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

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації
до виконання лабораторних робіт студентами
галузі знань 12 Інформаційні технології
спеціальності 123 Комп'ютерна інженерія

Частина 1

Дніпро
2018

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

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра автоматизації та комп'ютерних систем

Л.І. Цвіркун
Я.В. Панферова

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації
до виконання лабораторних робіт
студентами галузі знань 12 Інформаційні технології
спеціальності 123 Комп'ютерна інженерія

Частина 1

Дніпро
НТУ «ДП»
2018

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.

Автори:
Л.І. Цвіркун, канд. техн. наук, проф. (лаб. роботи 1 – 3);
Я.В. Панферова, асист. (лаб. роботи 4 – 14, додатки А – В).

Затверджено методичною комісією з галузі знань 12 Інформаційні технології (протокол № 4 від 30.03.18) за поданням кафедри автоматизації та комп’ютерних систем (протокол № 15 від 29.03.18).

Подано методичні рекомендації до виконання лабораторних робіт з дисципліни “Комп’ютерні мережі” студентами спеціальності 123 Комп'ютерна інженерія.

Відповідальний за випуск завідувач кафедри автоматизації та комп’ютерних систем В.В. Ткачов, д-р техн. наук, проф.

ЗМІСТ

Стор.

Вступ 5

1. Лабораторна робота № 1. Базове налаштування комутатора з використанням інтерфейсу командного рядка 6
   - 1.1. Мета лабораторної роботи 6
   - 1.2. Організація виконання лабораторної роботи 6
   - 1.3. Питання для підготовки до захисту лабораторної роботи 14
2. Лабораторна робота № 2. Вивчення інтерфейсу програми Wireshark 15
   - 2.1. Мета лабораторної роботи 15
   - 2.2. Організація виконання лабораторної роботи 15
   - 2.3. Питання для підготовки до захисту лабораторної роботи 19
3. Лабораторна робота № 3. Дослідження кадру протоколу Ethernet та пропускної здатності Fast Ethernet 20
   - 3.1. Мета лабораторної роботи 20
   - 3.2. Організація виконання лабораторної роботи 20
   - 3.3. Питання для підготовки до захисту лабораторної роботи 22
4. Лабораторна робота № 4. Вивчення протоколу ARP 23
   - 4.1. Мета лабораторної роботи 23
   - 4.2. Організація виконання лабораторної роботи 23
   - 4.3. Питання для підготовки до захисту лабораторної роботи 25
5. Лабораторна робота № 5. Вивчення протоколу IP 26
   - 5.1. Мета лабораторної роботи 26
   - 5.2. Організація виконання лабораторної роботи 26
   - 5.3. Питання для підготовки до захисту лабораторної роботи 27
6. Лабораторна робота № 6. Отримання відомостей про MAC-адреси і мережні налаштування TCP/IP 27
   - 6.1. Мета лабораторної роботи 27
   - 6.2. Організація виконання лабораторної роботи 27
   - 6.3. Питання для підготовки до захисту лабораторної роботи 28
7. Лабораторна робота № 7. Визначення IPv4-адрес 28
   - 7.1. Мета лабораторної роботи 28
   - 7.2. Організація виконання лабораторної роботи 28
   - 7.3. Питання для підготовки до захисту лабораторної роботи 31
8. Лабораторна робота № 8. Розрахунок підмереж за допомогою маски постійної довжини 31
   - 8.1. Мета лабораторної роботи 31
   - 8.2. Організація виконання лабораторної роботи 31
   - 8.3. Питання для підготовки до захисту лабораторної роботи 34
9. Лабораторна робота № 9. Розрахунок підмереж за допомогою маски змінної довжини 35
   - 9.1. Мета лабораторної роботи 35
   - 9.2. Організація виконання лабораторної роботи 35
   - 9.3. Питання для підготовки до захисту лабораторної роботи 36

10. Лабораторна робота № 10. Розрахунок сумарного маршруту 37
10.1. Мета лабораторної роботи 37
10.2. Організація виконання лабораторної роботи 37
10.3. Питання для підготовки до захисту лабораторної роботи 38
11. Лабораторна робота № 11. Побудова мережі в Cisco Packet Tracer і базове налаштування пристроїв 39
11.1. Мета лабораторної роботи 39
11.2. Організація виконання лабораторної роботи 39
11.3. Питання для підготовки до захисту лабораторної роботи 43
12. Лабораторна робота № 12. Вивчення програм і служб TCP/IP 44
12.1. Мета лабораторної роботи 44
12.2. Організація виконання лабораторної роботи 44
12.3. Питання для підготовки до захисту лабораторної роботи 45
13. Лабораторна робота № 13. Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP в Cisco Packet Tracer. 46
13.1. Мета лабораторної роботи 46
13.2. Організація виконання лабораторної роботи 46
13.3. Питання для підготовки до захисту лабораторної роботи 49
14. Лабораторна робота № 14. Вивчення транспортного протоколу TCP та протоколу передачі файлів FTP 50
14.1. Мета лабораторної роботи 50
14.2. Організація виконання лабораторної роботи 50
14.3. Питання для підготовки до захисту лабораторної роботи 52
Перелік посилань 53

Додаток А. Розрахунок пропускної здатності мережі Fast Ethernet для максимального і мінімального розміру кадрів 54
Додаток Б. Мережні та діагностичні команди Windows 56
Додаток В. Синтаксис мережної команди NET 57

ВСТУП

Методичні рекомендації призначені для студентів спеціальності 123 “Комп'ютерна інженерія”, 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 7, протоколами Ethernet, ARP, IP, TCP, UDP, HTTP, DHCP, DNS та FTP. Визначати типи IP-адрес та навчитися організовувати підмережі за допомогою маски постійної або змінної довжини та розраховувати сумарні маршрути.

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
БАЗОВЕ НАЛАШТУВАННЯ КОМУТАТОРА З ВИКОРИСТАННЯМ ІНТЕРФЕЙСУ КОМАНДНОГО РЯДКА

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;

– робота в командному рядку (Command Line Interface, CLI) операційної системи Cisco IOS;

– робота з контекстною довідкою в CLI;

– базове налаштування пристроїв Cisco.

Виконання лабораторної роботи складається з чотирьох частин. В першій частині необхідно побудувати мережу в програмі Cisco Packet Tracer. В другій частині вивчається робота з довідковою системою Cisco IOS. В третій частині виконується налаштування базових параметрів комутатора. В четвертій частині виконується налаштування ПК та перевірка 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;

– відповіді на поставленні запитанні в ході виконання роботи;

– команди базового налаштування пристроїв Cisco з детальним описом.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

Частина 1. Побудова мережі

Крок 1. Вибір пристроїв і побудова мережі

Запустити програму Cisco Packet Tracer та побудувати мережу, представлену на рис. 1.1. IP-адресація пристроїв надана 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 студента за списком в групі.

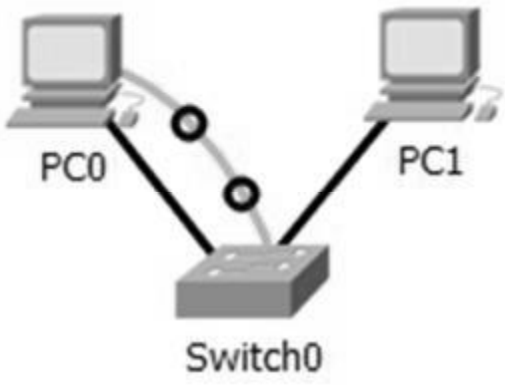

Рис. 1.1 – Топологія мережі

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*.

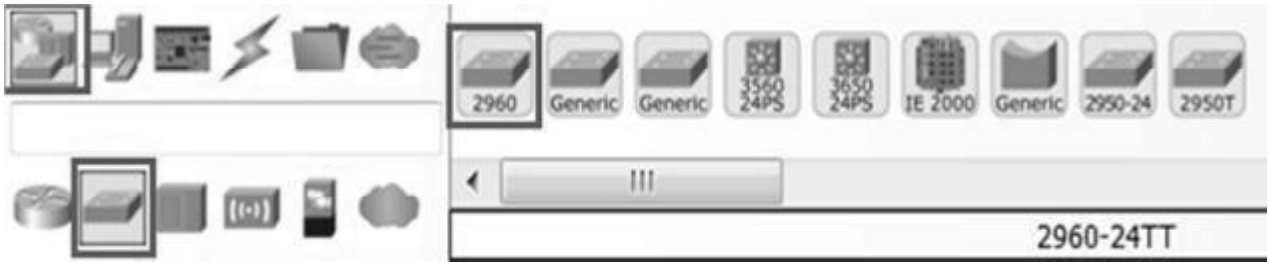

Рис. 1.2 – Панель вибору типових пристроїв і зв'язків

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.

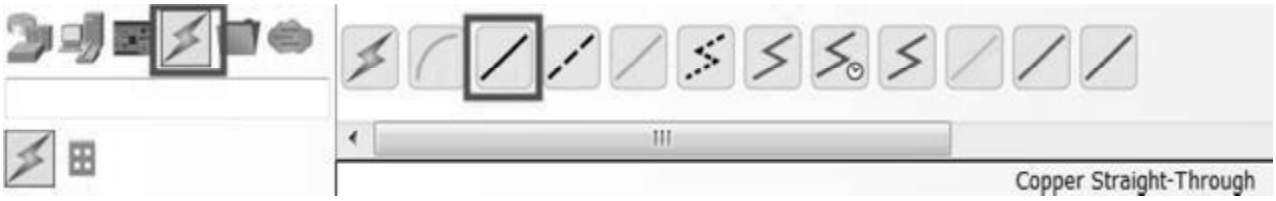

Рис. 1.3 – Панель вибору з'єднань

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. Консольне підключення до комутатора Switch0

1. У групі *Connections* виберіть світло-блакитний консольний кабель (Console).

2. Клацніть PC0. Виберіть варіант для підключення RS-232.

3. Перетягніть інший кінець консольного підключення до комутатора Switch0 і клацніть на ньому, щоб відкрити список підключень. Виберіть консольний порт (Console), щоб завершити підключення.

Крок 4. Встановлення сеансу термінального зв'язку з комутатором Switch0

1. Клацніть PC0 і відкрийте вкладку *Desktop* (Робочий стіл).

2. Клацніть значок програми *Terminal*. Перевірте правильність параметрів за замовчуванням, встановлених для порту. Параметри порту: 9600, 8, None, 1, None. Натисніть кнопку OK.

3. У вікні може бути показано кілька повідомлень. У будь-якої частини вікна має з'явитися повідомлення Press RETURN to get started! (Натисніть клавішу ENTER, щоб почати роботу). Натисніть клавішу Enter.

4. Яке запрошення показано на екрані? _____

5. Що означає символ після імені комутатора? _____

Частина 2. 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>?
```

Яка команда починається з букви «s»? _____

2. У командному рядку введіть «t» зі знаком питання в кінці (?).

```
Switch> t?
```

Які відображаються команди? _____

3. У командному рядку введіть «te» зі знаком питання в кінці (?).

```
Switch> te?
```

Які відображаються команди? _____

Крок 2. Вхід в привілейований режим

1. Наберіть «en» і натисніть клавішу Tab.

```
Switch> en<Tab>
```

Що відображається після натискання клавіші 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».

5. Перерахуйте десять доступних команд в привілейованому режимі. ____

Крок 3. Список команд show

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

```
Switch# show ?
```

Чи доступна команда running-config в даному режимі? _____

Крок 4. Використання довідкової системи при установці дати і часу

1. Введіть «show clock» в привілейованому режимі.

```
Switch# show clock
```

Яка відображається інформація та рік? _____

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

```
Switch# clock <ENTER>
```

Яка інформація відображається? _____

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 2017
```

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).

Частина 3. Налаштування базових параметрів комутатора

Крок 1. Перегляд поточної конфігурації комутатора

1. Виконайте команду «show running-config».

```
Switch# show running-config
```

Скільки у комутатора інтерфейсів FastEthernet? _____

Скільки у комутатора інтерфейсів Gigabit Ethernet? _____

Який діапазон значень, що відображаються в vty-лініях? _____

Яка команда відображає поточний зміст NVRAM? _____

2. Відкрийте вміст NVRAM «show startup-config». Чому комутатор відповідає повідомленням startup-config is not present? _____

Крок 2. Вхід в режим глобальної конфігурації

1. Наберіть «config» в привілейованому режимі. При введенні команди «config» IOS просить вказати той її варіант, який буде використовуватися:

```
Switch # config
Configuring from terminal, memory, or network [terminal]?
```

2. Натисніть Enter, щоб прийняти параметр за замовчуванням, вказаний в квадратних дужках.

Як змінився вигляд командного рядка і що це означає? _____

Крок 3. Заборона небажаних пошуків в DNS

Вимкніть пошук в DNS, щоб запобігти спробам комутатора перетворювати введені невірні команди таким чином, як ніби вони є іменами вузлів.

```
Switch (config) # no ip domain-lookup
```

Крок 4. Налаштування паролів привілейованого режиму

1. Встановіть незашифрований пароль *cisco* на вхід в привілейований режим.

```
Switch(config) #enable password cisco
```

2. Здійсніть вихід з режиму глобальної конфігурації через «Control+Z», а потім з привілейованого режиму командою «disable». Спробуйте тепер знову здійснити вхід в привілейований режим. Зверніть увагу, що при введенні паролю на екрані символи не відображаються.

3. Встановіть зашифрований пароль *class* на вхід в привілейований режим.

```
Switch(config) #enable secret class
```

4. Здійсніть вихід з режиму глобальної конфігурації, а потім з привілейованого режиму. Спробуйте тепер знову здійснити перехід в привілейований режим. Який при цьому пароль ви ввели? _____

5. Покажіть поточну конфігурацію комутатора.

```
Switch# show running-config
```

6. Знайдіть в поточній конфігурації паролі на вхід в привілейований режим. Зверніть увагу, як відображаються два пароля. Чому пароль enable secret відображається не так, як його ввели? _____

7. Видаліть незашифрований пароль на вхід в привілейований режим.

```
Switch(config) #no enable password
```

Крок 5. Налаштування доступу до консолі

1. Введіть «line ?» в режимі глобальної конфігурації.

```
Switch(config)# line ?
```

2. Встановіть пароль *cisco* на консоль:

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

3. Закрийте сеанс консолі, ввівши команду «exit» в привілейованому режимі.

```
Switch# exit
```

4. Переконайтеся, що доступ до консолі захищений паролем. Для цього натисніть клавішу Enter, щоб увійти в режим користувача.

Крок 6. Налаштування пароля на доступ по telnet або ssh

Лінії vty (virtual terminal line) потрібні для віддаленого адміністрування пристроєм по telnet або ssh.

Встановіть пароль *cisco* на лінії vty.

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

Крок 7. Налаштування імені комутатора

Встановіть для комутатора ім'я командою «hostname».

```
Switch(config)#hostname S1
```

Крок 8. Перевірка конфігурацій

1. Перегляньте поточну конфігурацію комутатора за допомогою команди привілейованого режиму «show running-config».

```
S1(config)#do show running-config
```

ПРИМІТКА. Приставка do дозволяє виконувати команди «show» в будь-якому режимі, не виходячи в привілейований.

2. Знайдіть налаштовані паролі і команди. Зверніть увагу, що паролі на консольні та термінальні лінії відображаються у відкритому вигляді.

Крок 9. Шифрування паролів

1. Зашифруйте всі поточні і наступні паролі.

```
S1(config)# service password-encryption
```

2. Перегляньте поточну конфігурацію.

3. Знайдіть налаштовані паролі і команди. Зверніть увагу, що паролі на консольні та термінальні лінії відображаються в зашифрованому вигляді.

Крок 10. Встановлення банера MOTD

Налаштуйте повідомлення, яке буде відображатися всім, хто входить в систему на комутаторі. Це повідомлення називається щоденним банером (MOTD). Текст банера можна укласти в подвійні лапки або використовувати будь-який символ, відмінний від символу в рядку MOTD.

```
S1(config)#banner motd #Building power will be off from 7:00 AM
until 9:00 AM this coming Tuesday#
```

Крок 11. Налаштування інтерфейсу керування комутатором

Через віртуальний інтерфейс комутатора (SVI) можна отримати віддалений доступ по telnet або ssh з метою відображення і налаштування його параметрів. На SVI-інтерфейсі можна сконфігурувати IP-адресу, яку зазвичай називають адресою керування. За замовчуванням через VLAN 1 забезпечується керування комутатором по мережі. Щоб налаштувати IP-адресу на комутаторі S1, використовуйте наступні команди.

```
S1(config) # interface vlan 1
S1(config-if) # ip address 192.168.1.254 255.255.255.0
S1(config-if) # no shutdown
%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan1, changed state to up
```

Крок 12. Перевірка налаштування інтерфейсу керування комутатором

Команда «show ip interface brief» в привілейованому режимі інформує про IP-адресу, а також про стан всіх портів і інтерфейсів комутатора. Для цього можна також використовувати команду «show running-config». Стан інтерфейсу VLAN 1 повинен бути up/up (працює/працює), а інтерфейсу призначений IP-адрес. Зверніть увагу, що стан портів комутатора F0/1 та F0/2 також up, оскільки до них підключені ПК.

Крок 13. Збереження конфігурації комутатора в NVRAM

Щоб внесені зміни не загубилися після перезавантаження системи і відключення живлення необхідно створити резервні копії файлу конфігурації в NVRAM.

S1# copy running-config startup-config

Яка найкоротша версія команди «copy running-config startup-config»? ____

Частина 4. Налаштування ПК

Крок 1. 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 2. 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

4. Для перевірки віддаленого підключення до комутатора через адресу управління SVI в командному рядку введіть команду «telnet *ip-адреса*».

PC> telnet 192.168.1.254

5. Введіть «quit», щоб завершити сеанс telnet.

Крок 3. 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. Для чого потрібна команда «login» при налаштуванні доступу до ліній vty та консолі?
4. Який слід використовувати кабель при підключенні двох ПК між собо?
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;

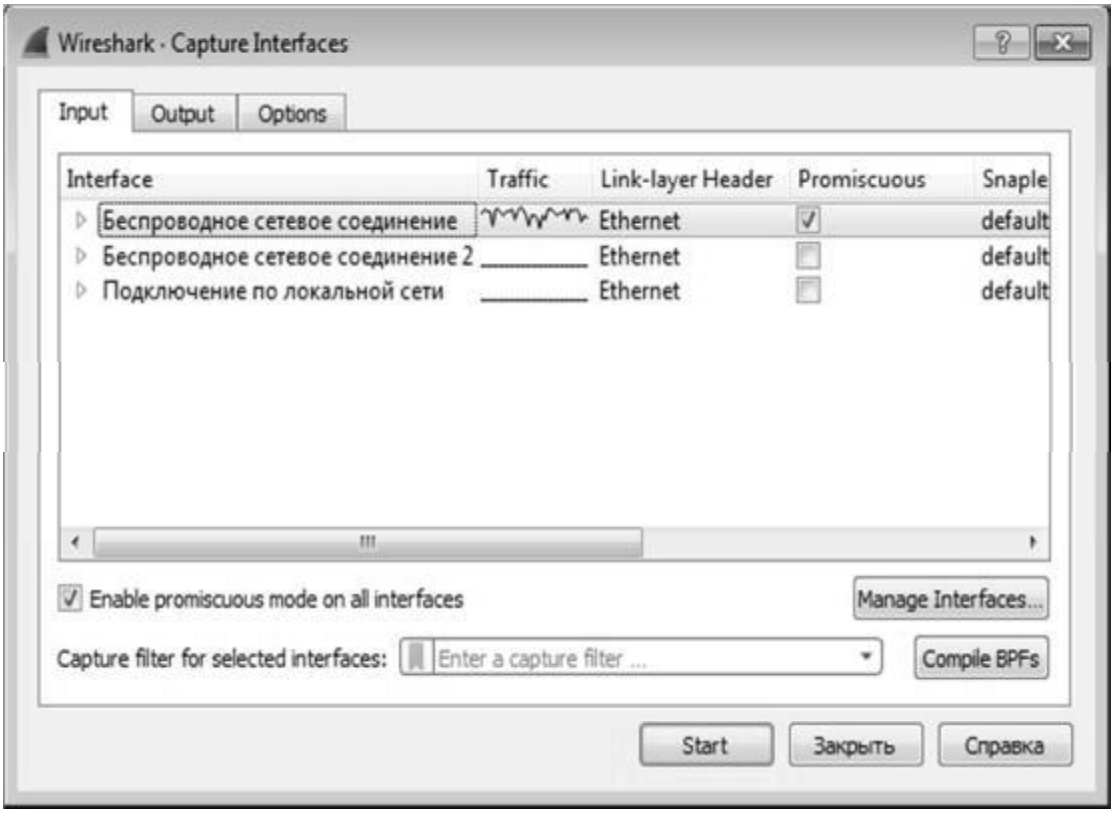

Рис. 2.1 − Вікно опцій захвату

– 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;

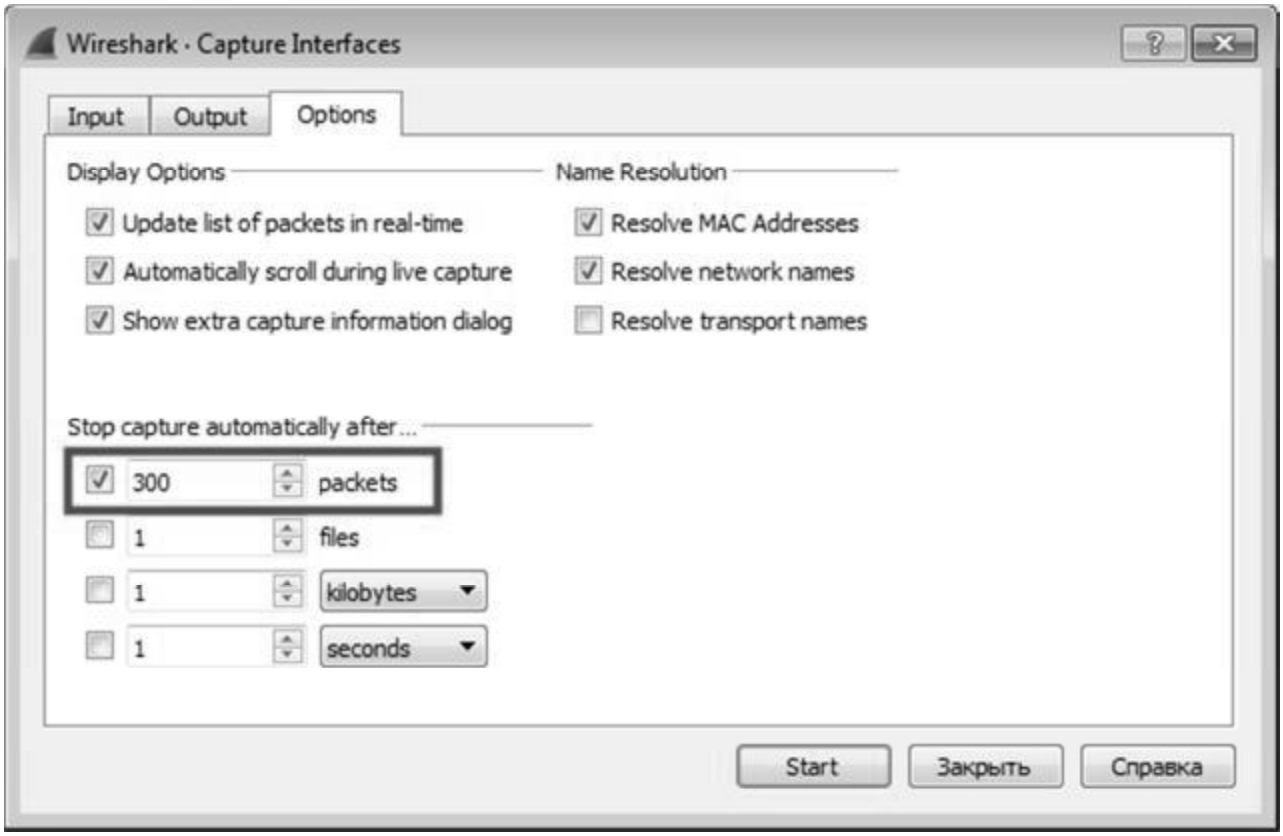

Рис. 2.2 – Вкладка Options вікна Capture Interfaces

– 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);

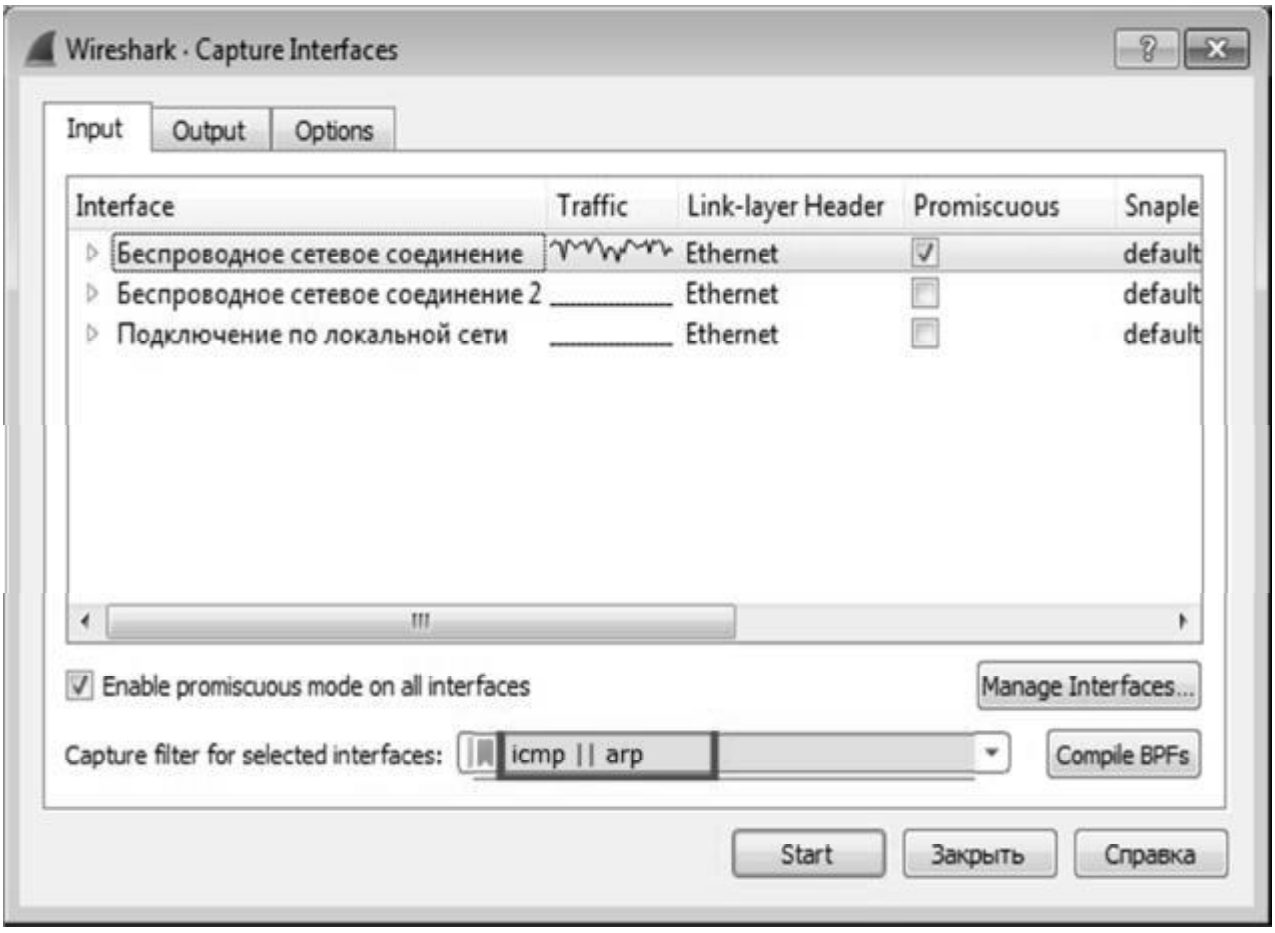

Рис. 2.3 − Вікно опцій на захват пакетів ARP та ICMP

– 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);

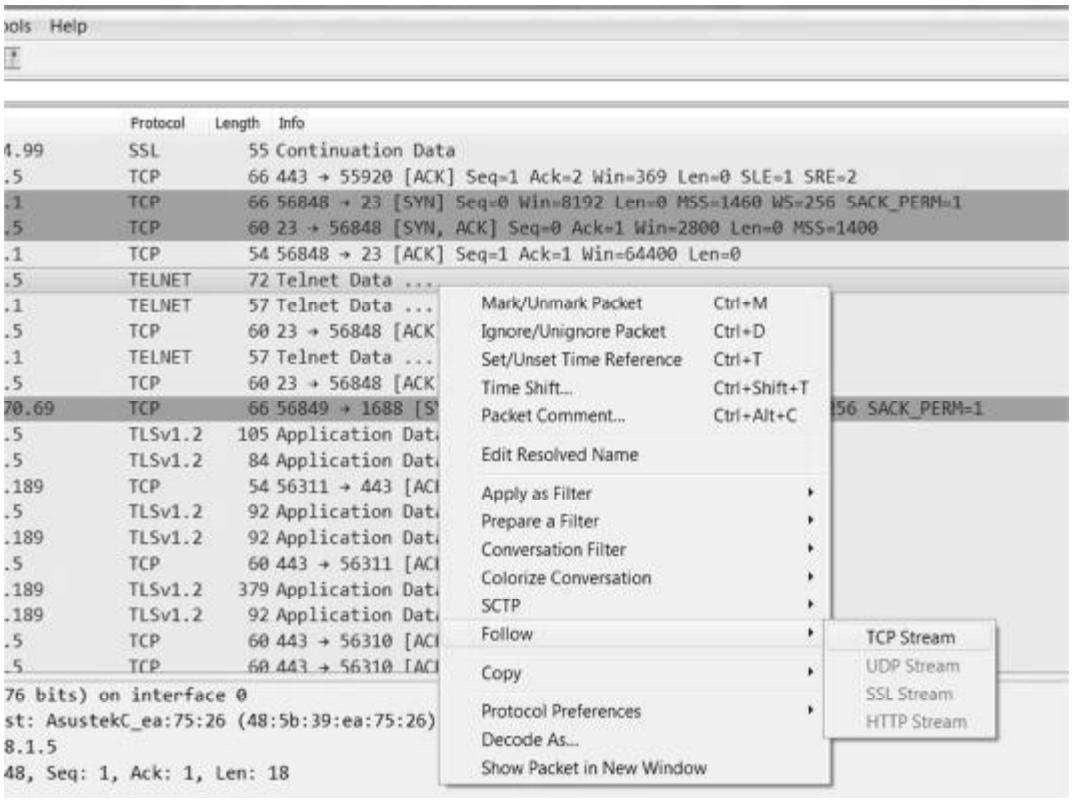

Рис. 2.4 – Відстеження всього потоку TCP для обраного пакету

– 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.
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.

Продовження табл. 2.1

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
ДОСЛІДЖЕННЯ КАДРУ ПРОТОКОЛУ ETHERNET ТА ПРОПУСКНОЇ ЗДАТНОСТІ FAST ETHERNET

3.1. Мета лабораторної роботи

Вивчення формату кадру Ethernet, призначень його полів та адресування в локальних мережах, дослідження залежності пропускної здатності мережі Fast Ethernet від розміру кадру.

3.2.Організація виконання лабораторної роботи

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

– протокол Ethernet і як він працює;

– адресація в Ethernet;

– структура заголовку кадру Ethernet.

– часові параметри Fast Ethernet;

– розрахунок пропускної здатності та часу передачі кадру в мережі Fast Ethernet (Додаток А).

Далі виконати такі дії:

– запустити командний рядок;

– визначити MAC-адрес мережної плати комп’ютера;

```
>ipconfig /all
```

– запустити програму Wireshark і отримати мережну статистику тривалістю в кілька хвилин. Для збільшення інтенсивності генерації кадрів відкрити будь-який сайт в браузері;

– виконати «ping» на сусідні вузли та шлюз і зупинити захват;

– отримати відомості про MAC-адреси в заголовках кадрів Ethernet, які були захоплені Wireshark, на відповідній вкладці вікна ***Endpoints*** (рис. 3.1) через меню ***Statistics->Endpoints***. Визначити, які типи MAC-адрес були захоплені Wireshark;

– відфільтрувати MAC-адреси широкомовної розсилки (рис. 3.2);

– у вікні захоплених пакетів вибрати будь-який широкомовний пакет і розглянути значення основних полів його заголовку Ethernet II (рис. 3.3). Визначити адреси, на які надходять дані кадри і пакети, для канального і мережного рівня.

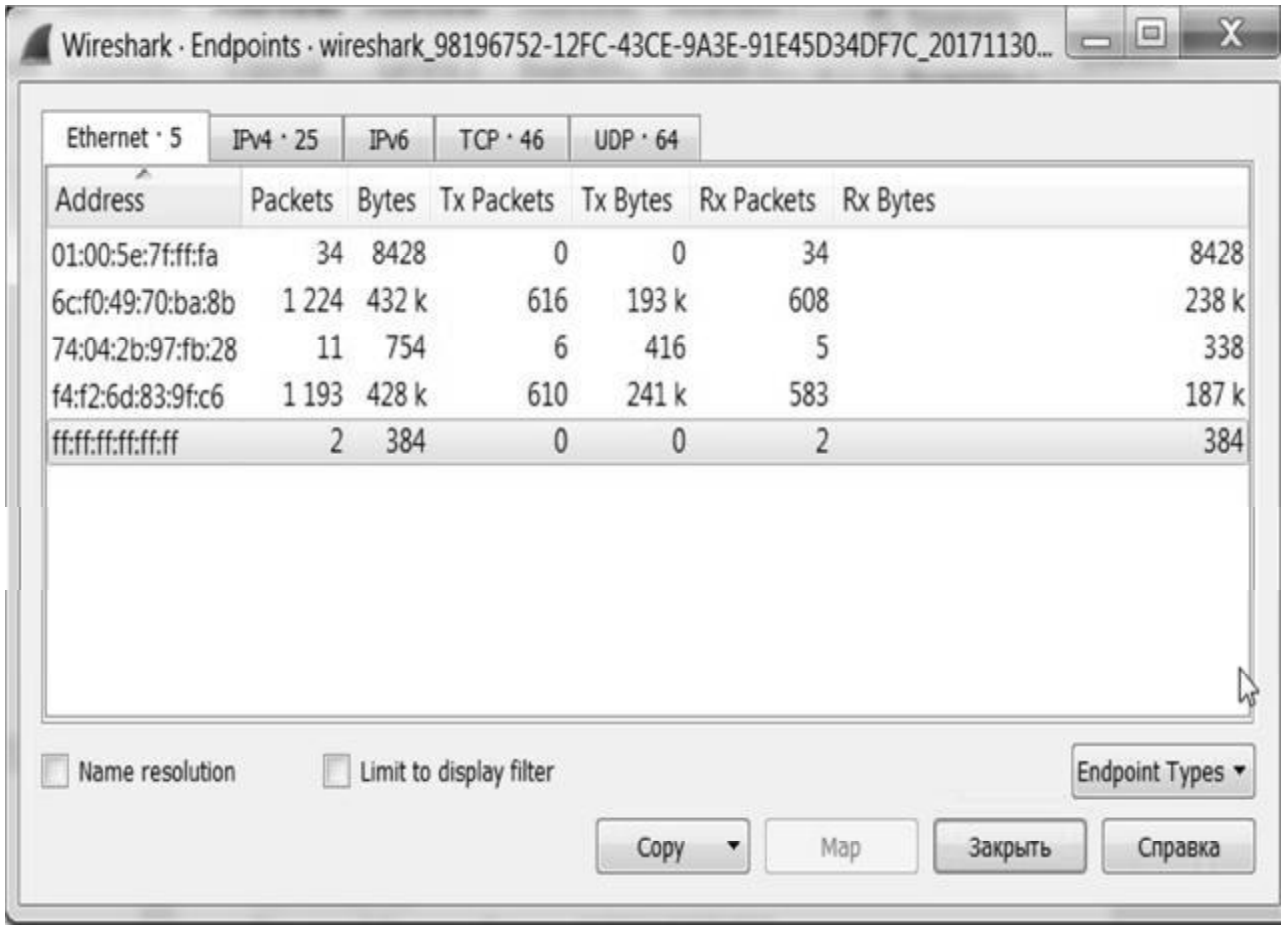

Рис. 3.1 – Вікно Endpoints

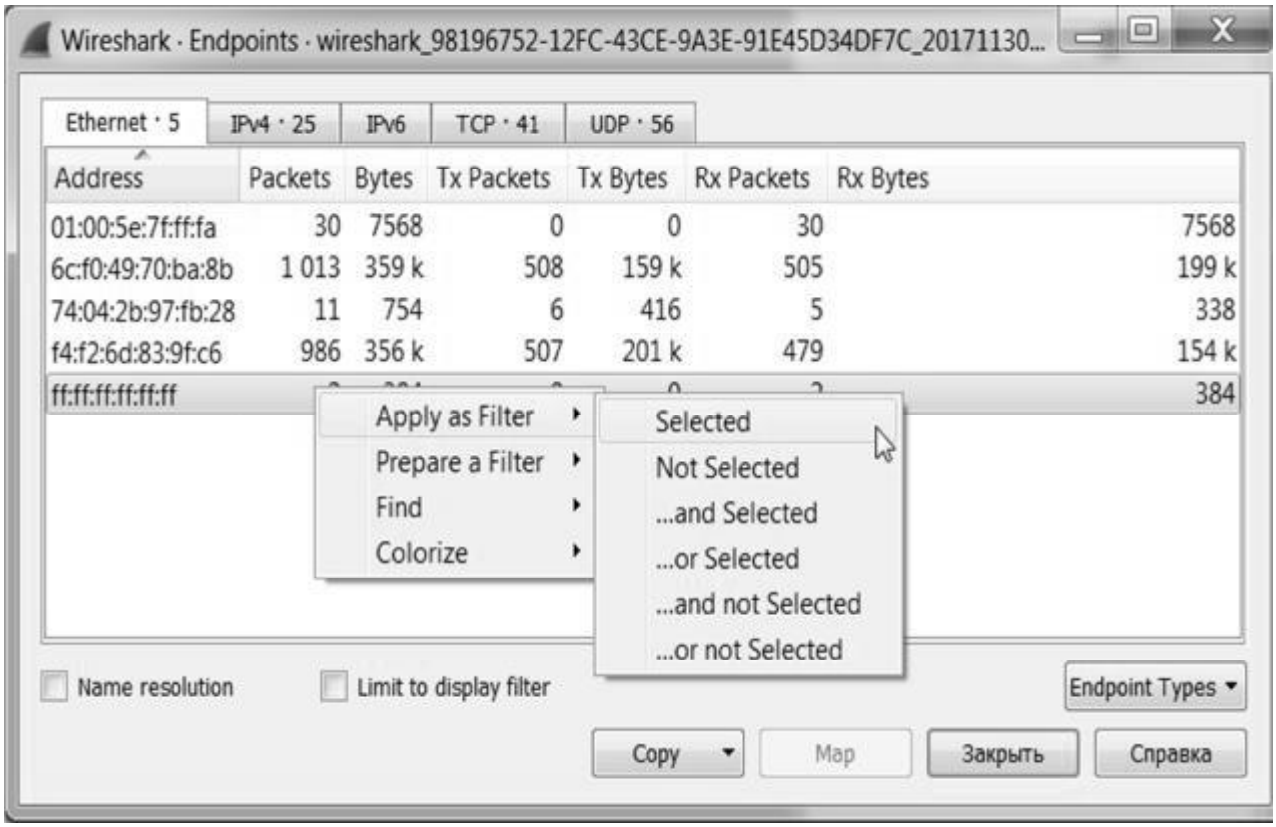

Рис. 3.2 – Фільтрація широкомовних кадрів

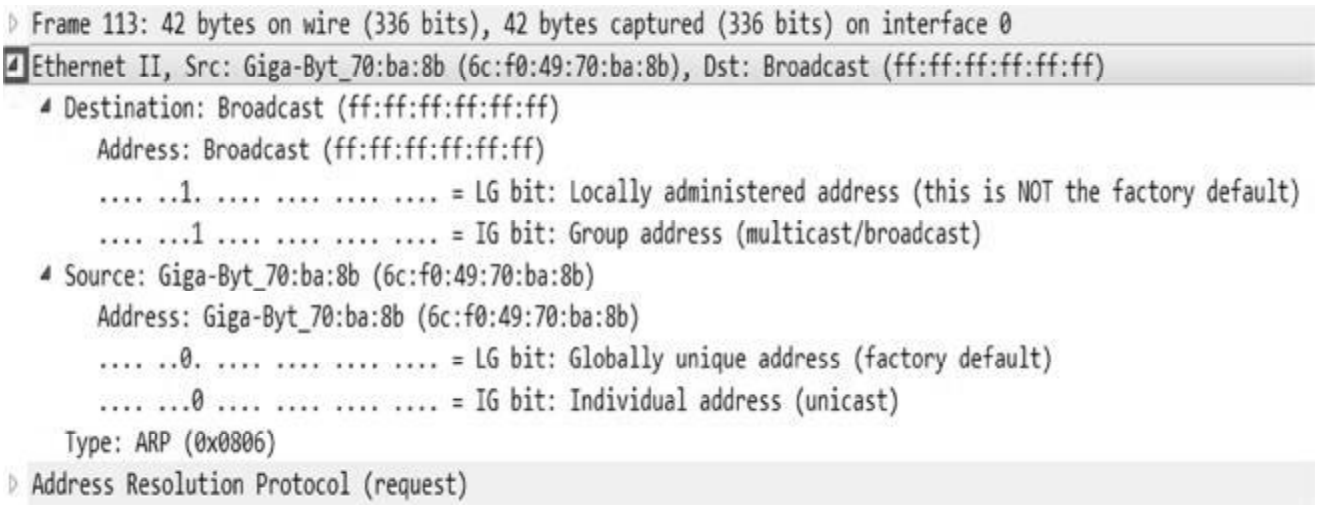

Рис. 3.3 − Ієрархічна структура заголовків

– відфільтрувати MAC-адреси багатоадресної розсилки, якщо вони були захоплені Wireshark. Вибрати будь-який пакет і розглянути значення основних полів його заголовку Ethernet II. Визначити адреси, на які надходять дані кадри і пакети, для канального і мережного рівня;

– побудувати графік затримки передачі файлу розміром *10*N* Мбайт в одному сегменті мережі Fast Ethernet, якщо довжина корисних даних кадру L = 128, 512, 1000, 1500, 4096 байт (N - номер за списком в групі);

– побудувати графік залежності пропускної здатності мережі Fast Ethernet від довжини корисних даних кадру L = 128, 512, 1000, 1500, 4096 байт.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис завдання з початковими умовами та даними;

– перелік MAC-адрес, які були захоплені Wireshark, з визначенням їх типу;

– структура заголовку Ethernet з описом його полів;

– графік затримки передачі файлу від довжини корисних даних;

– графік оцінки пропускної здатності мережі від довжини корисних даних.

3.3. Питання для підготовки до захисту лабораторної роботи

1. Чому дорівнюють максимальний та мінімальний розміри кадру Ethernet?

2. Яка частина в MAC-адресі відображає виробника мережної карти?

3. Які типи кадрів Ethernet бувають, в чому їх відмінності?

4. Який механізм управління доступом до середовища використовується в Ethernet?

5. Як записується широкомовний MAC-адрес Ethernet?

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
Не найдены записи в таблице ARP.
```

– 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 exo-запит за допомогою команди «ping» на кілька IP-адрес в Інтернет. Визначити, на який MAC-адрес призначення відправлялись exo-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.

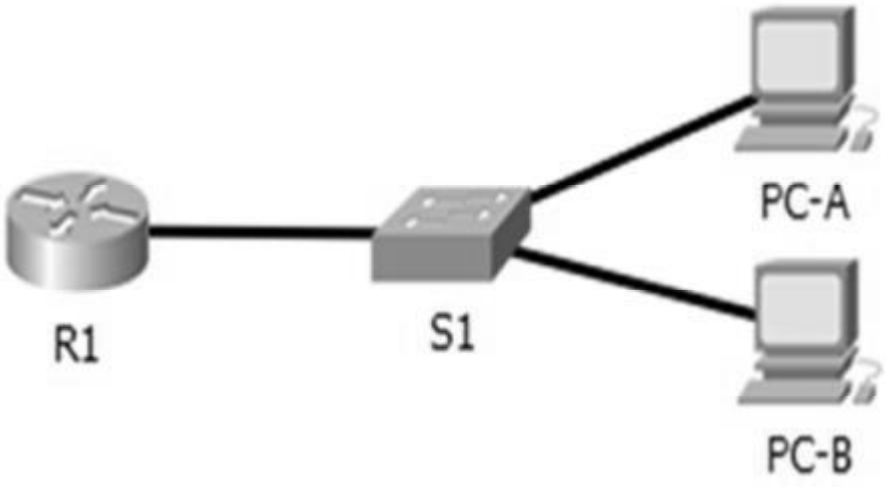

Рис. 4.1 − Топологія мережі

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

– 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
ФРАГМЕНТАЦІЯ IP

5.1. Мета лабораторної роботи

Дослідити процес фрагментації протоколу IP.

5.2. Організація лабораторної роботи

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

– функції протоколу IP;
– структура заголовка IP;
– максимально допустимий розмір пакета (MTU) каналу зв'язку;
– синтаксис команди «ping»;
– процес фрагментації IP-пакетів.

Далі виконати такі дії:

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

```
> ping /?
```

– визначити експериментальним способом MTU мережі, генеруючи ехо-запити на сусідній ПК із заборонним прапором фрагментації і розміром від 1500 байт, зменшуючи кожен раз розмір даних до успішної передачі ехо-пакету;

```
> ping –f –n 1 -l  1500 кінцевий_вузол
```

– запустити програму Wireshark і процес захоплення пакетів;

– згенерувати один ехо-пакет на сусідній вузол з дозволяючим прапором фрагментації і розміром поля даних, рівним MTU*3 + №*70, де № − номер за списком студента в групі;

– зупинити процес захоплення в Wireshark;

– знайти фрагментовані пакети ехо-запиту та заповнити табл. 5.1 значеннями полів фрагментів;

Таблиця 5.1

Значення полів фрагментів вихідного IP-пакету

№ фрагмента	ID	Total Length	DF	MF	Frafment Offset	Дані (байт)

– знайти фрагментовані пакети ехо-відповіді та заповнити табл. 5.1 значеннями полів фрагментів;

– визначити сумарний розмір всіх фрагментів та обґрунтувати різницю с завданим розміром вихідного пакету.

Підготувати звіт по лабораторній роботі, який повинен включати:

– тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– значення експериментально визначеного MTU каналу зв'язку;

– значення полів фрагментів ехо-запиту та ехо-відповіді у вигляді табл. 5.1;

– обґрунтування різниці між сумарним розміром всіх фрагментів та завданим розміром вихідного пакету.

5.3. Питання для підготовки до захисту лабораторної роботи

1. Які дві основні функції виконує протокол IP?

2. Який в IPv4 використовується механізм для запобігання нескінченної пересилки пакетів по мережі?

3. Які дії робитиме протокол IP, якщо один з фрагментів буде втрачено?

4. Пакет прибуває зі значенням біта M = 1, зміщення фрагментації має значення 0. Чи є цей пакет першим фрагментом, останнім фрагментом або середнім фрагментом?

5. Якщо отриманий розмір неподільного пакету в 1472 байт, чи означає це, що канал зв'язку використовує MTU = 1472?

6. ЛАБОРАТОРНА РОБОТА № 6
ОТРИМАННЯ ВІДОМОСТЕЙ ПРО MAC-АДРЕСИ І МЕРЕЖНІ НАЛАШТУВАННЯ TCP/IP

6.1. 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.

6.2. 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.

6.3. 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?

7. ЛАБОРАТОРНА РОБОТА № 7
ВИЗНАЧЕННЯ IPV4-АДРЕС

7.1. Мета лабораторної роботи

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

7.2. 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;
- структура IPv4-адреси;
- використання операції «І» для визначення мережної частини;
- одноадресна, широкомовна і багатоадресна розсилка IPv4;
- типи IPv4-адрес.

Далі виконати такі дії:

– використати операцію «І» для визначення мережної частини в IP-адресах, завданих в табл. 7.1;

Таблиця 7.1

Варіанти завдань

№ вар.	Завдання1		Завдання2	
	IP-адрес	Маска	IP-адрес	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
16.	152.205.232.105	255.255.192.0	144.112.213.91	/20
17.	107.214.175.68	255.255.224.0	210.254.11.42	/19
18.	57.198.77.193	255.255.240.0	11.104.213.125	/18
19.	122.227.157.232	255.255.128.0	201.24.249.88	/17
20.	228.219.147.134	255.255.252.0	17.124.16.162	/18
21.	151.22.163.204	255.248.0.0	55.174.76.242	/19
22.	37.128.54.52	255.255.192.0	72.96.79.110	/20
23.	59.145.202.91	255.255.224.0	92.9.234.56	/21
24.	162.202.242.90	255.255.240.0	144.186.231.149	/22
25.	159.25.94.89	255.255.252.0	178.15.86.139	/25

– заповнити табл. 7.2 відомостями для визначених мереж з табл. 7.1;

Таблиця 7.2

Відомості про мережі

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

– проаналізувати табл. 7.3 та визначити тип адреси: адрес вузла, адрес мережі, багатоадресна або широкомовна розсилка.

Таблиця 7.3

Адрес вузла, адрес мережі, багатоадресна або широкомовна розсилка

IP-адрес	Маска	Тип адреси
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. 7.4 і визначити тип адреси: загальний або приватний.

Таблиця 7.4

Загальний/приватний

IP-адрес/префікс	Загальний/приватний
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. 7.5 і визначити, чи є пара IP-адрес/префікс допустимою адресою вузла.

Таблиця 7.5

Допустима/недопустима адреса вузла

IP-адрес/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. 7.2−7.5.

7.3. Питання для підготовки до захисту лабораторної роботи

1. До якого класу належить IP-адрес комп'ютера учбового класу?
2. До якої IP-мережі належить IP-адрес комп'ютера учбового класу?
3. Чому при визначенні мережної адреси важлива маска мережі?
4. Яким пристроям зазвичай присвоюються статичні IP-адреси?
5. При налаштування 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?

8. ЛАБОРАТОРНА РОБОТА № 8
РОЗРАХУНОК ПІДМЕРЕЖ ЗА ДОПОМОГОЮ МАСКИ ПОСТІЙНОЇ ДОВЖИНИ

8.1. Мета лабораторної роботи

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

8.2. 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. 8.1.

Кількість вузлів у мережах LAN_N1-LAN_N6 та виділений мережний блок для їх адресації задані по табл. 8.1 згідно з варіантом.

Через маршрутизатор Central забезпечується доступ до Internet.

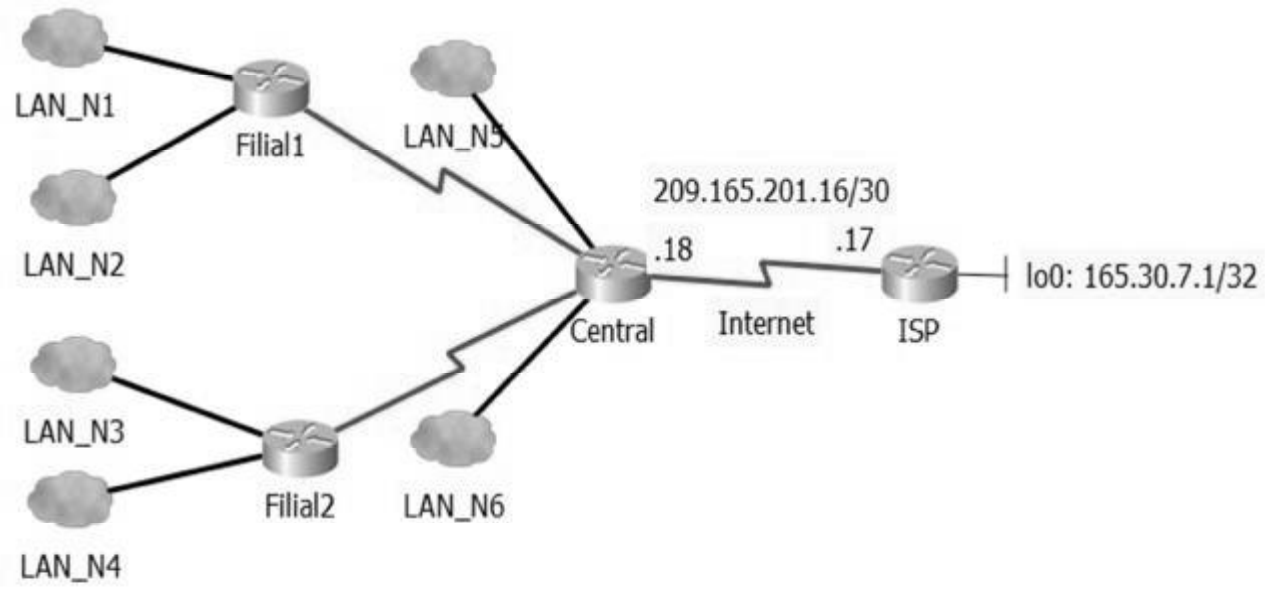

Рис. 8.1 – Топологія мережі

Таблиця 8.1

Варіанти завдань

№ вар.	Адрес 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. 8.2.

Таблиця 8.2

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. 8.3.

Таблиця 8.3

Відомості про підмережі

Назва підмережі	Необхідний розмір підмережі	Виділений розмір підмережі	Десятковий формат адреси підмережі	Перший використовуваний адрес вузла підмережі	Останній використовуваний адрес 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 в 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 таблиць 8.2 та 8.3;

– схему вирішення адресації заданої мережі у вигляді логічної топології згідно з рисунком 8.2.

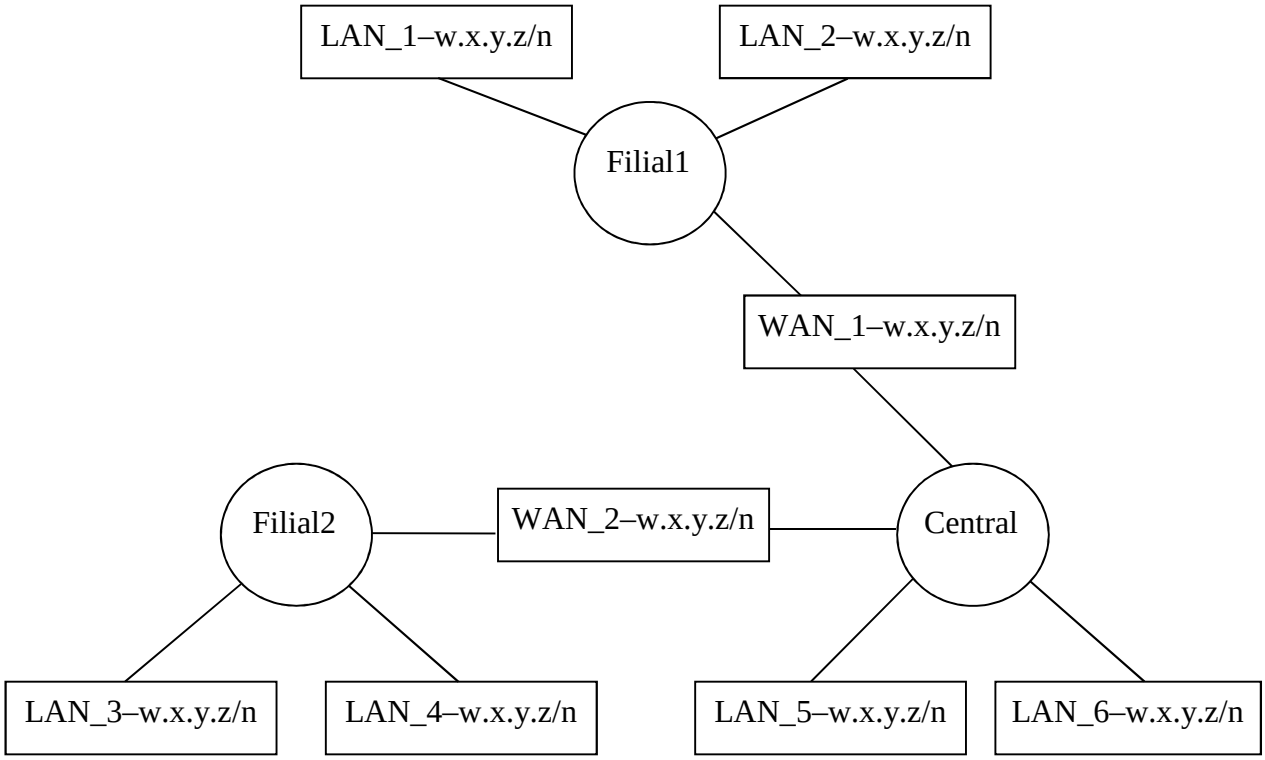

Рис. 8.2 – Логічна топологія методом маски постійної довжини

8.3. 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-адреси?

9. ЛАБОРАТОРНА РОБОТА № 9
РОЗРАХУНОК ПІДМЕРЕЖ ЗА ДОПОМОГОЮ МАСКИ ЗМІННОЇ ДОВЖИНИ

9.1. Мета лабораторної роботи

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

9.2. 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;

– IP-адресація в мережах;

– використання масок змінної довжини (Variable Length Subnet Mask, VLSM) в IP-адресації.

Далі розробити схему IP-адресації поділу мережі організації на підмережі за сценарієм, заданому в лабораторній роботі № 8, використовуючи маски змінної довжини (метод VLSM).

Для цього спочатку визначається найбільша підмережа та маска для неї. На звільнених бітах перша допустима комбінація присвоюється цій підмережі. У табл. 9.1 заносяться відповідні дані.

Тепер визначається наступна за розмірами підмережа та маска для неї та їй присвоюється наступна комбінація на звільнених бітах.

Так треба продовжувати поділ підмереж відповідного розміру на підмережі до тих пір, поки не буде досягнута потрібна кількість вузлів у кожній підмережі.

Відповідні результати необхідно надати у вигляді табл. 9.1.

Таблиця 9.1

Підмережі організації

Назва підмережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса

Призначити підмережу для кожного з каналів між маршрутизаторами. Починати треба з наступної доступної підмережі.

Заповнити табл. 9.2 відповідними адресами.

Таблиця 9.2

Підмережі каналів WAN між маршрутизаторами

Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
Канал WAN_N1 між маршрутизаторами Filial1 та Central				
Канал WAN_N2 між маршрутизаторами Filial2 та Central				

Порівняти з відповідями з лабораторної роботи № 8, дати пояснення в разі отримання різних результатів та відповісти на такі питання:

– кількість IP-адрес, доступних у вихідній мережі;

– кількість IP-адрес, доступних в розбитій мережі;

– який відсоток адресного простору використовується в вихідній мережі;

– який відсоток адресного простору використовується в розрахованій мережі.

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 з поясненнями;

– таблиця розподілу адрес підмереж LAN_N1 – LAN_N6 (таблиця 9.1);

– таблицю розподілу адрес підмереж WAN_N1 – WAN_N2 для каналів між маршрутизаторами (таблиця 9.2);

– логічна топологія мережі із застосуванням методу VLSM.

9.3. Питання для підготовки до захисту лабораторної роботи

1. Чи дозволяє метод VLSM збільшувати кількість адрес?
2. Які переваги дає метод VLSM?
3. Що таке розширений мережний префікс?
4. Яка маска відповідає діапазону IP-адрес від 128.7.64.1 до 128.7.79.254?
5. Яка частина IP-адреси 200.12.135.14 являє собою вузол за наявності маски підмережі за умовчанням?

10. ЛАБОРАТОРНА РОБОТА № 10
РОЗРАХУНОК СУМАРНОГО МАРШРУТУ

10.1. Мета лабораторної роботи

Навчитися розраховувати сумарний маршрут для кожного маршрутизатора, виконувати загальне підсумовування маршрутів, щоб маршрутизатор Central міг передавати більш лаконічну інформацію постачальнику послуг Інтернету.

10.2. Організація виконання лабораторної роботи

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

– супермережі та безкласова міждоменна маршрутизація (Classless Internet-Domain Routing, CIDR);

– об'єднання маршрутів;

– використання технології CIDR у маршрутизації;

– правило розрахунку сумарних маршрутів.

Далі розрахувати сумарні маршрути по можливості для кожного маршрутизатора в філіалах в розрахованій схемі IP-адресації з лабораторної роботи № 9, щоб вони могли передавати більш лаконічно відомості про свої підмережі.

Необхідно почати з маршрутизаторів в філіалах. Обчислити сумарний маршрут на Filial1 і дані занести у табл. 10.1. Далі заповнити табл. 10.2 для Filial2.

Потім розрахувати сумарний маршрут для Central (таблиця 10.3). Маршрутизатор Central виконає підсумовування своїх власних підмереж, а також сумарних маршрутів, отриманих від Filial1 та Filial2. Цим IP-адресом буде представлена мережа організації на маршрутизаторі постачальника послуг Інтернету ISP.

Таблиця 10.1

Таблиця підсумовування для Filial1

Назви підмереж	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
Сумарний маршрут			

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;

– опис завдання з початковими умовами і даними;

– розраховані сумарні маршрути для маршрутизаторів мережі організації, подані у вигляді таблиць 10.1−10.3;

– сумарний IP-адрес, яким буде представлена мережа організації на маршрутизаторі ISP.

Таблиця 10.2

Таблиця підсумовування для Filial2

Назви підмереж	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
Сумарний маршрут			

Таблиця 10.3

Таблиця підсумовування для Central

Назви підмереж	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
Сумарний маршрут від Filial1			
Сумарний маршрут від Filial2			
Сумарний маршрут			

10.3. Питання для підготовки до захисту лабораторної роботи

1. Як CIDR і VLSM сприяють економному використанню адресного простору?

2. Які завдання виконує маршрутизація CIDR?

3. Що є неодмінною умовою застосовування CIDR?

4. Чи можливо для мережі класу С використати префікс /20?

5. Що таке підсумовування маршрутів і як воно сприяє зменшенню таблиць маршрутів на маршрутизаторах?

11. ЛАБОРАТОРНА РОБОТА № 11
ПОБУДОВА МЕРЕЖІ В CISCO PACKET TRACER І БАЗОВЕ НАЛАШТУВАННЯ ПРИСТРОЇВ

11.1. Мета лабораторної роботи

Отримати навички в програмі Cisco Packet Tracer будувати розраховану в лабораторній роботі № 9 мережу, виконувати налаштування базових параметрів пристроїв і протокол SSH.

11.2. 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 № 8 (рис. 8.1). Кожну мережу (LAN_N1 − LAN_N6) подати двома ПК, за винятком LAN_N3. Мережу LAN_N3 зобразити згідно з рис. 11.1. 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.

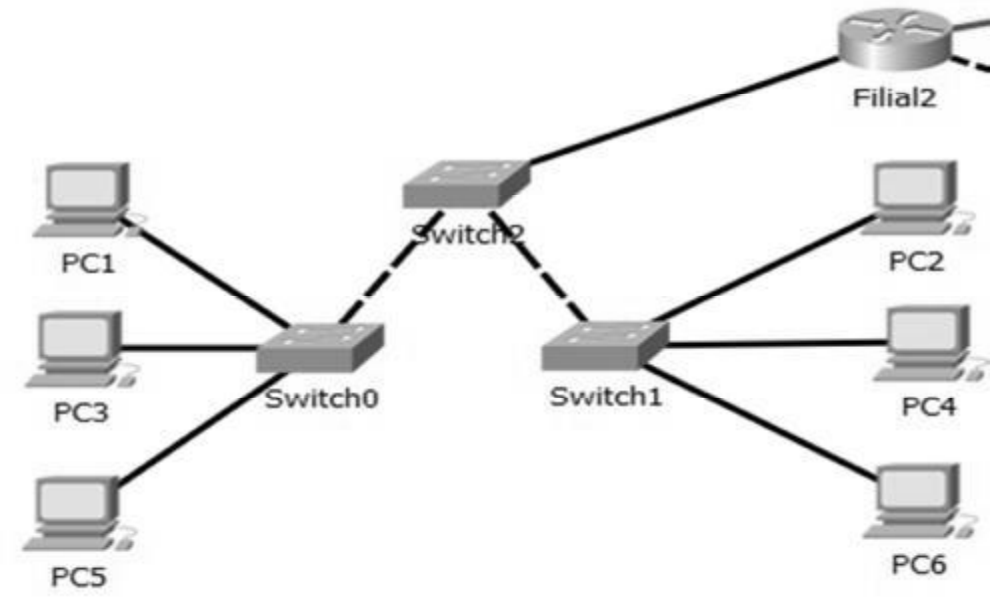

Рис. 11.1 − Топологія мережі LAN_N3

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. 11.2).

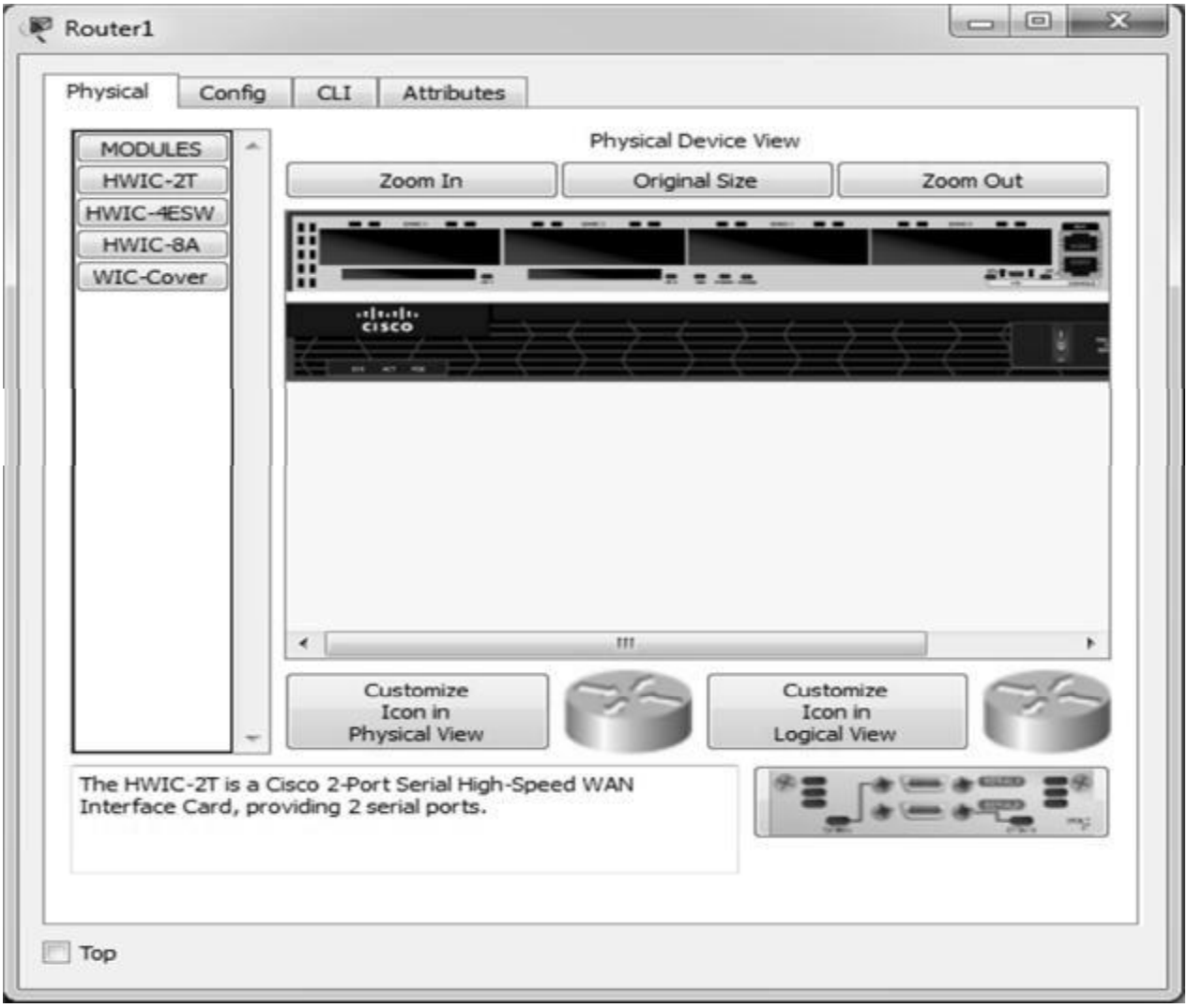

Рис. 11.2 − Вкладка *Physical* маршрутизатора

3. Для IP-адресації мережі використовувати розрахунки з лабораторній роботі № 9. Задокументувати схему IP-адресації і підключень пристроїв у вигляді табл. 11.1 з урахуванням таких вимог:

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

– другі з допустимих IP-адрес призначаються комутаторам;

– останні з використовуваних IP-адрес призначаються ПК.

Таблиця 11.1

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 замовчуванням. Заповнити табл. 11.2 відповідними даними для кожної робочої станції.

Таблиця 11.2

IP-адреси ПК

Назва мережі	IP-адрес ПК1	IP-адрес ПК2	Маска	Адреса шлюзу
LAN_N1				
LAN_N2				
LAN_N3				
LAN_N4				
LAN_N5				
LAN_N6				

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. 11.1. 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 по протоколу SSH

Використання Telnet небезпечно, оскільки текстові дані передаються в незашифрованому вигляді. Тому рекомендується по можливості використовувати протокол SSH. Відповідно до табл. 11.3 на комутаторі в заданій мережі перелаштуйте лінії VTY на доступ лише по протоколу SSH.

Таблиця 11.3

Комутатор для налаштування по SSH

Варіант	Комутатор в 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
7, 15, 23	LAN_N5
8, 16, 24, 25	LAN_N6

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 в локальних базах даних імен користувачів, а також для дозволу віддаленого доступу лише по протоколу 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. 11.1 і 11.2);

– застосовані команди з налаштувань та їх опис;

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

11.3. 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?

12. ЛАБОРАТОРНА РОБОТА № 12
ВИВЧЕННЯ ПРОГРАМ І СЛУЖБ TCP/IP

12.1. Мета лабораторної роботи

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

12.2. 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);

– запустити службу RasMan (Диспетчер підключень віддаленого доступу);

– додати нового користувача з ім'ям *testuser*;

– додати створеного користувача в групу *Адміністратори* та перевірити результат;

– встановити годинник комп'ютера за значенням годин сусіднього ПК;

– відобразити довідку по використанню команди «net share» та виконати наступні дії:

1) відобразити доступні для спільного використання мережні ресурси;

2) зробіть локальний диск загальним мережним ресурсом, використовуючи в якості імені своє прізвище латиницею, а в якості коментаря рядок «Мережний диск *Прізвище*», щоб тільки п’ять користувачів одночасно могли отримати доступ до нього;

3) вивести відомості створеного ресурсу;

– вивести список загальних мережних ресурсів сусіднього ПК;

– підключити створений сусідом ресурс в якості мережного диска «Z:» та перегляньте його вміст;

– дочекайтесь, поки сусід виконає аналогічні попередні дії, та проконтролюйте наявні поточні зв'язки робочих станцій командою «net session»;

– вивести список підключень вашого ПК командою «net stat» та знайти підключення сусіднього ПК до вашого вузла;

– відключити створений мережний диск;

– 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 ехо-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 ехо-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;

12.3. 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?

13. ЛАБОРАТОРНА РОБОТА № 13
ВПРОВАДЖЕННЯ І НАЛАШТУВАННЯ СЕРВІСІВ ВЕБ-СЕРВЕРУ, СЕРВЕРУ ЕЛЕКТРОННОЇ ПОШТИ, DHCP, DNS ТА FTP В CISCO PACKET TRACER

13.1. 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.

13.2. 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 № 11.

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) і 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.

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

3. Вибрати варіант On, щоб включити сервіс DNS.

4. Додати запис для MultiServer у відповідних полях:

   а) Name: aks.com;

   б) Address: IP-адреса MultiServer.

5. 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 aks.com», щоб перевірити роботу ServerDNS. Повинні отримати IP-адрес для імені aks.com.

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

6. В полі URL ввести aks.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. 13.1). Натиснути Add для додавання облікового запису.

Таблиця 13.1

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 в текстовому редакторі та при його закритті зберегти під назвою README.txt.

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

а) Введіть «ftp *IP-адреса MultiServer*». Зачекайте кілька секунд, поки клієнт підключиться.

б) Сервер виведе запит для введення імені користувача і пароля. Використати облікові дані для облікового запису administrator.

в) Рядок зміниться на ftp>. Ввести команду «dir» для перегляду вмісту каталогу. З'явиться каталог файлів на MultiServer.

г) Для перенесення файлу README.txt в рядку ftp> ввести «put README.txt». Файл README.txt буде переданий з вузла на MultiServer.

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

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

13.3. Питання для підготовки до захисту лабораторної роботи

1. Який протокол перетворює ім‘я aks.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?

14. ЛАБОРАТОРНА РОБОТА № 14
ВИВЧЕННЯ ТРАНСПОРТНОГО ПРОТОКОЛУ TCP ТА ПРОТОКОЛУ ПЕРЕДАЧІ ФАЙЛІВ FTP

14.1. Мета лабораторної роботи

Вивчити призначення та особливості функціонування протоколу транспортного рівня TCP та протоколу передачі файлів FTP.

14.2. Організація виконання лабораторної роботи

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

– функції протоколу TCP;
– функції і команди протоколу FTP;
– структура заголовку TCP;
– процеси встановлення, передачі і закриття з'єднань TCP.

Далі виконати такі дії:

– отримати від викладача файл, який містить дамп Wireshark декількох одночасних сесій TCP до одного і того ж ftp-сервера з одного клієнта;

– проаналізувати зібрані пакети та визначити:

1) адресу ftp-сервера _____;
2) адресу ftp-клієнта _____;

– подати у вигляді табл. 14.1 параметри сокетів всіх з'єднань. Для цього в Wireshark вибрати на панелі меню команду *Statistics-> Endpoints*. У діалоговому вікні вибрати вкладку TCP. Звернути увагу на призначення номерів портів на ftp-клієнті.

Таблиця 14.1

Параметри tcp-з’єднань

IP-адрес	Порт	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes

– за допомогою написання фільтрів в Wireshark з’ясувати, скільки зв'язків встановив клієнт з ftp-сервером та заповнити даними табл. 14.2;

Таблиця 14.2

Параметри з’єднань ftp-клієнта

IP-адрес	Порт	Логін	Пароль	Number	Time

– обрати одне з'єднання і представити всі його процеси (встановлення, передача даних, завершення) у вигляді діаграми станів. Для цього в Wireshark вибрати на панелі меню команду *Statistics-> Flow Graph*. У діалоговому вікні виконати налаштування відображення;

– для обраного в попередньому пункті з'єднання, які номери портів на клієнті використовувалися для обміну даними з ftp-сервером? Зобразити процес передачі даних у вигляді діаграми станів;

– з'ясувати, які файли були завантажені з ftp-сервера в даному дампі. Для цього використовуйте фільтр відображення команди "RETR" протоколу FTP;

– який файл і яким обсягом був переданий на сокеті 10.0.2.6:1228? На пакеті, в якому велася передача даних (FTP Data), натиснути правою кнопкою і вибрати *Follow ->TCP Stream* (або на панелі меню *Analyze-> Follow ->TCP Stream*). Потім у вікні вибрати Save as... (рис. 14.1), не забувши вказати розширення файлу. Якщо точно не відомо розширення файлу, то заголовок файлу може допомогти його «впізнати». В нашому випадку JFIF вказує, що це jpg файл.

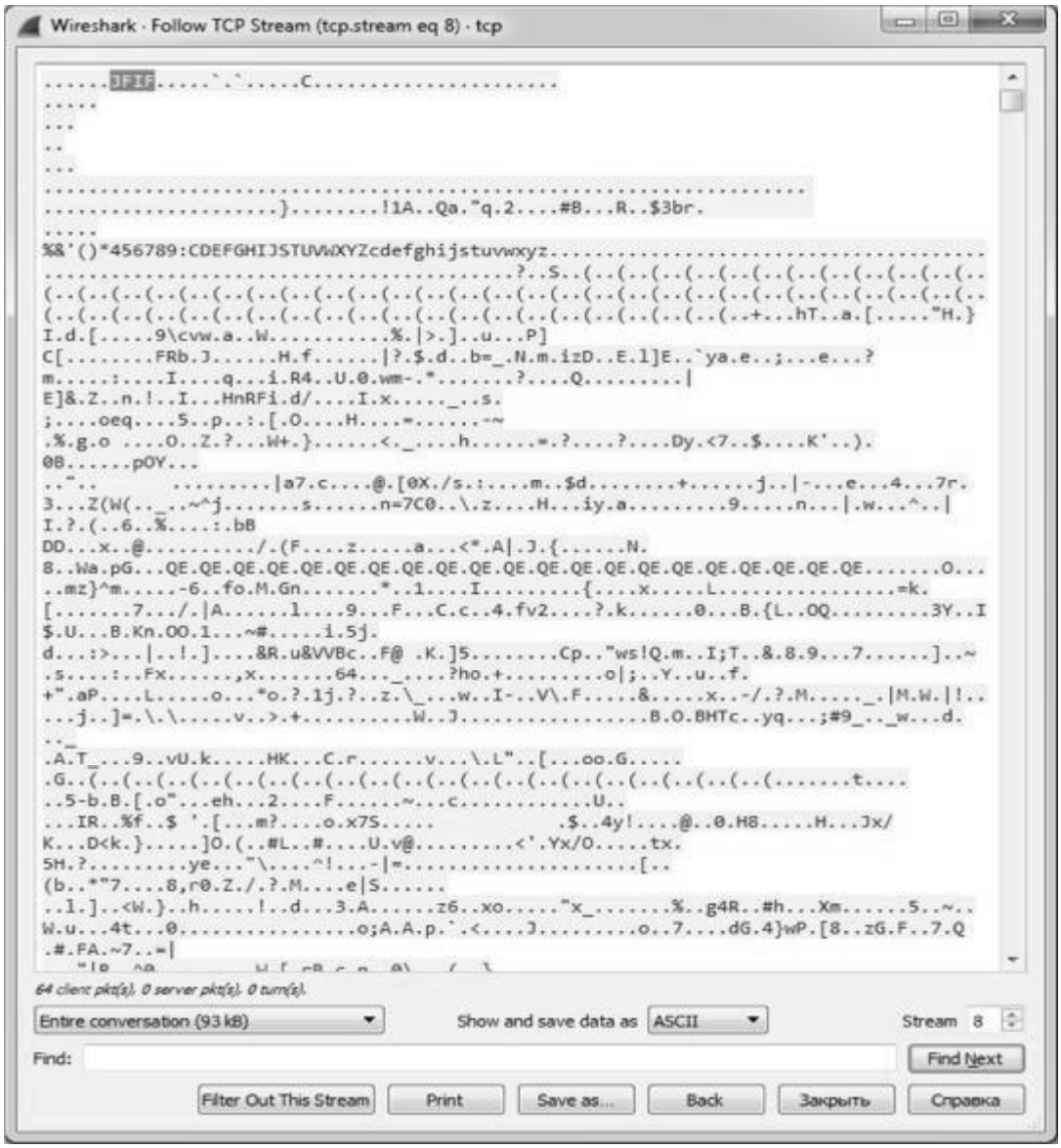

Рис. 14.1 – Вікно Follow TCP Stream

– встановити параметр Show and save data as на параметр Raw та зберегти файл з розширенням .jpg;

– переглянути збережений файл.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;

– відповіді на зазначені питання;

– діаграму станів для одного керуючого з'єднання ftp;

– діаграму станів передачі файлу;

– файл, який був переданий на сокеті 10.0.2.6:1228.

Пакети, що містять істотну інформацію для даної лабораторної роботи, повинні бути ретельно прокоментовані.

14.3. Питання для підготовки до захисту лабораторної роботи

1. Скільки TCP-сегментів повинно бути передано між двома комп'ютерами, щоб вони могли встановити TCP-з'єднання?

2. Який фактор визначає розмір вікна TCP?

3. Які два поля TCP -заголовку використовуються для підтвердження отримання даних?

4. Яка функція TCP гарантує встановлення сеансу?

5. Який порт використовується для передачі даних FTP?

ПЕРЕЛІК ПОСИЛАНЬ

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND 100-101, акад. изд.: Пер. с англ. - М.: ООО “И.Д. Вильямс”, 2015. − 912 с.

2. Леммл Т. CCNA: Cisco Certified Network Associate / Т. Лэммл. − М.: Лори, 2001. − XXVI, 613 с.

3. Леммл Т. Настройка маршрутизаторов Cisco / Т. Леммл. − М.: ЛОРИ, 2001. − XVI, 304 с.

4. Воробієнко П. Телекомунікаційні та інформаційні мережі / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. − К.: Саміт-книга, 2010. − 635 с.

5. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров / Х. Остерлох. − СПб.: ООО "ДиаСофтЮП", 2002. − 567 с.

6. Ретана А. Принципы проектирования корпоративных IP-сетей / А. Ретана, Д. Слайс, Р. Уайт. − М.: Изд. дом "Вильямс", 2002. − 367 с.

7. Амато Вито. Основы организации сетей Cisco / Вито Амато; пер. с англ. – испр. изд. – М.: Издательский дом «Вильямс», 2004. – Т. 1-2. – 512 с.

8. Ирвин Дж. Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль; пер. с англ. – СПб.: БХВ-Петербург, 2003. – 448 с.

9. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с: ил.

10. Сунчелей И.Р. Структурированные кабельные системы / И.Р. Сунчелей, С.К. Стрижаков, А.Б. Семенов. – 5-е изд. – М.: Изд-во Компания АйТи, ДМК, 2004. – 640 с.

11. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб.: Питер, 2003. – 992 с.

12. Cisco Networking Academy [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [Варшава : Akamai Technologies Inc., 1999-2018]. – Режим доступу: https://www.netacad.com (дата звернення 30.03.2018). – Назва з екрана.

13. Цвіркун, Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с.

14. Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с.

15. Комп’ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп’ютерна інженерія / Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.

Додаток А

Розрахунок пропускної здатності мережі Fast Ethernet для максимального і мінімального розмірів кадрів

Розмір кадру в байтах визначають за формулою:

$$N_k = N_s + N_d,$$

де N_s – службова інформація кадру Fast Ethernet разом з преамбулою, байт; N_s = 26 байт;

N_d – розмір поля даних кадру; N_{dmin}=46 байт; N_{dmax}=1500 байт;

Розмір мінімального і максимального кадру в байтах:

$$N_{kmin}=46+26=72 \text{ (байт)},$$

$$N_{kmax}=1500+26=1526 \text{ (байт)}.$$

Оскільки один байт дорівнює восьми бітам, мінімальний і максимальний розмір кадру в бітах:

$$N_{kmin}=72*8=576 \text{ (біт)},$$

$$N_{kmax}=1526*8=12208 \text{ (біт)}.$$

Пропускну здатність Fast Ethernet визначають за формулою:

$$N_{ps} = N_1 * N_2 * K \text{ (біт)},$$

де N_1 – кількість біт в одному кілобіті; N_1 = 1024;

N_2 – кількість кілобіт в одному мегабіті; N_2= 1024;

K – коефіцієнт швидкості передачі даних; K = 100.

$$N_{ps} = 1024 * 1024 * 100 = 104857600 \text{ (біт)}.$$

Якщо врахувати міжкадровий інтервал, то отримаємо довжину проходження кадрів:

$$L_k = N_{mi} + N_k,$$

де N_{mi} – міжкадровий інтервал; N_{mi} = 96 біт;

N_k – розмір кадру разом з службовою інформацією.

Тоді період проходження кадрів мінімальної і максимальної довжини:

$$L_{kmin} = 576 + 96 = 672 \text{ (біт)},$$

$$L_{kmax} = 12208 + 96 = 12304 \text{ (біт)}.$$

Тоді час проходження кадрів можна визначити за формулою:

$$T = \frac{L_k}{N_{ps}} * K_{mks},$$

де L_k – довжина проходження кадрів, біт;

N_{ps} – пропускна здатність Fast Ethernet, біт;

K_{mks} – кількість мікросекунд в одній секунді; $K_{mks} = 10^6$.

Час проходження мінімального і максимального кадрів:

$$T_{min} = \frac{672}{104857600} * 10^6 = 6{,}4 \text{(мкс)},$$

$$T_{max} = \frac{12304}{104857600} * 10^6 = 117{,}6 \text{(мкс)}.$$

Частоту передавання кадрів, тобто кількість кадрів, що проходять по мережі за 1 секунду можна визначити за формулою:

$$F = \frac{N_{ps}}{L_k}, \text{ (кадр/с)}.$$

Отримуємо частоту слідування кадрів при мінімальному і максимальному розмірі кадру:

$$F_{min} = \frac{104857600}{672} = 156038 \text{ (кадр/с)},$$

$$F_{max} = \frac{104857600}{12304} = 8522 \text{ (кадр/с)}.$$

Знаючи частоту проходження кадрів F і розмір поля даних кадру N_d в байтах, можна розрахувати корисну пропускну здатність мережі:

$$P = F * N_d * 8, \text{ (біт/с)},$$

$$P_{min} = F_{min} * L_{kmin} * 8 = 156038 * 46 * 8 = 57421984, \text{ (біт/с)},$$

$$P_{max} = F_{max} * L_{kmax} * 8 = 8522 * 1500 * 8 = 102264000, \text{ (біт/с)}.$$

Або в Мбіт/с:

$$P = \frac{P}{N_1 * N_2} \text{ (Мбіт/с)},$$

де N_1 - кількість біт в одному кілобіті; N_1 = 1024;

N_2 - кількість кілобіт в одному мегабіті; N_2= 1024;

$$P_{min} = \frac{57421984}{1024*1024} = 54.76 \text{ (Мбіт/с)},$$

$$P_{max} = \frac{102264000}{1024*1024} = 97.52 \text{ (Мбіт/с)}.$$

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

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації
до виконання лабораторних робіт
студентами галузі знань 12 Інформаційні технології
спеціальності 123 Комп'ютерна інженерія
Частина 1

Видано в редакції авторів

Підписано до друку 03.05.2018. Формат 30х42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 3,8.
Обл.-вид. арк. 3,8. Тираж 25 пр. Зам. №

Підготовлено до друку та видрукувано
у Національному технічному університеті "Дніпровська політехніка".
Свідоцтво про внесення до Державного реєстру ДК № 1842 від 11.06.2004.
49005, м. Дніпро, просп. Д. Яворницького, 19.