

УКРАЇНСЬКА ДЕРЖАВНА АКАДЕМІЯ  
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

ФАКУЛЬТЕТ АВТОМАТИКИ, ТЕЛЕМЕХАНІКИ ТА  
ЗВ'ЯЗКУ

Кафедра “Транспортний зв’язок”

МЕТОДИЧНІ ВКАЗІВКИ  
ДО ЛАБОРАТОРНОЇ РОБОТИ З ДИСЦИПЛІНИ  
“Автоматизація бізнес-процесів” спеціальності “Автоматика та  
автоматизація на транспорті”

для студентів факультету  
“Автоматика, телемеханіка і зв’язок” усіх форм навчання,  
студентів і магістрів ІПК та слухачів ФПК

Харків 2015

Методичні вказівки розглянуто та рекомендовано до друку на засіданні кафедри “Транспортний зв'язок” 19 березня 2014 р., протокол № 9.

Наведено теоретичні відомості про існуючі методи знаходження несправностей мережі локального доступу, збору статистичних даних щодо переданих та отриманих даних, помилки приймання/передачі, команди, які дозволяють отримати уявлення про технічний стан локальних мереж.

Методичні вказівки призначено для студентів факультету АТЗ всіх форм і термінів навчання, студентів і магістрів ІППК та слухачів ФПК.

Укладач

доц. М.О. Колісник

Рецензент

д.т.н., професор Є.Л. Казаков  
провідний співробітник Наукового центру повітряних сил  
Харківського університету повітряних сил ім. І. Кожедуба

# Лабораторна робота 4

## ДОСЛІДЖЕННЯ ПРИНЦИПІВ ОРГАНІЗАЦІЇ ТРАСУВАННЯ МАРШРУТІВ У ЛОКАЛЬНІЙ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ ТА ВИЗНАЧЕННЯ ЇЇ ТЕХНІЧНОГО СТАНУ

### 1 МЕТА РОБОТИ

Закріпити теоретичні знання і набути практичних навичок і умінь в дослідженні методів контролю параметрів трафіка в локальних обчислювальних мережах при реалізації бізнес-процесів; в проведенні пошуку несправностей в абонентській кабельній мережі, в проведенні аналізу потоку даних, що передається в мережі локального доступу; контролювати технічний стан маршрутизаторів мережі та мережевих карт персональних комп'ютерів, збирати і аналізувати статистичні дані стану обладнання локальних мереж, аналізувати час затримок у вузлах локальних мереж при передачі даних, аналізувати маршрути передачі даних і помилки, що виникають при їх передачі.

### 2 ЗАВДАННЯ ДЛЯ ДОМАШНЬОГО ОПРАЦЮВАННЯ

1 За літературою, конспектом лекцій і даними методичними вказівками вивчити принципи, методи і практичні прийоми організації вимірювань в мережі локального доступу.

2 Ознайомитись з особливостями роботи з командним рядком в операційній системі Windows 7.

3 Навчитись виявляти несправності мережі локального доступу.

4 Вивчити особливості використання протоколу ICMP.

5 Вивчити особливості використання команд *ping*, *tracert*, *ipconfig*, *netstat* в операційній системі Microsoft Windows 7 при аналізі технічного стану мереж.

## КОНТРОЛЬНІ ПИТАННЯ

1 Поясніть, з якою метою в мережах передачі даних використовується протокол *ICMP*?

2 Назвіть основні команди командного рядка для збору статистичних даних щодо переданих пакетів в мережі локального доступу.

3 Поясніть, яким чином можна отримати таблицю маршрутизації в командному рядку.

4 Поясніть призначення та принцип дії команди *ping*.

5 Яким чином, отримавши відлуння-відповіді виконання команди *ping*, можна зробити висновок про технічний стан мережі передачі даних?

6 Поясніть принцип дії та призначення команди *tracert*.

7 Поясніть призначення команди *netstat*.

8 Поясніть принцип дії та призначення команди *arp*.

9 Поясніть принцип дії та призначення команди *route print*.

10 Які параметри команди *ping* можна змінювати для отримання більш точної інформації про технічний стан мережі передачі даних?

11 Які параметри команди *tracert* можна змінювати для отримання більш точної інформації про технічний стан мережі передачі даних?

12 Які параметри команди *netstat* можна змінювати для отримання більш точної інформації про технічний стан мережі передачі даних?

13 Які параметри команди *arp* можна змінювати для отримання більш точної інформації про технічний стан мережі передачі даних?

14 Як отримати статистичні дані передачі даних в мережі, що побудована на основі технології Ethernet?

15 Як отримати статистичні дані в мережі передачі даних і додатково вивести роздруківку таблиці маршрутизації?

### 3 ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

**OSI** (взаємозв'язок відкритих систем) - кваліфікує стандарти для обміну інформацією між системами, які "відкриті" одна з одною для цієї мети в силу їх взаємного використання чинним стандартам.

**Відкрита система** - подання до еталонної моделі тих аспектів реальної відкритої системи, які доречні OSI.

**Реальна система** - набір з одного або декількох комп'ютерів, відповідного програмного забезпечення, периферійних пристроїв, терміналів, людей-операторів, фізичних процесів, засобів передачі інформації, і т.д., який утворює автономну систему, здатну цілком виконувати обробку інформації та/або передачу інформації.

**Реальна відкрита система** - реальна система, яка відповідає вимогам стандартів OSI в її зв'язку з іншими реальними системами.

**ICMP** (Internet Control Message Protocol) - протокол керуючих повідомлень в стеці протоколів TCP/IP, застосовуваний в міжнародній комп'ютерній мережі Internet.

**DHCP** (Dynamic Host Configuration Protocol) - протокол динамічної конфігурації вузла) - мережевий протокол, що дозволяє комп'ютерам автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP/IP. Даний протокол працює за моделлю «клієнт-сервер».

**ARP** (Address Resolution Protocol) - протокол дозволу адрес, призначений для визначення MAC-адреси за відомою IP-адресою.

**WINS** (Windows Internet Name Service) — служба NetBIOS-імен комп'ютерів з IP-адресами вузлів. Сервер **WINS** здійснює реєстрацію імен, виконання запитів і звільнення імен.

**Ping** (Packet Internet Groper) – програма, що використовується для перевірки налагодження набору протоколів TCP/IP.

**Мережевий адаптер** (Network Interface Card - NIC) – системна плата, що надає можливість обміну даними з мережею.

**IP-адреса** IPv4 - 32-бітова адреса, що використовується в мережі Internet.

**Маршрутизатор** (Router) – пристрій об'єднаних мереж, що пересилають пакети між мережами на основі адрес третього рівня.

**Пакет** (Packet) – логічно згрупована інформація, що включає в себе заголовок, який вміщує керуючу інформацію і (звичайно) дані користувачів.

**Фрейм** (Frame) - логічно згрупована інформація, що пересилається в вигляді блоку даних канального рівня по середовищу передачі даних.

**Стек протоколів** (Protocol Suite) – набір зв’язаних між собою комунікаційних протоколів, що функціонують спільно і як одне ціле керуючих функціонуванням деяких або всіх семи рівнів моделі OSI.

**Брандмауер** (Firewall) – програмне забезпечення, що працює на маршрутизаторі або сервері, або окремий апаратний компонент мережі, який захищає ресурси приватної мережі від несанкціонованого доступу користувачів з інших мереж.

**Хост** (Host) або **вузол** — будь-який пристрій, що надає сервіси формату «клієнт-сервер» в режимі сервера за будь-якими інтерфейсами і унікально визначений на цих інтерфейсах. В більш вузькому значенні под хостом можуть розуміти будь-який комп’ютер, сервер, підключений до локальної або глобальної мережі.

**GGP** (Gateway-to-Gateway Protocol) – протокол, який дозволяє здійснювати процес управління шлюзами, забезпечуючи їх взаємодію один з одним.

#### 4 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Всі мережі передачі даних в даний час повинні організовуватись на основі моделі взаємодії відкритих систем OSI (ISO) або на основі моделі TCP/IP. На рисунку 1 наведено модель OSI, модель TCP/IP та перелік відповідних їх рівням протоколів.

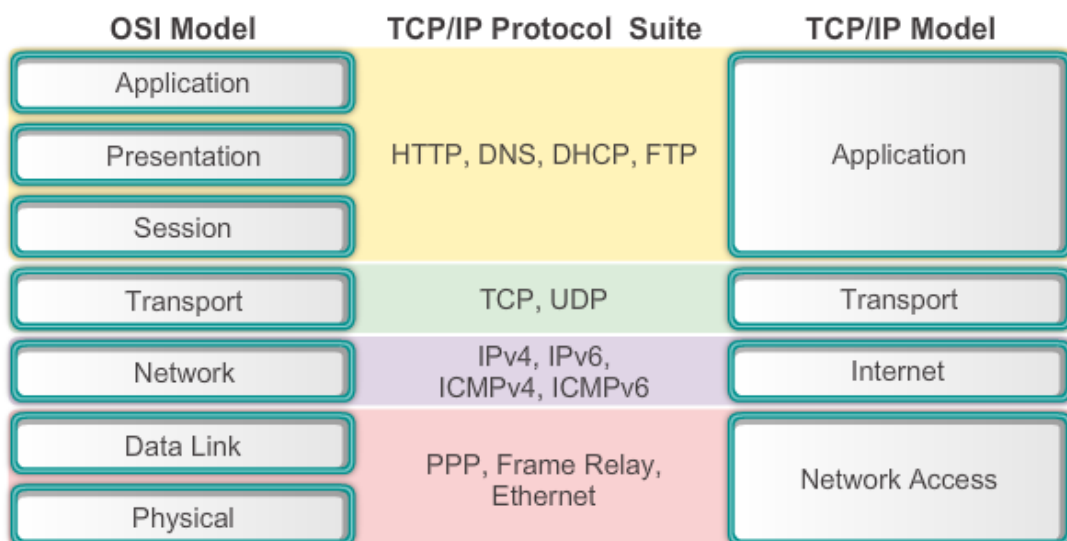


Рисунок 1 – Відповідність рівнів моделі OSI моделі TCP/IP

Три перших рівні моделі OSI визначають функції безпосередньо передачі даних. Від них залежить фізична доставка сигналу по мережі. Останні чотири рівні управляють передачею даних на рівні хост-машин.

### Рівень 1 – Фізичний (Physical)

Відповідає за наявність сигналу в лінії, передачу довільного сигналу. Описує природу середовища передачі даних (рівень напруги на обладнанні, радіочастоти, рівень загасання світлового сигналу в оптичному волокні та інші подібні аспекти).

### Рівень 2 – Канальний (Data Link)

Доступ до середовища передачі даних. Другий рівень забезпечує передачу фреймів (кадрів). Фрейм - це блоки даних, розділених для зручності і стабільності передачі на відрізки. На канальному рівні даним, переданим на фізичному рівні, призначається початок і кінець, вказується послідовність даних.

### Рівень 3 – Мережевий (Network)

Цей рівень користується можливостями, наданими йому рівнем 2. На рівні виконується обробка адрес і здійснюється маршрутизація між різними мережами.

### Рівень 4 – Транспортний (Transport)

Забезпечує зв'язок між кінцевими пристроями, завершує процес передачі даних, контролює потік даних, перевіряє правильність доставки і адресації. Простіше кажучи забезпечує зв'язок між двома пристроями.

### Рівень 5 - Сеансовий (Session)

Керує сеансами передачі даних, відновлює аварійно закінчені сеанси. Цей же рівень перетворює доменні імена, зручні для людей, в реальні мережеві адреси.

### Рівень 6 - Рівень уявлень (Presentation)

Рівень 6 встановлює взаємозв'язок між комп'ютерами, на цьому рівні вирішуються такі завдання, як перекодування переданої інформації.

## Рівень 7 - Рівень додатків (Application)

Служить прошарком між мережею та комп'ютерними програмами. Обслуговує тільки прикладні процеси. Перевіряє можливість ресурсів для роботи додатків.

В моделі TCP/IP перелік рівнів та відповідних протоколів наведено на рисунку 2.

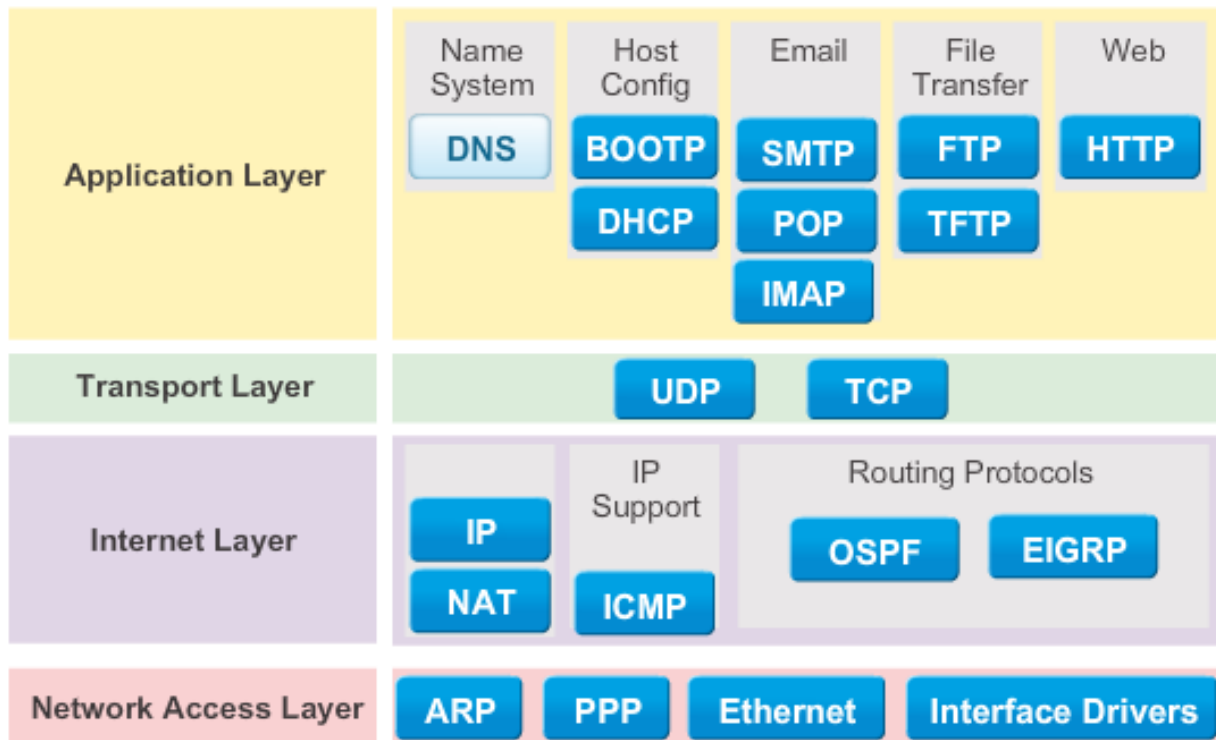


Рисунок 2 - Модель TCP/IP

Несправності передачі даних найчастіше виникають в середовищі передачі даних, з цієї причини шукати несправності доцільно саме на трьох перших рівнях моделі OSI.

На фізичному рівні в мережі локального доступу можуть виникати такі несправності, як відсутність сигналу в лінії з яких найбільш поширених причин:

- а) обрив кабелю;
- б) поганий контакт в місці приєднання кабелю;
- в) неправильне під'єднання рознімача до жил кабелю (не у відповідності до стандартів TIA/EIA 568A,B);



- г) непідключення кабелю;
- д) підключення кабелю не до того порту;
- е) відсутність живлення на обладнанні;
- ж) замикання контактів кабелю;
- к) несправність мережевого інтерфейсу.

Такі помилки і неполадки слід шукати на каналному рівні моделі OSI:

- а) неправильно задана тактова частота на послідовних інтерфейсах;
- б) неправильно заданий номер VLAN і тип порту;
- в) неправильно вказаний метод інкапсуляції;
- г) дублювання запитів і відповідей за протоколом **arp**;
- д) несправність мережевого інтерфейсу .

На мережевому рівні моделі OSI можуть виникати помилки і несправності внаслідок таких причин:

- а) неправильне зазначення IP мережі;
- б) неправильна IP адреса мережевого інтерфейсу;
- в) помилково вказано маску підмережі;
- г) неправильна адреса DNS сервера;
- д) неправильна маршрутизація;
- е) невиконання активізації роботи протоколу маршрутизації;
- ж) активізація неправильного протоколу маршрутизації.

На більш високих рівнях можуть траплятися помилки адміністрування, що призводять до несправностей мережі:

- а) у разі використання DHCP сервера - помилка в його конфігурації і неправильно вказана фізична адреса користувача;
- б) неправильне конфігурування брандмауером;
- в) несправний DNS сервер.

При вирішенні завдання пошуку та усунення неполадок потрібно виконати такий алгоритм дій.

а) отримати докладну інформацію про виниклу проблему. Чітко визначення і повний її опис;

б) визначити найбільш ймовірні причини виникнення проблеми, включаючи дані про проблеми подібного роду, що будь-коли виникали в тому ж сегменті мережі, з тим же абонентом. Розставити причини за пріоритетністю;

в) на третьому етапі складається план дій з вирішення проблеми, заснований на даних, отриманих на другому етапі;

г) реалізація плану дій повинна відбуватися з його строгим дотриманням. В іншому випадку можна зробити ще більше помилок і неефективно витратити час. Після виконання кожного кроку слід перевіряти, чи вирішено проблему, чи ні;

д) перевірити результати виконання процедур усунення неполадок. Необхідно переконатись в тому, що проблема вичерпана і мережа працює належним чином;

е) у тому випадку, якщо проблему не усунуто, варто переглянути дії, виконані на третьому і четвертому етапі.

Для визначення правильності функціонування мережі локального доступу використовується протокол ICMP в стеці протоколів TCP/IP.

Протокол Internet (IP) [1] використовується для обробки даних, що передається між хост-комп'ютерами в системі об'єднаних мереж, названій Catenet [2]. Пристрої, що здійснюють з'єднання різних мереж, називаються шлюзами. Для забезпечення управління шлюзи взаємодіють один з одним за допомогою протоколу Gateway-to-Gateway Protocol (GGP) [3, 4]. Часом шлюз чи хост-комп'ютер, що отримує дані, обмінюється інформацією з хост-комп'ютером, який відправляє ці дані. Саме для таких цілей використовується даний протокол - протокол контрольних повідомлень Internet (*ICMP*). *ICMP* використовує основні властивості протоколу Internet (IP), якщо б *ICMP* був протоколом більш високого рівня. Однак фактично *ICMP* є складовою частиною протоколу Internet і повинен бути складовою частиною кожного модуля IP.

Повідомлення *ICMP* повинні відправлятися в деяких скрутних ситуаціях. Наприклад, коли даних не може досягти свого адресата, коли шлюз не має достатньо місця у своєму буфері для

передачі будь-якої дейтаграми, або коли шлюз наказує хост-комп'ютеру відправляти інформацію з більш коротким маршрутом.

Протокол Internet не створений для того, щоб забезпечувати абсолютну надійність передачі інформації. Метою ж даних контрольних повідомлень є забезпечення зворотного зв'язку, оповіщення відправника даних про несправності, що виникають в комунікаційному обладнанні. Протокол не дає гарантій, що дейтаграма досягає свого адресата або що контрольне повідомлення буде повернене комп'ютеру, який відправив дані. Деякі з дейтаграм можуть зникнути в мережі, не викликавши при цьому ніяких оповіщень. Протоколи вищого рівня, що використовують протокол IP, повинні застосовувати свої власні процедури для забезпечення надійності передачі даних, якщо така потрібна.

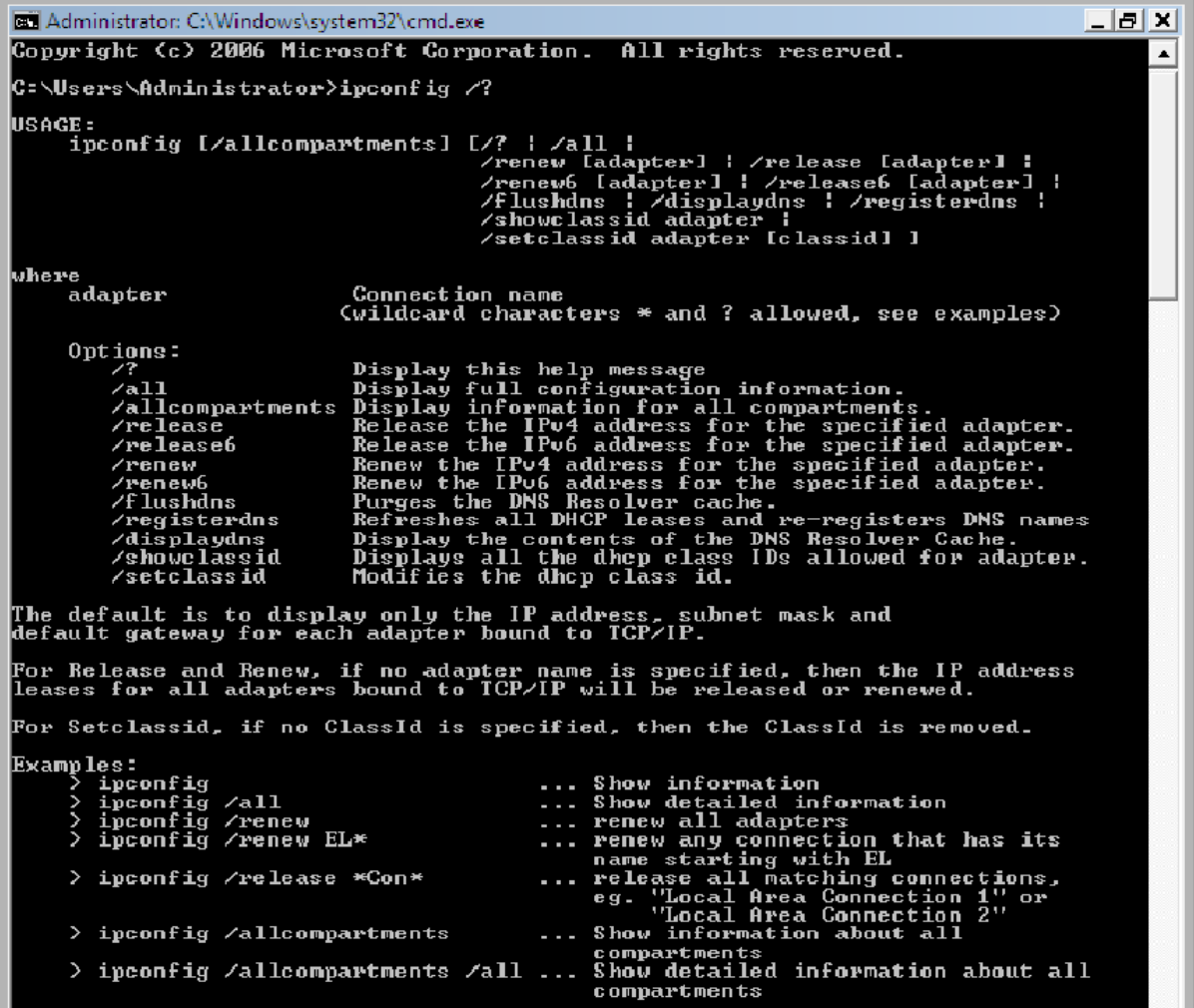
Повідомлення *ICMP* протоколу, як правило, сповіщають про помилки, що виникають при обробці дейтаграм. Щоб проблеми з передачею повідомлень не викликали появи нових повідомлень, щоб це у свою чергу не привело до лавиноподібного зростання кількості повідомлень, які циркулюють в мережі, констатується, що не можна посилати повідомлення про повідомлення. Також констатується, що *ICMP* повідомлення можна надсилати лише про проблеми, що виникають при обробці нульового фрагмента в сегментованій дейтаграмі (нульовий фрагмент має нуль в полі зсуву фрагмента). *ICMP* повідомлення посилаються за допомогою стандартного IP-заголовка. Перший байт в полі даних дейтаграмі - це поле типу *ICMP* повідомлення. Значення цього поля визначає формат всіх інших даних у дейтаграмі. Будь-яке поле, яке позначене "unused", зареєстровано для наступних розробок і повинно при відправленні містити нулі. Однак одержувач не повинен використовувати значення цих полів (за винятком процедури обчислення контрольної суми).

## **5 ПОРЯДОК ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ**

В ході виконання лабораторної роботи студенти повинні виконати наступні кроки для визначення технічного стану мережі локального доступу.

## 1 Перевірка конфігурації за допомогою засобу *ipconfig*

Щоб перевірити конфігурацію TCP/IP на комп'ютері за допомогою засобу *ipconfig*, натисніть кнопку **Пуск**, виберіть пункт **Виконати** та введіть команду *cmd*. Для отримання відомостей про конфігурацію комп'ютера, включаючи його IP-адресу, маску підмережі і шлюз за замовчуванням, можна використовувати команду *ipconfig* (рисунок 3).



```
Administrator: C:\Windows\system32\cmd.exe
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig /?
USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] ]
where
    adapter          Connection name
                    (wildcard characters * and ? allowed, see examples)

Options:
/?                Display this help message
/all             Display full configuration information.
/allcompartments Display information for all compartments.
/release        Release the IPv4 address for the specified adapter.
/release6      Release the IPv6 address for the specified adapter.
/renew         Renew the IPv4 address for the specified adapter.
/renew6       Renew the IPv6 address for the specified adapter.
/flushdns      Purges the DNS Resolver cache.
/registerdns   Refreshes all DHCP leases and re-registers DNS names.
/displaydns   Display the contents of the DNS Resolver Cache.
/showclassid  Displays all the dhcp class IDs allowed for adapter.
/setclassid   Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:
> ipconfig          ... Show information
> ipconfig /all    ... Show detailed information
> ipconfig /renew  ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                    name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                    eg. "Local Area Connection 1" or
                    "Local Area Connection 2"
> ipconfig /allcompartments ... Show information about all
                    compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                    compartments
```

Рисунок 3 – Синтаксис та параметри команди *ipconfig*

Якщо вказати для *ipconfig* параметр */all*, буде створений докладний звіт про конфігурацію всіх інтерфейсів, включаючи адаптери віддаленого доступу. Звіт *ipconfig* можна записати у файл, що дозволить вставляти його в інші документи. Для цього введіть команду

## *ipconfig ім'я\_папки ім'я\_файла.*

У результаті звіт буде збережений у файлі з вказаним ім'ям і поміщений у вказану папку.

Звіт команди *ipconfig* дозволяє виявити помилки в конфігурації мережі комп'ютера. Наприклад, якщо комп'ютер має IP-адресу, яку вже присвоєно іншому комп'ютеру, то маска підмережі буде мати значення **0.0.0.0**.

Якщо комп'ютер має IP-адресу 169.254.y.z і маску підмережі 255.255.0.0, то IP-адреса була призначена засобом автоматичного призначення IP-адрес APIPA операційної системи Windows 7. Це означає, що TCP/IP налаштований для автоматичної конфігурації, сервер DHCP не був знайдений і не була вказана альтернативна конфігурація. У цій конфігурації для інтерфейсу не заданий шлюз за замовчуванням.

Якщо комп'ютер має IP-адресу **0.0.0.0**, значить, він був перевизначений засобом опитування носія DHCP. Це може бути викликано тим, що мережевий адаптер не знайшов підключення до мережі, або тим, що протокол TCP/IP виявив IP-адресу, яка дублює присвоєну вручну адресу комп'ютера.

## **2 Перевірка підключення за допомогою команди *ping***

Більшість мережевих протоколів підтримує відлуння-протокол, що дозволяє провести найпростішу перевірку мережевого з'єднання. Відлуння-протокол дозволяє перевірити коректність маршрутизації мережевих пакетів.

Якщо в конфігурації TCP/IP не було виявлено помилок, необхідно перевірити можливість підключення комп'ютера до інших комп'ютерів в мережі TCP/IP. Для цього використовується команда *ping*.

За допомогою засобу *ping* можна перевірити підключення на рівні IP моделі TCP/IP або мережевому рівні моделі OSI. Команда *ping* відправляє на інший комп'ютер повідомлення з відлуння-запитом за протоколом **ICMP** і чекає пакетів відповіді від цього вузла (рисунки 4 та 5). Інформація, що виводиться командою *ping*, вміщує співвідношення кількості успішно отриманих відповідей до відправлених і середній час проходження пакетів до одержувача.

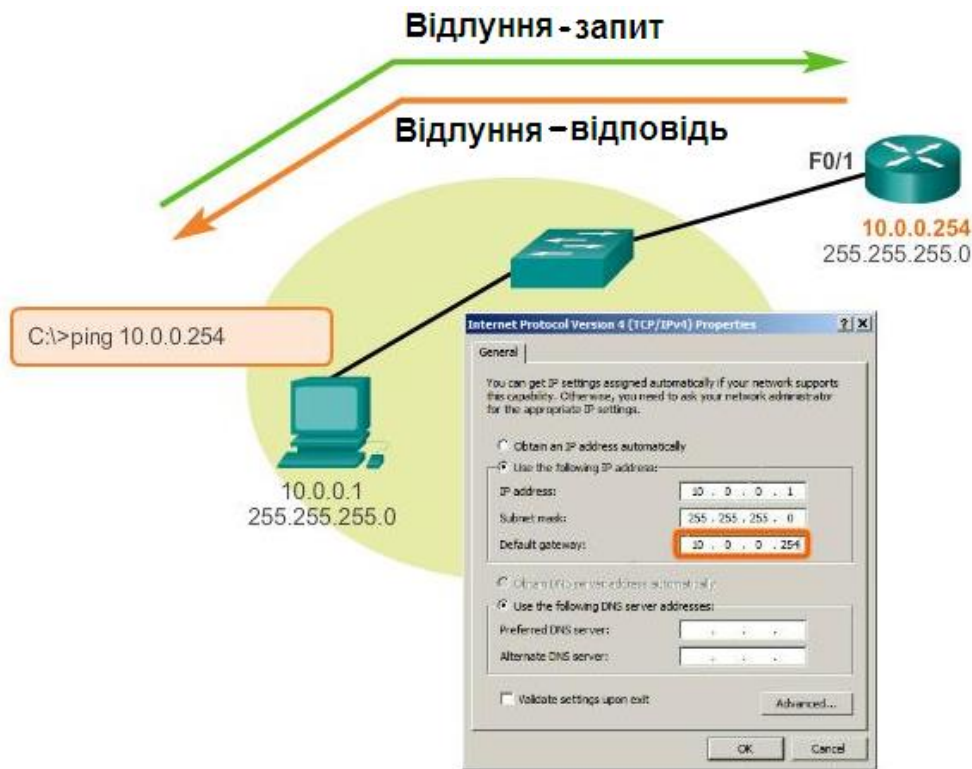


Рисунок 4 – Приклад контролю підключень в локальній мережі при передачі даних за протоколом IPv4 за допомогою команди *ping*

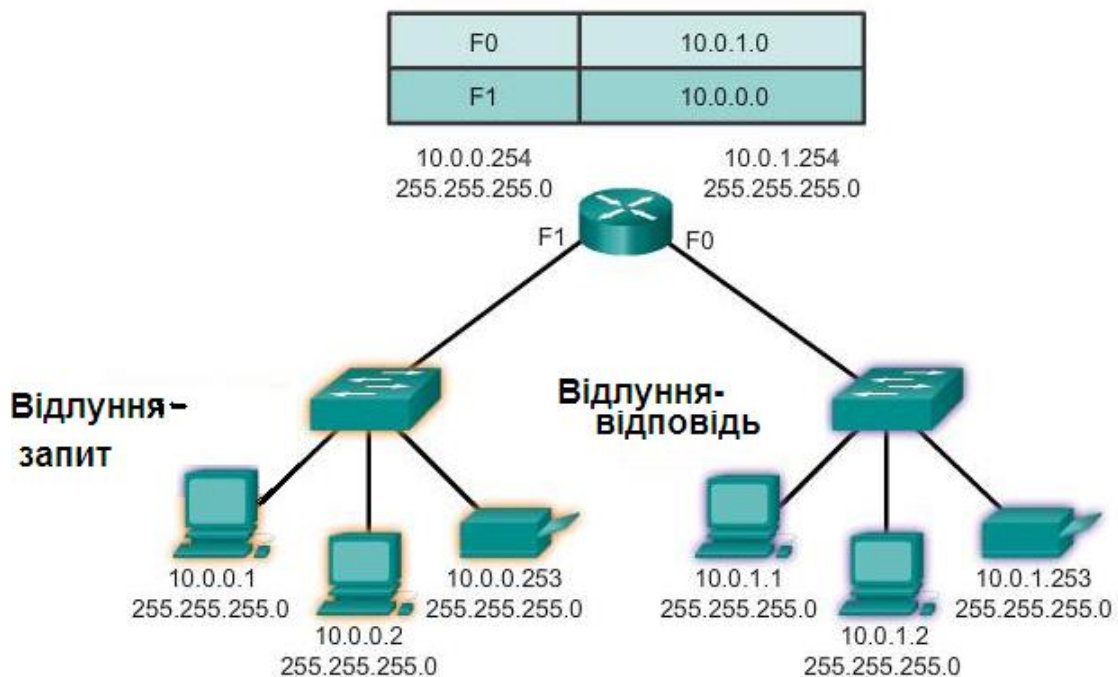


Рисунок 5 – Приклад контролю підключень у віддаленій локальній мережі при використанні команди *ping* віддаленого комп'ютера

За допомогою засобу *ping* можна дізнатися, чи може головний комп'ютер відправляти IP- пакети на комп'ютер - одержувач. Команду *ping* можна також використовувати для виявлення того, чим викликана проблема - несправністю мережевих пристроїв або несумісністю конфігурацій. Результати роботи такого відлуння-протокола можуть допомогти оцінити надійність з'єднання, затримки передачі пакетів, а також працездатність вузла.

Примітка - Якщо була виконана команда *ipconfig/all* і відобразилася конфігурація IP, то адресу замикання на себе і IP-адресу комп'ютера не потрібно перевіряти за допомогою команди *ping*. Ці завдання вже були виконані командою *ipconfig* при виведенні конфігурації.

При усуненні несправностей слід переконатися, що існує маршрутизація між локальним комп'ютером і вузлом мережі. Для цього використовується команда

### *ping IP-адреса.*

Примітка - IP-адреса є IP-адресою вузла мережі, до якого потрібно підключитися.

Щоб використовувати команду *ping*, необхідно виконати такі дії:

а) задати адресу замикання на себе (loopback - внутрішня зворотна петля), щоб перевірити працездатність стека протоколів TCP/IP і функції приймання і передачі мережевого адаптера. Для цього служить така команда:

### *ping 127.0.0.1.*

Якщо контроль за зворотного зв'язку завершиться помилкою, це означає, що стек IP не відповідає.

Подібна поведінка спостерігається в наступних випадках:

- несправні драйвери TCP;
- не працює мережевий адаптер;

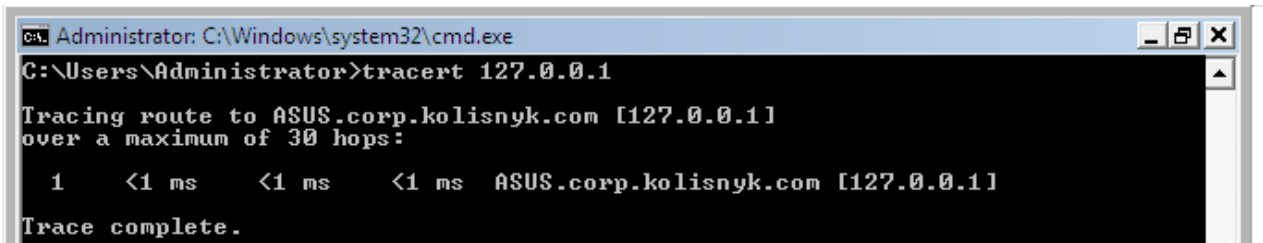
- інша служба заважає роботі протоколу IP.

б) необхідно звернутись за IP- адресою локального комп'ютера, щоб переконатися в тому, що він був правильно доданий в мережу. Якщо таблиця маршрутизації не містить помилок, ця процедура просто призведе до направлення пакета за адресою замикання на себе (loopback) **127.0.0.1** (рисунки 6 та 7).

*ping 127.0.0.1*

або

*tracert 127.0.0.1.*

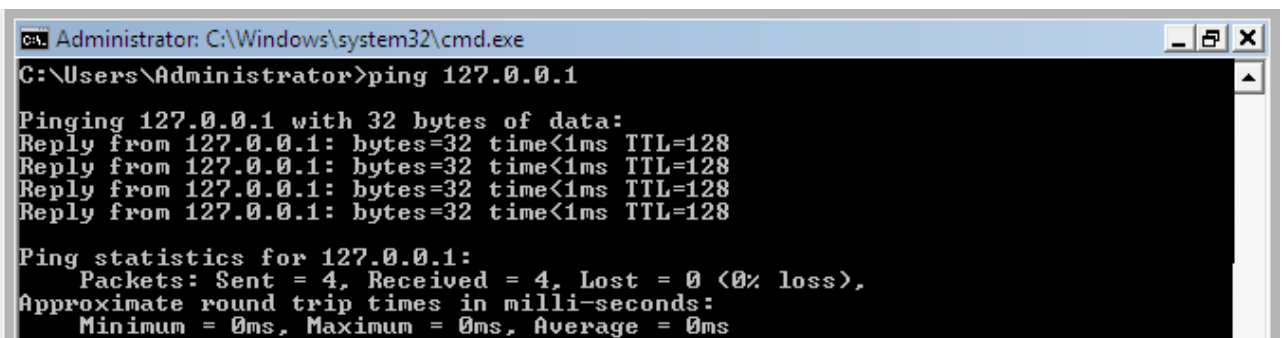


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>tracert 127.0.0.1

Tracing route to ASUS.corp.kolisnyk.com [127.0.0.1]
over a maximum of 30 hops:
  1    <1 ms    <1 ms    <1 ms    ASUS.corp.kolisnyk.com [127.0.0.1]

Trace complete.
```

Рисунок 6 – Перевірка працездатності стеку протоколів TCP/IP при замиканні петлі (loopback) при використанні команди *tracert*



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 7 – Перевірка працездатності стеку протоколів TCP/IP при замиканні петлі (loopback) при використанні команди *ping*

Для перевірки конфігурації адреси набору протоколів TCP/IP для локального пристрою служить така команда:



### *ping IP-адреса локального вузла.*

Якщо контроль за зворотного зв'язку виконаний успішно, але локальна IP-адреса не відповідає, можливо, проблема полягає в таблиці маршрутизації драйвера мережевого адаптера.

в) необхідно звернутись за IP-адресою шлюзу за замовчуванням, щоб перевірити його працездатність, можливість зв'язку з локальним вузлом локальної мережі і можливість доступу до інших мереж. Для цього служить така команда:

### *ping IP-адреси стандартного шлюзу.*

Якщо звернення завершилося невдало, це може означати, що проблема полягає в мережевому адаптері, маршрутизаторі/шлюзі, кабелі або іншому мережевому пристрої;

г) далі необхідно звернутись за IP-адресою віддаленого вузла, щоб перевірити можливість зв'язку з віддаленим пристроєм. Для цього служить така команда:

### *ping IP-адреса віддаленого вузла.*

Якщо звернення завершилося невдало, це може означати, що віддалений вузол не відповідає або проблема полягає в мережевих пристроях між комп'ютерами. Щоб виключити можливість відсутності відповіді віддаленого вузла, перевірте зв'язок з іншим віддаленим вузлом за допомогою команди *ping*;

д) зверніться за IP-адресою віддаленого вузла, щоб перевірити, чи може бути дозволено ім'я віддаленого вузла. Для цього служить така команда:

### *ping ім'я віддаленого вузла.*

Команда *ping* використовує дозвіл імен для дозволу імені комп'ютера в IP-адресу. Тому, якщо звернення за IP-адресою проводиться успішно, а звернення на ім'я - невдало, проблема полягає в дозволі імені вузла, а не в мережевому підключенні.

Перевірте, чи налаштовані для комп'ютера адреси сервера DNS (вручну у властивостях TCP/IP або автоматично). Якщо адреси сервера DNS виводяться командою *ipconfig/all*, треба звернутись за адресами серверів, щоб перевірити, чи доступні вони.

Коди, що повертаються командою *ping*, наведені в таблиці 1.

Таблиця 1 - Коди, що повертаються командою *ping*

Код	Значення	Імовірна причина
!	Кожний знак оклику означає отримання ICMP відлуння-відповіді	Пакет команди <i>ping</i> пересланий успішно
.	Кожна крапка означає, що минув час очікування відповіді мережевим сервером	Може бути ознакою одної з проблем: а) команда <i>ping</i> блокується списком керування доступу в маршрутизаторі; б) маршрутизатор не знайшов маршруту для доставки ICMP-повідомлення; в) в лінії є фізичні несправності з'єднання
U	Отримане нерозпізнане ICMP-повідомлення	Маршрутизатор не може знайти маршрут до адреси одержувача
C	Одержувач скидає отримані ICMP-пакети і вказує на необхідність придушення відправника даних	Пристрій на маршруті передачі, можливо, одержувач, отримав занадто багато пакетів даних; необхідно перевірити статистику черг пакетів
&	Минув час існування ICMP-пакета	Можливо, пакет зациквився

е) якщо на одному з етапів використання засобу *ping* виникають помилки, виконайте такі дії:

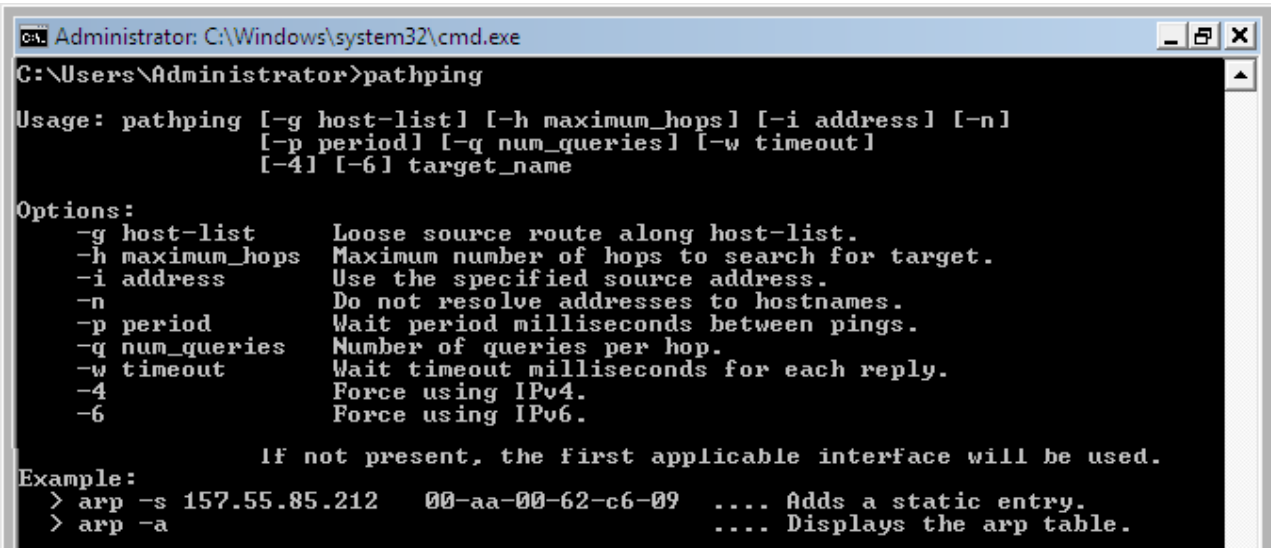
- переконайтеся, що IP-адреса локального комп'ютера дійсна і правильно задана на вкладці *Общие* діалогового вікна *Свойства протоколу Інтернету (TCP/IP)* або за допомогою засобу *ipconfig*;
- переконайтеся, що налаштований шлюз за замовчуванням і є зв'язок між вузлом і шлюзом за замовчуванням. Для вирішення проблем повинен бути налаштований тільки один шлюз за замовчуванням. Хоча шлюзів за замовчуванням може бути декілька, всі шлюзи крім першого використовуються тільки тоді, коли стек

TCP/IP визначає, що перший шлюз не працює. При усуненні неполадок визначається стан першого з налаштованих шлюзів. Для полегшення завдання всі інші шлюзи можна видалити.

### 3 Перевірка маршрутизації за допомогою засобу *PathPing*

*PathPing* - це засіб, який виявляє втрати пакетів на маршрутах їх проходження по мережі передачі даних, що включають кілька стрибків. Звернувшись за допомогою *PathPing* до віддаленого вузла, можна переконатися, що маршрутизатори, через які проходить пакет, працюють нормально (рисунок 8). Для цього служить така команда:

*pathping* IP-адреса віддаленого вузла.



```
C:\Users\Administrator>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
               [-p period] [-q num_queries] [-w timeout]
               [-4] [-6] target_name

Options:
  -g host-list      Loose source route along host-list.
  -h maximum_hops  Maximum number of hops to search for target.
  -i address        Use the specified source address.
  -n                Do not resolve addresses to hostnames.
  -p period         Wait period milliseconds between pings.
  -q num_queries    Number of queries per hop.
  -w timeout        Wait timeout milliseconds for each reply.
  -4                Force using IPv4.
  -6                Force using IPv6.

                If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a            .... Displays the arp table.
```

Рисунок 8 – Синтаксис та параметри команди *pathping*

### 4 Очистка кеша ARP за допомогою команди *arp*

Якщо звернення за адресою замикання на себе (127.0.0.1) і власною IP- адресою виконується успішно, але до всіх інших IP- адрес звернутися не вдається, необхідно очистити кеш протоколу ARP (рисунок 9).

```

C:\Users\Administrator>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                .... Displays the arp table.

```

Рисунок 9 – Синтаксис та параметри команди *arp*

За допомогою командного рядка виконайте одну з таких команд.

***arp -a*** (те ж саме *arp -g*).

Щоб видалити записи, введіть команду

***arp -d IP-адреса.***

Для очищення кеша ARP використовується така команда:

***netsh interface ip delete arpcache.***

## 5 Перевірка шлюзу за замовчуванням

Адреса шлюзу повинна знаходитися в тій же мережі, що і локальний вузол. Інакше повідомлення комп'ютері не будуть передаватися поза локальної мережі. Якщо адреса шлюзу належить тій же мережі, що і вузол, переконайтеся, що адреса шлюзу за

замовчуванням коректна. Шлюз за замовчуванням повинен бути маршрутизатором, а не тільки вузлом. Маршрутизатор повинен мати можливість передавати IP-дейтаграми.

## **6 Перевірка зв'язку за допомогою програмних засобів *tracert* или *Route***

Якщо шлюз за умовчанням відповідає правильно, зверніться до віддаленого вузла, щоб переконатись в правильній роботі міжмережєвих з'єднань. Якщо ці сполуки працюють некоректно, простежте шлях повідомлення до одержувача за допомогою службової команди *tracert*.

У більшості випадків при використанні команди *ping* відображаються чотири наступних повідомлення про помилки: **TTL Expired in Transit**. Це повідомлення про помилку означає, що кількість необхідних проходів через маршрутизатор перевищує час життя (TTL). Час життя можна збільшити за допомогою команди *ping -i*. Можливо, причина цієї помилки в тому, що маршрут проходження пакета є циклічним.

Щоб дізнатися, чи дійсно виник циклічний маршрут (через неправильну конфігурацію маршрутизаторів), використовуйте команду *tracert*.

**Destination Host Unreachable**. Це повідомлення про помилку означає, що до вузла - одержувача немає локального або віддаленого маршруту (на вузлі-відправнику або маршрутизаторі). Перевірте таблицю маршрутизації на локальному вузлі або маршрутизаторі.

**Request Timed Out**. Це повідомлення про помилку означає, що повідомлення з відлуння-запитами не було отримано протягом заданого періоду очікування. За замовчуванням він дорівнює 4 секундам. Період очікування можна збільшити за допомогою команди *ping -w*.

**Ping request could not find host**. Це повідомлення про помилку означає, що не вдається розв'язати ім'я вузла - одержувача. Перевірте ім'я і доступність серверів DNS или WINS.

## 7 Перевірка фільтрації пакетів

Помилки при фільтрації пакетів можуть порушити роботу системи дозволу адрес або підключення. Щоб дізнатися, чи є фільтрація пакетів джерелом проблеми, відключіть фільтрацію пакетів TCP/IP.

Для цього виконайте такі дії:

а) натисніть кнопку **Пуск** і послідовно оберіть пункти **Панель управління, Сеть и подключения к Интернету** і **Сетевые подключения**;

б) клацніть кнопкою миші значок підключення по локальній мережі, яке необхідно змінити, і оберіть пункт **Свойства**;

в) на вкладці **Общие** в списку **Отмеченные компоненты используются этим подключением** оберіть варіант **Протокол Интернета (TCP/IP)** і натисніть кнопку **Свойства**;

г) натисніть кнопку **Дополнительно** й перейдіть на вкладку **Параметры**;

д) у діалоговому вікні **Необязательные параметры** оберіть елемент **Фильтрация TCP/IP** і натисніть кнопку **Свойства**;

е) зніміть прапорець **Задействовать фильтрацию TCP/IP** (всі адаптери) і натисніть кнопку **ОК**. Спробуйте звернутись за адресою за його ім'ям DNS, ім'ям NetBIOS комп'ютера або IP-адресою. Якщо звернення виконане успішно, можливо, параметри фільтрації були неправильно встановлені або накладають занадто жорсткі обмеження. Наприклад, фільтрація може дозволити комп'ютеру виступати в ролі веб-сервера, але відключити ряд засобів, таких як віддалене адміністрування. Щоб розширити діапазон припустимих параметрів фільтрації, змініть припустимі значення для порту TCP, порту UDP і протоколу IP.

## 8 Перевірка підключення до визначеного сервера

Команда **netstat** відноситься до мережевих утиліт і доступна для використання в різних операційних системах. Команда **netstat** вміє показувати мережеві з'єднання (вхідні/вихідні), таблицю маршрутизації, статистику з мережних інтерфейсів і т.д.

Щоб визначити причину проблеми при підключенні до сервера через NetBIOS, виконайте команду *netstat -n* на цьому сервері. Це дозволить дізнатись, під яким ім'ям сервер зареєстрований в мережі.

Команда *netstat -n* виводить декілька імен, під якими зареєстрований комп'ютер. Серед цих імен повинне бути ім'я, схоже на те, що вказано на вкладці *Имя компьютера* вікна *Система*, доступного з панелі керування. Якщо такого імені немає, треба використовувати будь-яке інше унікальне ім'я, що виводиться командою *netstat* (рисунки 10 та 11).

Програмний засіб *Netstat* також може відображати кешовані записи віддалених комп'ютерів, що помічені #PRE в файлі Lmhosts або відносяться до нещодавно дозволених імен.

Якщо віддалені комп'ютери використовують для сервера одне і те саме ім'я, а інші комп'ютери знаходяться у віддаленій підмережі, переконайтесь, що для них задана відповідність «ім'я-адреса» в файлах Lmhosts або в серверах WINS.

```
C:\Users\Administrator>netstat /?
Displays protocol statistics and current TCP/IP network connections.
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

-a           Displays all connections and listening ports.
-b           Displays the executable involved in creating each connection or
            listening port. In some cases well-known executables host
            multiple independent components, and in these cases the
            sequence of components involved in creating the connection
            or listening port is displayed. In this case the executable
            name is in [] at the bottom, on top is the component it called,
            and so forth until TCP/IP was reached. Note that this option
            can be time-consuming and will fail unless you have sufficient
            permissions.
-e           Displays Ethernet statistics. This may be combined with the -s
            option.
-f           Displays Fully Qualified Domain Names (FQDN) for foreign
            addresses.
-n           Displays addresses and port numbers in numerical form.
-o           Displays the owning process ID associated with each connection.
-p proto     Shows connections for the protocol specified by proto; proto
            may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
            option to display per-protocol statistics, proto may be any of:
            IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r           Displays the routing table.
-s           Displays per-protocol statistics. By default, statistics are
            shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
            the -p option may be used to specify a subset of the default.
-t           Displays the current connection offload state.
interval    Redisplays selected statistics, pausing interval seconds
            between each display. Press CTRL+C to stop redisplaying
            statistics. If omitted, netstat will print the current
            configuration information once.
```

Рисунок 10 – Синтаксис та параметри команди *netstat*

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat
Active Connections

Proto Local Address           Foreign Address         State
TCP   127.0.0.1:19872          ASUS:49353              ESTABLISHED
TCP   127.0.0.1:49353        ASUS:19872              ESTABLISHED
TCP   192.168.1.4:49357      snt-re2-8a:http        ESTABLISHED
TCP   192.168.1.4:50528      fra07s29-in-f1:https   TIME_WAIT
TCP   192.168.1.4:50529      fra07s30-in-f14:https  TIME_WAIT
TCP   [::1]:389              ASUS:49159              ESTABLISHED
TCP   [::1]:389              ASUS:49160              ESTABLISHED
TCP   [::1]:389              ASUS:49165              ESTABLISHED
TCP   [::1]:49159            ASUS:ldap                ESTABLISHED
TCP   [::1]:49160            ASUS:ldap                ESTABLISHED
TCP   [::1]:49165            ASUS:ldap                ESTABLISHED
TCP   [fe80::1576:eb4e:2945:d046%11]:135  ASUS:50534              ESTABLISHED
TCP   [fe80::1576:eb4e:2945:d046%11]:389    ASUS:49171              ESTABLISHED
TCP   [fe80::1576:eb4e:2945:d046%11]:389    ASUS:49174              ESTABLISHED
TCP   [fe80::1576:eb4e:2945:d046%11]:49157  ASUS:49173              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49157  ASUS:49189              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49157  ASUS:49610              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49171  ASUS:ldap                ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49173  ASUS:49157              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49174  ASUS:ldap                ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49189  ASUS:49157              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:49610  ASUS:49157              ESTABLISHED
D
TCP   [fe80::1576:eb4e:2945:d046%11]:50527  ASUS:49157              TIME_WAIT
D
TCP   [fe80::1576:eb4e:2945:d046%11]:50534  ASUS:epmap              ESTABLISHED
D

```

Рисунок 11 – Приклад переліку активних підключень при використанні команди *netstat*

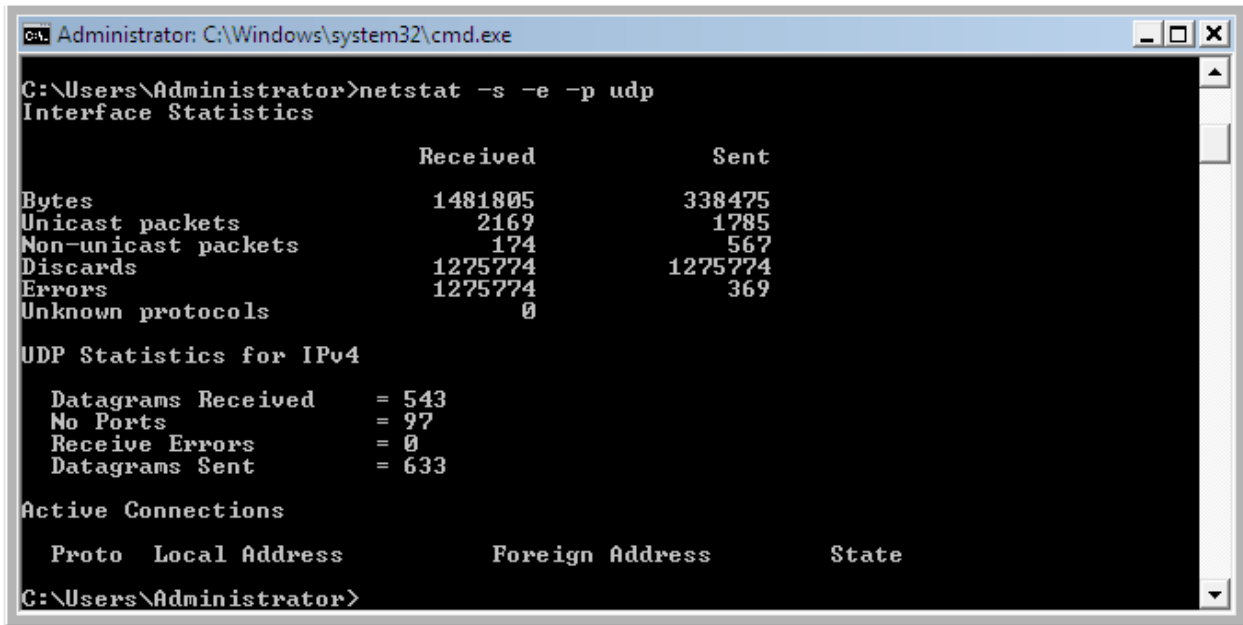
Для виведення статистики помилок в мережі, побудованій на основі технології Ethernet і статистики по всіх протоколах введіть таку команду (рисунок12):

*netstat -e -s.*

Для виведення статистики тільки за протоколами TCP і UDP введіть таку команду:

*netstat -s -p tcp udp.*





```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -s -e -p udp
Interface Statistics

                Received            Sent
Bytes            1481805            338475
Unicast packets    2169                1785
Non-unicast packets 174                 567
Discards          1275774            1275774
Errors            1275774            369
Unknown protocols    0

UDP Statistics for IPv4

Datagrams Received    = 543
No Ports              = 97
Receive Errors        = 0
Datagrams Sent        = 633

Active Connections

Proto Local Address          Foreign Address        State
C:\Users\Administrator>
```

Рисунок 12 – Приклад переліку статистичних даних з інтерфейсів при використанні команди *netstat*

Для виведення активних підключень TCP і кодів процесів кожні 5 секунд введіть таку команду:

***netstat -o 5.***

Для виведення активних підключень TCP і кодів процесів з використанням числового формату введіть таку команду (рисунки 13 та 14):

***netstat -n -o.***

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -n
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:19872 127.0.0.1:49353 ESTABLISHED
TCP 127.0.0.1:49353 127.0.0.1:19872 ESTABLISHED
TCP 192.168.1.4:49357 108.160.163.41:80 ESTABLISHED
TCP 192.168.1.4:50415 23.64.223.139:80 TIME_WAIT
TCP 192.168.1.4:50453 87.240.131.97:80 TIME_WAIT
TCP 192.168.1.4:50459 87.240.131.99:80 TIME_WAIT
TCP 192.168.1.4:50461 87.240.131.99:80 TIME_WAIT
TCP 192.168.1.4:50481 87.240.131.99:80 TIME_WAIT
TCP 192.168.1.4:50482 87.240.131.99:80 TIME_WAIT
TCP 192.168.1.4:50484 87.240.143.244:80 TIME_WAIT
TCP 192.168.1.4:50485 87.240.131.119:80 TIME_WAIT
TCP 192.168.1.4:50486 87.240.131.119:80 TIME_WAIT
TCP 192.168.1.4:50528 173.194.112.65:443 ESTABLISHED
TCP 192.168.1.4:50529 173.194.112.110:443 ESTABLISHED
TCP [::1]:389 [::1]:49159 ESTABLISHED
TCP [::1]:389 [::1]:49160 ESTABLISHED
TCP [::1]:389 [::1]:49165 ESTABLISHED
TCP [::1]:49159 [::1]:389 ESTABLISHED
TCP [::1]:49160 [::1]:389 ESTABLISHED
TCP [::1]:49165 [::1]:389 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:135 [fe80::1576:eb4e:2945:d046%11]:5052
4 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:135 [fe80::1576:eb4e:2945:d046%11]:5052
6 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:389 [fe80::1576:eb4e:2945:d046%11]:4917
1 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:389 [fe80::1576:eb4e:2945:d046%11]:4917
4 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49157 [fe80::1576:eb4e:2945:d046%11]:49
173 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49157 [fe80::1576:eb4e:2945:d046%11]:49
189 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49157 [fe80::1576:eb4e:2945:d046%11]:49
610 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49157 [fe80::1576:eb4e:2945:d046%11]:50
525 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49157 [fe80::1576:eb4e:2945:d046%11]:50
527 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49171 [fe80::1576:eb4e:2945:d046%11]:38
9 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49173 [fe80::1576:eb4e:2945:d046%11]:49
157 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49174 [fe80::1576:eb4e:2945:d046%11]:38
9 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49189 [fe80::1576:eb4e:2945:d046%11]:49
157 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:49610 [fe80::1576:eb4e:2945:d046%11]:49
157 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:50521 [fe80::1576:eb4e:2945:d046%11]:13
5 TIME_WAIT
TCP [fe80::1576:eb4e:2945:d046%11]:50524 [fe80::1576:eb4e:2945:d046%11]:13
5 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:50525 [fe80::1576:eb4e:2945:d046%11]:49
157 ESTABLISHED
TCP [fe80::1576:eb4e:2945:d046%11]:50526 [fe80::1576:eb4e:2945:d046%11]:13
5 ESTABLISHED

```

Рисунок 13 – Приклад переліку адрес і номерів портів у числовому поданні при використанні команди *netstat*

```

C:\Users\Administrator>netstat -n -o
Active Connections

Proto Local Address           Foreign Address         State                   PID
TCP   127.0.0.1:389            127.0.0.1:49160        ESTABLISHED            664
TCP   127.0.0.1:389            127.0.0.1:49162        ESTABLISHED            664
TCP   127.0.0.1:19872         127.0.0.1:49237        ESTABLISHED            3800
TCP   127.0.0.1:49160         127.0.0.1:389          ESTABLISHED            1200
TCP   127.0.0.1:49162         127.0.0.1:389          ESTABLISHED            1200
TCP   127.0.0.1:49237         127.0.0.1:19872        ESTABLISHED            3800
TCP   192.168.1.4:49257       108.160.163.46:80      ESTABLISHED            3800
TCP   192.168.1.4:64872       173.194.39.110:80      ESTABLISHED            4496
TCP   [fe80::1576:eb4e:2945:d046%11]:389 [fe80::1576:eb4e:2945:d046%11]:4918
3 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:389 [fe80::1576:eb4e:2945:d046%11]:4918
6 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:49156 [fe80::1576:eb4e:2945:d046%11]:49
176 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:49156 [fe80::1576:eb4e:2945:d046%11]:49
185 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:49156 [fe80::1576:eb4e:2945:d046%11]:49
388 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:49176 [fe80::1576:eb4e:2945:d046%11]:49
156 ESTABLISHED 2168
TCP   [fe80::1576:eb4e:2945:d046%11]:49183 [fe80::1576:eb4e:2945:d046%11]:38
9 ESTABLISHED 552
TCP   [fe80::1576:eb4e:2945:d046%11]:49185 [fe80::1576:eb4e:2945:d046%11]:49
156 ESTABLISHED 552
TCP   [fe80::1576:eb4e:2945:d046%11]:49186 [fe80::1576:eb4e:2945:d046%11]:38
9 ESTABLISHED 552
TCP   [fe80::1576:eb4e:2945:d046%11]:49388 [fe80::1576:eb4e:2945:d046%11]:49
156 ESTABLISHED 664
TCP   [fe80::1576:eb4e:2945:d046%11]:64869 [fe80::1576:eb4e:2945:d046%11]:13
5 TIME_WAIT 0

```

Рисунок 14 – Приклад виведення активних підключень TCP і кодів процесів з використанням числового формату при використанні команди *netstat*

Список всіх відкритих портів (TCP) можна отримати, якщо ввести команду (рисунок 15):

*netstat -at.*

Список всіх відкритих портів (UDP)

*netstat -au.*

Список портів, що прослуховуються (TCP),

*netstat -lt.*

```
C:\Users\Administrator>netstat -at
Active Connections
Proto Local Address           Foreign Address         State           Offload S
tate
TCP    0.0.0.0:88                ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:111             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:135             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:389             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:445             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:464             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:593             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:636             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:858             ASUS:0                 LISTENING      InHost
TCP    0.0.0.0:990             ASUS:0                 LISTENING      InHost
```

Рисунок 15 – Приклад виведення списку всіх відкритих портів TCP при використанні команди *netstat*

Статистика по всіх відкритих портах буде зібрана при виконанні команди (рисунок 16):

*netstat -s.*

Детальне відображення списку з відкритими портами - доданий персональний ідентифікаційний код PID та ім'я процесів може бути отримано при введенні команди

*netstat -p.*

Таблиці маршрутизації при використанні протоколів IPv4 і IPv6 можна вивести при виконанні команди (рисунок 17)

*netstat -r.*

Об'єднаємо всі ключі в корисну команду для перегляду відкритих TCP/UDP портів з іменами процесів (може знадобитися доступ до кореневого каталогу)

*netstat -ltupn.*

Список підключених хостів можна отримати при виконанні команди

```
netstat -lantp | grep ESTABLISHED | awk ' { print $ 5 }' | awk -F: ' { print $ 1 }' | sort -u .
```

```
Administrator: C:\Windows\system32\cmd.exe
Persistent Routes:
  None
C:\Users\Administrator>netstat -s

IPv4 Statistics

Packets Received                = 40980
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 0
Received Packets Discarded      = 96
Received Packets Delivered      = 42057
Output Requests                 = 30359
Routing Discards                = 0
Discarded Output Packets        = 19
Output Packet No Route          = 1
Reassembly Required             = 0
Reassembly Successful           = 0
Reassembly Failures            = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

IPv6 Statistics

Packets Received                = 0
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 0
Received Packets Discarded      = 0
Received Packets Delivered      = 15737
Output Requests                 = 15880
Routing Discards                = 0
Discarded Output Packets        = 0
Output Packet No Route          = 2
Reassembly Required             = 0
Reassembly Successful           = 0
Reassembly Failures            = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

ICMPv4 Statistics

                Received      Sent
Messages                20      13
Errors                   0        0
Destination Unreachable  20      13
Time Exceeded            0        0
Parameter Problems       0        0
Source Quenches          0        0
Redirects                 0        0
Echo Replies             0        0
Echos                    0        0
Timestamps               0        0
Timestamp Replies        0        0
Address Masks             0        0
Address Mask Replies      0        0
Router Solicitations     0        0
```

Рисунок 16 – Приклад виведення статистичних даних при використанні команди *netstat*

```

Administrator: C:\windows\system32\cmd.exe
C:\Users\Administrator>netstat -r
=====
Interface List
11 ...00 15 af 8b 91 04 ..... Atheros AR5007EG Wireless Network Adapter
1 ..... Software Loopback Interface 1
17 ..00 00 00 00 00 00 e0 isatap.{232F7290-6CCB-4D66-ACF5-9E8D586F9C83}
16 ...00 00 00 00 00 00 e0 isatap.{232F7290-6CCB-4D66-ACF5-9E8D586F9C83}
18 ...00 00 00 00 00 00 e0 isatap.{232F7290-6CCB-4D66-ACF5-9E8D586F9C83}
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1     192.168.1.4      25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.1.0                255.255.255.0   On-link         192.168.1.4      281
192.168.1.4                255.255.255.255 On-link         192.168.1.4      281
192.168.1.255             255.255.255.255 On-link         192.168.1.4      281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         192.168.1.4      281
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.1.4      281
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          192.168.1.1     Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128                    On-link
11 281 fe80::/64                 On-link
11 281 fe80::1576:eb4e:2945:d046/128
On-link
1 306 ff00::/8                   On-link
11 281 ff00::/8                   On-link
=====
Persistent Routes:
None
C:\Users\Administrator>

```

Рисунок 17 – Приклад виведення таблиць маршрутизації при використанні команди *netstat*

## 9 Перевірка віддалених підключень

Щоб визначити, чому не встановлюється підключення за протоколом TCP/IP з віддаленим комп'ютером, виконайте команду *netstat -a*, що показує стан усіх портів TCP і UDP локального комп'ютера.

Якщо підключення TCP працює правильно, в чергах Sent (Відправлено) і Received (Отримано) відображається 0 байт.

Якщо в одній з цих черг дані блокуються або вони мають стан «нерегулярні», підключення може бути несправним.

Якщо дані не блокуються, а черги перебувають у стані “typical”, то проблема, ймовірно, викликана затримкою у роботі мережі або програмі.

## 10 Перевірка таблиці маршрутизації за допомогою засобу *Route*

Для того щоб два вузли могли обмінюватись IP-дейтаграмами, вони повинні мати маршрути один до одного або використовувати стандартні шлюзи за замовчуванням. Щоб переглянути таблицю маршрутизації на комп'ютері під керуванням Windows 7, введіть команду *route print* (рисунок 18).



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 8:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\Administrator>route print
=====
Interface List
 11 ...00 15 af 8b 91 04 ..... Atheros AR5007EG Wireless Network Adapter
 1  ...00 00 00 00 00 00 e0 ..... Software Loopback Interface 1
 17 ...00 00 00 00 00 00 e0 isatap.{232F7290-6CCB-4D66-ACF5-9E8D586F9C83}
 16 ...00 00 00 00 00 00 e0 isatap.{232F7290-6CCB-4D66-ACF5-9E8D586F9C83}
 18 ...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          192.168.1.1     Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128 On-link
1 306 ff00::/8 On-link
=====
Persistent Routes:
None

C:\Users\Administrator>
```

Рисунок 18 – Синтаксис та параметри команди *route print*

## 11 Перевірка маршрутів за допомогою команди *Tracert*

Команда *tracert* (*tracert*) використовується для пошуку точок відмови на маршруті слідування пакетів від відправника до одержувача. Вона використовує лічильник часу життя пакета (Time-To-Live - TTL) як механізм, що забезпечує відповідь від кожного транзитного маршрутизатора на шляху до одержувача.

Синтаксис команди *tracert*:

```
tracert [-d] [-h максимальна_кількість_переходів] [-j список_вузлів]  
[-w інтервал] [ім'я_кінцевого_комп'ютера]/.
```

Засіб *Tracert* відправляє повідомлення з відлуння-запитами, збільшуючи на кожному кроці значення в IP-заголовку поля TTL, щоб визначити мережевий шлях між двома вузлами (рисунок 19). Потім програмний засіб *Tracert* аналізує повернуті ICMP-повідомлення.

Примітка - Кожен маршрутизатор, через який проходить шлях, повинен перед подальшою пересилкою пакета зменшити значення його поля TTL щонайменше на 1. Фактично, TTL - лічильник вузлів. Передбачається, що коли параметр TTL стає рівним 0, маршрутизатор посиляє системі - джерелу ICMP-повідомлення про закінчення часу. Команда *tracert* визначає маршрут, посылаючи перше відлуння-запит з полем TTL, рівним 1, і збільшуючи значення цього поля на одиницю для кожного наступного, відправляє відлуння-пакет до тих пір, поки кінцевий вузол не відповість або поки не буде досягнуто максимальне значення поля TTL. Максимальна кількість переходів за замовчуванням дорівнює 30 і може бути змінена за допомогою параметра *-h*. Шлях визначається з аналізу ICMP-повідомлень про закінчення часу, отриманих від проміжних маршрутизаторів, і відповідей точки призначення. Однак деякі маршрутизатори не посылають повідомлень про закінчення часу для пакетів з нульовими значеннями TTL і не видно для команди *tracert*. У цьому випадку для переходу відображається ряд зірочок (\*).



```
Administrator: C:\Windows\system32\cmd.exe
UDP [fe80::1576:eb4e:2945:d046%11]:88 **
UDP [fe80::1576:eb4e:2945:d046%11]:111 **
UDP [fe80::1576:eb4e:2945:d046%11]:389 **
UDP [fe80::1576:eb4e:2945:d046%11]:464 **

C:\Users\Administrator>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
-d          Do not resolve addresses to hostnames.
-h maximum_hops  Maximum number of hops to search for target.
-j host-list  Loose source route along host-list (IPv4-only).
-w timeout    Wait timeout milliseconds for each reply.
-R          Trace round-trip path (IPv6-only).
-S srcaddr   Source address to use (IPv6-only).
-4          Force using IPv4.
-6          Force using IPv6.

C:\Users\Administrator>
```

Рисунок 19 – Синтаксис та параметри команди *tracert*

Щоб виконати трасування маршруту за допомогою команди *tracert*, відкрийте вікно "*Командний рядок*" і введіть таку команду (рисунки 20 та 21):

*tracert ім'я\_вузла*

або

*tracert IP –адреса,*

де *ім'я\_вузла* або *IP- адреса* - ім'я вузла або IP- адреса віддаленого комп'ютера.

Наприклад, щоб виконати трасування маршруту від локального комп'ютера до вузла *www.microsoft.com*, введіть таку команду:

*tracert www.microsoft.com.*

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>tracert mail.ru

Tracing route to mail.ru [217.69.139.201]
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms    192.168.1.1
  1  *        *        *        Request timed out.
  2  34 ms   30 ms   30 ms   10.50.40.2
  3  *        *        *        Request timed out.
  4  53 ms   50 ms   68 ms   ae6.dl10.m9.net.mail.ru [94.100.183.94]
  5  49 ms   49 ms   49 ms   ae10.dl12.net.mail.ru [94.100.183.114]
  6  105 ms  56 ms   95 ms   ko.mail.ru [217.69.139.201]

Trace complete.
```

Рисунок 20 – Приклад трасування маршруту за ім'ям домена з використанням команди *tracert*

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>tracert 172.10.16.24

Tracing route to 172-10-16-24.lightspeed.clmasc.sbcglobal.net [172.10.16.24]
over a maximum of 30 hops:

  0  1 ms    1 ms    2 ms    192.168.1.1
  1  *        *        *        Request timed out.
  2  31 ms   30 ms   30 ms   10.50.19.2
  3  73 ms   69 ms   69 ms   dialup-212.162.26.85.frankfurt1.mik.net [212.162.26.85]
  4  145 ms  146 ms  151 ms  v1-3101-ve-127.ebr1.Budapest1.Level3.net [4.69.201.149]
  5  145 ms  144 ms  144 ms  ae-44-44.ebr3.Frankfurt1.Level3.net [4.69.201.114]
  6  145 ms  144 ms  144 ms  ae-83-83.csw3.Frankfurt1.Level3.net [4.69.163.101]
  7  149 ms  147 ms  145 ms  ae-82-82.ebr2.Frankfurt1.Level3.net [4.69.140.251]
  8  145 ms  145 ms  145 ms  ae-21-21.ebr2.London1.Level3.net [4.69.148.185]
  9  145 ms  143 ms  144 ms  ae-44-44.ebr1.NewYork1.Level3.net [4.69.137.78]
 10  146 ms  145 ms  146 ms  ae-81-81.csw3.NewYork1.Level3.net [4.69.134.74]
```

Рисунок 21 – Приклад трасування маршруту за IP-адресою з використанням команди *tracert*

Щоб команда *tracert* не дозволяла і не виводила на екран імена всіх маршрутизаторів на шляху, використовуйте параметр *-d*. Це спростить вигляд шляху. Наприклад, щоб виконати трасування маршруту від локального комп'ютера до вузла [www.microsoft.com](http://www.microsoft.com) без відображення імен маршрутизаторів, введіть таку команду:

## Примітки

1 Щоб відкрити командний рядок, натисніть кнопку **Пуск**, наведіть курсор на **Всі програми**, виберіть **Стандартні**, а потім клацніть **Командний рядок**.

Команда **tracert** визначає шлях, відправляючи ICMP-повідомлення «відлуння-запит» і «відлуння-відповідь» (подібно до команди **ping**) для виведення на екран відомостей про кожний пройдений маршрутизатор і про час обміну даними (RTT) з кожним з них. Політики фільтрування пакетів на маршрутизаторах, брандмауерах та інших шлюзах безпеки можуть забороняти пересилання цього трафіку.

2 Якщо трасування маршруту за допомогою програми **tracert** закінчилося невдачею, то на підставі виведених нею даних можна визначити, який проміжний маршрутизатор не пересилає дані далі чи робить це занадто повільно.

3 Для отримання докладних відомостей про перенаправлення і втрати пакетів на кожному маршрутизаторі і засланні, через які проходить цей шлях, використовуйте команду **pathping**.

4 Команда **tracert** послідовно опитує і вимірює час затримки до всіх маршрутизаторів на шляху проходження пакета, поки не буде досягнутий цільовий хост. **Tracert** дозволяє простежувати шлях, що не перевищує 30 стрибків. Якщо між якими-небудь двома маршрутизаторами спостерігається велике зростання затримки, значить, ця ділянка маршруту має несправності. **Tracert** визначає причину несправності, коли при проходженні через який-небудь маршрутизатор відбувається помилка або маршрут утворює замкнутий цикл.

Після того, як виявлений несправний маршрутизатор, необхідно або звернутись до адміністратора маршрутизатора з метою відновлення його справності, якщо маршрутизатор знаходиться в іншій мережі, або самотійно відновити працездатність маршрутизатора, якщо він знаходиться у даній мережі локального доступу.

При проведенні трасування маршруту проходження пакетів можуть бути отримані коди, наведені нижче, а також коди, наведені в таблиці 2:

- !N - мережа недосяжна;
- !H - вузол недосяжний;
- !P - неприпустимий протокол;
- !F - пакет перевищує припустиму довжину;
- !X - адміністративна заборона на доступ до вузла (фільтр, проксі-сервер, і т.ін.);
- \* - немає відгуку.

Таблиця 2 – Коди, що повертаються командою *tracert*

Код	Значення	Імовірна причина
nn msec	Час передачі пакета (в мілісекундах) між вузлами	Трасування пройшло успішно
*	Минув час очікування запиту	Пристрій, що контролюється, не отримав запит або не відповів на ICMP-повідомлення “packet life exceeded” (“перевищений час життя пакета”)
A	Пересилка пакетів адміністративно заборонена	Пристрій на маршруті, наприклад, маршрутизатор або брандмауер, блокує пакети команди <i>tracert</i> , але пересилає всі інші пакети
Q	Відправник скидає отримані ICMP-пакети і вимагає придушення джерела пакетів	Пристрій на маршруті передачі, можливо, одержувач, отримав надто багато пакетів даних; необхідно перевірити статистику черг пакетів
H	Отримане нерозпізнане ICMP-повідомлення	Можливо, виникло зациклення маршрутизації

Слід також враховувати, що основне завдання маршрутизаторів - це передавати пакети з корисною інформацією, а не відповідати на команди *tracert* і *ping*. Тому деякі маршрутизатори на шляху проходження пакета можуть здійснювати команду *ping* навіть із втратою пакетів, але при цьому цільовий хост буде доступний без втрати пакетів.

Примітка - Команда **tracert** має декілька параметрів, які можна змінювати при проведенні трасування маршрутів:

**-d** – запобігає спробі команди **tracert** дозволу IP-адрес проміжних маршрутизаторів в імена. Збільшує швидкість виведення результатів команди **tracert**;

**-h** – максимальна кількість переходів. Задає максимальну кількість переходів на шляху при пошуку кінцевого об'єкта. Значення за замовчуванням дорівнює 30;

**-j** – список вузлів. Вказується для повідомлень з відлуння-запитом 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 або декількома маршрутизаторами. Максимальна кількість адрес або імен у списку – 9. Список адрес являє набір IP-адрес (в точково - десятковій нотації), розділених пробілами;

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

**ім'я\_кінцевого\_комп'ютера** – задає точку призначення, зазначену IP-адресою або ім'ям вузла.

**-?** – відображає довідку в командному рядку.

## 12 Усунення несправностей в шлюзах

Якщо при налаштуванні було отримано таке повідомлення, з'ясуйте, чи знаходиться шлюз за замовчуванням в тій же логічній мережі, що і мережевий адаптер комп'ютера:

**Your default gateway does not belong to one of the configured interfaces**

Порівняйте частину IP-адреси шлюзу за замовчуванням, відповідну ідентифікатору мережі, з ідентифікаторами мережі

мережевих адаптерів комп'ютера. Зокрема, перевірте, чи результат дорівнює логічній операції “Г” IP- адреси і маски підмережі результату логічної операції “Г” основного шлюзу і маски підмережі.

Наприклад, якщо комп'ютер має один мережевий адаптер з IP-адресою 172.16.27.139 і маскою підмережі 255.255.0.0 , шлюз за замовчуванням повинен мати адресу 172.16.y.z. Ідентифікатор мережі для цього інтерфейсу IP - 172.16.0.0.

## **6 ЗМІСТ ЗВІТУ З ЛАБОРАТОРНОЇ РОБОТИ**

Згідно з завданням, отриманим від викладача, здійснити контроль технічного стану мережі локального доступу та провести трасування маршрутів передачі пакетів даних.

Всі результати контролю технічного стану локальної мережі необхідно відобразити у звіті з лабораторної роботи у вигляді скриншотів. В кінці звіту навести висновки щодо результатів проведеної лабораторної роботи.

## **СПИСОК ЛІТЕРАТУРИ**

1 ITU-T Recommendation. X.200 (1994 E). Data networks and open system communications. Open system interconnection – model and notation. Information technology – open systems interconnection – basic reference model: the basic model. – 63 p.

2 ISO/IEC 10731:1994. Information technology -- Open Systems Interconnection -- Basic Reference Model -- Conventions for the definition of OSI services TC ISO/IEC JTC 1 ICS 35.100.01. Document available as of 1994-12-15. – 23 p.

3 Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство. - 3-е изд., с испр.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2008. – 1168 с.

4 Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство: Пер. с англ. – М.: ООО “Издательский дом Вильямс”, 2008. – 994 с.

5 Современные компьютерные сети. 2-е изд. / В. Столлингс. – СПб.: Питер, 2003. – 783 с.