Лабораторна робота №1

Тема: Аналіз конфігурації локальної мережі
Мета: Ознайомитися із системними засобами ОС Windows, які можна використовувати для аналізу та налаштування локальної мережі

Питання до вивчення

1. Мережеві утиліти командного рядка. Утиліта hostname.
2. Команда net та її використання для аналізу мережі.
3. Призначення, синтаксис та параметри команди ipconfig.

Короткі теоретичні відомості

Для ознайомлення з параметрами команди NET можна скористатись довідкою Windows (розділ «Справочник по параметрам командной строки» або «Net (команды сетевых служб»).

Мережеві утиліти Windows запускаються з командного рядка (Пуск → Выполнить → cmd).

Утиліта hostname

Виводить ім'я локального комп'ютера (хоста). Вона доступна тільки після установки підтримки протоколу TCP/IP. Приклад виклику команди hostname:

G:\Windows\system32>hostname
Cdr1

Команда NET

Запуск команди **net** з параметром **/help** виводить список всіх команд, що підтримуються конкретною системою.

Для перегляду списку ресурсів мережі використовується команда **net view**. Запуск цієї команди без аргументів призведе до виведення на екран списку усіх комп'ютерів мережі.

Для того, щоб визначити загальнодоступні ресурси на конкретному комп'ютері, введіть команду:

net view \\[ім'я комп'ютера]

У мережах з декількома доменами чи робочими групами перелік доменів та робочих груп можна отримати ввівши команду:

net view /domain

а список комп'ютерів конкретного домену (робочої групи) - за допомогою команди:

net view /domain:[ім'я домену]

Спільне використання каталогів ініціюється з командної стрічки командою **net share**.

Наприклад, команда:

net share my_folder=d:\personal

забезпечує виділення для спільного використання в мережі папки personal під іменем my_folder.

Для обмеження кількості користувачів, які можуть одночасно працювати з цим ресурсом, слід вказати параметр /users:[кількість користувачів]. Команда net share без параметрів видає інформацію про виділені ресурси того комп'ютера, з якого вона введена. Слід зауважити, що за допомогою команди net share не можна виділити для спільного використання принтер.

Для встановлення зв'язку з виділеними для спільного користування ресурсами призначена команда **net use**. Введена без параметрів, ця команда видає список виділених ресурсів, з якими зв'язок вже встановлено.

Наприклад, для того, щоб під'єднатися до каталогу Public на комп'ютері Decprima, слід ввести команду

net use Z: \\Decprima\Public

Команда net use з параметром /delete скасовує спільне використання ресурсу. Наприклад, команда

net use /delete Z:

відміняє спільне використання ресурсу \\Decprima\Public і звільняє ім'я пристрою Z.

Команди NET для адміністративних цілей

Використовуючи ці команди в командних файлах або сценаріях реєстрації, можна розв'язувати задачі адміністрування. Так, під час виконання процедур розподіленого резервного копіювання та деяких інших важливих мережевих операцій важливо, щоб усі системні годинники комп'ютерів мережі були синхронізовані. Для цього використовують команду **net time**. Без параметрів ця команда виводить системний час.

Команда **net time \\[ім'я_комп'ютера]** виводить системний час комп'ютера з вказаним ім'ям.

Команда **net time /domain** виводить системний час домену. Використання ключового слова /set дає змогу встановити час у відповідності з системним часом на комп'ютері, якому адресовано запит. Наприклад, команда

net time /domain /set

синхронізує робочу станцію (чи сервер) з показами системного годинника домену.

Утиліта ipconfig

Виводить діагностичну інформацію про конфігурацію мережі TCP/IP. Ця утиліта дозволяє переглянути поточну конфігурацію IP-адрес компьютерів мережі. Синтаксис утиліти ipconfig:

ipconfig [/all | /renew [адаптер] | /release [адаптер]]

Для визначення IP-адрес та MAC-адрес можна використовувати команду **ipconfig** без параметрів та з параметром **/all**.

Завдання до виконання

1. Використовуючи стандартні мережеві утиліти, проаналізувати конфігурацію локальної мережі на платформі ОС Windows:
   a. визначити свою IP-адресу та MAC-адресу,
   b. дізнатися ім'я домена та імена комп'ютерів, що входять в домен,
   c. Вивести список комп’ютерів домену РМ,
   d. переглянути спільні ресурси свого комп’ютера,
   e. підключити спільний ресурс сусіднього комп’ютера як локальний диск T:,
   f. перевірити системний час домена та свого комп’ютера.

Контрольні питання

1. Як отримати свою IP-адресу та MAC-адресу?
2. Як дізнатися ім'я домена та імена комп'ютерів, що входять в домен?
3. Як вивести список комп’ютерів домену РМ?
4. Як переглянути спільні ресурси свого комп’ютера?
5. Як підключити спільний ресурс сусіднього комп’ютера як локальний диск T:?
6. Як перевірити системний час домена та свого комп’ютера?

Лабораторна робота №2

Тема: Команди діагностики мережі netsh diag та їх використання.
Мета: Ознайомитися із призначенням та параметрами групи команд netsh diag. Здобути навички використання команд для діагностики мережі.

Питання до вивчення

1. Призначення та систаксис команди netsh diag.
2. Параметри команди netsh diag.

Короткі теоретичні відомості

Для ознайомлення з параметрами команд netsh diag можна скористатись довідкою Windows (розділ «Справочник по параметрам командной строки» або відкрити довідник ntcmds.chm у папці C:\Windows\Help).

Мережеві утиліти Windows запускаються з командного рядка (Пуск → Выполнить → cmd). Команда діагностики мережі запускається з командного рядка в два прийоми: спочатку подають команду netsh, а після запрошення netsh> команду diag.

Завдання до виконання

1. За допомогою команди show adapter визначити індекс та повну назву мережевого адаптера комп'ютера. Перевірити дію команди ping adapter і визначити власну IP-адресу. Які ще адреси можна визначити за допомогою цієї команди?
2. Ознайомитися з командою show gateway. Яку інформацію вона надає? Перевірити зв'язок із шлюзом (команда ping gateway).
3. Визначити призначення команди ping loopback. Яка інша команда надає такі самі можливості діагностики?
4. Ознайомитися з командами show dhcp та show dns. Яку інформацію вони надають? Командами ping dhcp та ping dns перевірити зв'язок з DHCP-сервером та DNS-сервером.
5. Ознайомитися з можливостями команд show mail, connect mail та ping mail. Пояснити різницю між ними.
6. Описати дію команди show all.
7. Яку інформацію можна визначити командами show os, show version, show ip?

Лабораторна робота №3

Тема: Аналіз проходження пакетів даних через мережу.
Мета: Ознайомитися із системними засобами ОС Windows, які можна використовувати для контролю проходження пакетів даних.

Питання до вивчення

1. Призначення та синтаксис команди PING.
2. Параметри команди PING.
3. Призначення та синтаксис команди TRACERT.
4. Параметри команди TRACERT.

Короткі теоретичні відомості

Для ознайомлення з параметрами команд **ping** та **tracert** можна скористатись довідкою Windows (розділ «Справочник по параметрам командной строки» або відкрити довідник ntcmds.chm у папці C:\Windows\Help).

Мережеві утиліти Windows запускаються з командного рядка (Пуск → Выполнить → cmd).

Утиліта ping

Перевіряє з'єднання з видаленим комп'ютером або комп'ютерами. Ця команда доступна тільки після установки підтримки протоколу TCP/IP. Синтаксис утиліти ***ping**:*

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

-t
повторює запити до видаленого комп'ютера, поки програма не буде зупинена;

-a
транслює ім'я комп'ютера в адресу;

-n *лічильник*
передається число пакетів ECHO, задане параметром. За умовчанням - 4;

-l *розмір*
відправляються пакети типу ECHO, що містять порцію даних заданої довжини. За умовчанням - 32 байти, максимум - 65500;

-f
відправляє пакети з прапором заборони фрагментації (Do not Fragment). Пакети не розриватимуться при проходженні шлюзів на своєму маршруті;

-i *ttl*
встановлює час життя пакетів TTL (Time To Live);

-v *тип*
встановлює тип служби (Type Of Service) пакетів;

-r *лічильник*
записує маршрут відправлених і повернених пакетів в полі запису маршруту Record Route. Параметр лічильник задає число комп'ютерів в інтервалі від 1 до 9;

-s *число*
задає число ретрансляцій на маршруті, де робиться відмітка часу;

-j *список_вузлів*
направляє пакети по маршруту, що задається параметром *список_вузлів* Комп'ютери в списку можуть бути розділені проміжними шлюзами (вільна маршрутизація). Максимальна кількість, що вирішується протоколом IP, дорівнює 9;

-k *список_вузлів*

направляє пакети по маршруту, що задається параметром список_комп. Комп'ютери в списку не можуть бути розділені проміжними шлюзами (обмежена маршрутизація). Максимальна кількість, що вирішується протоколом IP, дорівнює 9;

-w *інтервал*

визначає в мілісекундах час очікування отримання повідомлення з ехо-відповіддю, яке відповідає повідомленню ехо-запитом. Якщо повідомлення з ехо-відповіддю не отримане в межах заданого інтервалу, то видається повідомлення про помилку "Request timed out" (Превышен интервал ожидания для запроса). Інтервал за умовчанням дорівнює 4000 (4 секунди).

ім'я_кінц_комп'ютера

задає точку призначення, якій прямують запити (IP-адреса або ім'я вузла);

Утиліта tracert (traceroute)

Визначає шлях до точки призначення за допомогою посилки в точку призначення ехо-повідомлень протоколу Internet Control Message Protocol (ICMP) з постійним збільшенням значень терміну життя (Time to Live, TTL). Виведений шлях — це список найближчих інтерфейсів маршрутизаторів, що знаходяться на шляху між вузлом джерела і точкою призначення. Ближнім інтерфейсом є інтерфейс маршрутизатора, який є найближчим до вузла відправника на шляху. Запущена без параметрів, команда **tracert** виводить довідку.

tracert [**-d**] [**-h** *максим_число_переходів*] [**-j** *список_вузлів*] [**-w** *інтервал*] [*ім'я_кінц_комп'ютера*]

-d

Запобігає спробам команди **tracert** транслювати IP-адреси проміжних маршрутизаторів в імена. Збільшує швидкість виведення результатів команди **tracert**.

-h *максим_число_переходів*

Задає максимальну кількість переходів на шляху пошуку кінцевого об'єкту. Значення за умовчанням дорівнює 30.

-j *список_вузлів*

Указує для повідомлень з ехо-запитом використання параметра вільної маршрутизації в заголовку IP з набором проміжних місць призначення, вказаних в *списку_вузлів*. При вільній маршрутизації успішні проміжні місця призначення можуть бути розділені одним або декількома маршрутизаторами. Максимальне число адрес або імен в списку — 9. *Список_вузлів* являє собою набір IP-адрес (у точково-десятковій нотації), розділених пропусками.

-w *інтервал*

Визначає в мілісекундах час очікування для отримання ехо-відповідей протоколу ICMP або ICMP-повідомлень про закінчення часу, відповідних даному повідомленню ехо-запиту. Якщо повідомлення не отримане протягом заданого часу, виводиться зірочка (*). Таймаут за умовчанням 4000 (4 секунди).

ім'я_кінцевого_комп'ютера

Задає точку призначення, вказану IP-адресою або іменем вузла.

Завдання до виконання

1. Вивчити синтаксис та параметри команд **ping** та **tracert.**
2. Дослідити, як впливає дозвіл фрагментації пакетів на швидкість відповіді (розмір пакету в межах 32–2048 байтів).

3. Дослідити, як впливає розмір пакету на швидкість відповіді (в межах 32–16384 байтів). Побудувати графік залежності часу доставки пакетів від розміру пакета.
4. Прослідкувати маршрут проходження пакетів до: сусіднього комп'ютера, комп'ютера сусідньої аудиторії, piper.kspu.kr.ua, www.kspu.kr.ua, інших комп'ютерів мережі університету, www.ukr.net або іншого сервера мережі Інтернет України.

Завдання для самостійної роботи

1. Дослідити маршрут проходження пакетів до одного з відомих зарубіжних сайтів: наприклад, google.com, yandex.ru тощо.
2. За допомогою інформаційних сайтів типу geoiptool.com (або серії whois) визначити місцеположення проміжних вузлів маршруту і нанести їх на карту світу (Європи).

Контрольні питання

1. Призначення та можливості команд **ping** та **tracert**.
2. Особливості спільного використання ключів –n та –t команди PING.
3. Який максимальний розмір пакету, який може бути відправлений без фрагментації?
4. Як впливає розмір пакету на швидкість відповіді команди **ping**.
5. Що визначає параметр –i команди **ping**?
6. Для чого використовують параметр –f команди **ping**?
7. Як визначити маршрут проходження пакетів даних до заданого кінцевого комп'ютера?
8. Який алгоритм одержання інформації про маршрут використовує команда **tracert?**

Лабораторна робота №4

Тема: Аналізатор пакетів даних мережевих протоколів Wireshark.
Мета: Здобути навички роботи з програмним засобом аналізу пакетів даних (на прикладі програми-сніфера Wireshark).

Питання до вивчення

1. Призначення програми Wireshark.
2. Інтерфейс програми Wireshark.

Короткі теоретичні відомості

Для ознайомлення з інтерфейсом програми Wireshark скористайтесь документом «Аналізатор пакетів Wireshark» або документацією користувача «Wireshark User's Guide».

Завдання до виконання

1. Запустіть програму Wireshark та програму-браузер.
2. Ознайомтеся з інтерфейсом програми Wireshark. Встановіть призначення основних зон робочої області.
3. Ознайомтеся з параметрами налаштування захоплення пакетів (Capture Options).
4. Запустіть захоплення пакетів[1].
5. Введіть до адресного рядка браузера адресу: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html і перейдіть на задану сторінку.
6. Зупиніть захоплення пакетів.
7. Застосуйте фільтр **http** до захоплених пакетів.
8. Навчіться розкривати / згортати інформацію про вибраний тип протоколу.
9. Навчіться зберігати захоплені пакети на диск та відкривати раніше захоплені пакети.
10. Визначте кількість та вміст захоплених пакетів протоколу HTTP.
11. Ознайомтеся з текстом запиту GET протоколу HTTP. Які поля він містить?
12. Ознайомтеся з текстом відповіді Web-сервера. Яка версія HTTP-протоколу? Який статус відповіді сервера? Які поля містить відповідь? Який вміст одержаної Web-сторінки? Яка довжина повідомлення? Яка дата і час останньої модифікації файлу на сервері?
13. Запустіть захоплення пакетів[2].
14. Введіть до адресного рядка браузера адресу: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html і перейдіть на задану сторінку. Поновіть одержану сторінку (F5).
15. Зупиніть захоплення пакетів.
16. Відфільтруйте пакети протоколу HTTP.
17. Дослідіть перший запит HTTP GET. Чи є в ньому поле “IF-MODIFIED-SINCE”?
18. Проаналізуйте відповідь сервера. Який вміст повернутої сторінки?
19. Дослідіть вміст другого запиту HTTP GET. Чи є в ньому поле “IF-MODIFIED-SINCE:”? Який вміст цього поля заголовку?
20. Який статус відповіді сервера? Який текст Web-сторінки повернув сервер цього разу?
21. Закрийте програму.

---

[1] У випадку відсутності прав на захоплення пакетів відкрийте файл «http-ethereal-trace-1» із захопленими раніше пакетами. Пункти 5–6 завдання також пропустіть.
[2] У випадку відсутності прав на захоплення пакетів відкрийте файл «http-ethereal-trace-2» із захопленими раніше пакетами. Пункти 14–15 завдання пропустіть.