

Міністерство освіти і науки України  
Центральноукраїнський національний технічний університет  
Механіко-технологічний факультет  
Кафедра кібербезпеки та програмного забезпечення

**Проектування комп'ютерних систем та мереж**

*Методичні рекомендації до виконання контрольних робіт для студентів  
заочної форми навчання галузі F Інформаційні технології*

**ЗАТВЕРДЖЕНО**

на засіданні кафедри кібербезпеки та  
програмного забезпечення, протокол № 1  
від 25 серпня 2025 року

Кропивницький

2025

Проектування комп'ютерних систем та мереж: Методичні рекомендації до виконання контрольних робіт для студентів заочної форми навчання галузі F Інформаційні технології. – Кропивницький: ЦНТУ – 2025. – 60 с./М-во освіти і науки України, Центральноукр. нац. техн. ун-т; /уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Коноплицька-Слободенюк О.К., Смірнов С.А. / – Кропивницький: ЦНТУ – 2025. – 60 с.

Укладачі: Смірнов О.А., Буравченко К.О., Смірнова Т.В., Коноплицька-Слободенюк О.К., Смірнов С.А.

Рецензенти: Коваленко О.В., докт. техн. наук, професор;  
Улічев О.С., канд. техн. наук.

© Центральноукраїнський  
національний технічний  
університет, 2025

## ЗМІСТ

<b>ВСТУП</b> .....	4
<b>Контрольна робота № 1.</b> Проектування мережевої інфраструктури корпоративного сегмента .....	8
<b>Контрольна робота № 2.</b> Проектування та обґрунтування схеми IP-адресації корпоративної мережі з оцінюванням альтернатив і ризиків .....	15
<b>Контрольна робота № 3.</b> Ієрархічне проектування CIDR IP адресації для корпоративної мережі .....	21
<b>Контрольна робота № 4.</b> Маршрутизація й аналіз пропускної здатності мережі .....	25
<b>Контрольна робота № 5.</b> Планування списків доступу і фільтрів портів .....	35
<b>Контрольна робота № 6.</b> Збирання мережевих даних, фільтрація та атрибуція віддалених ресурсів .....	37
<b>Контрольна робота № 7.</b> Профілювання, оптимізація продуктивності та енергоефективності маршрутизатора на базі OpenWrt у високонавантажених L3 сценаріях .....	45
<b>Контрольна робота № 8.</b> Масштабоване сегментування та розмежування трафіку в OpenWrt з залученням VLAN, DHCP, політики Firewall та міжсегментної маршрутизації .....	50
<b>Список використаної літератури</b> .....	56

## ВСТУП

**Метою викладання дисципліни «Проектування комп'ютерних систем та мереж» є формування у здобувачів вищої освіти ґрунтовних теоретичних знань, практичних умінь та навичок, необхідних для застосування в професійній діяльності у сфері проектування комп'ютерних систем та мереж.**

**У результаті вивчення навчальної дисципліни студент повинен:**

– **знати:** Системно-архітектурний підхід до побудови комп'ютерних мереж; Технології фізичного рівня, технічні характеристики і обмеження; Мережеву адресацію. Типи адрес стеку TCP/IP та моделювання адресного простору; Адресацію в корпоративній мережі. Плоскі й ієрархічні мережі, принципи обґрунтування архітектурного вибору; Статичні та динамічні IP-адреси, проектування та обмеження; Мережеві адреси NAT та PAT з оцінкою ризиків, вплив на експлуатацію; Фільтрацію трафіку з використанням списків контролю доступу. Розміщення стандартних і розширених ACL-списків з верифікацією правил і політик безпеки; Інженерні підходи до комутації та сегментації корпоративних мереж; VLAN і протокол VTP у контексті масштабування та керованості корпоративних мереж; Технології розумних, мобільних, зелених і безпечних обчислень з застосуванням комп'ютерних систем та мереж; Бездротові технології й пристрої, технічні характеристики та умови експлуатації; Забезпечення безпеки бездротових мереж; Усунення проблем з мережами на основі моделювання і верифікації гіпотез; Планування відновлення мережі з урахуванням інженерних, економічних і правових аспектів та управління ризиками.

– **вміти** проектувати мережеву інфраструктуру корпоративного сегмента; проектувати та обґрунтувати схеми IP-адресації корпоративної мережі з оцінюванням альтернатив і ризиків; ієрархічно проектувати CIDR IP адресацію для корпоративної мережі; реалізовувати маршрутизацію й аналіз пропускну здатності мережі; планувати списки доступу і фільтри портів; збирати мережеві дані, фільтрувати та проводити атрибуцію віддалених ресурсів; профілювати та оптимізувати продуктивність та енергоефективність маршрутизатора на базі

OpenWrt у високонавантажених L3 сценаріях; масштабоване сегментувати та розмежувати трафік в OpenWrt з залученням VLAN, DHCP, політики Firewall та міжсегментної маршрутизації.

### **Контроль знань**

Критерії оцінки іспиту:

**оцінку «відмінно» (90-100 балів, А)** – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

– засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

– засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;

– вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;

– самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

**оцінку «добре» (82-89 балів, В)** – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

– має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

– під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

**оцінку «добре» (74-81 бал, C)** заслуговує студент, який:

– в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

– опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

**оцінку «задовільно» (64-73 бали, D)** – заслуговує студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;

– ознайомлений з основною літературою, яка рекомендована програмою;

– допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

**оцінку «задовільно» (60-63 бали, E)** – заслуговує студент, який:

– володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

**оцінка «незадовільно» (35-59 балів, FX)** – виставляється студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

**оцінку «незадовільно» (35 балів, F)** – виставляється студенту, який:

– володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

– допускає грубі помилки при виконанні завдань, передбачених програмою;

– не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

**При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру**

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

**Шкала оцінювання: національна та ЄКТС**

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

## Контрольна робота №1

**Тема:** Проектування мережевої інфраструктури корпоративного сегмента

**Мета:** отримати навички проектування плану приміщень і плану комп'ютерної мережі з використанням інструментального засобу Microsoft Office Visio.

### Теоретичні відомості

*Пасивне мережеве обладнання.* При проектуванні комп'ютерних мереж в офісних приміщеннях використовують кабельні лотки та пластикові коробки. *Кабельний лоток* – це відкрита конструкція, призначена для монтажу дротів і кабелів. *Короб кабельний* – конструкція із пластмаси для монтажу кабельних мереж усередині приміщення. Пластикові коробки поділяються на кілька основних видів:

- *кабельний канал (кабель-канал)* – має просту конструкцію, він досить дешевий, деякі моделі дозволяють встановлювати розетки всередину кабель-каналу;

- *парапетні коробки* – встановлюються на рівні робочого місця, внутрішній простір такого короба розділений на секції, він має подвійну стінку, і практично всі види парапетного короба підтримують монтаж розеток;

- *короб на підлогу* – короб для монтажу на підлогу, має посилену конструкцію та стійку до стирання поверхню.

*Вимоги до серверної кімнати.* *Серверна кімната* – приміщення для великого телекомунікаційного або серверного обладнання. Розміри серверної повинні відповідати вимогам до розташовуваного в ній обладнання. Якщо такі дані на момент вибору приміщення відсутні, розрахунки ведуться виходячи із площі робочих місць, що обслуговуються: на кожні її 10 м<sup>2</sup> приймаються 0,07 м<sup>2</sup> для серверної. Мінімальна площа апаратної приймається 14 м<sup>2</sup>.

Серверна кімната повинна розташовуватися в приміщенні, яке не має зовнішніх стін будинку. Для забезпечення катастрофостійкості приміщень критичного електронного, електричного або механічного обладнання та комп'ютерів дані приміщення не допускається розміщати у підвальних

поверхах або нижче очікуваного рівня повідкових вод, і на верхніх поверхах будинку, оскільки вони сильніше інших страждають у випадку пожежі.

Конструкція стін приміщення повинна бути герметичною, при цьому стіни та двері повинні мати вогнестійкість не менш 45 хвилин, а міжповерхові перекриття, окрім цього, повинні мати гідроізоляцію. Ширина дверей у серверну повинна бути не менш 910 мм, висота – 2000 мм. Конструкція дверей має певні обмеження: полотно повинне відкриватися назовні на 180 градусів, а дверна коробка не повинна мати поріг. При використанні в серверній великогабаритного обладнання передбачається встановлення двостулкових дверей. Для забезпечення герметичності в конструкції дверей повинна бути ущільнювальна прокладка, а для підвищення рівня захисту від злому необхідно передбачити протиз'ємне пристосування.

У серверній не повинно бути вікон. Обов'язковою умовою в цьому приміщенні є наявність фальшпідлоги, що витримує навантаження від обладнання, що встановлюється, і працюючих з ним людей. Рекомендована відстань між плитою на підлозі та фальшпідлогою – 400 мм, при цьому просвіт між фальшпідлогою і фальшстелею повинен бути не менш 2440 мм. Фальшпідлогу рекомендується робити з легко знімних модулів. Матеріал, із якого вона виготовлена, повинен бути міцним, зносостійким, мати погану займистість і мати електричний опір відносно землі від 1 до 20 Ом. Використання килимових покриттів у таких приміщеннях суворо заборонене. Перекриття під фальшпідлогою повинне бути герметизованим або пофарбованим.

*Нумерація (маркування) розеток.* Усі розетки в комп'ютерній мережі повинні бути пронумеровані. Причому, номер розетки повинен бути зазначений (приклеєний, підписаний) безпосередньо поруч із розеткою. Для кожного користувача комп'ютерної мережі повинні бути зарезервовані 2 розетки: комп'ютерна для підключення комп'ютера користувача до комп'ютерної мережі та телефонна для підключення телефону. Правила нумерації розеток не регламентуються, але слід підкреслити, що кожна розетка повинна мати свій унікальний номер, а також пошук фізичного розташування розетки повинен бути не складним. Пропонується наступна складена нумерація розеток – 01-01-K01:

- перша і друга цифри – номер поверху;
- третя та четверта цифри – номер кімнати;
- п'ятий символ – тип розетки (К – комп'ютерна, Т – телефонна);
- шоста і сьома цифри – порядковий номер розетки.

*Типи кабельних сегментів.* При проектуванні комп'ютерної мережі необхідно враховувати характеристики кабельних сегментів. *Кабельний сегмент* – відрізок кабелю або ланцюг відрізків кабелів, електрично (оптично) з'єднаних один з одним, що забезпечують з'єднання двох або більше вузлів мережі. Особливо важливо враховувати довжину кабельного сегмента. В таблиці 1 надані основні характеристики кабельних сегментів.

Таблиця 1.1

Характеристики кабельних сегментів

<b>№</b>	<b>Стандарт</b>	<b>Швидкість передачі даних</b>	<b>Тип кабелю, що використовується</b>	<b>Максимальна довжина сегменту</b>
1	Ethernet 10Base-2	10 Мбіт/с	тонкий коаксіальний	185 м.
2	Ethernet 10Base-5	10 Мбіт/с	товстий коаксіальний	500 м.
3	Ethernet 10Base-F	10 Мбіт/с	волоконно-оптичний	2 км
4	Ethernet 10Base-T	10 Мбіт/с	вита пара	100 м.
5	Ethernet 100Base-FX	100 Мбіт/с	волоконно-оптичний	2000 м.
6	Ethernet 100Base-T	100 Мбіт/с	вита пара	100 м.
7	Ethernet 100Base-T2	100 Мбіт/с	UTP 3	100 м.
8	Ethernet 100Base-T4	100 Мбіт/с	UTP5, STP	100 м.
9	Ethernet 1000Base-CX	1000 Мбіт/с	STP	25 м.
10	Ethernet 1000Base-LX	1000 Мбіт/с	волоконно-оптичний	одномод. 5000 м. багатомод. 550 м.
11	Ethernet 1000Base-T	1000 Мбіт/с	UTP 5	100 м.

### Завдання до контрольної роботи:

Необхідно спроектувати план приміщення офісу та план комп'ютерної мережі. Вихідними даними для цього є: кількість кімнат в офісі, робочі місця користувачів комп'ютерної мережі та розподіл робочих місць в офісі (табл. 1.2).

Таблиця 1.2

#### Вхідні дані

<b>Варіант №1</b>		<b>Варіант №2</b>		<b>Варіант №3</b>		<b>Варіант №4</b>	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	7	1	1	1	4	1	4
2	6	2	6	2	8	2	8
3	9	3	7	3	10	3	8
4	5	4	10	4	3	4	3
5	5	5	5	5	5	5	5
6	2	6	7	6	4	6	8
7	1			7	1	7	1
<b>Варіант №5</b>		<b>Варіант №6</b>		<b>Варіант №7</b>		<b>Варіант №8</b>	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	5	1	5	1	25	1	30
2	8	2	7	2	5	2	3
3	10	3	12	3	1	3	2
4	5	4	1	4	7	4	1
5	5	5	9	5	15	5	1
6	3	6	5	6	3	6	4
7	1	7	1				

Варіант №9		Варіант №10		Варіант №11		Варіант №12	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	1	1	3	1	1	1	10
2	7	2	1	2	3	2	5
3	10	3	5	3	10	3	1
4	12	4	7	4	7	4	8
5	3	5	9	5	14	5	9
6	4	6	5	6	5	6	4
7	6	7	8	7	6	7	4
8	2	8	1				

На основі вхідних даних необхідно спроектувати план офісу, враховуючи, що одна з кімнат повинна бути серверною кімнатою з одним робочим місцем для адміністратора мережі (серверна кімната входить у перелік кімнат з вхідних даних). Також необхідно врахувати всі вимоги щодо розташування серверної кімнати (двері, вікна тощо).

При проектуванні офісу необхідно визначити робочі місця для персоналу, оснащені офісними меблями й персональними комп'ютерами. Також необхідно визначити можливе місце розташування для монтажу кабелю комп'ютерної мережі – місця для коробів, лотків і т.д.; визначити місце розташування для мережевого обладнання; визначити місце розташування телефонних і комп'ютерних розеток на робочих місцях користувачів і пронумерувати їх.

### **План виконання роботи**

1. Визначити форму периметру зовнішніх несучих стін будинку.
2. Спроектувати план поверху офісного будинку, тобто визначити розташування кімнат на поверсі офісного будинку. Необхідно також підписати номери кімнат. На поверсі повинні бути присутніми коридори для переміщень, серверна кімната, місця для комунікацій.

3. Показати розміри кімнат. Це необхідно для визначення порядку довжин кабельних сегментів від серверної до офісних кімнат.

4. Ґрунтуючись на вихідних даних визначити робочі місця користувачів комп'ютерної мережі. Для цього необхідно використовувати відповідні елементи Microsoft Office Visio: столи, стільці, комп'ютери і т.д.

5. Визначити місце розташування коробів, лотків, телефонних і комп'ютерних мережевих розеток. Короба, лотки й розетки необхідно пронумерувати.

6. Заповнити кабельний журнал, у якому необхідно вказати відповідність мережевого обладнання, порти мережевого обладнання, мережевої комп'ютерної розетки, номери кімнати й ім'я комп'ютера. Приклад кабельного журналу представлено в табл. 1.3.

Таблиця 1.3

Приклад кабельного журналу\*

№ п/п	Назва пристрою	№ порту	№ розетки	Ім'я комп'ютера	№ кімнати
1.	KM01	01	01-01-K01	01-01-01	01
		02	01-01-K02	01-01-02	
		03	01-01-K03	01-01-03	
2.	KM02	01	01-01-T01	01-01-01	
		02	01-01-T02	01-01-02	
		03	01-01-T03	01-01-03	
3.	KM03	01	01-02-K04	01-02-04	02
		02	01-02-K05	01-02-05	
		03	01-02-K06	01-02-06	
		04	01-02-K07	01-02-07	
4.	KM04	01	01-02-T04	01-02-04	
		02	01-02-T05	01-02-05	
		03	01-02-T06	01-02-06	
		04	01-02-T07	01-02-07	
5.	MP01	01	01-05-K36	01-05-36	03

\* умовні позначення: KM – комутатор, MP - маршрутизатор

### **Контрольні питання:**

1. Перерахуйте основні етапи створення документу у Visio.
2. Назвіть основні вимоги до створення серверної кімнати.
3. Яким чином нумеруються комп'ютерні і телефонні розетки у комп'ютерній мережі?
4. Перерахуйте основні характеристики типів кабельних сегментів.
5. З якою метою необхідно вказувати розміри кімнат на плані поверху?
6. Що таке кабельний лоток і пластиковий короб?
7. Що входить до робочого місця користувача комп'ютерної мережі?

## Контрольна робота №2

**Тема:** Проектування та обґрунтування схеми IP-адресації корпоративної мережі з оцінюванням альтернатив і ризиків

**Мета:** Одержати навички призначення IP-адрес і розподілу міської мережі на підмережі.

### Теоретичні відомості

*Порядок призначення IP-адрес.* За визначенням схема IP-адресації повинна забезпечувати унікальність нумерації мереж, а також унікальність нумерації вузлів у межах кожної з мереж. Отже, процедури призначення номерів як мережам, так і вузлам мереж повинні бути *централізованими*.

Коли справа стосується мережі, яка є частиною Інтернету, унікальність нумерації може бути забезпечена тільки зусиллями спеціально створених для цього центральних органів. У невеликій же автономній IP-мережі умова унікальності номерів мереж і вузлів може бути виконана силами мережевого адміністратора.

У цьому випадку в розпорядженні адміністратора є весь адресний простір, тому що збіг IP-адрес у незв'язаних між собою мережах не викличе ніяких негативних наслідків. Адміністратор може вибирати адреси довільно, дотримуючись лише синтаксичних правил, ураховуючи обмеження на особливі адреси.

Однак, при такому підході виключена можливість у майбутньому приєднати дану мережу до Інтернету. Дійсно, довільно обрані адреси даної мережі можуть збігтися із централізовано призначеними адресами Інтернету. Для того щоб уникнути колізій, пов'язаних з такого роду збігами, у стандартах Інтернету визначено декілька так званих приватних адрес, які рекомендують для автономного використання:

- у класі А – мережа 10.0.0.0;
- у класі В – діапазон з 16 мереж – 172.16.0.0-172.31.0.0;
- у класі С – діапазон з 255 мереж – 192.168.0.0-192.168.255.0.

Ці адреси виключені з адрес, які розподіляються централізовано, і становлять величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів. Варто також відзначити, що приватні адреси, як і при довільному виборі адрес, у різних автономних мережах можуть збігатися. У той же час використання приватних адрес для адресації автономних мереж робить можливим коректне підключення їх до Інтернету.

Розглянемо приклад призначення IP-адрес у мережі. Припустимо, що необхідно призначити IP-адреси для всіх інтерфейсів в мережі, використовуючи для цього діапазон 172.16.20.0/25.

На рис. 2.1 представлений приклад IP-адресації.

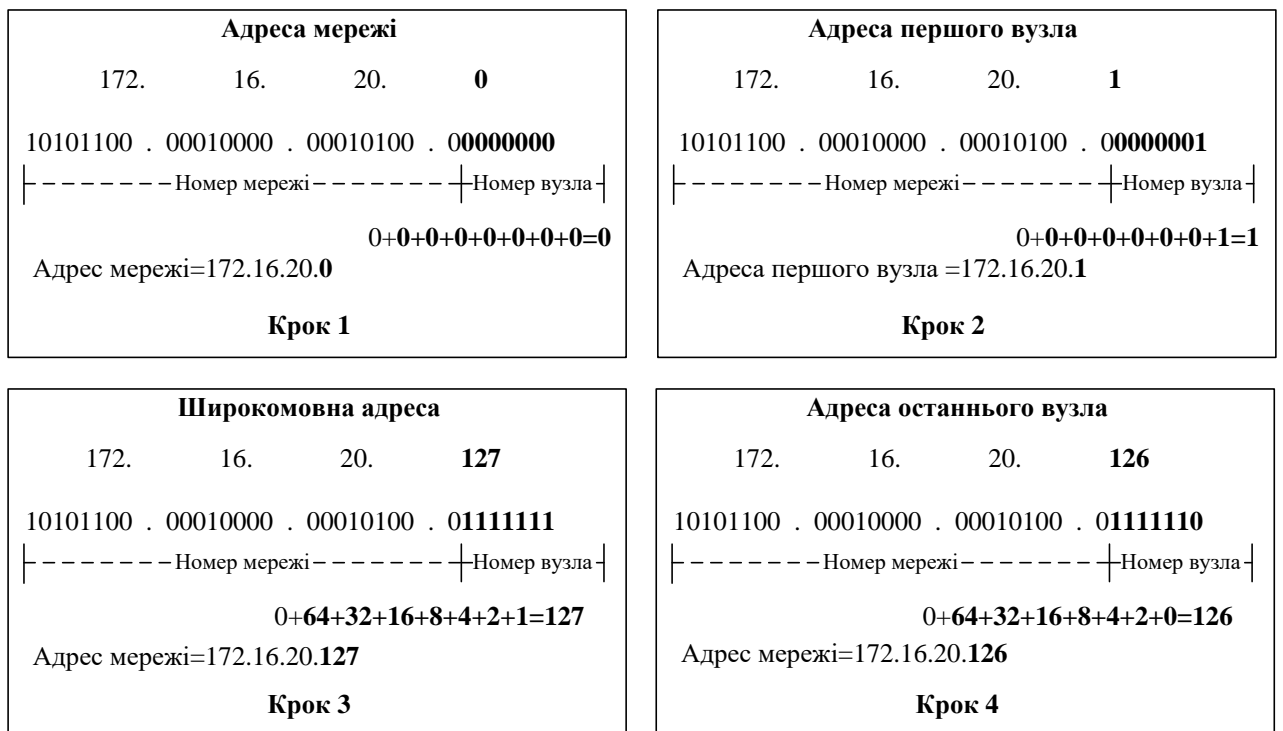


Рисунок 2.1 – Приклад IP-адресації

На першому кроці призначається адреса мережі. Маска мережі в цьому випадку включає 25 біт, а 7 останніх біт – це біти адрес робочих станцій. В адресі мережі останні 7 біт повинні приймати значення 0. У результаті була отримана адреса мережі 172.16.20.0 з маскою 255.255.255.128.

*На другому кроці* призначається адреса першого вузла в мережі. Адреса першого вузла в мережі є наступною адресою після адреси мережі. Для призначення першої, самої нижньої адреси вузла в мережі останній сьомий біт повинен прийняти значення 1. У результаті ми маємо адресу 172.16.20.1 з маскою 255.255.255.128.

*На третьому кроці* визначається широкомовна адреса. У широкомовній адресі необхідно, щоб розряди вузла були встановлені в 1, тобто в даному прикладі сім останніх бітів повинні бути встановлені в 1. У такий спосіб в останньому октеті ми одержимо значення 127, що дає нам широкомовну адресу 172.16.20.127.

*На четвертому кроці* призначається адреса останнього вузла в мережі. Адреса останнього вузла в мережі завжди менше широкомовної адреси. Це означає, що в адресі останнього вузла мережі останній біт повинен бути встановлений в 0, а при широкомовному запиті в 1. У такий спосіб адреса останнього вузла в мережі буде 172.16.20.126.

Кількість вузлів даної мережі дорівнює  $2^n - 2$ , де  $n$  – кількість бітів, виділених для адресації вузлів. Одна адреса віднімається, оскільки вона призначається широкомовному запитові, а одна – оскільки вона призначається адресі мережі. Тобто у нашому випадку кількість вузлів буде  $2^7 - 2$ , що дорівнює 126.

### **Завдання до контрольної роботи:**

1) Необхідно розробити схему IP-адресації для міської комп'ютерної мережі, яка об'єднує три відділення фірми:

- відділення №1 знаходиться в одноповерховому будинку;
- відділення №2 – у триповерховому;
- відділення №3 – у десятиповерховому будинку.

Кожне відділення – це окрема підмережа.

2) Розробити програмне забезпечення для автоматичного призначення IP-адрес підмережам і хостам та визначення широкомовних адрес при вказаних користувачем умовах.

## Вихідні дані

Варіант №1		Варіант №2		Варіант №3		Варіант №4	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	7	1	1	1	4	1	4
2	6	2	6	2	8	2	8
3	9	3	7	3	10	3	8
4	5	4	10	4	3	4	3
5	5	5	5	5	5	5	5
6	2	6	7	6	4	6	8
7	1			7	1	7	1
Варіант №5		Варіант №6		Варіант №7		Варіант №8	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	5	1	5	1	25	1	30
2	8	2	7	2	5	2	3
3	10	3	12	3	1	3	2
4	5	4	1	4	7	4	1
5	5	5	9	5	15	5	1
6	3	6	5	6	3	6	4
7	1	7	1				

Варіант №9		Варіант №10		Варіант №11		Варіант №12	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	1	1	3	1	1	1	10
2	7	2	1	2	3	2	5
3	10	3	5	3	10	3	1
4	12	4	7	4	7	4	8
5	3	5	9	5	14	5	9
6	4	6	5	6	5	6	4
7	6	7	8	7	6	7	4
8	2	8	1				

Також необхідно призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня.

Для кожної підмережі необхідно призначити: IP-адресу, маску підмережі та адресу широкомовного запиту. Після цього необхідно в рамках визначених підмереж визначити початкову й кінцеву адреси для робочих станцій. Також необхідно розрахувати кількість вузлів кожної підмережі.

*Для адресації використовувати мережу 192.168.0.0/16 та змінну довжину маски підмережі. Обов'язковою умовою є використання мінімальної можливої довжини хостової частини.*

### **План виконання завдання**

Для виконання даної контрольної роботи необхідно виконати наступні дії:

- визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня;
- для кожної підмережі призначити: IP-адресу, маску підмережі, адресу широкомовного запиту;

- призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня;
- у рамках підмереж для робочих станцій призначити початкову та кінцеву IP-адреси;
- розрахувати максимальну кількість вузлів кожної підмережі.

Результат розрахунків оформити у вигляді таблиці (див. табл. 2.2).

Таблиця 2.2

Зразок таблиці

Номер підмережі	IP-адреса підмережі	Маска підмережі	IP-адреса першого вузла	IP-адреса останнього вузла	Broadcast	Максимальна кількість вузлів у мережі
1	10.1.1.0	255.255.255.0	10.1.1.1	10.1.1.254	10.1.1.255	254

**Контрольні питання:**

1. Дайте характеристику класу комп'ютерних мереж – «міська мережа». Які відмінні ознаки має даний клас у порівнянні із класами локальні та глобальні мережі?
2. Які апаратні пристрої дозволяють розділити мережу на підмережі? На якому рівні моделі OSI вони працюють?
3. Що таке IP-адреса? Для чого вона необхідна?
4. Які класи мереж Вам відомі? За якою ознакою розділені ці мережі?
5. Що таке маска підмережі? Яку функцію вона виконує?
6. Опишіть процедуру призначення IP-адрес.

## Контрольна робота №3

**Тема:** Ієрархічне проектування CIDR IP адресації для корпоративної мережі

**Мета:** Набути навичок для створення ієрархічної IP-адресації у великих корпоративних мережах

### Завдання до контрольної роботи:

- 1) Ознайомтеся з теоретичним матеріалом представленим у Лекції №4
- 2) Створіть схему IP-адресації для зазначених у Вашому варіанті вимог. Додайте в таблицю вказану у Вашому варіанті відповідні значення для заповнення необхідної схеми IP-адресації. Намалюйте схему відповідної мережі.
- 3) Розробіть програмне забезпечення для автоматичного обчислення IP-адрес мереж, підмереж, хостів та ширококомовних розсилок для безкласової адресації при вказаних користувачем умовах.

### Варіант 1.

IP-адреса: 192.168.5.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
60	/26	64	192.168.5.0	.1-.62	.63
30					
25					
10					
2					
2					

**Варіант 2.**

IP-адреса: 172.16.6.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
25	/27	30	172.16.6.0	.1-.30	.31
25					
25					
12					
6					
2					

**Варіант 3.**

IP-адреса: 10.33.19.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
100	/25	126	10.33.19.0	.1-.126	.127
55					
30					
12					
2					
2					

**Варіант 4.**

IP-адреса: 192.168.5.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
60	/26	64	192.168.5.0	.1-.62	.63
30					
25					
10					
2					
2					

**Варіант 5.**

IP-адреса: 172.16.6.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
25	/27	30	172.16.6.0	.1-.30	.31
25					
25					
12					
6					
2					

## Варіант 6.

IP-адреса: 10.33.19.0/24

Необхідне число вузлів	Маска	Число вузлів	Підмережа	Діапазон адрес вузлів	Широкомовна адреса
100	/25	126	10.33.19.0	.1-.126	.127
55					
30					
12					
2					
2					

### Контрольні питання:

1. Для чого потрібні ієрархічні мережі? Чим IP-адресація у ієрархічних мережах відрізняється від IP-адресації у плоских мережах?
2. У чому перевага безкласової IP-адресації?
3. Як призначаються адреси підмережам і хостам при безкласовій маршрутизації.
4. Як визначити адресу широкомовного розсилання у безкласовій IP-адресації?
5. Чим відрізняється маска IP-адреси в класовій та безкласовій маршрутизації? Які функції виконує маска IP-адреси?

## Контрольна робота №4

**Тема:** Маршрутизація й аналіз пропускної здатності мереж

**Мета:** навчитися розробляти алгоритми маршрутизації

### Теоретичні відомості

Передача інформації в обчислювальних мережах припускає наявність процедури маршрутизації, що визначає маршрут передачі пакета від джерела до адресата. Одним з основних елементів процедури маршрутизації є маршрутні таблиці, які містяться в кожному з вузлів мережі й визначають у який із суміжних вузлів мережі повинен бути переданий пакет, якщо він призначений заданому вузлу. Критерієм доставки є мінімальний час передачі пакета від джерела до адресата. У найпростішому випадку, затримка передачі пакета може оцінюватися числом проміжних вузлів на шляху від джерела до адресата.

Задачу формування маршрутних таблиць можна розділити на два етапи:

1. Визначення довжини найкоротших шляхів між всіма парами вузлів.
2. Визначення значень елементів маршрутної таблиці.

### Визначення довжини найкоротших шляхів

Для визначення довжини найкоротшого шляху, можна використовувати алгоритм Дейкстри, що є одним найбільш відомих і ефективних алгоритмів рішення цієї задачі.

Позначки вершин  $d(x_i)$  розділяються на постійні й тимчасові. Постійні позначки дорівнюють довжині найкоротшого шляху від початкового вузла до заданого. У процесі роботи алгоритму всі вершини одержують постійні позначки. Для того щоб розрізнити позначки вершин будемо використовувати масив  $Z$ .

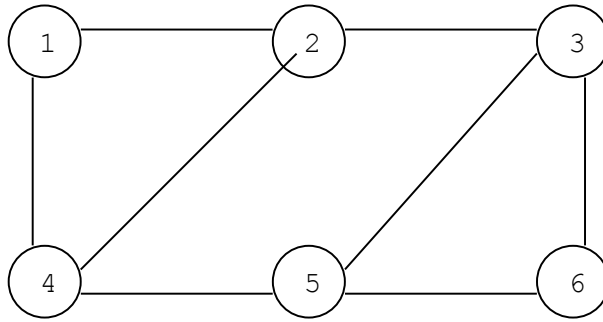
$$z(x_i) = \begin{cases} 1 & \text{– якщо позначка постійна} \\ 0 & \text{– якщо позначка тимчасова} \end{cases}$$

1. Виберемо початкову вершину  $s$  і встановимо  $d(s)=0, z(s)=1$ .
2. Для інших вершин  $x_i$  встановимо для них  $d(x_i)=\infty, z(x_i)=0$ .
3.  $P=s$ .
4. Оновлення позначок. Для всіх вершин суміжних вершині  $P$  змінимо позначки відповідно до виразу:  

$$d(x_i) = \min[d(x_i); d(p) + l(p, x_i)],$$
 де  $l(p, x_i)$  довжина ребра  $p, x_i$ .
5. Серед всіх вершин, що мають тимчасову позначку  $z(x_i)=0$  знайдемо вершину  $x_k$ , що має мінімальну позначку  $d(x_k)$ .
6. Встановимо  $z(x_k)=1, P=x_k$ .
7. Якщо не всі вершини одержали постійні позначки перейти на крок 4.
8. Кінець

Перебравши в якості початкової ( $s$ ), всі вершини графа ми одержимо матрицю найкоротших відстаней.

На рис.4.1 наведений приклад мережі, матриця суміжності вершин і матриця найкоротших відстаней розрахована за алгоритмом Дейкстри.



Матриця суміжності ( $l_{ij}$ )

```

0  1 99 1 99 99
1  0  1  1 99 99
99 1  0 99 1  1
  1 1 99 0 1 99
99 99 1  1 0  1
99 99 1 99 1  0
  
```

Матриця найкоротших відстаней ( $a_{ij}$ )

```

0  1  2  1  2  3
1  0  1  1  2  2
2  1  0  2  1  1
1  1  2  0  1  2
2  2  1  1  0  1
3  2  1  2  1  0
  
```

сума 46

Рисунок 4.1 – Приклад розрахунку найкоротших відстаней між вузлами комп'ютерної мережі

## Визначення значень елементів маршрутної таблиці

Елементи маршрутної таблиці  $M_{ij}$  визначаються за наступним правилом:

$$M_{ij}=k, \quad \text{якщо} \quad a_{ij}=l_{ik}+a_{kj} \quad (4.1)$$

Розглянемо застосування цього правила для визначення елемента  $M_{15}$ , що повинен бути рівним номеру вузла суміжного вузлу 1, у який варто передати пакет призначений вузлу 5. Вузлу 1 суміжні два вузли 2,4.

З матриці найкоротших відстаней слідує, що довжина найкоротшого шляху між вузлами 1 і 5 дорівнює 2 ( $a_{15}=2$ ).

Перевіримо правило (4.1) для вузла 2:

$$l_{12}=1, a_{25}=2 \quad 1+2 <> 2$$

Це означає, що вузол 2 не належить найкоротшому шляху з вузла 1 у вузол 5.

Перевіримо правило (4.1) для вузла 4:

$$l_{14}=1, a_{45}=1 \quad 1+1 = 2$$

Це означає, що вузол 4 належить найкоротшому шляху з вузла 1 у вузол 5 і отже  $M_{15}=4$ . Діючи аналогічним чином можна визначити інші елементи маршрутної таблиці. На рис. 4.2 наведений приклад маршрутної таблиці для мережі представленої на рис. 4.1

Маршрутна таблиця

1	2	2	4	4	4
1	2	3	4	4	3
2	2	3	5	5	6
1	2	5	4	5	5
4	4	3	4	5	6
5	3	3	5	5	6

Рисунок 4.2 – Приклад маршрутної таблиці

## Оцінка пропускної здатності мережі

Важливою характеристикою обчислювальної мережі є її пропускна здатність, що дорівнює максимальній інтенсивності вхідного потоку. Вхідний потік задається матрицею трафіку  $t_{ij}$ . Елементи цієї матриці рівні інтенсивності потоку даних переданих з вузла  $i$  у вузол  $j$ . Як одиниця виміру може бути використано – Мб/сек. Будемо вважати, що всі елементи матриці трафіку рівні 1.

Якщо передавати дані по найкоротших шляхах, використовуючи матрицю маршрутів, ми можемо визначити потоки даних для кожного каналу передачі даних  $q_{ij}$ . На рис. 4.3 показана матриця потоків, отримана для розглянутої мережі.

0	2	0	3	0	0
2	0	3	2	0	0
0	3	0	0	2	2
3	2	0	0	6	0
0	0	2	6	0	3
0	0	2	0	3	0

Сума = 46

Рівень трафіку = 8.33

Рисунок 4.3 – Матриця потоків

Можна показати, що якщо всі елементи матриці трафіку рівні 1, то сума всіх потоків у каналах мережі дорівнює сумі всіх елементів матриці найкоротших відстаней.

Тому можна стверджувати, що пропускна здатність збільшується при зменшенні середньої відстані між вузлами мережі.

Для оцінки пропускної здатності необхідно задати пропускну здатність каналів зв'язку. Будемо вважати, що в нашій мережі всі канали мають однакову

пропускну здатність  $C=50$ . Зміна вхідного потоку досягається пропорційною зміною всіх елементів матриці трафіку. Для цього будемо використовувати масштабний множник  $R$ , що називається рівнем трафіку.

Нижню оцінку цього коефіцієнта можна одержати з наступних міркувань. Визначивши потоки даних у всіх каналах мережі, знайдемо максимальне значення  $q_{ij}$ .

$$R_{\min} = C / \max(q_{ij}),$$

Для розглянутого прикладу  $C=50$ ,  $\max(q_{ij})=6$ .

$$R_{\min} = 50/6 = 8,33.$$

Дана оцінка дає нижню границю рівня трафіку, тому що не всі канали завантажені однаково. Можна вважати, що використовуючи оптимальні алгоритми маршрутизації вдасться рівномірно розподілити потік по всіх каналах, не збільшивши при цьому довжину шляхів. Тоді верхня оцінка рівня трафіку може бути отримана з наступного виразу:

$$R_{\max} = C * N / \text{SUM}(q_{ij}),$$

де  $N$  – число каналів.

Для розглянутого прикладу:  $R_{\max} = 50 * 8 / 46 = 8,7$

### **Завдання до контрольної роботи:**

1. Здійснити вручну наступні розрахунки (схему мережі взяти відповідно до свого варіанта):

– Визначити матрицю найкоротших відстаней, матрицю маршрутів і матрицю потоків у заданій мережі.

– Розрахувати нижню й верхню границі рівня трафіку.

2. Розробити програмне забезпечення для:

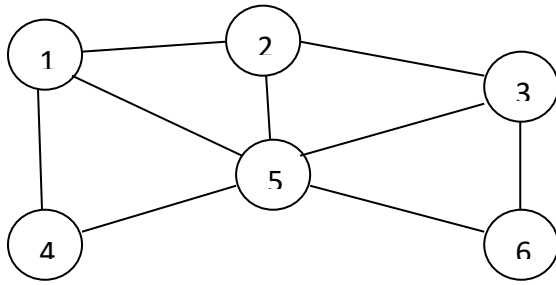
– моделювання комп'ютерної мережі у вигляді довільного графа (що генерується випадковим чином, або задається вручну),

– реалізувати пошук найкоротших відстаней у мережі взявши за основу алгоритм Дейкстри.

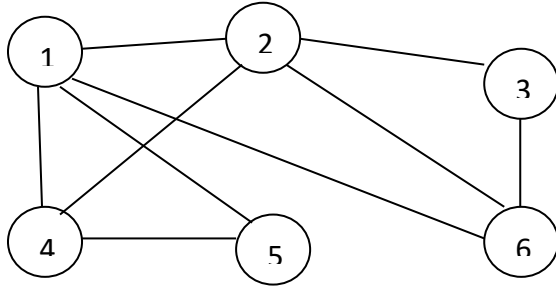
– реалізувати визначення матриці маршрутів і матриці потоків.

– реалізувати розрахунок нижньої та верхньої границі рівня трафіку.

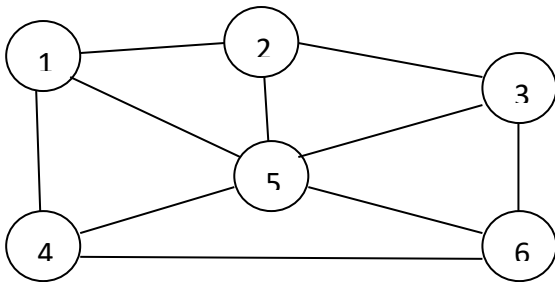
### **Варіант 1**



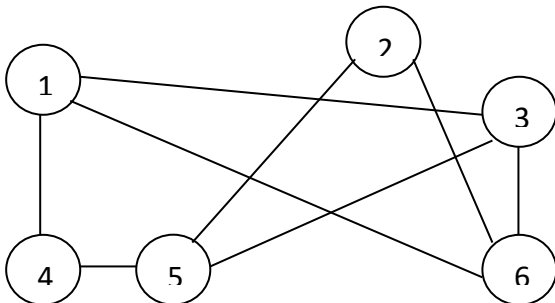
**Варіант 2**



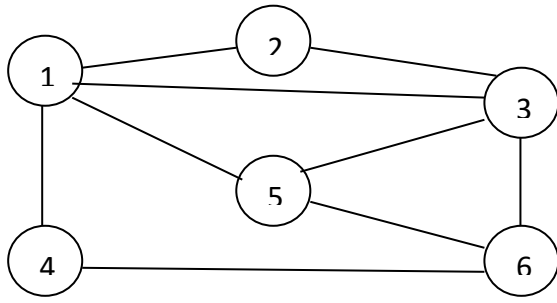
**Варіант 3**



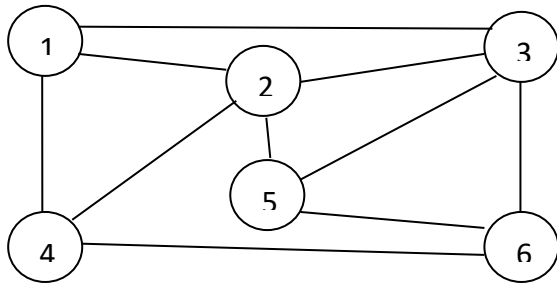
**Варіант 4**



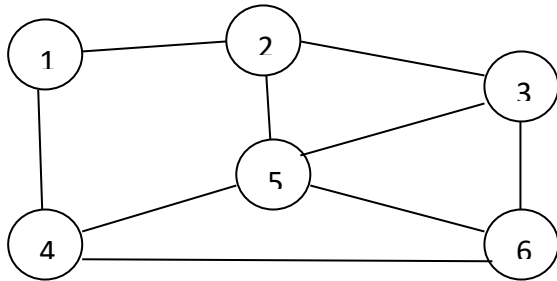
**Варіант 5**



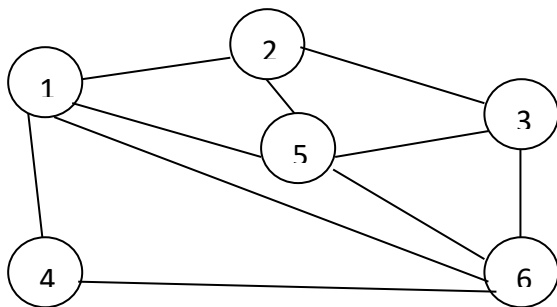
**Варіант 6**



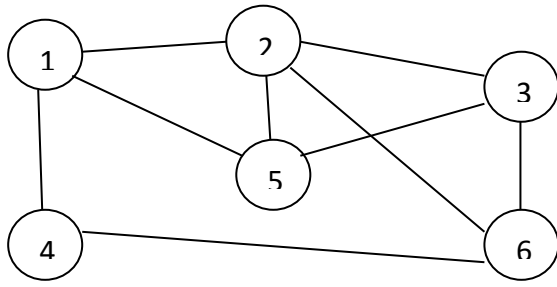
**Варіант 7**



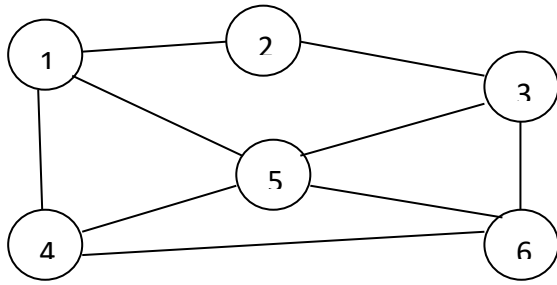
**Варіант 8**



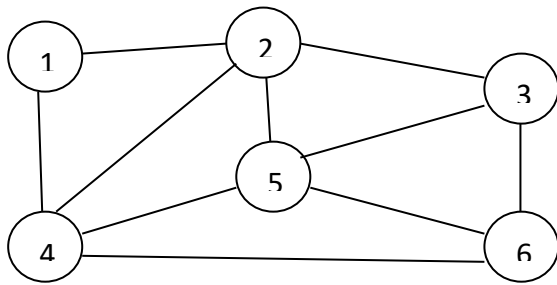
**Варіант 9**



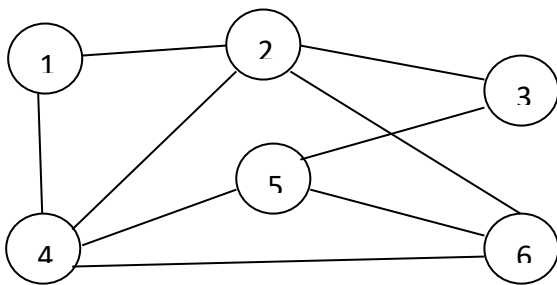
**Варіант 10**



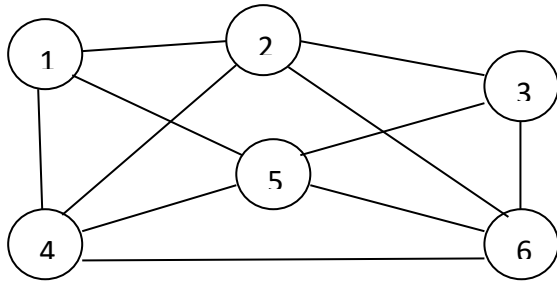
**Варіант 11**



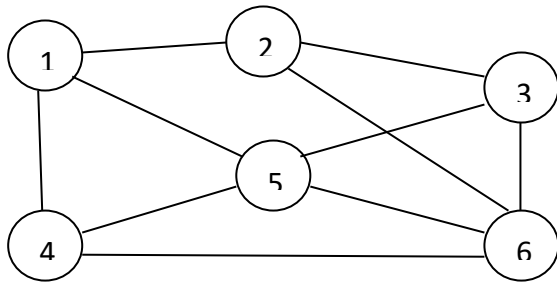
**Варіант 12**



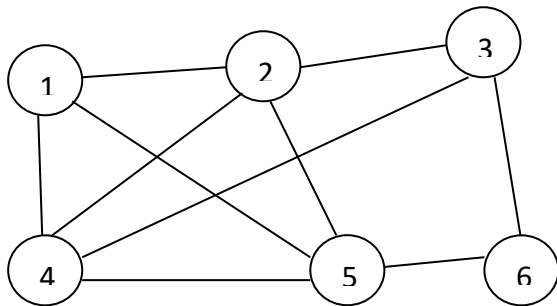
**Варіант 13**



**Варіант 14**



**Варіант 15**



## Контрольна робота №5

**Тема:** Планування списків доступу і фільтрів портів

**Мета:** навчитися на основі схеми мережі визначати місця, де необхідно впровадження списків доступу і фільтрів портів для захисту мережі

### Початкові дані

Уявіть, що ви спеціаліст служби підтримки, відправлений на об'єкт для роботи з мережею корпоративного клієнта, якому необхідно знизити загрозу порушень мережної безпеки.

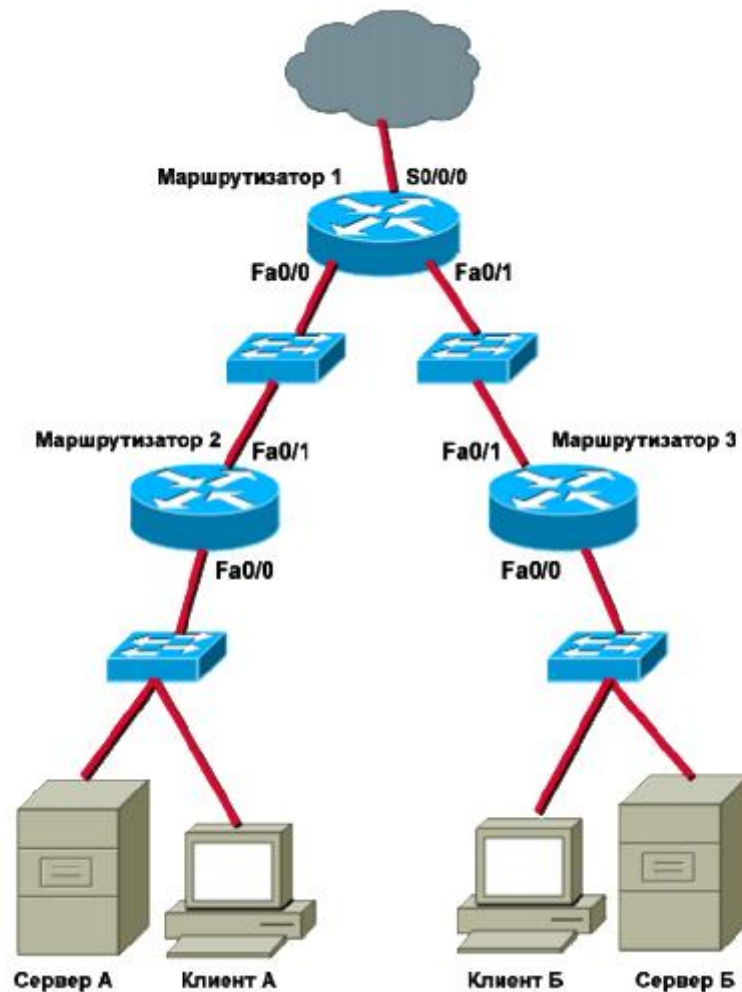


Рисунок 5.1 – Схема мережі корпоративного клієнта

### **Завдання до контрольної роботи:**

Визначити місця для розміщення списків доступу відповідно до побажань клієнта, для цього виконати кроки 1–3 та заповнити наведені таблиці.

**Розробити програму для моделювання роботи мережі з рисунку 5.1 з можливістю задавання різних списків доступу.**

#### **Крок 1.** Обмеження клієнта А одною мережею.

Вас просять обмежити доступ клієнта А тільки підмережею, до якої він в поточний момент підключений. Клієнту А необхідний доступ до сервера А, але мережа Інтернет і сервер В повинні бути йому недоступні. Де слід розмістити список доступу?

<b>Маршрутизатор</b>	<b>Інтерфейс</b>	<b>Дозволити або відхилити?</b>	<b>Вхідний або вихідний фільтр?</b>	<b>Підстава</b>

**Крок 2.** Обмежити доступ до сервера А для клієнта А, але дозволити доступ до сервера В і до мережі Інтернет.

Вас попросили заборонити доступ клієнту В до сервера А, але клієнту В потрібен доступ до мережі Інтернет та до сервера В. Де слід розмістити список доступу?

<b>Маршрутизатор</b>	<b>Інтерфейс</b>	<b>Дозволити або відхилити?</b>	<b>Вхідний або вихідний фільтр?</b>	<b>Підстава</b>

**Крок 3.** Дозволити доступ до маршрутизаторів, що використовують тільки протокол SSH, виключно клієнту А.

Вас попросили обмежити доступ до маршрутизаторів тільки клієнтом А, який буде виконувати функції керуючого ПК для цих маршрутизаторів. Вам необхідно обмежити доступ тільки протоколом SSH від клієнта А і запобігти доступу Telnet. Де слід розмістити список доступу?

*Підказка.* Для контролю доступу протоколу SSH і Telnet до маршрутизаторів потрібно декілька інтерфейсів на декількох маршрутизаторах.

Маршрутизатор	Інтерфейс	Вхідний або вихідний фільтр?	Порт	Дозволити або відхилити?	Підстава

**Контрольні питання:**

1. Навіщо потрібна фільтрація трафіку?
2. За якими критеріями можна дозволяти/забороняти трафік?
3. Що таке ACL-списки?
4. Які існують типи ACL-списків?
5. Яка структура групової маски ACL-списку?

## Контрольна робота №6

**Тема:** Збирання мережевих даних, фільтрація та атрибуція віддалених ресурсів

**Мета:** виконати збір мережевого трафіку за допомогою програми Wireshark, щоб ознайомитися з інтерфейсом і середовищем Wireshark; проаналізувати трафік для веб-сервера; створити фільтр для обмеження збору мережевих даних пакетами ICMP; відправити луна-запит віддаленому вузлу, щоб поспостерігати за роботою фільтра пакетів ICMP в ході збору мережевих даних.

### Попередня інформація/підготовка

У цій контрольній роботі ви встановите програму Wireshark, широко відомий аналізатор мережевих протоколів і засіб моніторингу. Програма Wireshark збирає всі пакети, відправлені або отримані мережевою інтерфейсною платою (NIC) комп'ютера. Її можна встановити або в контрольії, або вдома на ПК. Вам він знадобиться для відстеження та перегляду різних типів мережевих протоколів і трафіку. Раніше програма Wireshark була відома під ім'ям Ethereal.

**Програма Wireshark** поставляється **безкоштовно** і доступна за адресою **[www.wireshark.org](http://www.wireshark.org)**.

Для виконання контрольної роботи потрібні наступні ресурси:

- ПК під управлінням ОС Windows з мережею Ethernet і хоча б двома вузлами;
- програма Wireshark;
- підключення до мережі Інтернет (не обов'язково, але бажано);
- доступ до командного рядка ПК;
- доступ до мережевої конфігурації TCP/IP ПК.

## Завдання до контрольної роботи:

Виконати кроки 1-5 зазначені нижче.

### Крок 1. Установка і запуск програми Wireshark

Якщо програма Wireshark завантажувалася на ПК раніше, перейдіть в папку з програмою Wireshark Start>All Programs>Wireshark>Wireshark (пуск>програми>Wireshark>Wireshark) і клацніть значок додатки.

Якщо раніше програма Wireshark не встановлювалася, виконаєте наступні дії:

А. Вказавши шлях в локальній мережі до установника програми Wireshark, wireshark-setup-0.99.5.exe, завантажте установник на робочий стіл ПК.

Б. Клацніть установник два рази і дотримуйтесь його підказкам, приймаючи значення за замовчуванням (рис. 6.1).



Рисунок 6.1

1) Натисніть кнопку I Agree (прийняти) (рис. 6.2).

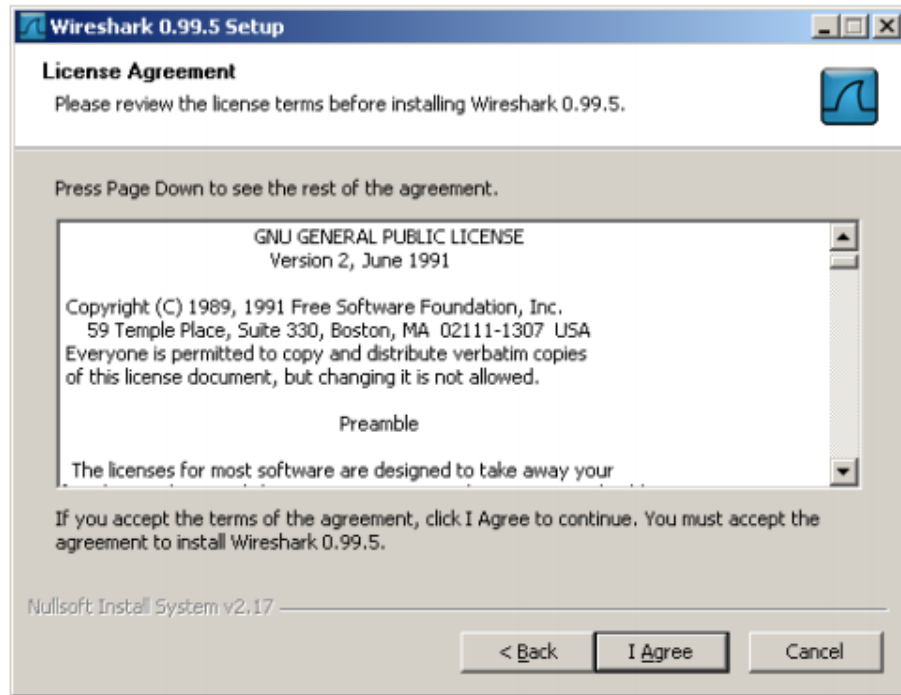


Рисунок 6.2

2) Переконайтеся, що на ПК встановлено WinPcap. У WinPcap входить драйвер для підтримки збору пакетів. Програма Wireshark використовує цю бібліотеку для збору динамічних мережевих даних в Windows (рис. 6.3).

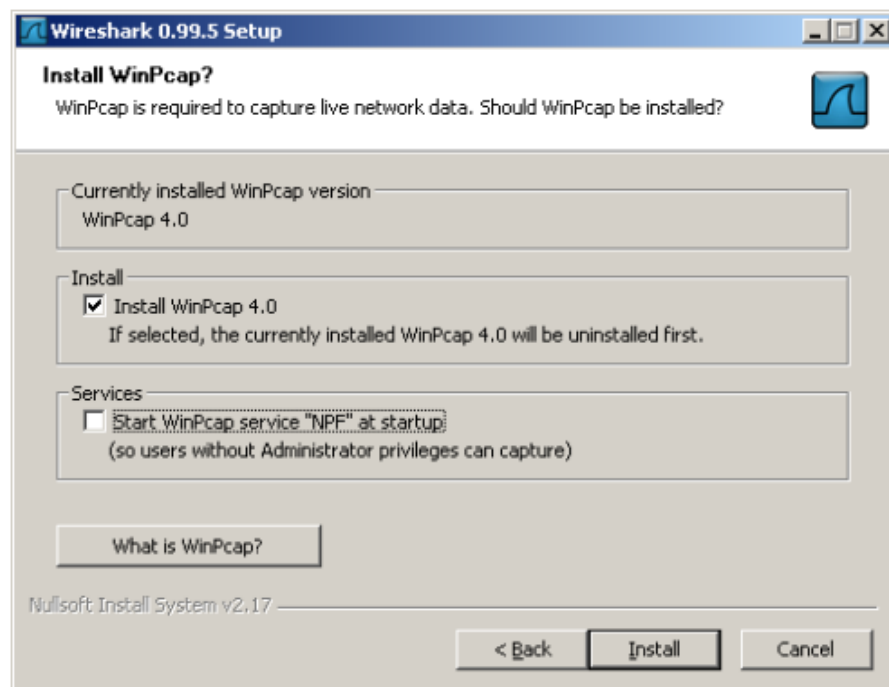


Рисунок 6.3

В. Натисніть Install (встановити) і слідуйте підказкам до кінця процесу установки.

Г. Після установки програми встановіть відповідний прапорець, щоб запустити програму Wireshark.

### **Крок 2.** Вибір інтерфейсу для збору пакетів

А. Запустіть додаток Wireshark.

Б. У меню Capture (збір) виберіть пункт Interfaces (інтерфейси) (рис. 6.4).

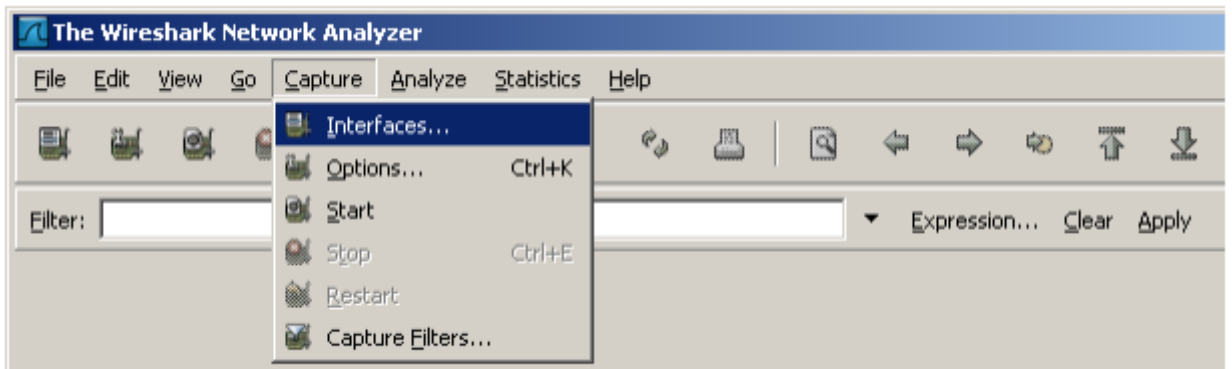


Рисунок 6.4

3) Натисніть кнопку Start (пуск) для інтерфейсу Ethernet (NIC), який потрібно використовувати для збору мережевого трафіку (рис. 6.5).

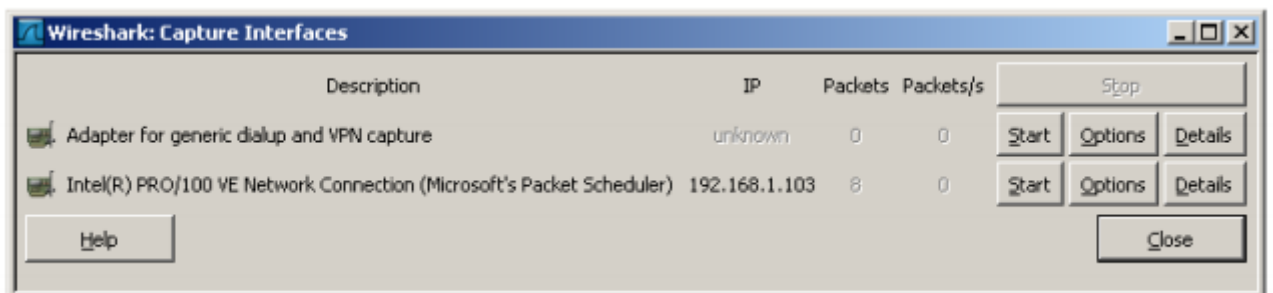


Рисунок 6.5

### **Крок 3.** Запуск збору мережевих даних

А. Продивіться меню і перегляньте панель інструментів в інтерфейсі запуску Wireshark.

Б. Натисніть кнопку New Live Capture (новий збір динамічних даних) і перегляньте відомості, зібрані Wireshark. Нехай збір даних триває протягом декількох хвилин, щоб ви могли поспостерігати за різними типами трафіку в мережі (рис. 6.6).

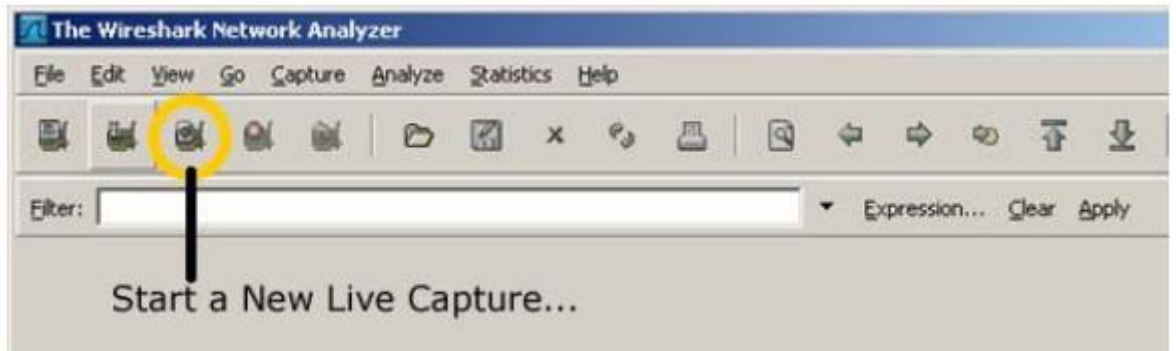


Рисунок 6.6

#### Крок 4. Аналіз відомостей про веб-трафіку

А. Якщо існує підключення до мережі Інтернет, відкрийте веб-браузер і перейдіть у вузол [www.google.com](http://www.google.com). Зверніть вікно Google і поверніться у Wireshark. Має бути відображений трафік, схожий з тим, що представлений нижче. Знайдіть стовпці Source, Destination та Protocol (джерело, адресу призначення і протокол) на екрані Wireshark (рис. 6.7).

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-Li_6e:fe:0b	Intel_63:ce:53	ARP	who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-Li_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.l.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 win=8190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 win=65535 Len=
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 win=64458 Len=
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, workstation, Server, P

Рисунок 6.7

4) Підключення до сервера Google почнеться з відправлення запиту на DNS-сервер для пошуку IP-адреси сервера. IP-адреса сервера призначення, скоріше всього, почнеться з 64.xxx

Б. Відкрийте ще одне вікно веб-оглядача і перейдіть в базу даних ARIN Whois <http://www.arin.net/whois/> або скористайтеся іншим засобом пошуку whois і введіть IP-адресу сервера призначення.

### Крок 5. Фільтрація збору мережевих даних

А. Відкрийте вікно командного рядка, вибравши Start> All Programs> Run (пуск> програми>виконати) і ввівши cmd. Або клацніть Start> All Programs> Accessories (пуск> всі програми> стандартні> командний рядок).

Б. Надішліть луна-запит за IP-адресою вузла у вашій локальній мережі і поспостерігайте за процесами у вікні збору Wireshark. Прокрутіть вниз і вгору вікно, в якому відображається трафік. Подивіться які використовуються типи протоколів.

В. У текстовому полі Filter (фільтр) введіть icmp і клацніть Apply (застосувати). Протокол управління повідомленнями в Інтернет (ICMP) - це протокол, використовуваний луна-запитом для перевірки мережевого підключення до іншого вузла.

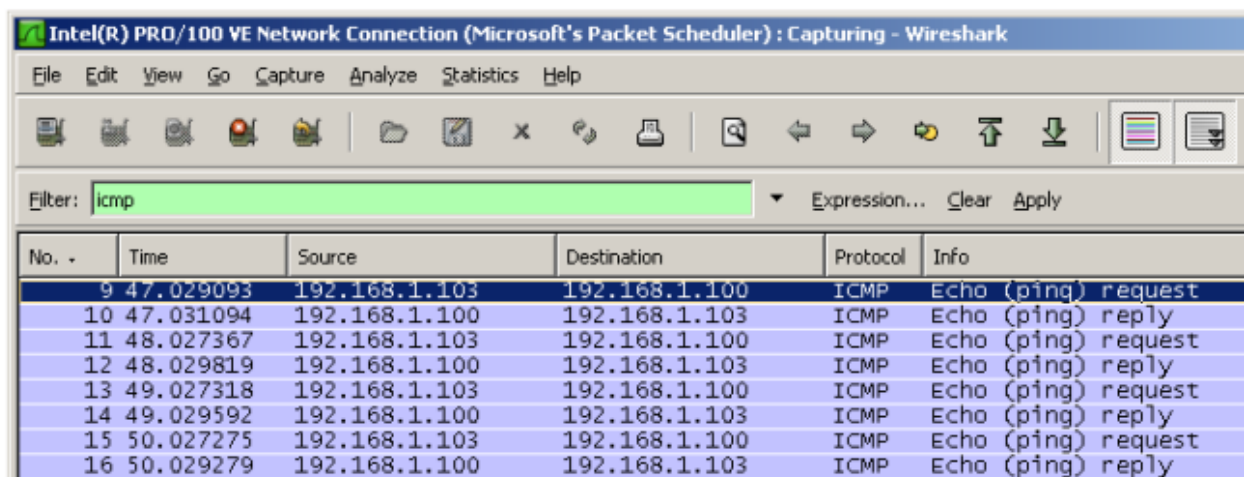


Рисунок 6.8

Г. Клацніть Filter (фільтр): Кнопка Expression (вираз) у вікні Wireshark. Прокрутіть список вниз і перегляньте можливості фільтрації. Подивіться чи є в списку протоколи TCP, HTTP, ARP та інші.

### **Контрольні питання:**

1. У полі фільтрів відображені сотні фільтрів. У великих мережах може бути багато різних типів трафіку у величезних обсягах. Які три фільтри з довгого списку, ви думаєте, можуть бути найбільш ефективні для мережевого адміністратора?
2. Програма Wireshark це засіб для позасмугового або внутрішньосмугового моніторингу мереж? Поясніть свою відповідь.
3. Яке було джерело і адреса призначення першого пакету, відправленого на сервер Google у кроці 4 контрольної роботи?
4. Яким способом можна визначити організацію по IP-адресі?
5. Які протоколи служать для підключення до веб-сервера і доставки веб-сторінки в ваш локальний вузол?
6. Яким кольором виділяється трафік у програмі Wireshark між вашим вузлом і веб-сервером Google?
7. Який трафік відображається при введенні команди ісmp в текстове поле Filter (фільтр)?

## Контрольна робота №7

**Тема:** Профілювання, оптимізація продуктивності та енергоефективності маршрутизатора на базі OpenWrt у високонавантажених L3 сценаріях

**Мета:** Здійснити інженерну оптимізацію маршрутизатора OpenWrt для підвищення пропускну здатності та зниження енергоспоживання на одиницю переданих даних.

**Знати:** Маршрутизація IPv4, базові поняття offload, MTU, QoS, основи вимірювань продуктивності

### Теоретичні відомості

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором).

#### **Базова конфігурація мережі та маршрутизації в OpenWrt:**

<https://openwrt.org/docs/start>

[https://openwrt.org/docs/guide-user/network/network\\_configuration](https://openwrt.org/docs/guide-user/network/network_configuration)

#### **Flow Offloading та його обмеження щодо QoS, firewall**

[https://openwrt.org/docs/guide-user/perf\\_and\\_log/flow\\_offloading](https://openwrt.org/docs/guide-user/perf_and_log/flow_offloading)

[https://openwrt.org/docs/guide-user/firewall/firewall\\_configuration](https://openwrt.org/docs/guide-user/firewall/firewall_configuration)

**SQM QoS (CAKE, fq\_codel) для контролю затримок і “bufferbloat”, налаштування і деталі**

<https://openwrt.org/docs/guide-user/network/traffic-shaping/sqm>

<https://openwrt.org/docs/guide-user/network/traffic-shaping/sqm-details>

[https://www.bufferbloat.net/projects/bloat/wiki/Getting\\_SQM\\_Running\\_Right/](https://www.bufferbloat.net/projects/bloat/wiki/Getting_SQM_Running_Right/)

#### **Firewall4, nftables, інструменти діагностики правил**

<https://openwrt.org/docs/guide->

[user/firewall/netfilter\\_iptables/netfilter\\_management](https://openwrt.org/docs/guide-user/firewall/netfilter_iptables/netfilter_management)

<https://openwrt.org/docs/guide-user/firewall/misc/nftables>

<https://github.com/openwrt/firewall4>

## **Інструменти вимірювання пропускної здатності (iperf3), параметри тестів**

<https://software.es.net/iperf/>

<https://github.com/esnet/iperf>

## **Захоплення трафіку для верифікації результатів (tcpdump, Wireshark)**

[https://openwrt.org/docs/guide-user/firewall/misc/tcpdump\\_wireshark](https://openwrt.org/docs/guide-user/firewall/misc/tcpdump_wireshark)

<https://openwrt.org/packages/pkgdata/tcpdump-mini>

## **Тюнінг та діагностика Ethernet інтерфейсів (ethtool)**

<https://openwrt.org/packages/pkgdata/ethtool>

## **Умови виконання**

Контрольна робота виконується на апаратно-програмному контрольному комплексі моделювання та дослідження складної розгалуженої мережевої інфраструктури з залученням серверу центру зберігання та обробки даних, що передбачено ресурсним забезпеченням кафедри КБПЗ ЦНТУ. При переході ЦНТУ у он-лайн навчання, формат взаємодії питати у викладача який проводить контрольну роботу.

Необхідне обладнання (погодити з викладачем який проводить контрольну роботу):

- Маршрутизатор який підтримує платформу OpenWrt;
- 2 хост-машини (генератор і приймач трафіку) або 1 хост + другий маршрутизатор;
- Програмне забезпечення: iperf3, ping, top/htop, collectd або прості логи, tc, ethtool, nftables/iptables;
- Засіб вимірювання споживання (для живлення 5/12V).

## **Завдання до контрольної роботи:**

Необхідно реалізувати та верифікувати на маршрутизаторі OpenWrt програмно технічні налаштування високошвидкісного мережевого тракту з урахуванням архітектури та взаємодії компонентів, щоб на підставі повторюваних вимірювань пропускної здатності, затримки і енергоефективності обґрунтувати оптимальний режим роботи мережевого рішення.

## **Покрокова реалізація контрольної роботи**

### **Підготовка**

1. Підготувати маршрутизатор з підтримкою OpenWrt та забезпечити адміністративний доступ (SSH або web інтерфейс).

2. Під'єднати два тестові хости до різних мережевих інтерфейсів маршрутизатора (На вибір LAN та WAN або LAN1 та LAN2 через VLAN), щоб трафік проходив транзитом через маршрутизатор.

3. Зафіксувати апаратні параметри стенда (модель роутера, CPU, RAM, тип і швидкість портів, версію OpenWrt, версію ядра).

### **Підготовка програмно-технічного середовища (базова конфігурація маршрутизації)**

4. Налаштувати дві IPv4 підмережі на різних інтерфейсах маршрутизатора, IP адреси тестових хостів (статично або через DHCP) у відповідних підмережах.

5. Перевірити взаємозв'язок (виконати ping між хостами через маршрутизатор).

6. Зафіксувати маршрутні таблиці на маршрутизаторі та на тестових хостах.

### **Формування базової точки відліку продуктивності**

7. Встановити та налаштувати інструменти вимірювань (iperf3 та інші).

8. Виконати серію вимірювань пропускної здатності для TCP та UDP (один потік, декілька паралельних потоків (щоб навантажити CPU, datapath)).

9. Виміряти затримку (ping) та jitter (для UDP).

10. Зафіксувати системні метрики маршрутизатора під час тестів (завантаження CPU, використання RAM, наявність softirq/irq навантаження).

11. Оформити результати як “базовий профіль” (Baseline), який буде використовуватись для порівняння.

### **Дослідження залежності продуктивності від параметрів трафіку**

12. Повторити вимірювання пропускної здатності з різними розмірами пакетів (для UDP) та різною кількістю потоків (для TCP і UDP), визначити режим, у якому маршрутизатор досягає максимальної пропускної здатності, та режим, у якому зростає затримка або спостерігається деградація. Зробити висновок, що є первинним обмеженням (пропускна здатність інтерфейсу, CPU маршрутизатора або налаштування програмного тракту).

### **Реалізація оптимізаційних сценаріїв**

13. Реалізувати **не менше трьох** оптимізаційних змін конфігурації (окремими сценаріями), наприклад:

- включення flow offload (software або hardware);
- зміна політик firewall, що впливають на fast path;
- налаштування або зміна режиму SQM;
- тюнінг MTU або MSS clamping (за потреби для TCP);
- вимкнення або оптимізація сервісів, що створюють додаткове навантаження.

14. Після кожної оптимізації повторити весь набір вимірювань із пунктів «Формування базової точки відліку продуктивності кроки 7-11» та «Дослідження залежності продуктивності від параметрів трафіку крок 12». Для кожного сценарію зафіксувати, які саме параметри були змінені, і додати коротке технічне обґрунтування.

### **Вимірювання енергоспоживання та розрахунок енергоефективності**

15. Виміряти споживану потужність маршрутизатора у стані простою (Idle) та під навантаженням (для Baseline і для кожного оптимізованого сценарію). Розрахувати показники енергоефективності: пропускна здатність на ват (Gbps/W); енергія на 1 ГБ переданих даних (J/GB). Порівняти сценарії за “продуктивність-енергоефективність” і визначити оптимальний набір налаштувань.

## **Оформлення звіту**

У звіт контрольної роботи помістити:

- Завдання л/роботи.
- Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскрини, та інші матеріали для підтвердження виконання л/роботи):
  - Зберегти конфігурації OpenWrt (мінімум /etc/config/network, /etc/config/firewall, /etc/config/sqm або інші, що змінювались).
  - Додати файл протоколу експериментів (послідовність команд, параметри запуску іperf3, час вимірювань, умови тестування).
  - Підсумкова таблиця з результатами Baseline та всіх оптимізаційних сценаріїв.
  - сформулювати інженерний висновок у вигляді рекомендацій (які налаштування доцільно застосовувати для високошвидкісного режиму з урахуванням енергоефективності.)

Контрольну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

## **Контрольні питання:**

1. Чому throughput може впирається в CPU навіть за 1 Gbps порту?
2. Як flow offload впливає на firewall і QoS, які ризики?
3. Чому SQM може зменшувати пропускну здатність, але підвищувати якість сервісу?
4. Яка метрика енергоефективності коректніша для порівняння сценаріїв і чому?
5. Як змінюється продуктивність при різних розмірах пакета і кількості потоків?

## Контрольна робота №8

**Тема:** Масштабоване сегментування та розмежування трафіку в OpenWrt з залученням VLAN, DHCP, політики Firewall та міжсегментної маршрутизації

**Мета:** Спроекувати і реалізувати багатосегментну мережу на OpenWrt з керованою адресацією та політиками доступу між VLAN, перевірити масштабованість і вплив правил безпеки на продуктивність.

**Знати:** VLAN, DHCP, L3 маршрутизація, stateful firewall

### Теоретичні відомості

У зв'язку з великим обсягом інформації використовувати електронну документацію (погоджувати з лектором).

#### Мережна конфігурація OpenWrt (UCI)

[https://openwrt.org/docs/guide-user/network/network\\_configuration](https://openwrt.org/docs/guide-user/network/network_configuration)

<https://openwrt.org/docs/guide-user/base-system/basic-networking>

#### VLAN та сегментація (DSA і класичний switch)

<https://openwrt.org/docs/guide-user/network/dsa/dsa-mini-tutorial>

<https://openwrt.org/docs/guide-user/network/dsa/convertng-to-dsa>

[https://openwrt.org/docs/guide-user/network/vlan/switch\\_configuration](https://openwrt.org/docs/guide-user/network/vlan/switch_configuration)

<https://openwrt.org/docs/techref/swconfig>

[https://openwrt.org/uk/docs/guide-user/network/vlan/creating\\_virtual\\_switches](https://openwrt.org/uk/docs/guide-user/network/vlan/creating_virtual_switches)

[https://openwrt.org/docs/guide-user/network/vlan/managed\\_switch](https://openwrt.org/docs/guide-user/network/vlan/managed_switch)

#### DHCP (dnsmasq, /etc/config/dhcp) для окремих VLAN

<https://openwrt.org/docs/guide-user/base-system/dhcp>

[https://openwrt.org/docs/guide-user/base-system/dhcp\\_configuration](https://openwrt.org/docs/guide-user/base-system/dhcp_configuration)

#### Firewall (fw4, nftables, зони та правила)

[https://openwrt.org/docs/guide-user/firewall/firewall\\_configuration](https://openwrt.org/docs/guide-user/firewall/firewall_configuration)

<https://openwrt.org/docs/guide-user/firewall/misc/nftables>

## **Верифікація та вимірювання впливу правил на продуктивність**

[https://openwrt.org/docs/guide-user/firewall/misc/tcpdump\\_wireshark](https://openwrt.org/docs/guide-user/firewall/misc/tcpdump_wireshark)

<https://software.es.net/iperf/>

<https://github.com/esnet/iperf>

### **Умови виконання контрольної роботи**

Контрольна робота виконується на апаратно-програмному контрольному комплексі моделювання та дослідження складної розгалуженої мережевої інфраструктури з залученням серверу центру зберігання та обробки даних, що передбачено ресурсним забезпеченням кафедри КБПЗ ЦНТУ. При переході ЦНТУ у он-лайн навчання, формат взаємодії питати у викладача який проводить контрольну роботу. Необхідне обладнання (погодити з викладачем який проводить контрольну роботу):

- Маршрутизатор який підтримує платформу OpenWrt;
- Комутатор з підтримкою VLAN;
- 2-4 клієнтські вузли;
- Програмне забезпечення: iperf3; ping; traceroute; tcpdump; Wireshark.

### **Завдання до контрольної роботи:**

Необхідно спроектувати та реалізувати на маршрутизаторі OpenWrt масштабовану багатосегментну мережу з VLAN, DHCP і політиками firewall для розмежування трафіку між сегментами, після чого верифікувати коректність доступів і оцінити вплив правил на продуктивність.

### **Покрокова реалізація контрольної роботи**

#### **Підготовка стенда та фіксація вихідних умов**

1. Підготувати маршрутизатор з OpenWrt та забезпечити адміністративний доступ (SSH або Web інтерфейс). Під'єднати маршрутизатор до комутатора, організувавши trunk порт для передачі декількох VLAN. Підготувати не менше двох клієнтських вузлів (фізичних або віртуальних) для підключення в різні VLAN.

2. Зафіксувати параметри середовища (модель обладнання, версію OpenWrt, тип конфігурації комутації (DSA чи інша), перелік портів, що використовуються).

### **Проектування логічної сегментації та адресного плану**

3. Необхідно визначити мінімум три сегменти (VLAN) як приклад:

- VLAN10 Admin;
- VLAN20 Users;
- VLAN30 IoT.

4. Призначити для кожного VLAN окрему IPv4 підмережу, адресу шлюзу, DHCP діапазон та (за потреби) DNS параметри. Оформити адресний план у вигляді таблиці “VLAN → Підмережа → Gateway → DHCP range → Призначення”.

### **Реалізація VLAN на рівні L2 у OpenWrt**

5. Налаштувати trunk інтерфейс між OpenWrt і комутатором для передачі трафіку. Налаштувати access порти для підключення клієнтів у відповідні VLAN. Створити логічні інтерфейси для VLAN у OpenWrt та прив’язати їх до відповідних мереж (network).

### **Налаштування L3 шлюзів і міжсегментної маршрутизації**

6. Призначити IP адресу шлюзу (gateway) на кожному VLAN інтерфейсі OpenWrt та перевірити, що клієнти у своїх VLAN бачать шлюз (ping до gateway). Також перевірити базову міжсегментну маршрутизацію (тимчасово дозволивши трафік для тесту або використавши контрольні правила).

### **Налаштування DHCP для кожного VLAN**

7. Увімкнути DHCP сервер для кожного VLAN, встановити діапазони видачі адрес, час оренди (lease time). Створити 2 статичні резервування DHCP (DHCP reservations) для визначених клієнтів. Перевірити коректність отримання параметрів DHCP на клієнтах (IP, gateway, DNS).

### **Проектування політик доступу та реалізація Firewall**

8. Сформувати матрицю доступів (хто куди може) для щонайменше таких вимог:

- Users → WAN дозволено.
- Users → Admin заборонено, окрім одного явно визначеного сервісу або хоста.

– IoT → LAN заборонено, → WAN дозволено з обмеженнями (мінімум за портами або за DNS).

– Admin → усі VLAN дозволено (адміністративний доступ).

Опціонально: дозволити лише необхідні сервісні протоколи (DNS, NTP) з “нижчих” сегментів.

9. Реалізувати політики у firewall OpenWrt через зони та правила. Увімкнути вибіркоче логування для мінімум одного критичного правила (block або allow) і обмежити інтенсивність логів, щоб не вплинути на продуктивність.

### **Верифікація коректності сегментації і політик**

10. Перевірити доступність сервісів згідно матриці доступів (ping, traceroute, доступ до конкретних портів). Виконати тести – спробувати заборонені напрямки і підтвердити блокування (за результатами тестів і логів). У результаті зафіксувати фактичні результати у вигляді таблиці “тест → очікування → факт”.

### **Перевірка масштабованості конфігурації**

11. Додати четвертий VLAN (наприклад VLAN40 Lab) за тим самим шаблоном (VLAN, інтерфейс, IP план, DHCP, зона/правила firewall). Порівняти, як збільшується кількість сутностей (інтерфейси, DHCP scope, правила) та сформулювати підхід, який зменшує складність при розширенні (зонування, шаблонні правила, групування підмереж).

### **Оцінювання впливу firewall політик на продуктивність**

12. Виконати вимірювання throughput між двома VLAN (iperf3) для двох режимів (“мінімальний firewall” (базові дозволи для роботи) та “посилений firewall” (з повним набором правил і логуванням). Зафіксувати latency (ping) та завантаження CPU маршрутизатора під час тестів. Зробити висновок, які правила або режими найбільше впливають на продуктивність і чому.

### **Оформлення артефактів та відтворюваність результату**

13. Необхідно зберегти конфігурації OpenWrt (/etc/config/network, /etc/config/dhcp, /etc/config/firewall). Додати адресний план і матрицю доступів у звіт та додати протокол тестів (команди, параметри, результати) та підсумкові висновки щодо масштабування і продуктивності.

## Оформлення звіту

У звіт контрольної роботи помістити:

- Завдання контрольної роботи.
- Покрокові матеріали що повністю підтверджують виконання л/роботи (текст, таблиці, принтскріни, та інші матеріали для підтвердження виконання л/роботи):
  - Зберегти конфігурації OpenWrt (мінімум /etc/config/network, /etc/config/firewall, /etc/config/sqm або інші, що змінювались).
  - Додати файл протоколу експериментів (послідовність команд, параметри запуску іperf3, час вимірювань, умови тестування).
  - Підсумкова таблиця з результатами Baseline та всіх оптимізаційних сценаріїв.
  - сформулювати інженерний висновок у вигляді рекомендацій (які налаштування доцільно застосовувати для високошвидкісного режиму з урахуванням енергоефективності.)

Контрольну роботу оформляти по загальноприйнятій формі (ДСТУ) та аналогічно до інших предметів кафедри КБПЗ ЦНТУ.

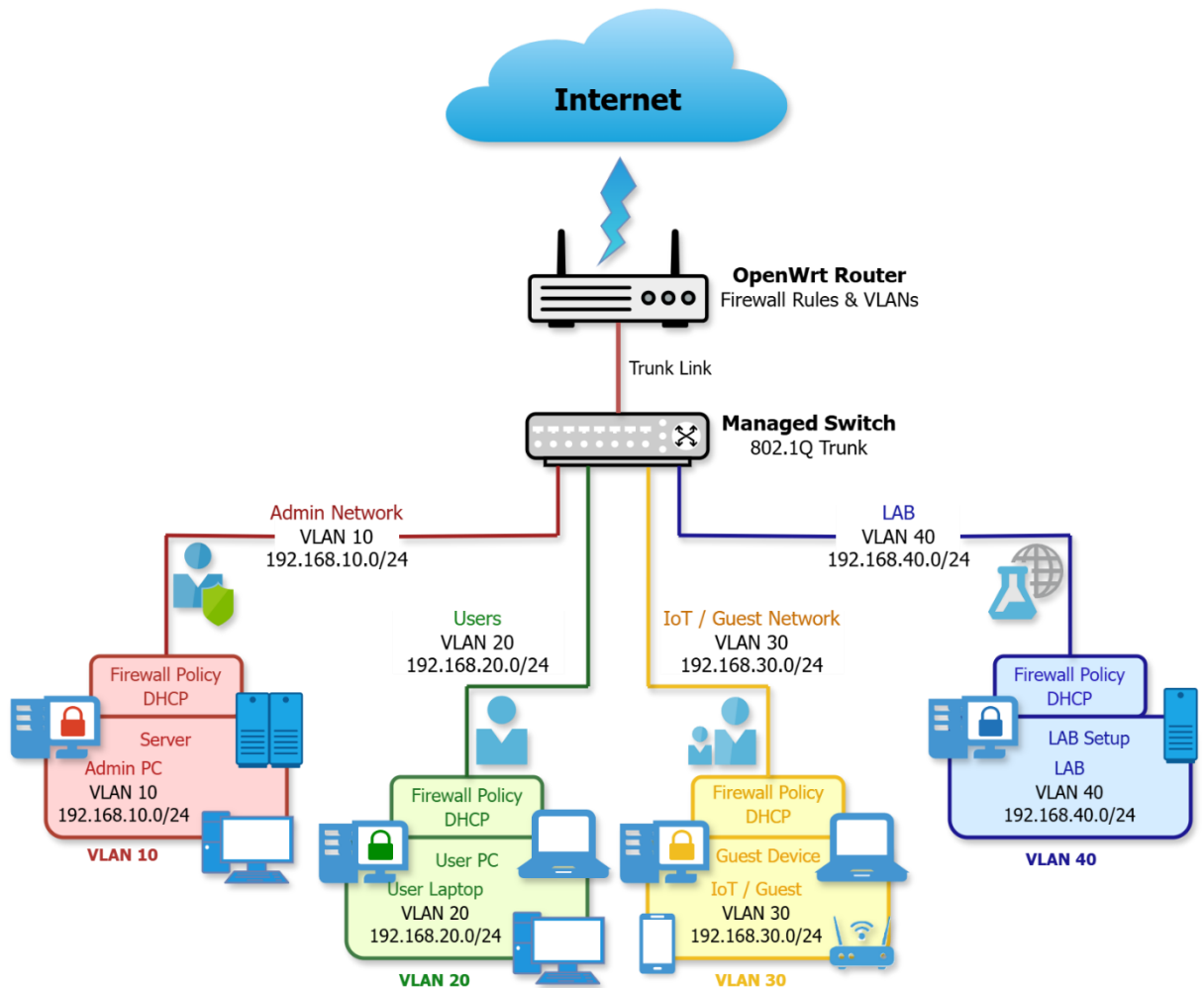


Рисунок 8.1 – Приклад реалізації

### Контрольні питання:

6. Чим L2 сегментація VLAN відрізняється від L3 сегментації і що краще для масштабування?
7. Як stateful firewall впливає на продуктивність при великій кількості потоків?
8. Які типові помилки при trunk/access конфігурації в OpenWrt і як їх діагностувати?
9. Як організувати політики доступу так, щоб їх було легко розширювати (додавання VLAN без “хаосу”)?
10. Чому окремі DHCP-політики важливі для ізольованих сегментів?

## Список використаної літератури

1. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/8855>
2. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/9799>
3. Смірнов О.А., Кавун С.В., Коваленко О.В., Дреєв О.М. Мережеві інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.
4. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.
5. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова Гриф “Навчальний посібник” надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 1.12.2011 року № 1/11-11258. – Кіровоград: КНТУ 2012. – 454 с.
6. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
7. Дослідження і проектування комп'ютерних систем та мереж: навч. посіб. / В.С. Глухов, А.Т. Костик; М-во освіти і науки України, Львівська політехніка. Львів: «Магнолія 2006». 2025. 253 с. Режим доступу: <https://opac.kntu.kr.ua/bib/8698>
8. Комп'ютерні мережі: підручник / Є.В. Буров – Львів: «Магнолія 2006». 2025 – 262 с. Режим доступу: <https://opac.kntu.kr.ua/bib/8692>
9. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
10. Комп'ютерні мережі. Підручник. Том другий /Є.В. Буров, М.М. Митник/ Львів: Видавництво ПП «Магнолія 2006», 2024. – 204 с.
11. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco: навчальний посібник. [Текст] / А.А. Єфіменко. – Житомир: Державний університет «Житомирська політехніка», 2021. – 116 с.

12. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс]: навч. посіб. / Б. Ю. Жураковський, І.О. Зенів; – Київ: КПІ ім. Ігоря Сікорського, 2020. – 336 с.
13. Комп'ютерні мережі: підручник / Азаров О.Д., Захарченко с.М., Кадук О.В., Орлова М.М., Тарасенко В.П. – Вінниця: ВНТУ. – 2020. – 378 с.
14. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків: ХНУМГ ім. О. М. Бекетова, 2019. – 99 с
15. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.
16. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осіпова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.
17. Оліфер В.Г. Комп'ютерні мережі. Принципи, технології, протоколи. Підручник / В.Г. Оліфер, Н.А.Оліфер. – 2020. – 467 с.
18. Е. Таненбаум, Д. Уезеролл «Комп'ютерні мережі». – [5-е вид.]. – 2016. – 960 с.
19. Wendell Odom. «CCNA 200-301 Official Cert Guide, Volume 1». Cisco Press. 2020. – 848 p.
20. Wendell Odom. «CCNA 200-301 Official Cert Guide, Volume 2 Premium Edition eBook and Practice Test». Cisco Press. 2020. – 624 p.
21. Scott Jernigan «CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition». 2022. – 976 p.
22. Doug Lowe «Networking For Dummies 12th Edition». 2020. – 480 p.
23. Ramon Nastase «Computer Networking: The Beginner's guide for Mastering Computer Networking, the Internet and the OSI Model». 2018. – 186 p.
24. Russ White & Ethan Banks «Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient, Modern Networks». 2017. – 832 p.
25. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105014300075>
26. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105014301897>
27. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.

- <https://doi.org/10.15866/iremos.v18i1.25596> (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-105008769373&origin=recordpage>
28. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241. Available: [https://ceur-ws.org/Vol-3909/#Paper\\_18.pdf](https://ceur-ws.org/Vol-3909/#Paper_18.pdf) (Scopus). Режим доступу: <https://www.scopus.com/pages/publications/85217281478>
  29. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402. DOI: 10.1201/9781003457428-16. (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85201885928&origin=resultslst>
  30. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447. DOI: 10.1201/9781003457428-17 (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85201858596&origin=resultslst>
  31. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56 (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85176960353&origin=resultslst>
  32. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265. (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85176927818&origin=resultslst>
  33. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223. (Scopus). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85162950840&origin=resultslst&sort=plf-f>
  34. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications*

- Technologies*, vol 131. 2024. **Springer**, Singapore. pp. 21-34. (**Scopus**). Режим доступу: [https://www.scopus.com/record/display.uri?eid=2-s2.0-85134768958&origin=resultslist&sort=plf-f&featureToggles=FEATURE\\_NEW\\_DOC\\_DETAILS\\_EXPORT:1,FEATURE\\_EXPORT\\_REDESIGN:1](https://www.scopus.com/record/display.uri?eid=2-s2.0-85134768958&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1,FEATURE_EXPORT_REDESIGN:1)
35. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346. (**Scopus**). Режим доступу: [https://www.scopus.com/record/display.uri?eid=2-s2.0-85096438117&origin=SingleRecordEmailAlert&dgcid=raven\\_sc\\_author\\_ru\\_email&txGid=1e91df71a9e62824506812d4d2f72e33](https://www.scopus.com/record/display.uri?eid=2-s2.0-85096438117&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_email&txGid=1e91df71a9e62824506812d4d2f72e33)
36. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379. (**Scopus**). Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85086304936&origin=resultslist&sort=plf-f&src=s&sid=4f00231d7103e01bb1909823c51f297e&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm>
37. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), с. 6-27. Режим доступу: <https://doi.org/10.28925/2663-4023.2024.24.627>  
<https://csecurity.kubg.edu.ua/index.php/journal/article/view/588> (Фахове видання. Категорія «Б»)
38. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35. Режим доступу: <https://doi.org/10.32347/uwt.2023.13.1203>, <http://uwtech.knuba.edu.ua/article/view/298874> (Фахове видання. Категорія «Б»)
39. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, с. 49-56. Режим доступу: <https://doi.org/10.20998/2522-9052.2023.2.07> (Фахове видання. Категорія «Б»)
40. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. с. 79-95 Режим доступу: <http://ais.khpi.edu.ua/article/view/247293> (Фахове видання. Категорія «Б»)
41. Смірнов, О.А., Усік П.С., Полігенько О.О., Одарченко Р.С., Терещенко Л.Ю. «Інформаційна технологія та програмне забезпечення для підвищення ефективності планування підсистеми базових станцій

стільникового зв'язку». *Проблеми телекомунікацій*. № 1(26). с. 83-96. 2020. Режим доступу: <https://pt.nure.ua/articles/informacijna-tehnologiya-ta-programne-zabezpechennya-dlya-pidvishhennya-efektivnosti-planuvannya-pidsistemi-bazovih-stancij-stilnikovogo-zv-yazku/> **Фахове видання.**

**Категорія «Б»**

42. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки*. №4. с. 103-110. 2020. Режим доступу: <https://er.chdtu.edu.ua/handle/ChSTU/1890> . **(Фахове видання. Категорія «Б»)**
43. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кибербезпека: освіта, наука, техніка*. № 3(7). с. 43-62. 2020. Режим доступу: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/132/132> **(Фахове видання. Категорія «Б»)**
44. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». *Центральноукраїнський науковий вісник. Технічні науки*. № 2(33). с. 161-172, 2019.
45. Дреєва Г.М., Смірнов О.А., Дреєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. *Центральноукраїнський науковий вісник. Технічні науки*. № 1(32). с. 173-183, 2019. Режим доступу: [http://nbuv.gov.ua/j-pdf/znpkntu\\_2019\\_1\\_22.pdf](http://nbuv.gov.ua/j-pdf/znpkntu_2019_1_22.pdf)