Методичні вказівки до виконання лабораторних робіт

Лабораторна робота №1

Утиліти TCP/IP

Мета роботи: практично оволодіти роботою з утилітами TCP/IP, необхідними в наступних роботах.

Рекомендації для навчання

Діагностичні утиліти TCP/IP.

TCP/IP включає діагностичні утиліти, призначені для перевірки конфігурації стека та перевірки підключення до мережі.

Утиліта	Застосування
hostname	Виводить назву локального хоста. Використовується без параметрів.
ipconfig	Відображає значення для поточної конфігурації стека TCP/IP: IP-адреса, маска підмережі, адреса шлюзу за замовчуванням, адреса служби імен WINS (Windows Internet Naming Service) та DNS (Domain Name System)
ping	Перевіряє правильність конфігурації TCP/IP і перевіряє зв'язок з віддаленим хостом.
tracert	Перевіряє маршрут до віддаленого комп'ютера шляхом надсилання ехо-пакетів протоколу Internet Control Message Protocol (ICMP). Відображає маршрут пакетів на віддалений комп'ютер.
arp	Дисплеї для перегляду та зміни протоколу роздільної здатності адрес (ARP)
route	Модифікує таблиці маршрутизації IP. Відображає вміст таблиці, додає і видаляє IP-маршрути.
netstat	Відображає статистику та актуальну інформацію по TCP/IP з'єднанню.
nslookup	Перевіряє записи хостів і псевдоніми доменів, служби доменів хостів та інформацію про операційну систему шляхом запиту DNS-серверів.
telnet	Підключається до іншого хоста за допомогою протоколу емуляції терміналу TELNET. Він використовується для перевірки працездатності мережевих служб, що використовують порти TCP (наприклад, можливість підключення до поштового сервера за протоколами POP3 і SMTP).

1. Переконайтеся, що конфігурація TCP/IP правильна, використовуючи ipconfig.

Під час виправлення неполадок і неполадок мережі TCP/IP спочатку слід переконатися в правильності конфігурації TCP/IP. Для цього використовується утиліта ipconfig.

Ця команда корисна на комп'ютерах з протоколом динамічної конфігурації хоста (DHCP), оскільки вона дозволяє користувачам визначати, яку конфігурацію мережі TCP/IP і значення було встановлено DHCP.

Синтаксис:

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

Параметри:

all	відображає весь список параметрів. Без цього ключа відображаються лише IP-адреса, маска та шлюз за замовчуванням;
renew[adapter]	оновлює параметри конфігурації DHCP для вказаного мережевого адаптера;
release[adapter]	звільняє IP-адресу, виділену DHCP; adapter – назва мережевого адаптера;
displaydns	відображає інформацію про вміст локального кешу DNS-клієнта, який використовується для вирішення доменних імен.

Таким чином, утиліта ipconfig дозволяє дізнатися, чи ініціалізована конфігурація і чи не дублюються IP-адреси:

- якщо конфігурація ініціалізована, то з'являється IP-адреса, маска, шлюз;
- якщо IP-адреси дублюються, маска мережі буде 0.0.0.0;
- якщо комп'ютер не може отримати IP-адресу під час використання DHCP, вона буде 0.0.0.0.

2. Тестування зв'язку за допомогою утиліти *ping*.

Утиліта ping (Packet Internet Grouper) використовується для перевірки конфігурації TCP/IP та діагностики помилок підключення. Він визначає доступність і функціонування того чи іншого господаря. Використання ping є найкращим способом перевірки існування маршруту між локальним комп'ютером і мережевим хостом. Хост – це будь-який мережевий пристрій (комп'ютер, маршрутизатор), який обмінюється даними з іншими мережевими пристроями через TCP/IP.

Команда ping перевіряє з'єднання з віддаленим вузлом, надсилаючи відлуння ICMP цьому вузлу та прослуховуючи відповіді відлуння. Ping чекає на кожен відправлений пакет і друкує кількість відправлених і отриманих пакетів. Кожен отриманий пакет перевіряється відповідно до відправленого повідомлення. Якщо зв'язок між хостами поганий, то з повідомлень пінгу буде зрозуміло, скільки пакетів втрачено.

За замовчуванням передається 4 ехо-пакета довжиною 32 байти (можливі й інші варіанти значення за замовчуванням) - періодична послідовність символів в алфавіті у верхньому регістрі. Ping дозволяє змінити розмір і кількість пакетів, вказати, чи записувати маршрут, який він використовує, яке значення time-to-live (ttl) встановити, чи можна фрагментувати пакет і так далі. Коли надходить відповідь, поле часу вказує, скільки часу (у мілісекундах) потрібно, щоб надісланий пакет досяг віддаленого хоста та повернувся назад. Оскільки за замовчуванням значення очікування відповіді становить 1 секунду, всі значення в цьому полі будуть менше 1000 мілісекунд. Якщо ви отримали повідомлення "Request time out", можливо, якщо ви збільшите тайм-аут відповіді, пакет дійде до віддаленого хосту. Зробити це можна за допомогою перемикача –w.

Ping можна використовувати для перевірки як імені хоста (DNS або NetBIOS), так і його IP-адреси. Якщо пінг IP-адреси вдався, а ім'я не вдалося, це означає, що проблема полягає в збігу адреси та імені, а не в мережевому з'єднанні.

Утиліта ping використовується наступними способами:

1) Щоб переконатися, що TCP/IP встановлений і налаштований правильно на локальному комп'ютері, команда ping вказує адресу зворотного зв'язку: ping 127.0.0.1

Якщо тест пройдено, ви отримаєте наступну відповідь:

Відповідь від 127.0.0.1: кількість байтів=32 час<1 мс TTL=128
Відповідь від 127.0.0.1: кількість байтів=32 час<1 мс TTL=128
Відповідь від 127.0.0.1: кількість байтів=32 час<1 мс TTL=128
Відповідь від 127.0.0.1: кількість байтів=32 час<1 мс TTL=128

2) Щоб переконатися в тому, що комп'ютер коректно доданий в мережу і IP-адреса не дублюється, використовується IP-адреса локального комп'ютера:

ping адреса localhost_IP

3) Щоб переконатися, що шлюз за замовчуванням працює і що можна встановити з'єднання з будь-яким локальним хостом у локальній мережі, встановлюється IP-адреса шлюзу за замовчуванням:

ping адреса gateway_IP

4) Для перевірки можливості встановлення з'єднання через роутер у команді ping вказується IP-адреса віддаленого хоста:

Пропінгуйте IP_address віддаленого хоста

Синтаксис:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k список хостів]] [-w timeout] destination-list

Параметри:

-t виконує команду ping перед перериванням. Control-Break - перегляд статистики і продовження. Control-C - Перервати виконання команди;

-a дозволяє визначити доменне ім'я віддаленого комп'ютера за його IP-адресою;

-n count надсилає кількість ECHO-пакетів, задану параметром count;

-l length відправляє пакети з довжиною в байти (максимальна довжина становить 8192 байти);

-f відправляє пакет з встановленим прапорцем "Не фрагментувати". Цей пакет не буде фрагментуватися на маршрутизаторах по дорозі;

-i ttl встановлює час життя пакета на ttl (кожен маршрутизатор зменшує ttl на одиницю);

-v tos встановлює тип поля "service" на значення tos;

-r count записує шлях до вихідного пакета та пакета, що повертається, у поле запису шляху. Кількість - від 1 до 9 хостів;

-s count дозволяє обмежити кількість переходів з однієї підмережі в іншу (hops). Count встановлює максимально можливу кількість стрибків;

-j host-list маршрутизує пакети, використовуючи список хостів, визначений параметром host-list. Послідовні хости можуть бути розділені проміжними маршрутизаторами (гнучка статична маршрутизація). Максимальна кількість хостів у списку, дозволеному IP – 9;

-k host-list маршрутизує пакети через список хостів, визначений у host-list. Послідовні хости не можуть бути розділені проміжними маршрутизаторами (жорстка статична маршрутизація). Максимальна кількість хостів – 9;

-w timeout визначає час очікування відповіді від віддаленого хоста в мілісекундах (1 секунда за замовчуванням);

destination-list вказує віддалений хост, на який повинні бути спрямовані пакети ping.

Приклад використання утиліти ping:

C:\WINDOWS>ping –n 10 www.netscape.com

Обмін пакетами з www.netscape.com [205.188.247.65] до 32 байт:

Відповідь 205.188.247.65: Байт=32 Час=194 мс TTL=48
Відповідь 205.188.247.65: кількість байтів=32 час=240мс TTL=48
Відповідь від 205.188.247.65: кількість байтів=32 час=173мс TTL=48
Відповідь від 205.188.247.65: кількість байтів=32 час=250мс TTL=48
Відповідь 205.188.247.65: кількість байтів=32 час=187мс TTL=48
Відповідь 205.188.247.65: кількість байтів=32 час=239мс TTL=48
Відповідь 205.188.247.65: кількість байтів=32 час=263 мс TTL=48
Відповідь 205.188.247.65: Кількість байтів=32 час=230мс TTL=48
Відповідь: 205.188.247.65: кількість байтів=32 час=185мс TTL=48
Відповідь від 205.188.247.65: кількість байтів=32 час=406 мс TTL=48
Статистика Ping для 205.188.247.65:
Пакети: відправлено = 10, отримано = 10, втрачено = 0 (0% втрати)
Приблизний час передачі та прийому:
Найнижчий = 173 мс, найвищий = 406 мс, середній = 236 мс

Якщо немає можливості перевірити доступність хоста, утиліта виводить інформацію про помилку. Нижче наведено приклад відповіді утиліти ping при спробі відправити запит на неіснуючий хост.

Обмін пакетами від 172.16.6.21 до 32 байт:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Статистика пінгу за 172.16.6.21: Пакети: відправлено = 4, отримано = 0, втрачено = 4 (100% втрати),

приблизний час передачі та прийому: мінімум = 0мс, найбільший = 0мс, середній = 0мс

Утиліта не повідомляє, що хоста немає, але що відповідь на відправлений запит не була отримана протягом відведеного часу. Причиною може бути перевантаження або неправильна настройка роутерів і т.д. Помилка «мережа недоступна» (network unreachable) прямо вказує на проблеми маршрутизації.

3. Вивчіть маршрут між мережевими з'єднаннями за допомогою утиліти *tracert*.

Tracert — це утиліта для відстеження маршрутів. Він використовує поле TTL (time-to-live) IP-пакета та повідомлень про помилки ICMP для визначення маршруту від одного хоста до іншого.

Утиліта tracert може бути більш повною та зручною, ніж ping, особливо у випадках, коли віддалений хост недоступний. З його допомогою можна визначити зону проблем зі зв'язком (у інтернет-провайдера, в основній мережі, в мережі віддаленого хоста) по тому, на яку відстань буде відслідковуватися маршрут. При виникненні проблем утиліта відображає зірочки (*) або повідомлення на кшталт «Destination net unreachable», «Destination host unreachable», «Request time-out», «Time Exeededed».

Утиліта tracert працює наступним чином: на кожен хост, через який проходить маршрут до віддаленого хосту, відправляється 3 тестових ехо-пакета. На екрані відображається час очікування для кожної відповіді пакета (це можна змінити за допомогою опції -w). Пакети відправляються з різним терміном служби. Кожен маршрутизатор на шляху зменшує TTL на одиницю перед пересиланням пакета. Таким чином, термін служби є лічильником проміжних точок видачі (хмелю). Коли термін служби пакета досягне нуля, очікується, що маршрутизатор надішле ICMP-повідомлення «Час виконання» на вихідний комп'ютер. Маршрут визначається відправкою першого ехо-пакета з TTL=1. Потім TTL збільшується на 1 у кожному наступному пакеті, доки пакет не досягне віддаленого хоста або не буде досягнуто максимально можливого TTL (за замовчуванням 30, що визначається параметром -h).

Маршрут визначається шляхом вивчення повідомлень ICMP, які надсилаються назад проміжними маршрутизаторами.

Примітка: Деякі маршрутизатори просто безшумно знищують пакети з простроченим TTL і не будуть видимі утиліті tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] ім’я_цільового_хоста

Параметри:

-d	вказує, що вам не потрібно розпізнавати адреси для імен хостів;
-h maximum_hops	вказує максимальну кількість переходів (хопів) для пошуку цілі;
-j host-list	вказує нежорстку статичну маршрутизацію відповідно до host-list;
-w timeout	визначає, що ви повинні очікувати відповідь на кожен ехо-пакет протягом вказаної кількості мс.

4. Утиліта *arp*.

Основне призначення протоколу ARP полягає в перекладі IP-адрес на відповідні локальні адреси. Для цього в протоколі ARP використовується інформація з таблиці ARP (кеш ARP). Якщо необхідний запис в таблиці не знайдена, протокол ARP відправляє широкомовний запит на всі комп'ютери локальної підмережі в спробі знайти власника цього IP-адреси. Кеш може містити два типи записів: статичні та динамічні. Статичні записи вводяться вручну і зберігаються в кеші постійно. Динамічні записи кешуються в результаті широкомовних запитів. Для них існує поняття життєвого часу. Якщо запис не було заявлено протягом певного часу (за замовчуванням 2 хвилини), його буде видалено з кешу.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметри:

-s статичні записи кешу;

-d Видалити запис для певної IP-адреси з кешу;

-a перегляд вмісту кешу для всіх мережевих адаптерів на локальному комп'ютері;

inet_addr - IP-адреса;

eth_addr - MAC-адреса.

Виведення таблиці кешу ARP для інтерфейсу, якому призначена IP-адреса 10.0.0.99:

arp -a -N 10.0.0.99

Додавання статичного запису кешу ARP, який зіставляє IP-адресу 10.0.0.80 з фізичною адресою 00-AA-00-4F-2A-9C:

arp - 10.0.0.80 00-AA-00-4F-2A-9C

5. Утиліта route.

Утиліта **route** призначена для роботи з локальною таблицею маршрутизації. У ньому є наступне

Синтаксис:
route [-f] [-p] [команда [вузол] [MASK маска] [шлюз] [METRIC метрика] [IF інтерфейс]]

Параметри:

-f Очищення таблиці маршрутів.

-p Якщо його вказано в поєднанні з командою ADD, він створює постійний запис, який зберігається і після перезавантаження комп'ютера. За замовчуванням записи таблиці маршрутизації не зберігаються при перезавантаженні.

команда Одна з чотирьох команд:

PRINT - відображення інформації про маршрут;

ADD - додавання маршруту;

DELETE - видалити маршрут;

CHANGE - змінити маршрут.

вузол Адресований вузол

маска Маска підмережі Маска за замовчуванням – 255.255.255

шлюз Адреса шлюзу

метрика метрика маршруту;

інтерфейс Ідентифікатор інтерфейсу, який буде використовуватися для пересилання пакета

Для команд PRINT і DELETE можна використовувати символи узагальнення при вказівці адресного хоста або шлюзу. Параметр шлюзу для цих команд можна опустити.

При додаванні та зміні маршрутів утиліта маршруту звіряє введену інформацію з умовою (NODE & MASK) == NODE. Якщо ця умова не виконується, утиліта генерує повідомлення про помилку і не додає і не змінює маршрут.

Утиліта шукає назви мереж у файлі мереж. Пошук назв шлюзів здійснюється у файлі hosts. Обидва файли знаходяться в папці %systemroot%\system32\drivers\etc. Наявність і заповнення цих файлів не обов’язкове для нормального функціонування утиліти route і роботи

маршрутизації.

Хоча в більшості випадків він не потрібен на робочій станції, ви можете вручну редагувати таблиці маршрутизації.

Приклад використання утиліти route:

route add 172.16.6.0 MASK 255.255.255.0 172.16.11.1 METRIC 1 IF 0x1000003

6. Утиліта *netstat*.

Утиліта netstat дозволяє отримувати статичну інформацію по деяких протоколах стека (TCP, UDP, IP, ICMP), а також відображає інформацію про поточні мережевих підключеннях. Особливо він корисний на брандмауерах, з його допомогою можна виявити порушення безпеки периметра мережі.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметри:

-a виводить список усіх мережевих з'єднань та портів для прослуховування на локальному комп'ютері;

-e відображає статистику інтерфейсів Ethernet (наприклад, кількість прийнятих і відправлених байтів);

-n відображає дані щодо усіх поточних з'єднань (наприклад, TCP) для всіх мережевих інтерфейсів на локальному комп'ютері. Для кожного підключення відображається інформація про IP-адреси локального та віддаленого інтерфейсів, а також номери використовуваних портів;

-s відображає статистичну інформацію для протоколів UDP, TCP, ICMP, IP. Клавіша "/more" дозволяє переглядати інформацію посторінково;

-r виводить вміст таблиці маршрутизації.

7. Утиліта *nslookup*.

Утиліта **nslookup** призначена для діагностики служби DNS, у найпростішому випадку для запиту DNS-серверів для перетворення імен на IP-адреси. В цілому утиліта дозволяє переглядати будь-які записи DNS-сервера:

A – канонічне ім'я хоста, якому доменне ім'я відповідає ip-адресою.

SOA - *початок* повноважень, початковий запис, єдиний для зони;

MX – поштові сервери (хости, які приймають пошту для заданого домену);

NS – сервери імен (містять авторитетні DNS-сервери для зони);

PTR – покажчик (використовується для перетворення IP-адреси назад у символьне ім'я хоста)

Тощо.

Утиліта nslookup досить складна і містить власний інтерпретатор команд.

У найпростішому випадку (без входу в командний режим) **утиліта nslookup** має наступне

Синтаксис:

nslookup хост [сервер]

```
nslookup wikipedia.org
```

Параметри:

Хост Ім'я хоста DNS, яке потрібно перевести на IP-адресу.

Сервер Адреса DNS-сервера, який буде використовуватися для визначення імені. Якщо цей параметр не вказано, адреси DNS-серверів із параметрів конфігурації TCP/IP використовуватимуться послідовно.

Приклади використання утиліти nslookup:

1. Отримати список серверів імен для домену yandex.ru без входу в командний режим (за допомогою ключів).

```
C:\> nslookup -type=ns yandex.ru
Default Server:  dns.google
Address:  8.8.8.8

Неавторитетна відповідь:
yandex.ru       nameserver = ns1.yandex.ru
yandex.ru       nameserver = ns2.yandex.ru
```

2. Отримайте запис SOA домену yandex.ru з авторитетного сервера за допомогою оболонки nslookup.

```
C:\>nslookup
Сервер за замовчуванням: dns.google
Адреса: 217.10.39.4
> set type=SOA
> ns2.yandex.ru сервера
Сервер за замовчуванням: ns2.yandex.ru
Адреса: 213.180.199.34
> yandex.ru
Сервер: ns1.yandex.ru
Адреса: 213.180.193.1
>yandex.ru
        Сервер первинних імен = ns1.yandex.ru
        Відповідальна пошта ADDR = sysadmin.yandex-team.r
        серійний = 2009022707
        Оновлення = 1800 (30 хв)
        повторна спроба = 900 (15 хв)
        термін дії = 2592000 (30 днів)
        за замовчуванням TTL = 900 (15 хв)
yandex.ru сервер імен = ns1.yandex.ru
yandex.ru сервер імен = ns2.yandex.ru
ns1.yandex.ru інтернет-адреса = 213.180.193.1
ns2.yandex.ru інтернет-адреса = 213.180.199.34
> вихід
```

3. Отримайте адресу поштового сервера для домену yandex.ru.

```
C:\ >nslookup
Сервер за замовчуванням: dns01.catv.ext.ru
Адреса: 217.10.44.35
> множина q=mx
> yandex.ru
Сервер: dns01.catv.ext.ru
```

Адреса: 217.10.44.35
Неавторитетна відповідь:
yandex.ru Перевага MX = 10, поштовий обмінник = mx2.yandex.ru
yandex.ru Перевага MX = 10, поштовий обмінник = mx3.yandex.ru
yandex.ru Перевага MX = 10, поштовий обмінник = mx1.yandex.ru
yandex.ru сервер імен = ns2.yandex.ru
yandex.ru сервер імен = ns1.yandex.ru
mx1.yandex.ru інтернет-адреса = 77.88.21.89
mx2.yandex.ru інтернет-адреса = 93.158.134.89
mx3.yandex.ru інтернет-адреса = 213.180.204.89
ns2.yandex.ru інтернет-адреса = 213.180.199.34
>

Вказавши ключ type=any, ви можете отримати всі записи про вузол або домен. Ключі querytype, t, q еквівалентні типу.

8. Утиліта *telnet.*

Утиліта telnet (_en. **TELecommunication NET**work) реалізує клієнтську частину мережевого протоколу telnet, яка організовує текстовий інтерфейс по мережі (з використанням транспортного протоколу TCP).

Історично склалося так, що Telnet використовувався для віддаленого доступу до CLI операційних систем. Згодом його почали використовувати і для інших текстових інтерфейсів, включаючи MUD-ігри та анімоване ASCII-мистецтво. Теоретично навіть обидві сторони протоколу можуть бути програмами, а не людьми.

Іноді telnet-клієнти використовуються для доступу до інших протоколів, заснованих на транспорті TCP.

Протокол telnet використовується в керуючому з'єднанні FTP, що означає, що вхід на сервер за допомогою `команди telnet ftp.example.net ftp` для виконання налагодження та експериментів не тільки можливий, але **й правильний** (на відміну від використання telnet-клієнтів для доступу до HTTP, IRC та більшості інших протоколів).

Протокол не передбачав шифрування та аутентифікації даних. Тому він вразливий до будь-якого виду TCP-атаки. В даний час для функціональності віддаленого доступу використовується мережевий протокол SSH (особливо версії 2), який був створений з урахуванням безпеки. Майте на увазі, що сеанс telnet має дуже низький рівень безпеки, якщо він не проводиться в повністю контрольованій мережі або з безпекою мережевого рівня (різні реалізації віртуальних приватних мереж). Через свою ненадійність від telnet як засобу управління операційними системами давно відмовилися.

Однак клієнт telnet підходить для ручного доступу (наприклад, з метою налагодження) до протоколів прикладного рівня, таких як HTTP, IRC, SMTP, POP3 та інших текстово-орієнтованих протоколів, заснованих на транспорті TCP.

За замовчуванням (якщо порт не вказано) telnet використовує порт 23.

Синтаксис:

telnet host_name port_number

Приклади використання утиліти telnet:

1) Доступ до поштового сервера за протоколом POP3 (перевірка працездатності поштової скриньки).

Тип:
telnet mail_server ім'я 110

Відповідь сервера: +OK Hello there.

Введіть свою адресу електронної пошти як ім'я користувача:
user test@ztu.edu.ua

Відповідь сервера: +OK Password required.

Вводимо пароль для цієї поштової скриньки:
pass *пароль*

Відповідь сервера:+OK logged in.

Щоб вийти, введіть:
quit

+OK Bye-bye

2) Перевірка доступу до smtp сервера.

Вводимо:
telnet mail_server ім'я 25

Якщо ви отримали повідомлення, що починається з цифри 2, то у вас є доступ до smtp сервера, інакше можна судити про помилку.

Завдання на лабораторну роботу

А. Вивчіть методичні вказівки до виконання лабораторних робіт.
Б. Виконуйте вправи.
В. Скласти звіт про виконану лабораторну роботу, описавши вправи і давши короткі відповіді на контрольні питання.

Вправа 1. Отримуйте довідкову інформацію про команди.

Відобразіть довідкову інформацію про всі обговорювані утиліти (див. таблицю в п.1). Для цього введіть назву утиліти без параметрів або з /?. Щоб отримати довідкову інформацію про nslookup, вам потрібно увійти в режим команд, ввівши nslookup без параметрів, і ввести команду help.

Вивчіть ключі, які використовуються для запуску утиліт.

Вправа 2. Отримайте ім'я хоста.

Відобразити ім'я локального хоста за допомогою команди hostname.

Вправа 3. Вивчіть утиліту ipconfig.

Перевірте конфігурацію TCP/IP за допомогою утиліти ipconfig. Заповніть таблицю:

Ім'я хоста	
IP-адреса	
Маска підмережі	
Основний шлюз	
Чи використовується DHCP (адреса сервера DHCP)	
Опис адаптера	
Фізична адреса мережного адаптера	
Адреса DNS-сервера	
Адреса сервера WINS	

Вправа 4. Тестування зв'язку за допомогою утиліти ping.

А. Переконайтеся, що TCP/IP встановлено та налаштовано правильно на локальному комп'ютері.
Б. Перевірте, чи правильно додано локальний комп'ютер до мережі та чи не дублюється IP-адреса.
В. Перевірте шлюз за замовчуванням, надіславши 5 64-байтових відлунь.
Г. Перевірте, чи можна встановити з'єднання з віддаленим хостом.
Д. За допомогою команди ping перевірте наступні адреси та позначте час відповіді для кожної з них. Спробуйте змінити налаштування пінгу, щоб збільшити час відгуку. Визначте IP-адреси хостів.
   А) ya.ru
   Б) mail.ru
   В) Будь-який вузол з локальної мережі

Вправа 5. Визначте шлях до IP-пакета.

Використовуйте команду tracert, щоб перевірити, через які проміжні вузли надходить сигнал за адресами, переліченими нижче. Встановіть час життя на 10.

Вправа 6: Перегляньте кеш ARP.

Використовуйте утиліту arp для перегляду таблиці ARP на локальному комп'ютері.
Кешувати будь-який статичний запис на локальному комп'ютері.

Вправа 7: Перегляньте таблицю локальних маршрутів.
Використовуйте утиліту маршруту для перегляду локальної таблиці маршрутів.

Вправа 8. Отримуйте інформацію про поточні мережеві підключення та протоколи в стеку TCP/IP.
Використовуйте утиліту netstat для списку мережевих підключень і статистичної інформації для протоколів UDP, TCP, ICMP, IP.

Вправа 9. Отримайте інформацію DNS за допомогою nslookup.
1) Дізнайтеся IP-адреси вузлів:
www.wikipedia.org
www.yahoo.com
cisco.com
duckduckgo.com

2) З'ясувати авторитетні (компетентні) сервери для цих вузлів.
3) Отримати запис SOA з одного з цих серверів для домену duckduckgo.com
.

Вправа 10. Діагностуйте TCP-з'єднання за допомогою утиліти telnet.

1) Перевірте, чи приймає хост підключення SMB cisco.com (порт 445).
2) Приєднайтеся до хост 80.250.190.7 порт 4899
3) Дізнайтеся, який поштовий сервер використовує Microsoft (використовуйте nslookup + telnet)

Контрольні питання

А. Розширити терміни: хост, шлюз, перехід, час життя пакетів, маршрут, маска мережі, авторитетний/неавторитетний (компетентний) DNS-сервер, TCP-порт, цикл зворотного зв'язку, час відгуку.
Б. Які утиліти можна використовувати для перевірки правильності налаштування TCP/IP?
В. Як ping перевіряє з'єднання з віддаленим хостом?
Г. Скільки проміжних маршрутизаторів може пройти IP-пакет, якщо термін його служби становить 30?
Д. Як працює утиліта tracert?
Е. Для чого потрібен протокол ARP?
Ж. Як утиліта ping перетворює імена хостів на ip-адреси (і навпаки)?
З. Які можуть бути причини невдалого завершення ping і tracert? (Тайм-аут запиту, мережа недоступна, пакет TTL).
И. Чи завжди можна дізнатися символьне ім'я вузла за його IP-адресою?
К. Який тип запису виконує найпростіша форма nslookup запиту до DNS-сервера?