ВБУДОВАНІ ЗАСОБИ АНАЛІЗУ КОНФІГУРАЦІЇ І СТАНУ МЕРЕЖІ НА ОСНОВІ TCP/IP

1 Мета роботи

1. Аналіз вбудованих засобів діагностики мережі на базі TCP/IP та придбання практичних навичок діагностики.

2 Ключові положення

2.1 Основні утиліти, які використовуються для діагностики мереж на базі TCP/IP

Мережа Інтернет – найбільша і єдина у своєму роді мережа у світі. Серед глобальних мереж вона займає унікальне положення. Правильніше її розглядати як деяку надмережу – об'єднання багатьох мереж, що зберігають самостійне значення. Дійсно, Інтернет не має ні чітко вираженого власника, ні національної приналежності. Будь-яка мережа може мати зв'язок з Інтернет і, отже, розглядатися як її частина, якщо в ній використовуються прийняті для Інтернет протоколи TCP/IP (*Transmission Control Protocol / Internet Protocol)* або є конвертори в протоколи TCP/IP. TCP/IP – це промисловий стандарт стека протоколів, розроблений для глобальних мереж. До складу сімейства входять протоколи UDP, ARP, ICMP, TELNET, FTP і багато інших.

В міру прояву нестабільної роботи окремих вузлів мережі на основі TCP/IP найбільш суттєвим питанням стає можливість її моніторингу й аналізу . Одним з методів діагностування мереж є утиліти (короткі програми), що входять до складу пакета програмного забезпечення протоколу TCP/IP. Основними утилітами, використовуваними в сучасних операційних системах (ОС), є:

- **Ping –** процедура, що служить для перевірки працездатності каналів і вузлів.
- **Tracert** (Traceroute) **–** відображає адреси всіх маршрутизаторів на шляху від клієнта до вилученого хоста.
- **Nslookup –** перевіряє правильність перетворення імен в адреси і навпаки.
- **Netstat –** відображає статистику і поточні з'єднання по протоколу TCP/IP.

- **Ipconfig** – показує настроювання протоколу IP. За замовчуванням відображається тільки IP-адреса, маска підмережі і стандартний шлюз для кожного підімкненого адаптера, для якого виконана прив'язка до TCP/IP.

- **Winipcfg –** утиліта, аналогічна Ipconfig**,** але працююча не в режимі командного рядка, а шляхом застосування графічного інтерфейсу. Її можна використовувати тільки в ОС Windows 98.

- **Finger –** служить для одержання інформації про користувача вилученої машини.

- **Telnet –** використовує стандартний протокол Інтернет для одержання термінального доступу до вилученої машини.

- **Whois –** здійснює пошук у базі даних Whois інформації про реєстрацію доменного імені мережі, телефонні номери користувачів, e-mail адреси, поштові адреси тощо.

- **Net Time –** синхронізує системний час з еталонним сервером.

2.2 Утиліти ping і tracert

Утиліти ping і tracert (traceroute) , використовувані незалежно або разом, визначають шлях, яким пакет прямує по мережі до адресата, а також час, за який він його досягає.
Ґрунтуючись на результатах тестів ping і tracert, можна визначити місце, де відбувся збій.

Утиліта Ping за допомогою відправлення повідомлень з луною-запитом по протоколу ICMP (Internet Control Message Protocol) перевіряє з'єднання на рівні протоколу IP з іншим комп'ютером, який підтримує TCP/IP. Після кожної передачі виводиться відповідне повідомлення з луною-відповіддю. Команда ping, запущена без параметрів, виводить довідку.

Синтаксис
ping [**-t**] [**-a**] [**-n** *лічильник*] [**-l** *розмір*] [**-f**] [**-i** *TTL*] [**-v** *тип*] [**-r** *лічильник*]
[**-s** *лічильник*] [{**-j** *список_вузлів* | **-k** *список_вузлів*}] [**-w** *інтервал*]
[*ім'я_кінцевого_комп'ютера*]

Параметри
Параметри утиліти Ping подані в таблиці 2.1

Таблиця 2.1 – Параметри утиліти Ping

Ідентифі-Катор пара-метра	Призначення
1	2
-t	Задає для команди ping відправлення повідомлень з луною-запитом до точки призначення до тих пір, поки команда не буде перервана. Для переривання команди і виводу статистики необхідно натиснути комбінацію клавиш CTRL-BREAK. Для переривання команди ping і виходу з неї необхідно натиснути клавіші CTRL-C
-a	Задає дозвіл імені вузла по IP-адресі призначення. У випадку успішного виконання виводиться ім'я відповідного вузла
-n *лічиль-ник*	Задає число повідомлень з луною-запитом, що відправляються. За замовчуванням — 4
-l *розмір*	Задає довжину (у байтах) поля даних у відправлених повідомленнях з луною-запитом. За замовчуванням — 32 байти. Максимальний *розмір* — 65527
-f	Задає відправлення повідомлень з луною-запитом із прапором «Don't Fragment» у IP-заголовку, який встановлюється на 1. Повідомлення з луною-запитом не фрагментуються маршрутизаторами на шляху до місця призначення. Цей параметр корисний для усунення проблем, що постають з максимальним блоком даних (Maximum Transmission Unit) для каналу
-i *TTL*	Для повідомлень з луною-запитом, що відправляються , задає значення поля TTL (Time to Live) у IP-заголовку. За замовчуванням береться значення TTL, встановлене за замовчуванням для вузла. Наприклад, для вузлів Windows XP це значення звичайно дорівнює 128. Максимальне значення *TTL* — 255
-v *тип*	Для повідомлень з луною-запитом, що відправляються , задає значення поля типу служби (TOS) у IP-заголовку. *Тип* — це десяткове значення від 0 до 255. За замовчуванням це значення дорівнює 0
-r *лічиль-ник*	Задає параметр запису маршруту (Record Route) у IP-заголовку для запису шляху, по якому проходить повідомлення з луною-запитом і відповідне йому повідомлення з луною-відповіддю. Кожен перехід (проміжний маршрутизатор) у шляху використовує параметр запису маршруту. По можливості значення *лічильника* задається

	рівним або більшим, ніж кількість переходів між джерелом і місцем призначення. Параметр *лічильник* має значення від 1 до 9
-s *лічиль-ник*	Указує варіант штампа часу Інтернету (Internet Timestamp) у заголовку IP для запису часу прибуття повідомлення з луною-запитом і відповідного йому повідомлення з луною-відповіддю для кожного переходу. Параметр *лічильник* має значення від 1 до 4

Продовження таблиці 2.1

1	2
-j *список_ вузлів*	Для повідомлень з луною-запитом указує використання параметра вільної маршрутизації в IP-заголовку з набором проміжних точок призначення, зазначеним у *списку вузлів*. При вільній маршрутизації послідовні проміжні точки призначення можуть бути розділені одним або декількома маршрутизаторами. Максимальне число адрес або імен у списку вузлів — 9. Список вузлів — це набір IP-адрес (у точково-десятковій нотації), розділених пробілами
-k *список_ вузлів*	Для повідомлень з луною-запитом указує використання параметра строгої маршрутизації в IP-заголовку з набором проміжних точок призначення, зазначеним у *списку вузлів*. При строгій маршрутизації наступна проміжна точка призначення повинна бути доступною напряму (вона повинна бути сусідньою в інтерфейсі маршрутизатора). Максимальне число адрес або імен у списку вузлів дорівнює 9. Список вузлів — це набір IP-адрес (у точково-десятковій нотації), розділених пробілами
-w *інтервал*	Визначає в мілісекундах час чекання одержання повідомлення з луною-відповіддю, відповідного повідомленню з луною-запитом. Якщо повідомлення з луною-відповіддю не отримано в межах заданого інтервалу, то видається повідомлення про помилку "Request timed out". Інтервал за замовчуванням дорівнює 4000 (4 секунди)
ім'я_кін-цевого_ комп'ю-тера	Задає точку призначення, ідентифіковану IP-адресою або ім'ям вузла
-?	Відображає довідку в командному рядку

Наведений нижче приклад містить результати роботи команди ping:

C:\>ping -l 64 www.nnm.ru
Обмін пакетами з www.nnm.ru [213.248.7.66] по 64 байт:

Відповідь від 213.248.7.66: число байт=64 год=491мс TTL=44
Відповідь від 213.248.7.66: число байт=64 год=711мс TTL=44
Відповідь від 213.248.7.66: число байт=64 год=831мс TTL=44
Відповідь від 213.248.7.66: число байт=64 год=471мс TTL=44

Статистика Ping для 213.248.7.66:
Пакетів: послано = 4, отримано = 4, загублено = 0 (0% втрат),
Приблизний час передачі і прийому:
найменший = 471мс, найбільший = 831мс, середній = 626мс

Утиліта Tracert визначає шлях до точки призначення за допомогою посилання в точку призначення лун-повідомлень протоколу ICMP з постійним збільшенням значень терміну життя (TTL) у заголовках пакетів. Виведений шлях — це список найближчих інтерфейсів маршрутизаторів, що знаходяться на дорозі між вузлом джерела і точкою призначення. Ближчий інтерфейс являє собою інтерфейс маршрутизатора, що є найближчим до вузла відправника на шляху. Запущена без параметрів, команда tracert виводить довідку.

Синтаксис
tracert [**-d**] [**-h** *максимальне_число_переходів*] [**-j** *список_вузлів*] [**-w** *інтервал*] [*ім'я_кінцевого_комп'ютера*]

Параметри
Параметри утиліти Tracert подані в таблиці 2.2

Таблиця 2.2 – Параметри утиліти Tracert

Ідентифікатор параметра	Призначення
-d	Запобігає здійсненню перетворення IP-адрес проміжних маршрутизаторів в імена. Збільшує швидкість виводу результатів команди tracert
-h *максимальне_чи-*	Задає максимальну кількість переходів на шляху при пошуку кінцевого об'єкта. Значення за замовчуванням дорівнює 30

сло_переходів	
-j *список_вузлів*	Для повідомлень з луною-запитом указує використання параметра вільної маршрутизації в заголовку IP з набором проміжних місць призначення, зазначених у *списку вузлів*. При вільній маршрутизації успішні проміжні місця призначення можуть бути розділені одним чи декількома маршрутизаторами. Максимальне число адрес або імен у списку — 9. *Список вузлів* представляє набір IP-адрес (у точково-десятковій нотації), розділених пробілами
-w *інтервал*	Визначає в мілісекундах час чекання для одержання лун-відповідей протоколу ICMP або ICMP-повідомлень про час, який минув, що відповідають даному повідомленню луни-запиту. Якщо повідомлення не отримане протягом заданого часу, виводиться зірочка (*). Таймаут за замовчуванням 4000 (4 секунди)
ім'я_кінцевого_комп'ютера	Задає точку призначення, зазначену IP-адресою або ім'ям вузла
-?	Відображає довідку в командному рядку

Примітка.

Кожен маршрутизатор, через який проходить шлях, зобов'язаний перед подальшим пересиланням пакета зменшити значення поля TTL у його заголовку на 1. Фактично, TTL — лічильник вузлів. Передбачається, що коли параметр TTL дорівнює 0, маршрутизатор посилає системі-джерелу повідомлення ICMP про час, який минув.

Команда tracert визначає маршрут, посилаючи перший луна-запит з полем TTL, яке дорівнює 1. Далі, значення цього поля збільшуються на одиницю для кожного наступного луна-пакета, що відправляється, до тих пір, поки кінцевий вузол дасть відповідь чи поки не буде досягнуте максимальне значення поля TTL. Максимальна кількість переходів за замовчуванням дорівнює 30 і може бути змінена за допомогою параметра -h. Шлях визначається з аналізу повідомлень ICMP про час, що минув, отриманих від проміжних маршрутизаторів, і лун-відповідей точки призначення. Однак деякі маршрутизатори не посилають повідомлень про час, що минув, для пакетів з нульовими значеннями TTL і тому їх не бачить команда tracert. У цьому випадку для переходу відображається ряд зірочок (*).

Приклад:

C:\>tracert -h 10 www.aport.ru

Трасування маршруту до aport.ru [194.67.18.8]
з максимальним числом переходів10:

```
  1   120 ms   120 ms   121 ms  max3.farlep.net [213.130.1.251]
  2   130 ms   120 ms   120 ms  teller-10mb-gw.farlep.net [213.130.1.254]
  3   120 ms   120 ms   791 ms  core-0-0FE.farlep.net [213.130.0.28]
  4      141  ms      140  ms      160  ms     core-0-pa4T-1-0-201fr.kiev.farlep.net
[213.130.0.102]
  5   801 ms   150 ms   150 ms  router113.ukrsat.com [212.35.171.113]
  6   161 ms   150 ms   160 ms  cyclone.ukrsat.com [212.35.160.97]
  7   731 ms   731 ms   751 ms  NO-NIT-TN-6.taide.net [193.219.192.6]
  8   711 ms   711 ms   701 ms  NO-NIT-TN-8.taide.net [193.219.193.138]
  9   711 ms   701 ms   711 ms  oso-okr-i1-pos1-1.telia.net [213.248.78.49]
 10   701 ms   711 ms   691 ms  s-bb1-pos0-0-0.telia.net [213.248.66.89]
Трасування закінчене.
```

3 Ключові питання

3.1 Перелічте основні утиліти, вбудовані в ОС, які призначені для аналізу конфігурації і стану мережі на основі TCP/IP.
3.2 Укажіть призначення й основні параметри утиліти ping
3.3 Укажіть призначення й основні параметри утиліти tracert.
3.3 Що виконує команда ping 127.0.0.1?
3.4 Укажіть призначення утиліти nslookup.
3.5 Для чого використовується утиліта netstat ?
3.6 Що виводить за замовчуванням утиліта ipconfig?

3.7 Для чого використовується утиліта Telnet?

4 Домашнє завдання

4.1 Вивчіть, користуючись даним методичним керівництвом, основні вбудовані засоби, що призначені для аналізу конфігурації і стану мережі на основі TCP/IP.

4.2 Підготуйте протокол лабораторної роботи, у якому відбити тему, мету роботи, короткий опис утиліт, що призначені для аналізу конфігурації і стану мережі на основі TCP/IP.

4.3 Підготуйте відповіді на ключові питання п.3.

5 Лабораторне завдання

5.1 Завдання 1. Використання утиліт ping і tracert для аналізу конфігурації і стану мережі на основі TCP/IP

1. Використовуючи утиліту ping, перевірте з'єднання з наступними/ вузлами: www.google.com, www.ukr.net, www.fila-lab.de, www.yahoo.com, www.altavista.com, www.suitt.edu.ua. Запишіть, до яких вузлів можна отримати доступ, а до яких – ні. Запишіть час доступу до вузлів.
   2. Виконайте утиліту ping з адресами www.fila-lab.de, www.yahoo.com, www.suitt.edu.ua та з усіма ключами табл. 2.1. (Результати запишіть або зробіть скрін з кожним ключем, лише одного сайту)
   3. Використовуючи утиліту tracert, визначте маршрути до хостів www.google.com, www.fila-lab.de, www.yahoo.com, www.suitt.edu.ua. Для кожного розглянутого маршруту запишіть загальну кількість маршрутизаторів, їх IP-адреси та доменні імена.
   (Результати запишіть або зробіть скрін з кожним ключем, лише одного сайту)
   4. Виконайте утиліту tracert, з ключами -d -h, визначте маршрути до хостів www.google.com, www.fila-lab.de, www.yahoo.com, www.suitt.edu.ua.
   (Результати запишіть або зробіть скрін з кожним ключем, лише одного сайту)
   Примітка. Щоб відкрити вікно командного рядка, натисніть кнопку "Пуск" та виберіть команди в пошуковій строці наберіть cmd.