МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт студентами спеціальностей 122 Комп'ютерні науки та 172 Телекомунікації та радіотехніка

Дніпро
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних технологій та комп'ютерної інженерії

Л.І. Цвіркун
Я.В. Панферова
Л.В. Бешта

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт студентами спеціальностей 122 Комп'ютерні науки та 172 Телекомунікації та радіотехніка

Дніпро
НТУ «ДП»
2021

Цвіркун Л.І.
Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами спеціальностей 122 Комп’ютерні науки та 172 Телекомунікації та радіотехніка / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2021. – 43 с.

Автори:
Л.І. Цвіркун, канд. техн. наук, проф. (лаб. роботи 1 – 3);
Я.В. Панферова, асист. (лаб. роботи 7 – 9, додатки А – В);
Л.В. Бешта, асист. (лаб. роботи 4 – 6).

Затверджено методичною комісією спеціальності 123 Комп’ютерна інженерія (протокол № 2 від 18.02.21) за поданням кафедри інформаційних технологій та комп’ютерної інженерії (протокол № 14 від 08.02.21).

Подано методичні рекомендації до виконання лабораторних робіт з дисципліни «Комп’ютерні мережі» студентами спеціальностей 122 Комп’ютерні науки та 172 Телекомунікації та радіотехніка.

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп’ютерної інженерії В.В. Гнатушенко, д-р техн. наук, проф.

ЗМІСТ

Стор.

ВСТУП

Методичні рекомендації призначені для студентів спеціальностей 122 Комп'ютерні науки та 172 Телекомунікації та радіотехніка, що вивчають дисципліну «Комп'ютерні мережі».

Методичні рекомендації включають низку частково взаємопов'язаних робіт, під час виконання яких студенти мають можливість отримати досвід роботи з мережним аналізатором Wireshark, командами операційної системи Windows 10, протоколами Ethernet, ARP, IP, TCP, UDP, HTTP, DHCP, DNS та FTP. Визначати типи IP-адрес та навчитися організовувати підмережі за допомогою маски постійної.

Перед виконання лабораторної роботи студенти повинні:

– ознайомитися з методичними рекомендаціями;

– повторити лекційний матеріал, пов'язаний з лабораторною роботою;

– підготовити відповіді на питання, які наведені у методичних рекомендаціях наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп'ютері, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

Загальні вимоги до виконання лабораторної роботи, що мають забезпечити максимальну оцінку:

– повна відповідність звіту про виконання лабораторної роботи методичним рекомендаціям;

– володіння теоретичним матеріалом про предмет досліджень;

– загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу;

– відповідність оформлення звіту чинним стандартам.

1. ЛАБОРАТОРНА РОБОТА № 1
ВИВЧЕННЯ ІНТЕРФЕЙСУ ПРОГРАМИ CISCO PACKET TRACER

1.1. Мета лабораторної роботи

Ознайомитись з програмою Cisco Packet Tracer для моделювання комп'ютерних мереж. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички з базового налаштування мережних пристроїв.

1.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– інтерфейс програми Cisco Packet Tracer;
– побудова мережі в Packet Tracer;
– налаштування пристроїв мережі.

Під час виконання лабораторної роботи необхідно побудувати мережу в програмі Cisco Packet Tracer. Виконати налаштування базових параметрів комутатора та виконати налаштування ПК з перевіркою їх взаємодії між собою.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– результати перевірки підключення до мережі.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

Крок 1. Вибір пристроїв і побудова мережі

Запустити програму Cisco Packet Tracer та побудувати мережу, представлену на рис. 1.1. IP-адресація пристроїв подана в табл. 1.1.

Таблиця 1.1

Адресація пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Switch0	VLAN1	192.168.№.254	255.255.255.0
PC0	Мережний адаптер (NIC)	192.168.№.1	255.255.255.0
PC1	Мережний адаптер (NIC)	192.168.№.2	255.255.255.0

де № − номер, за яким студент записаний у журналі групи.

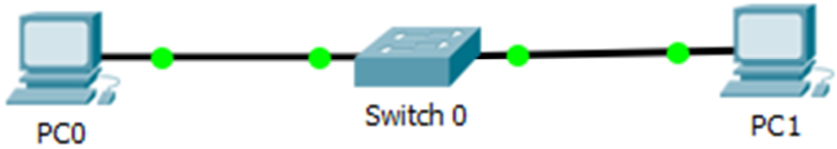

Рис. 1.1. Топологія мережі

Для цього додати в робочу область один комутатор серії 2960-24TT з групи елементів *Switches* панелі вибору типових пристроїв і зв'язків (рис. 1.2) та два комп'ютера PC-PT з групи *End Devise*.

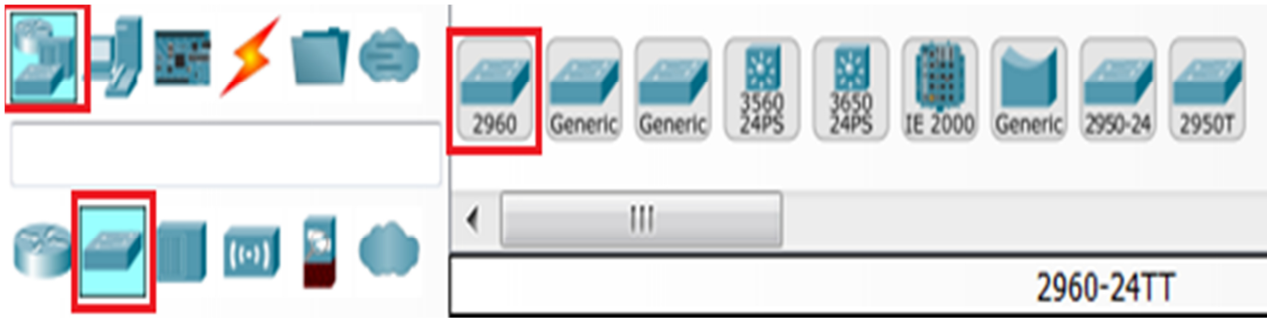

Рис. 1.2. Панель вибору типових пристроїв і зв'язків

Крок 2. Під'єднання ПК до комутатора прямим кабелем

1. Клацніть значок *Connections* (у вигляді блискавки) на панелі вибору пристроїв і зв'язків та виберіть прямий кабель (Copper Straight-Through), клацнувши по ньому (рис. 1.3). Курсор прийме вид роз'єму з кінцем кабелю, що звисає.

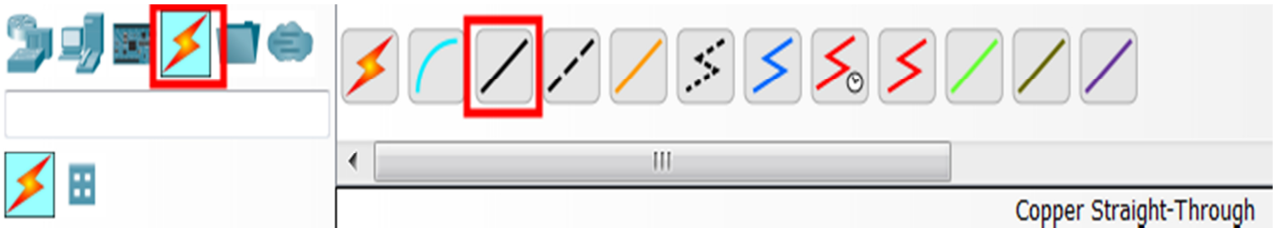

Рис. 1.3. Панель вибору з'єднань

2. Клацніть PC0. У вікні виберіть варіант для підключення FastEthernet0.
3. Перетягніть інший кінець підключення до комутатора Switch0 і клацніть на ньому, щоб відкрити список підключень. Виберіть FastEthernet0/1, щоб завершити підключення.
4. Аналогічно зробіть підключення PC1 до комутатора, підключивши до порту FastEthernet0/2 комутатора Switch0.

Крок 3. Налаштування IP-адрес на ПК

1. Клацніть PC0. У вікні управління відкрийте вкладку *Desktop*.
2. Оберіть додаток *IP Configuration* і введіть дані з табл. 1.1 для PC0.
3. Повторіть налаштування IP-адреси для PC1.

Крок 4. Перевірка підключення до мережі

Підключення до мережі можна перевірити за допомогою команди «ping». Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вживати відповідні заходи щодо усунення неполадок

1. Клацніть PC0. Закрийте вікно *IP Configuration*, якщо воно відкрито. На вкладці *Desktop* виберіть додаток *Command Prompt* (Командний рядок).
2. З командного рядка надішліть ехо-запит на IP-адресу комп'ютера PC1.
   PC> ping 192.168.1.2
3. З командного рядка надішліть ехо-запит на IP-адресу комутатора.
   PC> ping 192.168.1.254

Крок 5. Формування навантажувального трафіку в Cisco Packet Tracer

Для організації трафіку можна використовувати додаток *Traffic Generat*or.

1. У вікні управління PC1 у вкладці *Desktop* виберіть додаток *Traffic Generator*.
2. Вкажіть наступні налаштування (рис. 1.4).

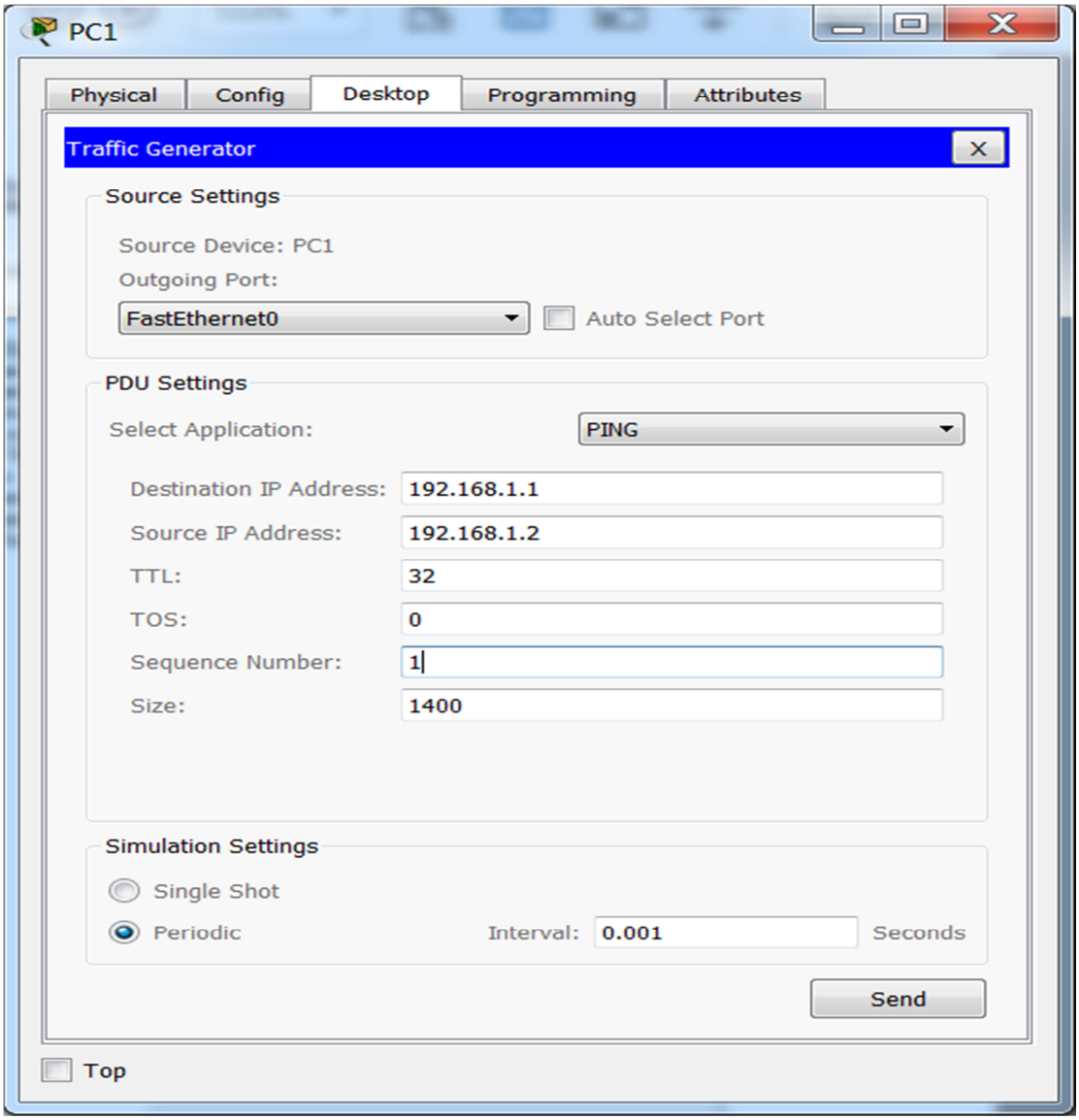

Рис. 1.4. Налаштування генератора трафіку

3. Після натискання кнопки Send між PC1 і PC0 почнеться активний обмін даними. Не закривайте вікно, щоб не перервати потік трафіку!

Зверніть увагу, як змінилася активність мережних інтерфейсів (блимання зелених маркерів на лініях зв'язку).

1.3. Питання для підготовки до захисту лабораторної роботи

1. Чому на комутаторі порти знаходяться в відключеному стані?
2. Що може бути перешкодою для передачі ехо-запиту за допомогою команди «ping» між комп'ютерами?
3. Яким чином в Packet Tracer виконується налаштування кінцевих пристроїв?
4. Який слід використовувати кабель при підключенні двох ПК між собою?
5. На якому рівні моделі OSI працює комутатор?

2. ЛАБОРАТОРНА РОБОТА № 2
ВИВЧЕННЯ ІНТЕРФЕЙСУ ПРОГРАМИ WIRESHARK

2.1. Мета лабораторної роботи

Ознайомитись з програмою Wireshark для аналізу мережних протоколів. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички з написання фільтрів. Вивчити стек TCP/IP та взаємодію протоколів.

2.2.Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– робота з командним рядком операційної системи Windows 7;
– діагностичні команди та засоби Windows 7 для роботи в мережі;
– модель OSI та взаємодія протоколів;
– стек протоколів TCP/IP;
– функціональні можливості програми Wireshark;
– правила написання фільтрів для аналізаторів мережних протоколів.

Далі виконати такі дії:

− запустити програму Wireshark;

– відкрити вікно конфігурації захвату (рис. 2.1). Для цього потрібно перейти в меню *Capture->Options* або по комбінації клавіш CTRL+K;

– обрати інтерфейс, на якому буде виконуватися захоплення пакетів;

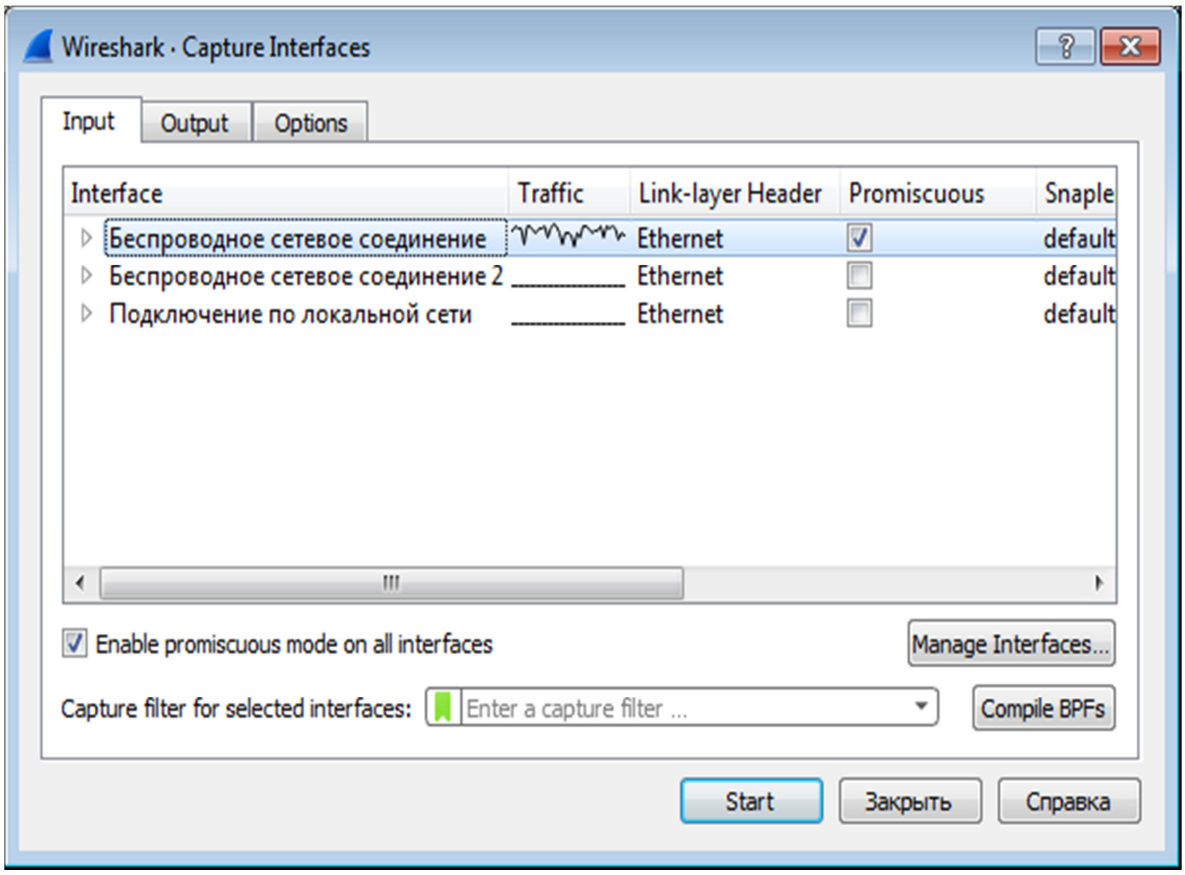

Рис. 2.1. Вікно опцій захвату

– на вкладці *Options* (рис. 2.2) встановити параметр зупинки захоплення після захвату 300·N (де N – номер по списку в групі) пакетів без фільтра та почати захоплення пакетів;

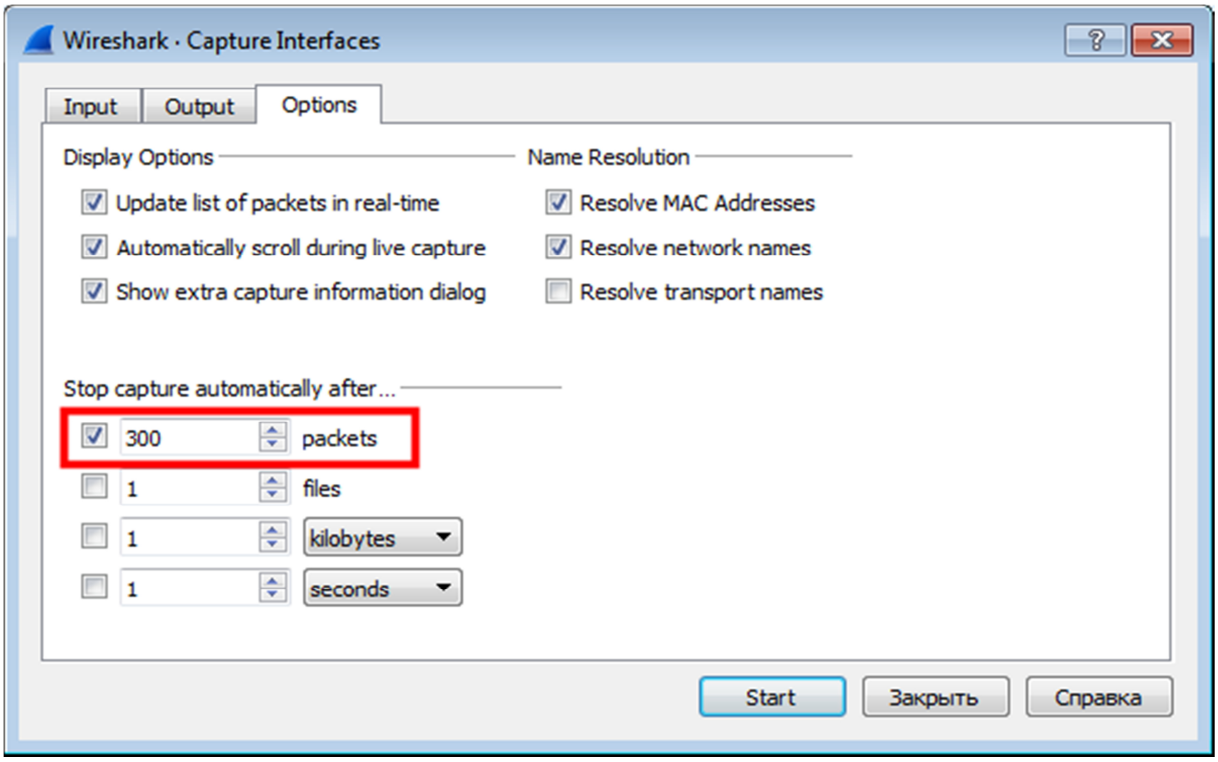

Рис. 2.2. Вкладка Options вікна Capture Interfaces

– після зупинки захоплення використовуючи пункти меню *Statistics* визначити характеристики отриманого мережного трафіку, а саме:

1) які протоколи використовувались в мережі;
2) відсоткове співвідношення трафіку різних протоколів в мережі;
3) середню швидкість трафіку (кадрів/с, байт/с);
4) мінімальний і максимальний розміри кадрів;
5) IPv4-адреси и порти TCP та UDP, між якими велася передача даних.

– візуалізувати графік отриманих даних за допомогою пункту меню *Statistics->Io Graphs*;

– візуалізувати інформаційні потоки за допомогою пункту меню *Statistics->Flow Graph*;

– здійснити новий захват пакетів, настроївши фільтр на захват пакетів ARP та ICMP (рис. 2.3);

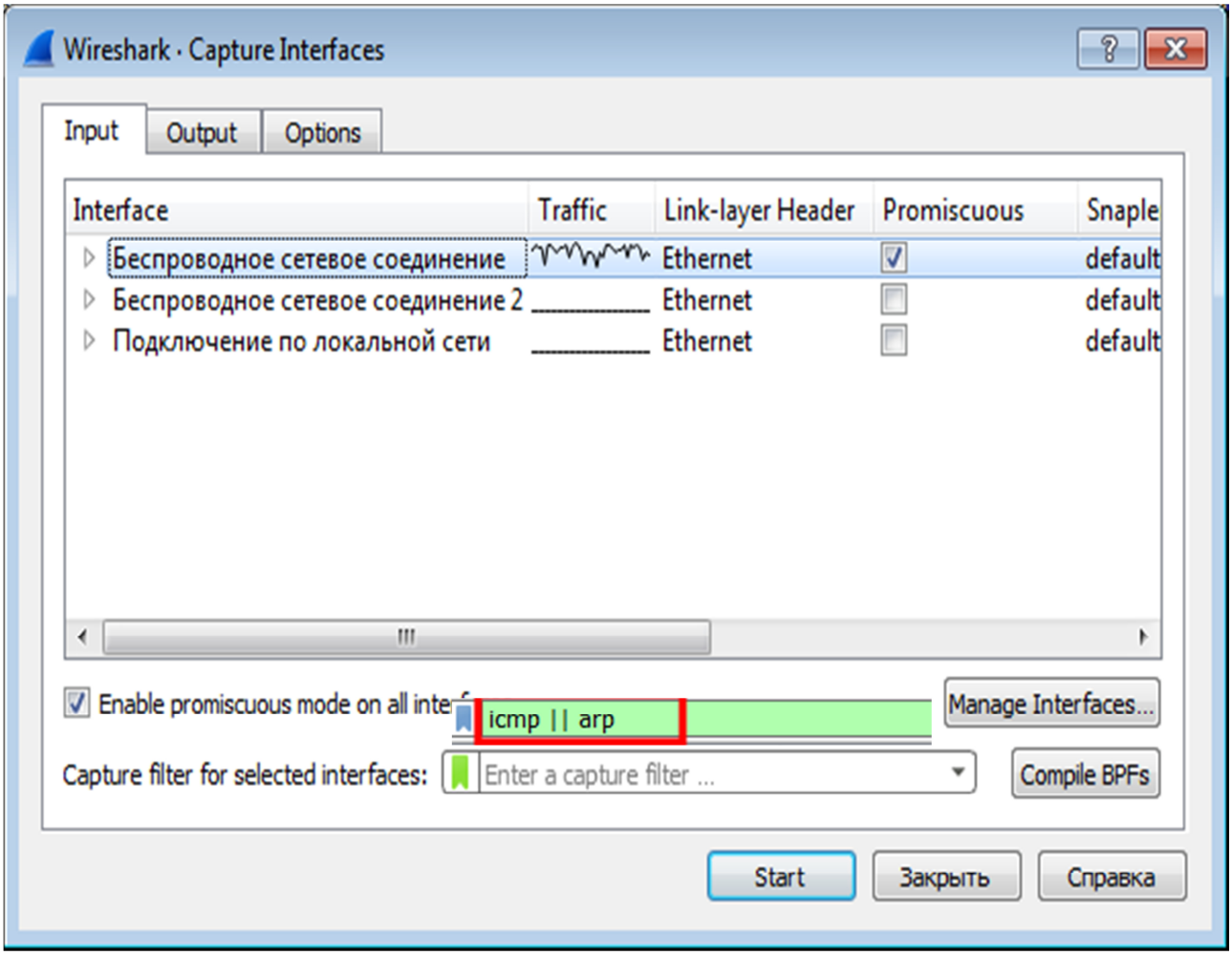

Рис. 2.3. Вікно опцій на захват пакетів ARP та ICMP

– відкрити командний рядок (Пуск->Стандартні->Командний рядок);
– переглянути список доступних вузлів;

> net view

– відправити ехо-запити на сусідні вузли;

>ping кінцевий_вузол

– зупинити захват, отримавши необхідні дані;

– відкрити в Wireshark файл с захопленими пакетами під час підключення до маршрутизатора по telnet на ПК (надається викладачем). Визначити IP-адреси цих пристроїв. Визначити пароль, який передавався під час встановлення сеансу до маршрутизатора. Для цього на будь-якому пакеті, в якому велася передача даних по telnet, натиснути правою кнопкою і вибрати *Follow ->TCP Stream* або на панелі меню *Analyze-> Follow ->TCP Stream* (рис. 2.4);

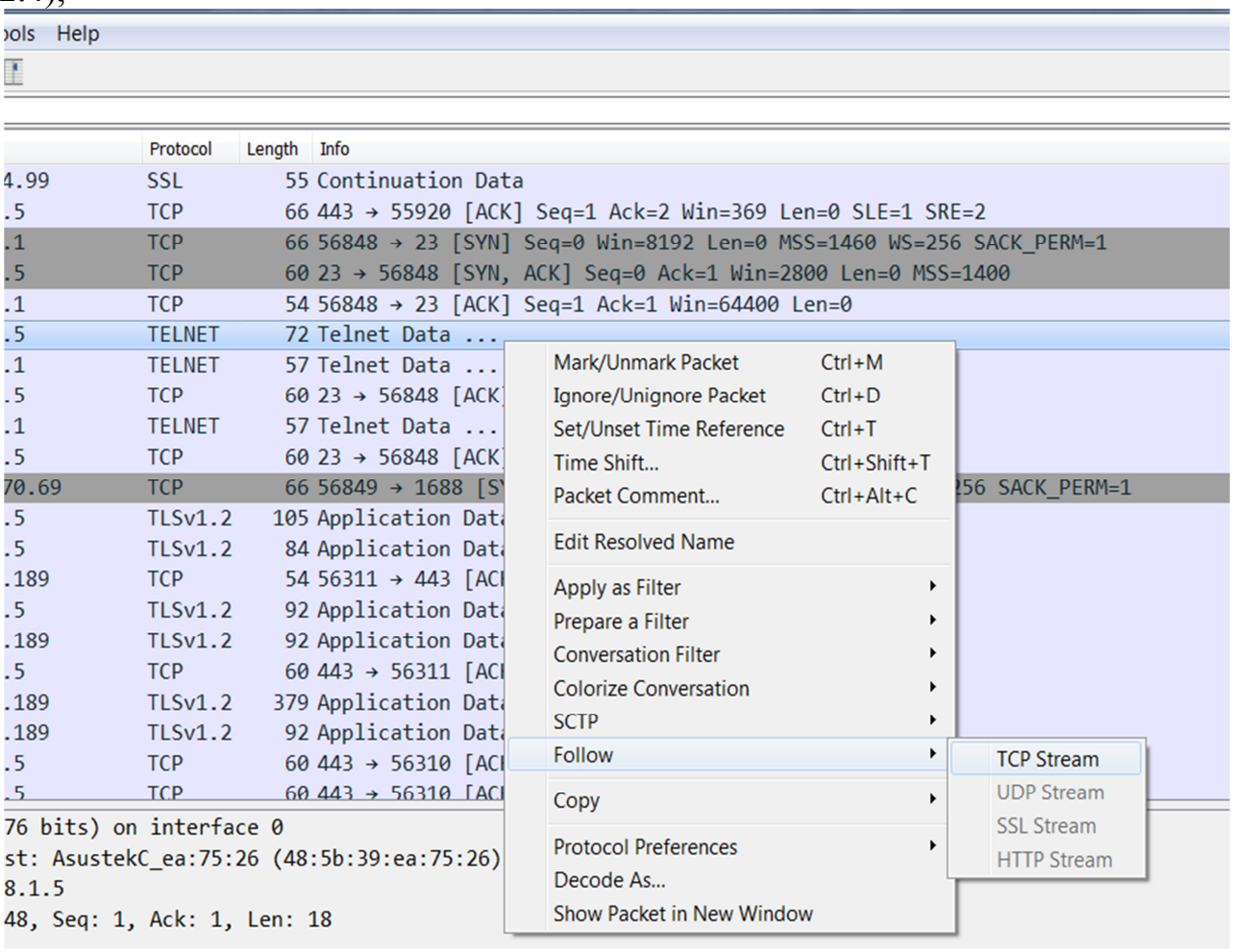

Рис. 2.4. Відстеження всього потоку TCP для обраного пакету

– навести приклад написання фільтру відображення за варіантом згідно з табл. 2.1.

Таблиця 2.1

Варіанти фільтрів відображення

№	Фільтр відображення
1.	Тільки трафік від вузлів з MAC-адресами виробника TP-LINK, які починаються з f4:f2:6d.
2.	Тільки трафік icmp, виключаючи exo-запити (type=8) та exo-відповіді (type=0).
3.	IP-пакети від вузла 192.168.0.5 довжиною більше 1450 байт.
4.	Тільки трафік між машинами в локальній підмережі 192.168.30.0/24.

Продовження табл. 2.1

№	Фільтр відображення
5.	IP-пакети з встановленим прапором фрагментації (mf) від вузла 10.0.0.5.
6.	TCP-пакети з встановленим прапором зняття з'єднання (res) на порт 23.
7.	TCP-пакети з вузла 192.168.10.5 з встановленим прапором встановлення з'єднання (syn).
8.	Весь вхідний трафік, виключаючи трафік SSH (TCP порт 22) генерований вузлом 192.168.5.101.
9.	Тільки трафік від вузла з MAC-адресом f4:f2:6d:54:a0:78, які включали в себе DNS-запити.
10.	Широкомовний трафік без ARP-запитів.
11.	Всі HTTP-запити типу GET на адрес 91.198.36.14 .
12.	IGMP-звіти приналежності (Membership Query Message) до групи 224.0.0.113.
13.	Тільки ARP-запити від вузла 192.168.0.10.
14.	Тільки DHCP-запити від вузла з MAC-адресом 6c:f0:49:70:ba:8b.
15.	Тільки DHCP-відповіді від вузла 192.168.0.1 MAC-адрес 6c:f0:49:70:ba:8b.
16.	Тільки пакети з широкомовними адресами 255.255.255.255 на порт призначення 68 протоколу UDP.
17.	IP-пакети між машинами в локальній підмережі 180.15.30.0/24 з довжиною пакету більше 1400 байт.
18.	FTP-пакети с запитами від клієнта 185.15.1.10.
19.	DNS-пакети від вузла 192.168.15.26
20.	Всі ARP-відповіді крім вузла 192168.0.10.
21.	Всі telnet-пакети з командою «End of File» від вузла 195.15.2.3.
22.	Всі DHCP-пакети від вузла 192.168.0.5.
23.	Тільки broadcast і multicast-пакети мережі 172.16.0.0/16.
24.	Тільки ARP-відповіді від вузла 192.168.0.10
25.	Тільки пакети http, які містили javascript в полі content_type.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– статичні дані захопленого мережного трафіку;
– скріншоти програми Wireshark в ході виконання роботи з описом дій;
– фільтр відображення за варіантом згідно з табл. 2.1.

2.3. Питання для підготовки до захисту лабораторної роботи

1. У якому випадку вузол може бачити всі пакети в сегменті Ethernet?
2. Який протокол канального рівня підтримує мережа учбового класу?
3. Які типи адрес необхідні для взаємодії вузлів в локальній мережі?
4. Дайте визначення терміну "інкапсуляція", використовуючи як приклад будь-який захоплений пакет.
5. До якого рівню моделі OSI відноситься протокол IP?

3. ЛАБОРАТОРНА РОБОТА № 3
ОТРИМАННЯ ВІДОМОСТЕЙ ПРО MAC-АДРЕСИ І МЕРЕЖНІ НАЛАШТУВАННЯ TCP/IP

3.1. Мета лабораторної роботи

Вивчити команди командного рядка для отримання відомостей про MAC-адреси вузла і поточні мережні налаштування TCP/IP. Отримувати відомості про клієнтські сервіси DHCP і DNS і оновлювати їх. Вивчити інформацію, яка міститься в таблиці маршрутизації ПК.

3.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні матеріали, такі питання:

– мережні та діагностичні команди Windows (Додаток Б);

– синтаксис діагностичних команд «getmac», «ipconfig», «nbtstat» та «route».

Далі виконати такі дії:

– відобразити довідку по використанню команди «ipconfig»;

– вивести повну конфігурацію TCP/IP для всіх адаптерів;

– вивести на екран вміст кешу служби розпізнавання імен DNS;

– скинути кеш служби розпізнавання імен DNS;

– оновити мережні налаштування, отримані від DHCP-сервера тільки для адаптера локальної мережі;

– відобразити довідку по використанню команди «getmac»;

– отримати детальну інформацію про MAC-адреси всіх існуючих на локальному комп'ютері мережних адаптерів;

– отримати інформацію про MAC-адреси всіх існуючих на локальному комп'ютері мережних адаптерів в форматі CSV без відображення рядка заголовків стовпців;

– відобразити довідку по використанню команди «route»;

– відобразити таблицю маршрутизації вузла та проаналізувати її записи;

– відобразити довідку по використанню команди «nbtstat»;

– відобразити таблицю NetBIOS-імен на локальному комп'ютері;

– відобразити розв'язання NetBIOS-імен та статистику реєстрації;

– відобразити таблиці сеансів з IP-адресами.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– лістинг командного рядку в ході виконання лабораторної роботи.

3.3. Питання для підготовки до захисту лабораторної роботи

1. Як можна з‘ясувати MAC-адресу комп’ютера?
2. Як можна з‘ясувати IP-адресу комп’ютера?
3. Як можна з‘ясувати MAC-адресу комп’ютера в локальній мережі?
4. Як оновити IP-адрес комп’ютера?
5. Як з‘ясувати кеш служби розпізнавання імен DNS?

4. ЛАБОРАТОРНА РОБОТА № 4
ВИВЧЕННЯ ПРОТОКОЛУ ARP

4.1. Мета лабораторної роботи

Вивчити роботу протоколу ARP, отримати практичні навички по роботі з командою ARP в командному рядку Windows 7.

4.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– робота з командним рядком операційної системи Windows;
– функції та робота протоколу ARP;
– синтаксис команди «arp»;
– структура заголовку протоколу ARP.

Виконання лабораторної роботи складається з двох частин. В першій частині необхідно дослідити роботу протоколу ARP в локальній мережі. В другій частині виконується вивчення роботи протоколу ARP в Cisco Packet Tracer.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

Частина 1. Вивчення роботи протоколу ARP в локальній мережі

Роботу слід проводити парами з використанням двох комп'ютерів, підключених до одного сегмента локальної мережі та IP-адресами, які належать одній IP-мережі. ПК повинні мати вихід в Інтернет.

Далі виконати такі дії:

– відкрити вікно командного рядка на ПК і відобразити довідкову інформацію по команді «arp»;

```
> arp /?
```

– відобразити ARP-таблицю;

```
> arp –a
```

– запустити програму Wireshark;

– вибрати мережний інтерфейс, на якому буде виконуватися захоплення повідомлень ARP, та почати захоплення;

– в командному рядку очистити ARP-таблицю;

```
> arp –d *
```

– переконатися в тому, що ARP-таблиця очищена;

```
> arp –a
```

– надіслати ехо-запит за допомогою команди «ping» зі свого ПК на інший ПК в мережі для динамічного додавання запису в ARP-таблицю;

```
> ping кінцевий_вузол
```

– після відправки ехо-запиту зупинити захоплення даних програмою Wireshark;

– налаштувати в Wireshark фільтр на відображення тільки пакетів ARP та ICMP;

– на підставі отриманих даних визначити і замалювати структуру запиту і відповіді протоколу ARP та звернути увагу на інкапсуляцію ARP-повідомлень;

– відобразити ARP-таблицю, визначити MAC-адрес сусіднього вузла та перевірити це значення на сусідньому вузлі;

– завести в ARP-таблицю статичний запис для сусіднього ПК з вигаданою MAC-адресою;

– відобразити ARP-таблицю щоб переконатися, що запис введено. Звернути увагу на її статус;

– перевірити доступність ПК;

– видалити доданий запис;

– зупинити захоплення та зберегти в файл дамп захоплених пакетів;

– почати нове захоплення даних програмою Wireshark;

– надіслати ехо-запит за допомогою команди «ping» на кілька IP-адрес в Інтернет. Визначити, на який MAC-адрес призначення відправлялись ехо-запити. Якому пристрою в мережі він належить?

Частина 2. Вивчення роботи протоколу ARP в Cisco Packet Tracer

Побудувати в Cisco Packet Tracer мережу згідно з рис. 4.1 та налаштувати обладнання відповідно до табл. 4.1.

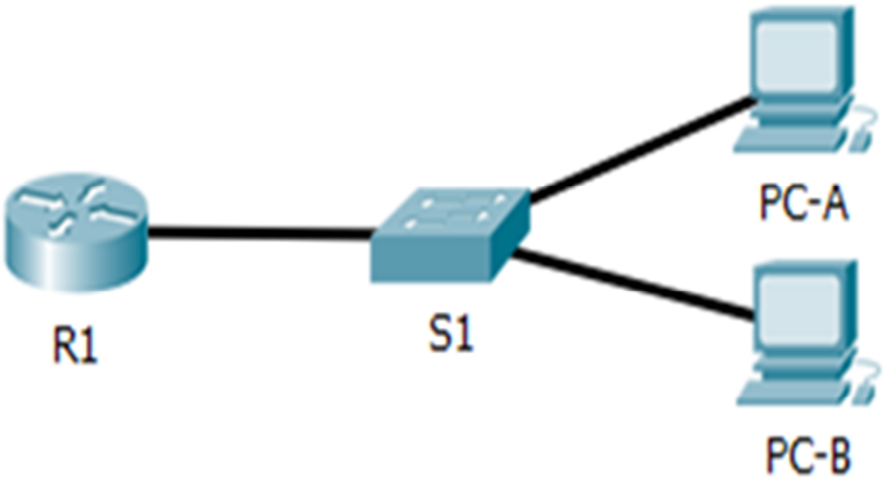

Рис. 4.1. Топологія мережі

Таблиця 4.1

Таблиця адресації пристроїв

Пристрій	Модель	Інтерфейс	IP-адрес	Маска	Шлюз
R1	2911	G0/0	192.168.1.1	255.255.255.0	-
S1	2960	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A		NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B		NIC	192.168.1.4	255.255.255.0	192.168.1.1

Далі:

– визначити MAC-адреси PC-A та PC-B;

– визначити MAC-адреси інтерфейсів маршрутизатора і комутатора;

#show interface *interface*

– з командного рядка PC-A відправити exo-запити на S1 та R1;

– з командного рядка PC-A відправити exo-запит на PC-B;

– відобразити ARP та MAC-таблиці на комутаторі та маршрутизаторі та проаналізувати їх.

#show mac address-table

#show arp

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис завдання з початковими умовами та даними;

– скріншоти командного рядка в ході виконання роботи;

– структура заголовків ARP-запиту та відповідна йому ARP-відповідь, захоплені в Wireshark;

– дамп захоплених пакетів в Wireshark надіслати на поштову адресу викладача;

– значення MAC-адрес задіяних інтерфейсів всіх пристроїв в мережі, побудованій в Cisco Packet Tracer;

– вміст ARP та MAC-таблиць комутатора та маршрутизатора в мережі, побудованій в Cisco Packet Tracer.

4.3. Питання для підготовки до захисту лабораторної роботи

1. Як і коли видаляються статичні записи в arp-таблиці?
2. Навіщо додавати статичні записи ARP-таблицю?
3. При виконанні команди «ping» на IP-адреси в Інтернет, який IP-адрес призначення був в ARP-запиті і чому?
4. При виконанні команди «ping» на IP-адреси в Інтернет, на який MAC-адрес призначення відправлялись exo-запити?
5. Коли в мережі виникають широкомовні ARP-запити?

5. ЛАБОРАТОРНА РОБОТА № 5
ВИЗНАЧЕННЯ IPV4-АДРЕС

5.1. Мета лабораторної роботи

Навчитися визначати структуру IPv4-адрес, у тому числі мережну частину, частину вузла і маску підмережі, визначати різні типи IPv4-адрес та їх використання.

5.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, такі питання:

– правила переходу з двійкової системи числення в десяткову та навпаки;
– структуру IPv4-адрес;
– використання операції «І» для визначення мережної частини;
– одноадресне, широкомовне і багатоадресне розсилання IPv4;
– типи IPv4-адрес.

Далі виконати такі дії:

– використати операцію «І» для визначення мережної частини в IP-адресах, зазначених в табл. 5.1;

Таблиця 5.1

Варіанти завдань

№ вар.	Завдання 1		Завдання 2	
	IP-адреса	Маска	IP-адреса	Префікс
1.	72.60.124.23	255.255.224.0	13.165.140.153	/10
2.	238.78.57.116	255.248.0.0	59.3.115.89	/11
3.	60.255.110.21	255.255.192.0	112.231.164.30	/12
4.	12.211.92.185	255.128.0.0	123.210.206.234	/13
5.	165.114.253.9	255.255.252.0	220.24.105.100	/14
6.	253.171.224.98	255.255.240.0	3.174.130.238	/15
7.	225.194.116.5	255.240.0.0	79.80.159.149	/20
8.	92.159.7.53	255.255.252.0	112.37.195.31	/17
9.	43.117.230.183	255.255.192.0	98.107.124.156	/18
10.	146.247.87.2	255.255.240.0	55.160.113.10	/19
11.	188.233.122.101	255.255.224.0	56.211.33.164	/21
12.	192.19.3.8	255.255.254.0	53.119.203.221	/22
13.	84.6.223.106	255.255.252.0	67.200.116.39	/23
14.	216.45.42.190	255.255.248.0	243.162.237.152	/22
15.	138.46.140.94	255.248.0.0	4.82.38.2	/21

Продовження табл. 5.1

№ вар.	Завдання 1		Завдання	
	IP-адреса	Маска	IP-адреса	Префікс
16.	152.205.232.105	255.255.192.0	144.112.213.91	/20
16.	107.214.175.68	255.255.224.0	210.254.11.42	/19
17.	57.198.77.193	255.255.240.0	11.104.213.125	/18
18.	122.227.157.232	255.255.128.0	201.24.249.88	/17
19.	228.219.147.134	255.255.252.0	17.124.16.162	/18
20.	151.22.163.204	255.248.0.0	55.174.76.242	/19
21.	37.128.54.52	255.255.192.0	72.96.79.110	/20
22.	59.145.202.91	255.255.224.0	92.9.234.56	/21
23.	162.202.242.90	255.255.240.0	144.186.231.149	/22
24.	159.25.94.89	255.255.252.0	178.15.86.139	/25

– заповнити табл. 5.2 відомостями для визначених мереж з табл. 5.1;

Таблиця 5.2

Відомості про мережі

IP-адрес мережі	Маска або префікс	Адреса першого вузла	Адреса останнього вузла	Широкомовна адреса	Кількість вузлів
…	…	…	…	…	…

– проаналізувати табл. 5.3 та визначити тип адреси: адреса вузла, адреса мережі, багатоадресне або широкомовне розсилання;

Таблиця 5.3

Адреса вузла, адреса мережі, багатоадресне або широкомовне розсилання

IP-адреса	Маска	Тип адрес
10.1.1.1	255.255.255.252	
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

– проаналізувати табл. 5.4 і визначити тип адреси: загальна або приватна;

Таблиця 5.4

Тип адреси: загальна/приватна

IP-адреса/префікс	Загальна/приватна
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

– проаналізувати табл. 5.5 і визначити, чи є пара IP-адрес/префікс допустимою адресою вузла.

Таблиця 5.5

Допустима/недопустима адреса вузла

IP-адреса/префікс	Допустима/недопустима адреса	Причина
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– заповнені відповідями табл. 5.2 − 5.5.

5.3. Питання для підготовки до захисту лабораторної роботи

1. До якого класу належить IP-адреса комп'ютера навчального класу?
2. До якої IP-мережі належить IP-адреса комп'ютера навчального класу?
3. Чому при визначенні мережної адреси важлива маска мережі?
4. Яким пристроям зазвичай присвоюються статичні IP-адреси?
5. При налаштуванні двох ПК в одній мережі ПК-А присвоєно IP-адресу 192.168.1.18, а ПК-Б IP-адресу 192.168.1.33. Маска мережі обох комп'ютерів: 255.255.255.240. Чи зможуть ці ПК взаємодіяти один з одним безпосередньо?

6. ЛАБОРАТОРНА РОБОТА № 6
РОЗРАХУНОК ПІДМЕРЕЖ ЗА ДОПОМОГОЮ МАСКИ ПОСТІЙНОЇ ДОВЖИНИ

6.1. Мета лабораторної роботи

Навчитися розбивати мережу на підмережі за допомогою маски постійної довжини, визначати адреси підмереж, а також діапазон IP-адрес вузлів для підмереж.

6.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– правила переходу з двійкової системи числення в десяткову та навпаки;
– сегментація мереж;
– використання масок в IP-адресації.

Далі розробити схему IP-адресації поділу мережі організації на підмережі з використанням маски постійної довжини для відповідності вимогам топології, поданої на рис. 6.1.

Кількість вузлів у мережах LAN_N1-LAN_N6 та виділений мережний блок для їх адресації задані по табл. 6.1 згідно з варіантом.

Через маршрутизатор Central забезпечується доступ до Internet.

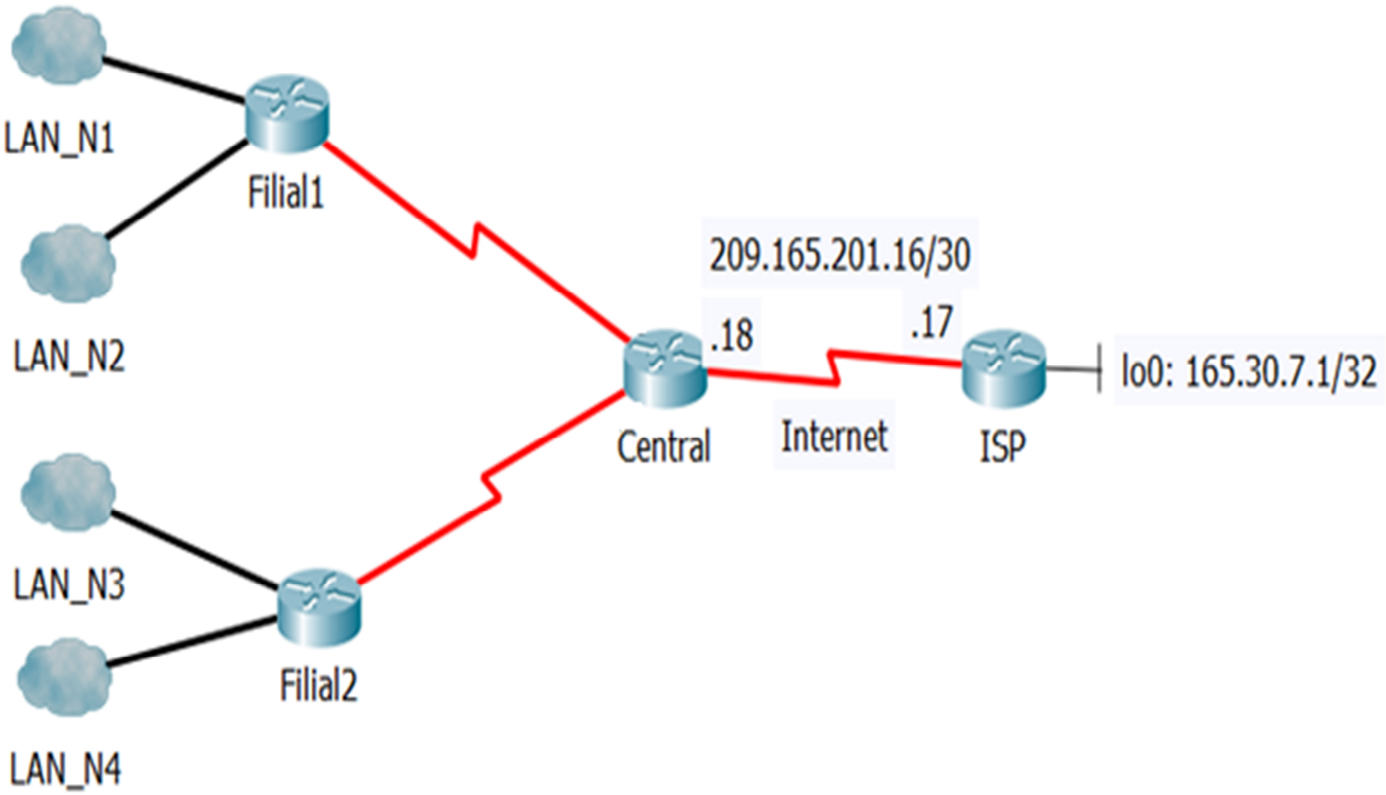

Рис. 6.1. Топологія мережі

Таблиця 6.1

Варіанти завдань

№ вар.	Адреса мережі	LAN_N1	LAN_N2	LAN_N3	LAN_N4	LAN_N5	LAN_N6
1.	180.16.0.0/17	500	600	250	2000	40	50
2.	190.17.0.0/18	1200	1500	180	200	120	90
3.	145.10.0.0/19	56	60	300	410	80	120
4.	175.30.0.0/17	360	400	200	1000	30	800
5.	185.138.0.0/18	150	200	260	300	80	100
6.	178.13.0.0/19	250	200	1000	800	20	28
7.	182.210.0.0/17	100	120	50	60	400	380
8.	190.10.0.0/18	60	55	190	210	110	80
9.	181.140.0.0/19	250	180	98	110	60	45
10.	175.28.0.0/17	42	50	290	430	70	95
11.	184.48.0.0/18	110	90	20	15	450	381
12.	188.98.0.0/19	52	60	113	96	451	365
13.	18.48.0.0/17	85	78	168	190	560	680
14.	187.68.0.0/18	36	60	96	115	260	300
15.	190.16.0.0/19	68	92	200	240	20	15
16.	179.20.0.0/17	20	18	450	500	800	1000
17.	189.87.0.0/18	58	40	620	780	105	98
18.	179.91.0.0/19	20	15	103	78	502	362
19.	177.131.0.0/17	165	201	30	25	262	368
20.	177.13.0.0/18	86	90	154	160	52	40
21.	19.16.0.0/19	69	84	165	205	262	359
22.	123.12.64.0/18	57	33	232	155	53	50
23.	154.16.64.0/19	198	164	55	60	177	152
24.	181.137.0.0/20	149	213	179	168	40	35
25.	145.198.0.0/18	184	230	91	87	30	26

Необхідно задати схему поділу мережі на підмережі в заданому сценарії враховуючи кількість комп'ютерів в кожної підмережі. При цьому IP-адреси будуть потрібні для кожного інтерфейсу локальної мережі кожного маршрутизатора.

Скласти схему поділу на підмережі, що відповідає зазначеним умовам, допоможуть відповіді на такі запитання:

1. Скільки адрес вузлів необхідно для найбільшої підмережі?
2. Яка мінімальна кількість необхідних підмереж?
3. Які маски підмереж відповідають максимальній необхідній кількості адрес вузлів?
4. Які маски підмереж відповідають мінімальній необхідній кількості підмереж?
5. З огляду на відповіді, яка маска підмережі відповідає максимальній необхідній кількості адрес вузлів та мінімальній необхідній кількості підмереж?

З'ясувавши, яка маска підмережі відповідає всім зазначеним вимогам, заповнити наведену нижче табл. 6.2.

Таблиця 6.2

Визначення маски підмережі в організації

Вихідна адреса мережі	Вихідна маска мережі в десятковому вигляді	Розрахована маска підмережі в десятковому вигляді	Кількість зарезервованих біт для адреси підмережі	Кількість комбінацій підмереж для визначеної маски
…	…	…	…	…

Розрахувати підмережі з новою маскою і занести інформацію в табл. 6.3.

Таблиця 6.3

Відомості про підмережі

Назва підмережі	Необхідний розмір підмережі	Виділений розмір підмережі	Десятковий формат адреси підмережі	Перша використовувана адреса вузла підмережі	Остання використовувана адреса вузла підмережі	Широкомовна адреса

Дати відповіді на такі питання:

– кількість необхідних IP-адрес (N);

– кількість IP-адрес, необхідних для кожного каналу WAN між маршрутизаторами;

– кількість IP-адрес, доступних у вихідній мережі ($N_{поч}$);

– кількість IP-адрес, доступних у розбитій мережі ($N_{роз}$);

– який відсоток адресного простору використовується в вихідній мережі ($N/N_{поч}$ *100);

– який відсоток адресного простору використовується в розрахованій мережі ($N/N_{роз}$ *100).

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;

– опис завдання з початковими умовами і даними;

– відповіді на зазначені питання;

– розрахунок адресації мережі згідно із завданням, поданий у вигляді табл. 6.2 та 6.3;

– схему вирішення адресації заданої мережі у вигляді логічної топології згідно з рис. 6.2.

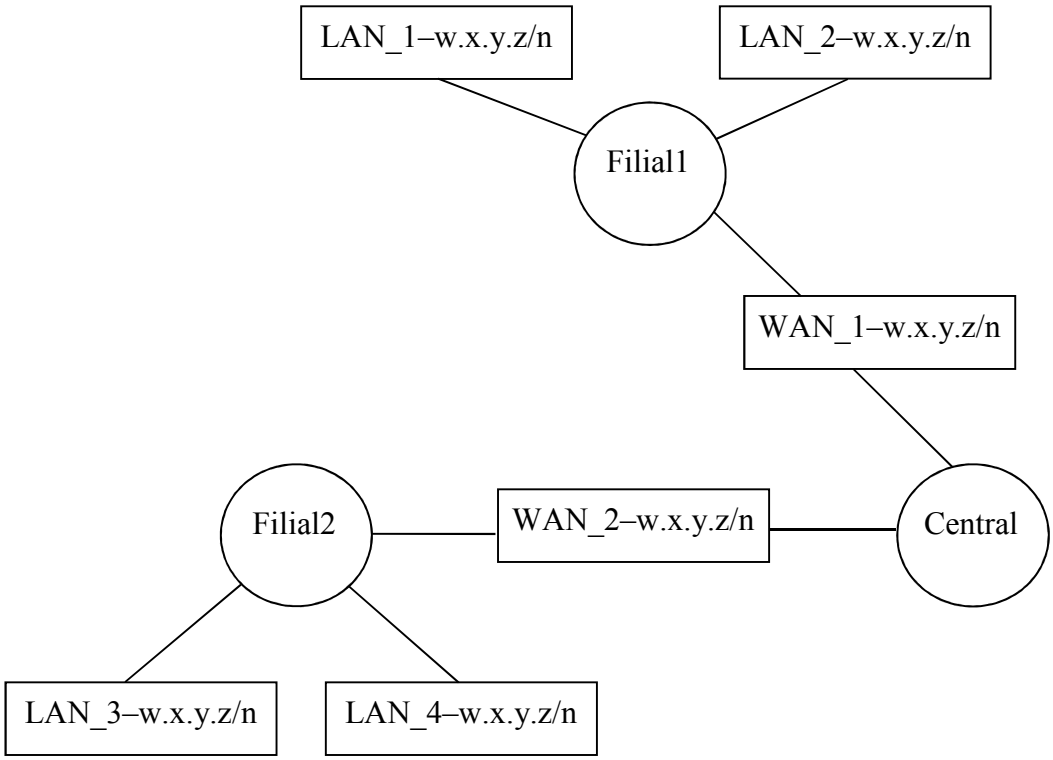

Рис. 6.2. Логічна топологія методом маски постійної довжини

6.3. Питання для підготовки до захисту лабораторної роботи

1. Який є запас на випадок появи додаткових мереж?
2. Який є запас на випадок збільшення числа вузлів?
3. Який основний мотив розбиття IP-мереж на підмережі?
4. Який недолік розрахунку мереж за допомогою маски постійної довжини?
5. Чому маска підмережі так важлива при аналізі IPv4-адрес?

7. ЛАБОРАТОРНА РОБОТА № 7
ПОБУДОВА МЕРЕЖІ В CISCO PACKET TRACER І БАЗОВЕ НАЛАШТУВАННЯ ПРИСТРОЇВ

7.1. Мета лабораторної роботи

Отримати навички в програмі Cisco Packet Tracer будувати розраховану в лабораторній роботі № 6 мережу, виконувати налаштування базових параметрів пристроїв і протокол SSH.

7.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– інтерфейс програми Cisco Packet Tracer;
– робота з командним рядком (CLI) операційної системи Cisco IOS;
– робота з контекстною довідкою в CLI;
– базова конфігурація пристроїв Cisco;
– безпечне управління віддаленими підключеннями по протоколу SSH;
– функція безпеки портів на комутаторах Cisco.

Далі виконати наведені кроки.

Крок 1. Побудова мережі і налаштування ПК

1. Запустити програму Cisco Packet Tracer та побудувати модель мережі з лабораторної роботи № 6 (рис. 6.1). Кожну мережу (LAN_N1 − LAN_N4) подати двома ПК, за винятком LAN_N3. Мережу LAN_N3 зобразити згідно з рис. 7.1. Для об'єднання ПК в одну мережу використовувати комутатори серії Cisco Catalyst 2960. Для об’єднання мереж в філіалах (Filial1 та Filial2) використовувати маршрутизатори серії Cisco 2811, а на Central − серії Cisco 2911.

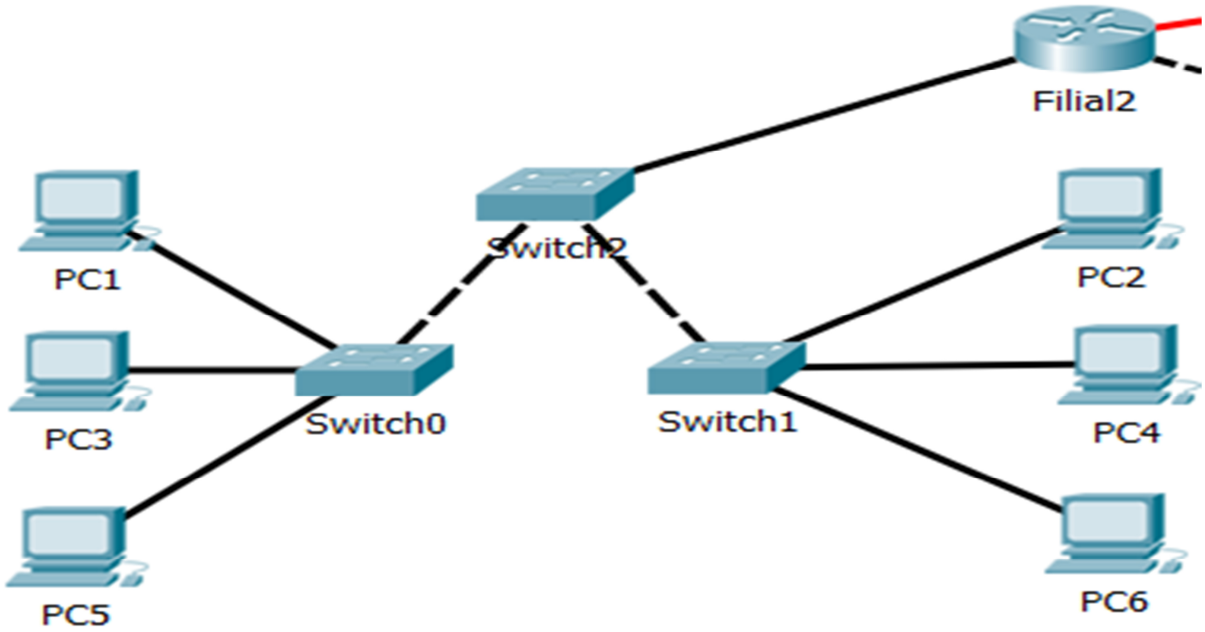

Рис. 7.1. Топологія мережі LAN_N3

2. З’єднати пристрої відповідними інтерфейсами. Між маршрутизаторами використовувати послідовний кабель. Для підключення через даний кабель, необхідно додати інтерфейсну панель HW1C-2T на вкладці *Physical* у вікні властивостей кінцевого пристрою (рис. 7.2).

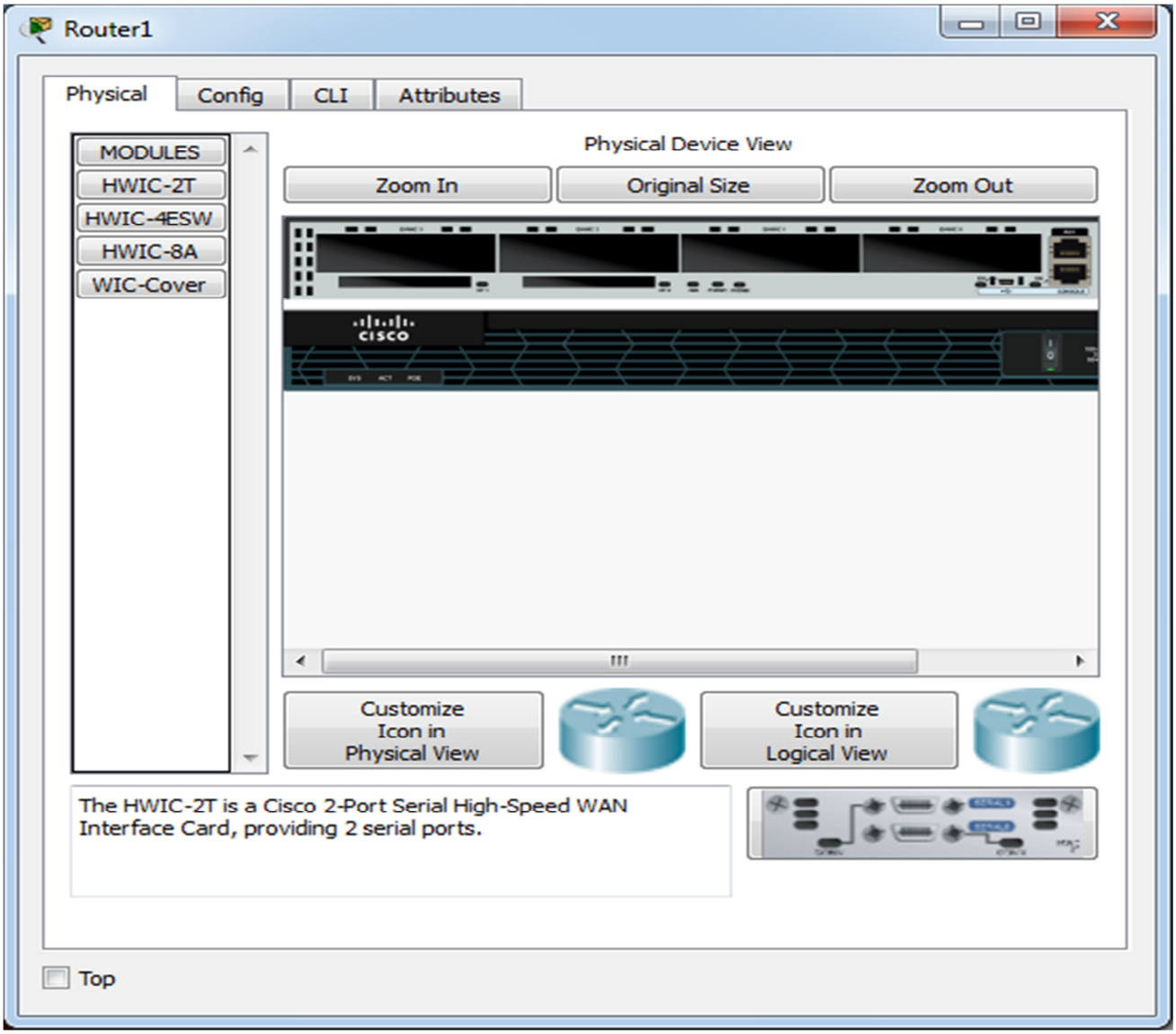

Рис. 7.2. Вкладка *Physical* маршрутизатора

3. Для IP-адресації мережі використовувати розрахунки з лабораторній роботі № 9. Задокументувати схему IP-адресації і підключень пристроїв у вигляді табл. 7.1 з урахуванням таких вимог:

– перші допустимі IP-адреси призначаються інтерфейсам маршрутизаторів у локальних мережах;

– другі з допустимих IP-адрес призначаються комутаторам;

– останні з використовуваних IP-адрес призначаються ПК.

Таблиця 7.1

Адресація пристроїв і їх підключення

Пристрій	Інтерфейс	IP-адрес	Префікс	Маска мережі	Підключення	
					Назва пристрою	Інтерфейс
…	…	…	…	…	…	…

4. Кожному ПК задати IP-адресу, маску і шлюз за умовчуванням. Заповнити табл. 7.2 відповідними даними для кожної робочої станції.

Таблиця 7.2

IP-адреси ПК

Назва мережі	IP-адреса ПК1	IP-адреса ПК2	Маска	Адреса шлюзу
LAN_N1				
LAN_N2				
LAN_N3				
LAN_N4				

5. На каналі підключення граничного маршрутизатора організації Central до Internet-провайдера ISP назначити першу допустиму адресу мережі 209.165.20.224/28, а маршрутизатору організації наступну.

Крок 2. Налаштування базової конфігурації маршрутизаторів

1. Заборонити пошук DNS (DNS lookup), щоб не виконувалось перетворення доменних імен у випадку помилкового введення в командний рядок не інтерпретованих слів замість коректних команд.

```
Router>enable
Router#configure terminal
Router(config) # no ip domain-lookup
```

2. Задати в налаштуваннях конфігурації кожного маршрутизатора унікальне ім'я і налаштувати використовувані інтерфейси згідно із заповненою табл. 7.1. На послідовних DCE-інтерфейсах маршрутизаторів встановити тактову частоту значенням 128000. Приклад налаштувань на маршрутизаторі Central:

```
Router(config)#hostname Central
Central(config)#interface serial 0/0
Central(config-if)#ip address 192.168.1.1 255.255.255.0
Central(config-if)#clock rate 128000
Central(config-if)#no shutdown
Central(config-if)#exit
```

3. Задати на всіх пристроях пароль до консолі та лінії vty *cisco*.

```
Central(config)#line console 0
Central(config-line)#password cisco
Central(config-line)#login
Central(config-line)#exit
```

Central(config)#line vty 0 4
Central(config-line)#password cisco
Central(config-line)#login
Central(config-line)#exit

4. Задати пароль до привілейованого режиму *class*.
   Central(config)#enable secret class
5. Зашифрувати всі паролі, що зберігаються у відкритому вигляді.
   Central(config)#service password-encryption
6. Налаштувати банер MOTD.
   Central(config)#banner motd #Router of Central office#
   Central(config)#exit
7. Зберегти конфігурацію.
   Central#copy running-config startup-config

Крок 3. Перевірка і тестування конфігурації

1. Для перевірки правильного налаштування ПК виконати «ping» з командного рядка вузлів в локальних мережах. Чи успішно виконані ехо-запити?
2. Виконати «ping» з командного рядка вузлів в віддалених мережах. Чи успішно виконані ехо-запити? Якщо ні, обґрунтуйте свою відповідь.
3. Виконати тестування доступності локальних інтерфейсів маршрутизаторів за допомогою команди «ping» з командного рядка ПК у відповідних мережах. Чи успішно виконані ехо-запити?
4. Перевірити налаштування конфігурації маршрутизаторів за допомогою команди «show ip interface brief».
5. За допомогою командного рядка на будь-якому вузлі підключитися до маршрутизатора в локальній мережі через Telnet.

Крок 4. Забезпечення захищеної комунікації за протоколом SSH

Використання Telnet небезпечно, оскільки текстові дані передаються в незашифрованому вигляді. Тому рекомендується по можливості використовувати протокол SSH. Відповідно до табл. 7.3 на комутаторі в заданій мережі перелаштуйте лінії VTY на доступ лише по протоколу SSH.

Таблиця 7.3

Комутатор для налаштування за протоколом SSH

Варіант	Комутатор у мережі
1, 9, 17	LAN_N1
2, 10, 18	LAN_N2
3, 11, 19	LAN_N3 – Switch0
4, 12, 20	LAN_N3 – Switch1
5, 13, 21	LAN_N3 – Switch2
6, 14, 22	LAN_N4

1. Присвойте домену ім'я за правилом *Family.Group*. Наприклад:
   Switch(config)# ip domain-name Ivanov.123-17
2. Для шифрування даних створіть ключ RSA довжиною 1024 біт.
   Switch(config)# crypto key generate rsa
   Після запиту введіть 1024.
3. Створіть користувача-адміністратора *admin* з паролем *cisco123*.
   Switch(config)# username admin password cisco123
4. Налаштуйте лінії VTY для перевірки реєстраційних даних у локальних базах даних імен користувачів, а також для дозволу віддаленого доступу лише за протоколом SSH. Видаліть існуючий пароль лінії VTY.
   Switch(config-line)# login local
   Switch(config-line)# transport input ssh
   Switch(config-line)# no password cisco

Крок 5. Перевірка реалізації протоколу SSH

1. Спробуйте за допомогою командного рядка на вузлі підключитися до комутатора через Telnet. Спроба повинна завершитися невдачею.
   > telnet *кінцевий_вузол*
2. Введіть «ssh» і натисніть Enter, не додаючи будь-яких параметрів, щоб відобразити інструкції використання команди. Параметр *-l* — це буква «L», а не цифра 1.
3. Спробуйте увійти до системи через протокол SSH.
   > ssh -l admin *кінцевий_вузол*
4. Після успішного входу перейдіть в режим привілейованого доступу і збережіть конфігурацію.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– схему логічної топології мережі;
– таблиці призначень IP-адрес (табл. 7.1 і 7.2);
– застосовані команди з налаштувань та їх опис;
– проект мережі з назвою за правилом *Family.Group.pkt* (відправити на поштову скриню викладача).

7.3. Питання для підготовки до захисту лабораторної роботи

1. Що позначає символ # після імені маршрутизатора?
2. При роботі в командному рядку Cisco IOS, які є основні режими введення команд?
3. Що повинні показувати вихідні дані для активних інтерфейсів з правильними налаштуваннями?
4. Що повинні показувати вихідні дані для інтерфейсів, що не налаштовані?
5. Чому не виконується ping до вузлів в віддалених мережах?

8. ЛАБОРАТОРНА РОБОТА № 8
ВИВЧЕННЯ ПРОГРАМ І СЛУЖБ TCP/IP

8.1. Мета лабораторної роботи

Отримати навички застосовувати команди, що дозволяють контролювати параметри мережних адаптерів і перевіряти працездатність мережі та служб.

8.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– робота з командним рядком (CLI) операційної системи Windows;
– мережні і діагностичні команди Windows (Додаток Б);
– синтаксис мережної команди «net» (Додаток В).

Роботу слід проводити в мережі, до якої підключено мінімум два комп'ютери, які належать одній IP-мережі і знаходяться в одному домені. ПК повинні мати вихід в Інтернет. Роботу слід виконувати в парі з сусідом.

Далі виконати такі дії, вивчаючи для кожної команди як можна більше доступних опцій:

– відобразити повне ім'я комп'ютера в мережі;
– відобразити довідку по використанню команди «netstat» та отримати наступні відомості:
  1) список всіх підключених портів та навести список, що знаходяться в режимі ESTABLISHED;
  2) статистику протоколів TCP, IP та ICMP;
  3) статистику мережного адаптера;
  4) список в числовому форматі усіх з'єднань TCP та UDP і пов'язані з ними програми;
– відобразити довідку по використанню команди «net» та отримати наступні відомості:
  1) список комп'ютерів, що знаходяться в даний момент в мережі;
  2) поточні значення параметрів, що визначають вимоги до паролів і входу в мережу, а також інформацію про домен;
  3) поточні значення параметрів налаштування служби робочої станції;
  4) список запущених служб;
  5) список облікових записів користувачів для даного комп'ютера;
  6) список груп користувачів даного комп'ютера;
  7) список користувачів локальної групи *Адміністратори* даного ПК;
  8) поточну дату і час на сусідньому ПК;
– відобразити довідку по використанню команди «net stop» (net help stop) та зупинити службу Spooler (Диспетчер друку);
– відобразити довідку по використанню команди «net share» та відобразити доступні для спільного використання мережні ресурси;

– використовуючи команди «nslookup», «ping», «tracert» та «pathping» отримати відомості про веб-сайт регіонального інтернет-реєстратора (Regional Internet Registry, RIR), розташованого в Австралії (www.apnic.net). Відстежити шлях (маршрут), проаналізувати якість каналу зв'язку (використовуючи exo-пакети різної довжини і кількості);

– використовуючи команди «nslookup», «ping», «tracert» та «pathping» отримати відомості про один віддалений домен, відстежити шлях (маршрут), проаналізувати якість каналу зв'язку (використовуючи exo-пакети різної довжини і кількості). Використовувати домен, у якого вузли розміщені на інших континентах, та не використовувати загальновідомі домени (такі, як google.com або yandex.ru), а також домени мережі інституту;

– відобразити довідку по використанню команди «netsh» та змінити в командному рядку IP-адресу на значення 192.168.30.*номер варіанту*/24.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис завдання з початковими умовами та даними;

– скріншоти командного рядка в ході виконання роботи;

8.3. Питання для підготовки до захисту лабораторної роботи

1. Що таке localhost?
2. Яка область застосування команди «net»?
3. Яка область застосування команди «netsh»?
4. Як включити і зупинити мережні служби робочої станції?
5. Який результат виведе команда «netstat» з параметрами -asr?
6. Який результат виведе команда «tracert»?

9. ЛАБОРАТОРНА РОБОТА № 9
ВПРОВАДЖЕННЯ І НАЛАШТУВАННЯ СЕРВІСІВ ВЕБ-СЕРВЕРУ, СЕРВЕРУ ЕЛЕКТРОННОЇ ПОШТИ, DHCP, DNS ТА FTP В CISCO PACKET TRACER

9.1. Мета лабораторної роботи

Вивчити призначення та особливості сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP, їх налаштування та перевірку в програмі Cisco Packet Tracer.

9.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні матеріали, такі питання:

– використання портів сервісами веб-серверу, серверу електронної пошти, DHCP, DNS та FTP;

– функції протоколів HTTP, SMTP, POP3, DHCP, DNS та FTP.

Вихідними даними є побудована мережа в Cisco Packet Tracer з лабораторної роботи № 7.

Виконання лабораторної роботи складається з п’ятьох частин. В першій частині необхідно налаштувати веб-сервіс. В другій частині налаштування серверу електронної пошти. В третій частині виконується налаштування записів на DNS-сервері. В четвертій частині налаштування серверу DHCP та перевірка сервісів DHCP та DNS. В п‘ятій частині налаштування FTP-сервісу на MultiServer.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис застосованих сервісів та їх параметри налаштувань;

– проект мережі з назвою за правилом *Family.Group.Server.pkt* (відправити на поштову скриню викладача).

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

Частина 1. Налаштування та перевірка веб-серверу

Крок 1. Налаштування веб-серверу

1. Додати в мережу LAN_N1 сервер *Server-PT* з групи *End Devise*, дати йому назву MultiServer та привласнити IP-адресу з діапазону допустимих IP-адрес цієї підмережі.
2. На MultiServer відкрити вкладку *Services* і вибрати розділ *HTTP*.
3. Вибрати варіант On, щоб включити HTTP і HTTP Secure (HTTPS).
4. Необов'язковий крок. Змінити HTML-код.

Крок 2. Перевірка працездатності веб-серверу

1. На будь-якому вузлі в мережі LAN_N1 відкрити вкладку *Desktop* та вибрати додаток *Web Browser.*
2. В полі URL ввести IP-адресу MultiServer і натиснути кнопку Go. Відкриється веб-сайт MultiServer.
3. Перевірити працездатність веб-серверу з вузлів в інших підмережах через його IP-адресу.

Частина 2. Налаштування та перевірка серверу електронної пошти

Крок 1. Налаштування MultiServer для відправки (SMTP) й отримання (POP3) повідомлень електронної пошти

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *EMAIL*.
2. Вибрати варіант On, щоб включити SMTP і POP3.
3. Призначте ім'я домену multiserver.pt і натиснути кнопку Set.
4. Створити користувача з ім'ям test-user1 та і паролем cisco. Натиснути + для додавання користувача.
5. Створити користувача з ім'ям test-user2 та і паролем cisco. Натиснути + для додавання користувача.

Крок 2. Налаштування та перевірка ПК для використання сервісу електронної пошти

1. На будь-якому вузлі в мережі відкрити вкладку *Desktop* та вибрати додаток *Email*.
2. Ввести відповідні значення у відповідних полях:
   а) Your Name: Tets User1;
   б) Email Address: test-user@multiserver.pt;
   в) Incoming Mail Server: IP-адреса MultiServer;
   г) Outgoing Mail Server: IP-адреса MultiServer;
   д) User Name (Ім'я користувача): test-user1;
   е) Password: cisco;
   ж) Натиснути кнопку Save. З'явиться вікно поштового оглядача.
3. Натиснути кнопку Receive. Якщо всі налаштування клієнта і сервера виконані правильно, у вікні поштового оглядача з'явиться повідомлення про підтвердження Receive Mail Success.
4. Вибрати інший ПК в мережі, відкрити вкладку *Desktop* та вибрати додаток *Email*.
5. Виконати відповідні налаштування email для test-user2.

Крок 3. Відправка електронної пошти від test-user1 до test-user2

1. У вікні *Mail Browser* на test-user1 натиснути кнопку Compose.
2. Ввести наступні значення у відповідних полях:
   а) To: test-user2@multiserver.pt;
   б) Subject: вкажіть тему повідомлення;
   в) Email Body: введіть текст листа.
3. Натиснути Send.

4. Натиснути кнопку Receive на test-user2 і переконатися, що він отримав повідомлення електронної пошти. Двічі клацнути повідомлення електронної пошти.

5. Натиснути кнопку Reply, ввести відповідь і натиснути кнопку Send.

6. Переконатися, що test-user1 отримав відповідь.

Частина 3. Налаштування записів на DNS-сервері

Крок 1. Налаштування записів на DNS-сервері

1. Додати в мережу LAN_N2 сервер *Server-PT* з групи *End Devise*, дати йому назву ServerDNS та привласнити IP-адресу з діапазону допустимих IP-адрес цієї підмережі.

1. На ServerDNS відкрити вкладку *Services* і вибрати розділ *DNS*.

2. Вибрати варіант On, щоб включити сервіс DNS.

3. Додати запис для MultiServer у відповідних полях:

   а) Name: netacad.com;

   б) Address: IP-адреса MultiServer.

4. Натиснути кнопку Add щоб додати запис.

Частина 4. Налаштування серверу DHCP та перевірка сервісів DHCP та DNS

Крок 1. Налаштування серверу DHCP

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *DHCP*.

2. Вибрати варіант On, щоб включити сервіс DHCP.

3. Ввести відповідні значення у відповідних полях:

   а) Pool Name: Dhcp_Lan1;

   б) Default Gateway: IP-адреса шлюза;

   в) DNS Server: IP-адреса ServerDNS;

   г) Start IP Address: виключити перші 10 адрес;

   д) Subnet Mask: маска мережі LAN_N1;

4. Натиснути кнопку Add щоб додати запис.

Крок 2. Перевірка сервісу DHCP для вузлів в LAN_N1

1. На кожному вузлі LAN_N1 відкрити вкладку *Desktop* і вибрати розділ *IP Configuration*.

2. Вибрати варіант DHCP і дочекатися виконання запиту DHCP.

Крок 3. Перевірка сервісу DNS

1. На MultiServer відкрити вкладку *Desktop* і в розділі *IP Configuration* в полі DNS Server вказати IP-адресу ServerDNS.

2. На будь-якому вузлі в мережі LAN_N1 відкрити вкладку *Desktop* та вибрати додаток *Command Prompt.*

3. Виконати команду «ping» на IP-адресу ServerDNS, щоб протестувати своє з'єднання.

4. Виконати команду «nslookup netacad.com», щоб перевірити роботу ServerDNS. Повинні отримати IP-адрес для імені netacad.com.

5. Закрити додаток *Command Prompt* та відкрити *Web Browser.*

6. В полі URL ввести netacad.com і натиснути кнопку Go. Відкриється веб-сайт MultiServer.

7. Перевірити працездатність веб-серверу з вузлів в інших підмережах, додавши в налаштуваннях IP-адресу ServerDNS.

Частина 5. Налаштування FTP-сервісу на MultiServer

Крок 1. Налаштування FTP-сервісу на MultiServer

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *FTP*.

2. Вибрати варіант On, щоб включити сервіс FTP.

3. У розділі User Setup створити облікові записи користувачів (табл. 9.1). Натиснути Add для додавання облікового запису.

Таблиця 9.1

Облікові записи на сервері FTP

Ім’я користувача	Пароль	Дозволи
anonymous	anonymous	Read List
administrator	cisco	full permission

Крок 2. Відправка конфігураційного файлу на FTP-сервер

1. На будь-якому вузлі в мережі відкрити вкладку *Desktop* і вибрати додаток *Text Editor.*

2. Набрати текст у текстовому редакторі та при його закритті зберегти під назвою README.txt.

3. На вкладці *Desktop* відкрити вікно командного рядка і виконати такі дії:

а) введіть «ftp *IP-адреса MultiServer»*, зачекайте кілька секунд, поки клієнт підключиться;

б) сервер виведе запит для введення імені користувача і пароля, використайте облікові дані для облікового запису administrator;

в) рядок зміниться на ftp>, введіть команду «dir» для перегляду змісту каталогу, з'явиться каталог файлів на MultiServer;

г) для перенесення файлу README.txt в рядку ftp> введіть «put README.txt», файл README.txt буде переданий з вузла на MultiServer.

д) введіть команду «dir», щоб упевнитися, що файл був переданий, файл README.txt тепер є в списку файлів каталогу;

е) закрийте FTP-клієнт, ввівши команду «quit», командний рядок набуде вигляду PC>.

9.3. Питання для підготовки до захисту лабораторної роботи

1. Який протокол перетворює ім‘я netacad.com в IP-адресу?
2. Який протокол транспортного рівня використовується для передачі DNS?
3. Які переваги використання DHCP?
4. У чому полягає основне призначення DNS?
5. У чому недолік доступу до FTP з командного рядка?

ПЕРЕЛІК ПОСИЛАНЬ

1. Воробієнко П. Телекомунікаційні та інформаційні мережі / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. − Київ: Саміт-книга, 2010. − 635 с.
2. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.
3. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.
4. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
5. Цвіркун Л.І. Інженерна та комп’ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна ; М-во освіти і науки України, НТУ “Дніпровська політехніка”. – Дніпро: НТУ “ДП” , 2018. – 209 с.
6. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров / Х. Остерлох. − Санкт-Петербург: ООО "ДиаСофтЮП", 2002. − 567 с.
7. Ирвин Дж. Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль; пер. с англ. – Санкт-Петербург: БХВ-Петербург, 2003. – 448 с.
8. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – Санкт-Петербург: Питер, 2010. – 944 с: ил.
9. Сунчелей И.Р. Структурированные кабельные системы / И.Р. Сунчелей, С.К. Стрижаков, А.Б. Семенов. – 5-е изд. – Москва: Изд-во Компания АйТи, ДМК, 2004. – 640 с.
10. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – Санкт-Петербург: Питер, 2003. – 992 с.
11. Цвіркун Л.І. Інженерна та комп’ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна ; М-во освіти і науки України, НТУ “Дніпровська політехніка”. – Дніпро: НТУ “ДП” , 2018. – 209 с.

Додаток А
Використання довідкової системи Cisco IOS

В IOS доступна довідка по командам. В даний момент відображається запрошення, зване режимом користувача, і пристрій очікує введення команд. Найпростіший спосіб викликати довідку, це ввести знак питання (?) в будь-якому місці командного рядка.

Крок 1. Вивчення довідки по Cisco IOS

1. Відкрийте список всіх допустимих команд в режимі користувача.
   Switch>?
2. У командному рядку введіть «t» зі знаком питання в кінці (?).
   Switch> t?
3. У командному рядку введіть «te» зі знаком питання в кінці (?).
   Switch> te?

Крок 2. Вхід в привілейований режим

1. Наберіть «en» і натисніть клавішу Tab.
   Switch> en<Tab>

2.Введіть команду «enable» і натисніть клавішу Enter. Як змінився вигляд командного рядка маршрутизатора і що це означає?

3.У привілейованому режимі введіть знак питання «?».
   Switch #?

4. На екрані повинен з'явитися список команд. У нижній частині екрана з'явиться рядок «-more-». Для того щоб продовжити виведення списку команд натисніть або клавішу Enter (вивід на екран лінію за лінією), або Space (вивід посторінково). Щоб вийти з перегляду списку команд, натисніть «q».

Крок 3. Список команд show

Виведіть всі команди show, ввівши «show ?» в привілейованому режимі.
   Switch# show ?

Крок 4. Використання довідкової системи при установці дати і часу

1. Введіть «show clock» в привілейованому режимі.
   Switch# show clock

2. Використовуйте контекстну довідку і команду «clock», щоб встановити поточний час на комутаторі. Введіть команду «clock» і натисніть клавішу Enter.
   Switch# clock <ENTER>

3. IOS видала повідомлення % Incomplete command, яке означає, що для команди «clock» потрібні додаткові параметри. У довідці можна отримати додаткові відомості про час, якщо ввести після команди пробіл і знак питання (?).

4. Введіть з клавіатури «clock ?» І потім натисніть Enter. Відзначте відмінності в реакції комутатора на ваші дії при введенні цих команд.
   Switch# clock ?

5. Встановіть час на комутаторі шляхом введення з клавіатури «clock ?» І дотримуйтесь далі опису команди з екрану допомоги:

Switch# clock ?
Switch# clock set ?
Switch# clock set 10:30:30 ?
Switch# clock set 10:30:30 17 April ?
Switch# clock set 10:30:30 17 April 2020

6. Поверніться в привілейований режим, натиснувши Ctrl+Z. Введіть «show clock» щоб переглянути поточні час і дату на маршрутизаторі.

Switch# show clock

Крок 5. Редагування команд в Cisco IOS

1. У привілейованому режимі введіть «show history» та не натискайте клавішу Enter.

2. Натисніть «Ctrl+A». Дана команда встановить курсор на початок рядка.

3. Натисніть «Ctrl+E». Дана команда встановить курсор в кінець рядка.

4. Натисніть «Ctrl+A», а потім «Ctrl+F». Дана команда встановлює курсор на один символ вперед.

5. Натисніть «Ctrl+B». Дана команда встановлює курсор на один символ назад.

6. Натисніть Enter, а після цього «Ctrl+P». Дана послідовність повторює останню введену команду. Натисніть кнопку «Вгору». Це також повторить останню введену команду.

7. Використовуйте інші гарячі клавіші в консолі за необхідності:

«Ctrl+W» − стерти попереднє слово;

«Ctrl+U» − стерти всю лінію;

«Ctrl+C» − вихід з режиму конфігурації;

«Ctrl+Z» − застосувати поточну команду і вийти з режиму конфігурації;

«Ctrl+Shift+6» − зупинка тривалих процесів (так званий escape sequence).

Додаток Б
Мережні та діагностичні команди Windows

Таблиця ДБ.1

Мережні та діагностичні команди Windows

Команда	Опис
arp	Вивід і редагування таблиці трансляції IP-адрес в фізичні з використанням протоколу дозволу адрес (ARP)
getmac	Вивід MAC-адрес мережних адаптерів комп'ютера. Команда «getmac» може використовуватися для отримання інформації про MAC-адреси віддаленого комп'ютера в мережі, проте необхідно щоб користувач мав право доступу
ftp	Обмін файлами з комп'ютером, на якому запущена служба сервера FTP
hostname	Вивід мережної назви комп'ютера. Ця команда доступна тільки після установки підтримки протоколу TCP/IP
ipconfig	Вивід всіх поточних налаштувань TCP/IP на комп'ютері і поновлення параметрів DHCP і DNS. При виклику команди «ipconfig» без параметрів виводяться IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера
nbtstat	Засіб діагностики розпізнавання імен NetBIOS. Вивід статистики протоколу і поточних підключень TCP/IP за допомогою NBT (NetBIOS через TCP/IP)
netstat	Вивід стану TCP-з'єднань та портів, що прослуховуються комп'ютером. Крім цього виводить статистику Ethernet, таблиці маршрутизації, статистику IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP через IPv6 і UDP через IPv6)
nslookup	Діагностична команда для виведення відомостей в базі даних DNS-сервера, які відносяться до вузла або домену
netsh	Найбільш повна і функціональна команда для керування конфігурацією різних мережних служб на локальному або віддалених комп'ютерах з використанням командного рядка. Можливості «netsh» настільки великі, що важко знайти мережне завдання, яке неможливо було б вирішити за допомогою цієї команди
ping	Перевірка з'єднань в мережах на основі TCP/IP та служби перетворення імен DNS
tracert	Діагностична команда, призначена для визначення маршруту IP-пакетів до точки призначення за допомогою ехо-повідомлень протоколу ICMP (Internet Control Message Protocol) та повідомляє час, необхідний для досягнення кожного вузла по шляху до заданого вузла
pathping	Засіб визначення маршруту, що поєднує функції команд «ping» і «tracert». Ця команда показує ступінь втрати пакетів на будь-якому маршрутизаторі або каналі та дозволяє визначити, які маршрутизатори або канали викликають неполадки в роботі мережі
route	Вивід та зміна таблиці маршрутизації на комп'ютері
net	Управління налаштуваннями мережі в командному рядку Windows. Синтаксис наведено в Додатку В

Додаток В
Синтаксис мережної команди NET

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

Таблиця ДВ.1

Синтаксис мережної команди NET в Windows Vista, 7, 8 та 10

Параметр	Опис
NET ACCOUNTS	Налаштування параметрів облікового запису. Без параметрів виводить поточні значення параметрів, що визначають вимоги до паролів і входу в мережу, а також інформацію про домен. **[/FORCELOGOFF:{minutes | NO}] [/MINPWLEN:length] [/MAXPWAGE:{days | UNLIMITED}] [/MINPWAGE:days] [/UNIQUEPW:number] [/DOMAIN]**
NET COMPUTER	Додає або видаляє комп'ютери з бази даних домену. Ця команда може використовуватися тільки на контролерах домену **\\computername {/ADD | /DEL}**
NET CONFIG	Відображає інформацію про налаштування служб робочої станції або служби сервера. **[SERVER | WORKSTATION]**
NET CONTINUE	Продовжує роботу служби Windows або ресурсу, раніше призупинену за допомогою команди **NET PAUSE**. **[service]**
NET START	Використовується для запуску служб Windows або ресурсів. Без параметрів виводить список запущених служб. **[service]**
NET STOP	Зупиняє службу Windows або ресурс. **[service]**
NET PAUSE	Призупиняє службу Windows або ресурс . **[service]**
NET FILE	Відображає список відкритих по мережі файлів і може примусово закривати загальний файл і знімати файлові блокування. **[id [/CLOSE]]**
NET GROUP	Додавання, видалення, перегляд та керування робочими групами мережі на контролері домену і відноситься до об'єктів Active Directory. **[groupname [/COMMENT:"text"]] [/DOMAIN]** **groupname {/ADD [/COMMENT:"text"] | /DELETE} [/DOMAIN]** **groupname username [...] {/ADD | /DELETE} [/DOMAIN]**
NET LOCALGROUP	Додавання, видалення, перегляд та керування робочими групами мережі на контролері домену і відноситься до локальних робочих груп комп'ютера. **[groupname [/COMMENT:"text"]] [/DOMAIN]** **groupname {/ADD [/COMMENT:"text"] | /DELETE} [/DOMAIN]** **groupname name [...] {/ADD | /DELETE} [/DOMAIN]**

Продовження табл. ДВ.1

Параметр	Опис
NET SESSION	Завершує поточні сеанси зв'язку між комп'ютером і іншими комп'ютерами мережі або виводить їх список. Ця команда використовується тільки на серверах. **[\\computername] [/DELETE]**
NET SHARE	Дозволяє управляти загальними ресурсами. Без параметрів виводить відомості про всі загальні ресурси локального комп'ютера. **sharename** **sharename=drive:path [/USERS:number | /UNLIMITED]** **[/REMARK:"text"]** **[/CACHE:Manual | Documents| Programs | None]** **sharename [/USERS:number | /UNLIMITED]** **[/REMARK:"text"]** **[/CACHE:Manual | Documents | Programs | None]** **{sharename | devicename | drive:path} /DELETE**
NET STATISTICS	Виводить журнал статистики для локальної служби робочої станції або служби сервера. Без параметрів виводить список служб, для яких може накопичуватися статистика. **[WORKSTATION | SERVER]**
NET TIME	Синхронізує показання годинника комп'ютера з показаннями годин іншого комп'ютера або домену або відображає час для комп'ютера або домену. Без параметрів виводиться поточна дата і час, встановлені на комп'ютері, призначеному сервером часу для даного домену. **[\\computername | /DOMAIN[:domainname] |** **/RTSDOMAIN[:domainname]] [/SET]** **[\\computername] /QUERYSNTP** **[\\computername] /SETSNTP[:ntp server list]**
NET USE	Підключає комп'ютер до спільно використовуваного ресурсу або відключає комп'ютер від нього. Без параметрів виводить список з'єднань для даного комп'ютера. **[devicename | *] [\\computername\sharename[\volume] [password | *]]** **[/USER:[domainname\]username]** **[/USER:[dotted domain name\]username]** **[/USER:[username@dotted domain name]** **[/SMARTCARD]** **[/SAVECRED]** **[[/DELETE] | [/PERSISTENT:{YES | NO}]]** **NET USE {devicename | *} [password | *] /HOME** **NET USE [/PERSISTENT:{YES | NO}]**
NET USER	Дозволяє створювати і змінювати облікові записи користувачів на комп'ютерах. При виконанні команди без параметрів відображається список облікових записів користувачів даного комп'ютера. **[username [password | *] [options]] [/DOMAIN]** **username {password | *} /ADD [options] [/DOMAIN]** **username [/DELETE] [/DOMAIN]**

Закінчення табл. ДВ.1

Параметр	Опис
NET VIEW	Виводить список доменів, комп'ютерів або загальних ресурсів на даному комп'ютері. Без параметрів виводить список комп'ютерів в поточному домені. **[\\computername [/CACHE] | /DOMAIN[:domainname]]** **NET VIEW /NETWORK:NW [\\computername]**

Цвіркун Леонід Іванович
Панферова Яна Володимирівна
Бешта Лілія Валеріївна

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт студентами спеціальностей 122 Комп'ютерні науки та 172 Телекомунікації та радіотехніка

Видано в редакції авторів

Підписано до друку 19.03.2021. Формат 30х42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 2,2.
Обл.-вид. арк. 2,2. Тираж 20 пр. Зам. №

Національний технічний університет
"Дніпровська політехніка".
49005, м. Дніпро, просп. Д. Яворницького, 19.