вже відповіли, і досягти наступний за маршрутом. Якщо послідовно відправляти на вузол-призначення пакети, що відрізняються значенням TTL на 1, то отримаємо пакети з ICMP-повідомленням «time exceeded in transit» від усіх проміжних вузлів-маршрутизаторів.

```
vgorbenko@vgorbenko-HP-EliteBook-8460p:~$ traceroute www.yahoo.com
traceroute to www.yahoo.com (87.248.98.8), 30 hops max, 60 byte packets
 1  router.asus.com (192.168.1.1)  2.954 ms  2.890 ms  2.841 ms
 2  herr.znu.edu.ua (10.1.10.1)  2.797 ms  2.767 ms  2.992 ms
 3  212.111.202.5 (212.111.202.5)  5.937 ms  5.922 ms  9.064 ms
 4  fe0-1-701.zpr0.uran.ua (212.111.192.233)  15.632 ms  15.639 ms  15.594 ms
 5  ae2-236.RT.NTL.KIV.UA.retn.net (87.245.237.16)  15.546 ms  15.508 ms  15.466 ms
 6  ae2-7.RT.IRX.VIE.AT.retn.net (87.245.233.137)  47.133 ms  40.517 ms  34.958 ms
 7  193.203.0.242 (193.203.0.242)  34.980 ms 193.203.0.42 (193.203.0.42)  34.958 ms  34.935 ms
 8  UNKNOWN-188-125-89-X.yahoo.com (188.125.89.53)  53.516 ms  53.498 ms  53.480 ms
 9  UNKNOWN-188-125-89-X.yahoo.com (188.125.89.53)  53.370 ms  53.754 ms xe-4-2-0.pat1.tc2.yahoo.com (66.196.65.210)  53.643 ms
10  ge-4-2-0.pat1.the.yahoo.com (66.196.65.208)  53.683 ms  53.677 ms UNKNOWN-66-196-65-X.yahoo.com (66.196.65.217)  69.698 ms
11  UNKNOWN-66-196-65-X.yahoo.com (66.196.65.217)  69.751 ms  78.933 ms  78.896 ms
12  eth-2-5.bas1-1-prd.ir2.yahoo.com (217.146.186.79)  78.825 ms et-1-1-0.msr1.ir2.yahoo.com (66.196.65.19)  82.150 ms  70.400 ms
13  eth-1-5.bas1-1-prd.ir2.yahoo.com (217.146.185.176)  79.827 ms media-router-fp2.prod1.media.vip.ir2.yahoo.com (87.248.98.8)  66.214 ms
```

На кінцевому вузлі пакет з TTL=1 не відкидається та ICMP-повідомленням «time exceeded in transit» не створюється. Для визначення того, що вузол-призначення був досягнутий, усі пакети відправляються на порт, який не використовується. Його номер дорівнює 33434 + (максимальна кількість транзитних вузлів) - 1. Після отримання такого пакету вузол-призначення повертає ICMP-

повідомлення про помилку «порт недоступний». Саме це дозволяє визначити, що вузол-призначення досягнуто.

Команда netstat входить до стандартного набору мережевих утиліт операційних систем Windows, Linux, UNIX. За її допомогою можна отримати інформацію про підключення до комп'ютерної мережі, статистику відповідно до кожного інтерфейсу, таблиці маршрутизації, masquerade, multicast та інше.

Визначення активних підключень до комп'ютерної мережі виконується наступним чином:

команда **netstat -a** дозволяє визначити всі підключення

```
# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        *:*                     LISTEN
udp6       0      0 fe80::20c:29ff:fe68:ntp [::]:*

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     20492    /var/run/mysqld/mysqld.sock
unix  2      [ ACC ]     STREAM     LISTENING     23323    /var/run/php5-fpm.sock
```

команда **netstat -at** дозволяє визначити TCP підключення

```
# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
```

команда **netstat -au** дозволяє визначити UDP підключення

```
# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:domain        *:*
udp        0      0 *:bootpc                *:*
udp6       0      0 fe80::20c:29ff:fe68:ntp [::]:*
```

Для визначення портів, що знаходяться у стані прослуховування, використовується ключ -l. Наприклад: команда **netstat -lt** використовується для визначення TCP-портів, що знаходяться у стані прослуховування.

Для отримання статистики по кожного протоколу використовується команда **netstat -s**, наприклад:

```
# netstat -s
Ip:
    11150 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    11149 incoming packets delivered
    11635 requests sent out
Icmp:
    13791 ICMP messages received
    12 input ICMP message failed.
Tcp:
    15020 active connections openings
    97955 passive connection openings
    135 failed connection attempts
Udp:
    2841 packets received
    180 packets to unknown port received.
.....
```

Для отримання PID та імені процесу за форматом «PID/Program Name» netstat використовується з опцією -p, яку можна поєднувати з іншими опціями. Як правило вона використовується при налагоджені для визначення того, яка програма використовує який порт. Наприклад:

```
# netstat -pt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 org-ru-putty.vm.udf:www 52-106.plus.kerch:55723 ESTABLISHED 9486/nginx: worker
tcp        0      0 org-ru-putty.vm.udf:www 52-106.plus.kerch:55757 ESTABLISHED 9486/nginx: worker
```

Для безперервного виводу інформації netstat використовується опція -c. Наприклад:

```
# netstat -c
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 org-ru-putty.vm.udf:www 182.131.74.202:59933    FIN_WAIT2
tcp        0      0 org-ru-putty.vm.udf:www 182.131.74.202:63761    FIN_WAIT2
tcp        0      0 org-ru-putty.vm.udf:www 92-181-66-102-irk.:4585 ESTABLISHED
^C
```

Перервати вивід можна одночасним натисканням CTRL-C.

Список мережевих інтерфейсів отримується за допомогою команди **netstat -i**, а більш розширена інформація про інтерфейси отримується за допомогою: **netstat -ie**. Наприклад:

```
# netstat -ie
Kernel Interface table
eth0      Link encap:Ethernet  HWaddr 00:0c:29:68:4c:a4
          inet addr:192.168.128.134  Bcast:192.168.128.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe68:4ca4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24278 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33203025 (33.2 MB)  TX bytes:665822 (665.8 KB)
          Interrupt:19 Base address:0x2000
```

Взагалі можна використати набір із декількох опцій для отримання певної визначеної інформації:

```
# netstat -lnptux
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      9614/nginx
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      601/sshd
udp        0      0 8.8.4.4:123             0.0.0.0:*                           574/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           574/ntpd
udp        0      0 0.0.0.0:123             0.0.0.0:*                           574/ntpd
Active UNIX domain sockets (only servers)
Proto RefCnt Flags    Type       State    I-Node   PID/Program name  Path
unix  2      [ ACC ]  STREAM   LISTENING  4233     826/python        /var/run/fail2ban/fail2ban.sock
unix  2      [ ACC ]  STREAM   LISTENING  8122     2561/mysqld       /var/run/mysqld/mysqld.sock
unix  2      [ ACC ]  STREAM   LISTENING  160413   7301/php-fpm.conf /var/run/php5-fpm.sock
```

Універсальною консольною утилітою є ip, реалізація якої доступна в операційних системах клону Linux та UNIX. Утиліта ip об'єднує можливості ifconfig, arp, route та деяких інших утиліт та команд для управління мережею Linux.

Утиліта ip має значну функціональність та дозволяє визначати властивості підключення до комп'ютерної мережі, IP-адреси інтерефейсів та arp таблицю, налаштовувати політики маршрутизації, змінювати записи arp таблиці та деякі параметри стеку TCP/IP. Значна кількість функцій потребує дещо специфічного її використання. Синтаксис командного рядку цієї утиліти виглядає наступним чином:

ip [опції] об'єкт команда [параметри]

Опції є глобальними налаштуваннями, що впливають на роботу всієї утиліти незалежно від інших аргументів та можуть не задаватись. Об'єктом у командному

рядку виступає об’єкт або пристрій, для якого виконується команда. Командою є певна дія з об’єктом, якій можуть надаватись деякі параметри.

Основними опціями є: -V (отримати інформацію про утиліту та її версію); -h (виводити інформацію у зручному для людини форматі); -b (читати команди із наданого файлу); -s (виводити статистичну інформацію); -f (специфікує сімейство протоколів, що буде використовуватись); -o (вказує на вивід кожного запису з нового рядку); -r (вказує на необхідність використання резолверу системних імен).

Об’єктами у командному рядку утиліти ip можуть бути: address (мережева адреса інтерфейсу); link (фізичний мережевий пристрій); monitor (моніторинг стану пристроїв); neighbour (управління ARP); route (управління маршрутизацією); rule (правила маршрутизації); tunnel (тунелювання IP), а також інші.

Під час введення ім’я об’єкту може бути скорочено до однієї або до кількох літер, у залежності від однозначності. Наприклад, команду ip address show можна записати як ip a show.

Серед типових команд, що можуть виконуватись над об’єктами є: add, change, del або delete, flush, get, list або show, monitor, replace, restore, save, set, а також update. Для отримання переліку команд, що виконуються для певного об’єкту, слід задати: ip об’єкт help

Наприклад, ip link help виводить довідку за командами для об’єкту link.

Якщо команду не задано, то за замовчуванням виконується команда show.

Параметри залежать від об’єкта та вказаної команди. Найчастіше використовуються наступні: dev ім’я_пристрою; up (увімкнути); down (вимкнути); llarrr MAC-адреса; initcwnd розмір вікна перевантаження TCP при ініціалізації; window розмір вікна TCP; cwnd розмір вікна перевантаження TCP; type тип; via (підключитись до роутеру); default маршрут за замовчуванням; blackhole - маршрут "чорна дірка" (відкидає пакети і не посилає ICMP-повідомлення про недоступність); prohibit - маршрут "заборони" (відкидати пакети та повертати ICMP повідомлення про заборону доступу); unreachable - маршрут "недосяжний" (відкидати пакети та відправляти ICMP пакети про недосяжність вузла).

Наведемо деякі приклади використання утиліти ip.

ip link show — показує стан усіх мережевих інтерфейсів.

ip link show eth0 — показує стан інтерфейсу з ім'ям eth0.

ip link list up — показує стан усіх увімкнених мережевих інтерфейсів.

ip link set eth1 up — включає мережевий інтерфейс з ім'ям eth1.

ip link set eth1 down — виключає eth1.

ip neigh show — показує усі записи ARP

ip nei add 1.1.1.13 lladdr AA:BB:CC:DD:EE:FF dev eth0 — додає до ARP-таблиці запис для певної IP адреси, де 1.1.1.13 — IP-адреса, AA:BB:CC:DD:EE:FF — MAC-адреса, eth0 — мережевий пристрій.

ip address show - показати усі IP-адреси та їх інтерфейси

ip a l permanent — показати тільки статичні IP-адреси

ip a l dynamic — показати тільки динамічні IP-адреси

ip addr add 1.1.1.13/24 dev eth0 — задати IP-адресу для інтерфейсу eth0

ip addr del 1.1.1.13/24 dev eth0 — видалити IP-адресу інтерфейсу eth0

ip add flush dev eth0 - видалити усі IP-адреси інтерфейсу eth0

З точки зору адміністрування комп'ютерних мереж важливою функцією утиліти ip є можливість налаштовувати мережеві маршрути. Таблиці маршрутизації для утілити ip ідентифікуються за номером (від 1 до 255). За замовчуванням використовується таблиця маршрутизації 254. Для відображення усіх маршрутів таблиці маршрутизації використовується командний рядок: ip r sh.

ip route show table nnn — показує усі маршрути з таблиці 255

ip route get 10.10.20.0/24 — показує маршрут до цієї підмережі

ip route get 10.10.20.0/24 from 192.168.12.9 — показує маршрут до заданої підмережі від вказаного інтерфейсу

ip route add 10.10.20.0/24 via 192.168.50.100 — створює маршрут до заданої підмережі через інтерфейс за вказаною IP-адресою

ip route delete 10.10.20.0/24 - видаляє маршрут до підмережі

ip route del 10.10.20.0/24 via 192.168.50.100 - видаляє маршрут до підмережі через заданий інтерфейс

ip route add default via 192.168.50.100 — створює маршрут за замовчуванням

ip route add 10.10.20.0/24 dev eth0 — створює маршрут до вказаної підмережі через вказаний інтерфейс

ip route add table nnn 10.10.20.0/24 dev eth0 — додає до певної таблиці маршрутизації вказаний маршрут

ip route add blackhole 10.10.20.0/24 dev eth0 - створює маршрут типу blackhole

ip route add unreachable 10.10.20.0/24 dev eth0 — створює маршрут типу unreachable

ЗАВДАННЯ

1. Для виконання роботи використовуйте програми “Командний рядок” (ОС Windows) та “Термінал” (ОС Linux).
2. Вивчить призначення, синтаксис та опції (ключі) наступних мережевих утиліт:
   - hostname;
   - ipconfig (для Windows) та ifconfig (для Linux);
   - ping;
   - arp;
   - netstat;
   - route;
   - tracert (для Windows) та traceroute (для Linux);
   - ip (для Linux).
3. За допомогою hostname визначте ім’я комп’ютера.
4. Використовуйте ipconfig (для Windows) та ifconfig (для Linux) для визначення мережевих інтерфейсів комп’ютера, за яким виконується робота. З отриманої інформації визначте IP-адресу, мережеву маску, адресу широкомовлення, MAC-адресу та кількість прийнятої та переданої інформації.
5. Використайте команду ping для наступних адрес:
   - 10.1.100.31 (в мережі ЗНУ)

- www.znu.edu.ua
- www.ukr.net

6. Виконайте команду arp без задавання опцій та окремо з опціями -a та -n. Порівняйте отримані результати.
7. Для виконання команди netstat використовуйте наступні опції: -r, -i, -g, -s, -v, -p, -l.
8. Виконайте команду route без задавання опцій та з опцією -n.
9. Виконайте команди tracert (для Windows) та traceroute (для Linux) для наступних адрес:
   - 10.1.100.31 (в мережі ЗНУ)
   - www.znu.edu.ua
   - www.ukr.net
10. Використовуючи утиліту ip виконайте завдання пунктів 4, 6, 8 для комп'ютера, що працює під операційною системою Linux. Порівняйте з отриманими результатами за допомогою утиліт, вказаних у цих пунктах.
11. Підготуйте звіт, в який занесіть результати за пунктами 3-10.

Контрольні запитання

1. Що таке утиліти?
2. Для чого використовуються утиліти?
3. За допомогою яких утиліт можна визначити IP-адресу комп'ютера?
4. Як можна визначити існування (наявність підключення до мережі) комп'ютера з певною IP-адресою?
5. Що таке TTL?
6. Для чого призначено таблицю маршрутизації?
7. Яку інформацію містить ARP-таблиця?
8. Як визначити маршрут (проміжні вузли-маршрутизатори) до певного вузлу-призначення?
9. Що дозволяє визначити утиліта netstat ?
10. Який загальний синтаксис командного рядку використання утиліти ip?