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 лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та програмного забезпечення, протокол № 1 від 15.08.2022

Кропивницький
2023

Проектування комп’ютерних систем та мереж: Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2023. – 49 с./М-во освіти і науки України, Центральноукр. нац. техн. ун-т; /уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А. / – Кропивницький: ЦНТУ – 2023. – 49 с.

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

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

ЗМІСТ

ВСТУП……..……4

Лабораторна робота №1. Створення проекту комп'ютерної мережі ……..9

Лабораторна робота №2. Проектування схеми IP-адресації……..…15

Лабораторна робота №3. Проектування безкласової IP-адресації…….…21

Лабораторна робота №4. Маршрутизація й аналіз пропускної здатності мережі……..…24

Лабораторна робота №5. Планування списків доступу і фільтрів портів……..……33

Лабораторна робота №6-7. Збирання мережевих даних……..……...36

ВСТУП

Метою освітньої компоненти «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.

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій магістра з комп'ютерної інженерії**:

– СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

– СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

– СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.

– СК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.

– СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

– СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.

У результаті вивчення дисципліни студент повинен забезпечити наступні **програмні результати навчання:**

– РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.

– РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії,

необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

– РН5. Розробляти і реалізовувати проекти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проекти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

– РН9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

– РН10. Здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії, аналізувати та оцінювати цю інформацію.

– РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

У результаті вивчення навчальної дисципліни студент повинен:

– знати: основи організації мереж; технології фізичного рівня; мережна адресація; типи адрес стеку TCP/IP; адресація в корпоративній мережі. плоскі й ієрархічні мережі; статичні та динамічні IP-адреси; мережні адреси NAT та PAT; фільтрація трафіку з використанням списків контролю доступу; розміщення стандартних і розширених ACL-списків; комутація мережі; VLAN і протокол VTP; технології розумних, мобільних, зелених і безпечних обчислень з застосуванням комп'ютерних систем та мереж; бездротові технології й пристрої; забезпечення безпеки бездротових мереж; усунення проблем з мережами; планування відновлення мережі.

– вміти програмно реалізовувати наступні проекти: Створення проекту комп'ютерної мережі; Проектування схеми IP-адресації; Проектування безкласової IP-адресації; Маршрутизація й аналіз пропускної здатності мережі; Планування списків доступу і фільтрів портів; Збирання мережевих даних.

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, С) 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

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90-100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>1-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Лабораторна робота №1

Створення проекту комп'ютерної мережі

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

Теоретична частина

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

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

– *парапетні короби* – 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^{2}приймаються 0,07 м^2 для серверної. Мінімальна площа апаратної приймається 14 м^2.

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-К01:

– першаі 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

Характеристики кабельних сегментів

№	Стандарт	Швидкість передачі даних	Тип кабелю, що використовується	Максимальна довжина сегменту
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 лабораторної 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. 2).

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).

Таблиця 2 Вхідні 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				

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 номера 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, номера кімнати й ім'я комп'ютера. Приклад кабельного журналу представлено в табл. 3.

Таблиця 3 Приклад кабельного журналу*

№ п/п	Назва пристрою	№ порту	№ розетки	Ім’я комп’ютера	№ кімнати
1.	КМ01	01	01-01-К01	01-01-01	01
		02	01-01-К02	01-01-02	
		03	01-01-К03	01-01-03	
2.	КМ02	01	01-01-Т01	01-01-01	
		02	01-01-Т02	01-01-02	
		03	01-01-Т03	01-01-03	
3.	КМ03	01	01-02-К04	01-02-04	02
		02	01-02-К05	01-02-05	
		03	01-02-К06	01-02-06	
		04	01-02-К07	01-02-07	
4.	КМ04	01	01-02-Т04	01-02-04	
		02	01-02-Т05	01-02-05	
		03	01-02-Т06	01-02-06	
		04	01-02-Т07	01-02-07	
5.	МР01	01	01-05-К36	01-05-36	03

* умовні позначення: КМ – комутатор, МР - 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?

Лабораторна робота №2

Проектування схеми IP-адресації

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

Теоретична частина

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 A – мережа 10.0.0.0;
- у класі B – діапазон з 16 мереж – 172.16.0.0-172.31.0.0;
- у класі C – 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. 1 представлений 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.

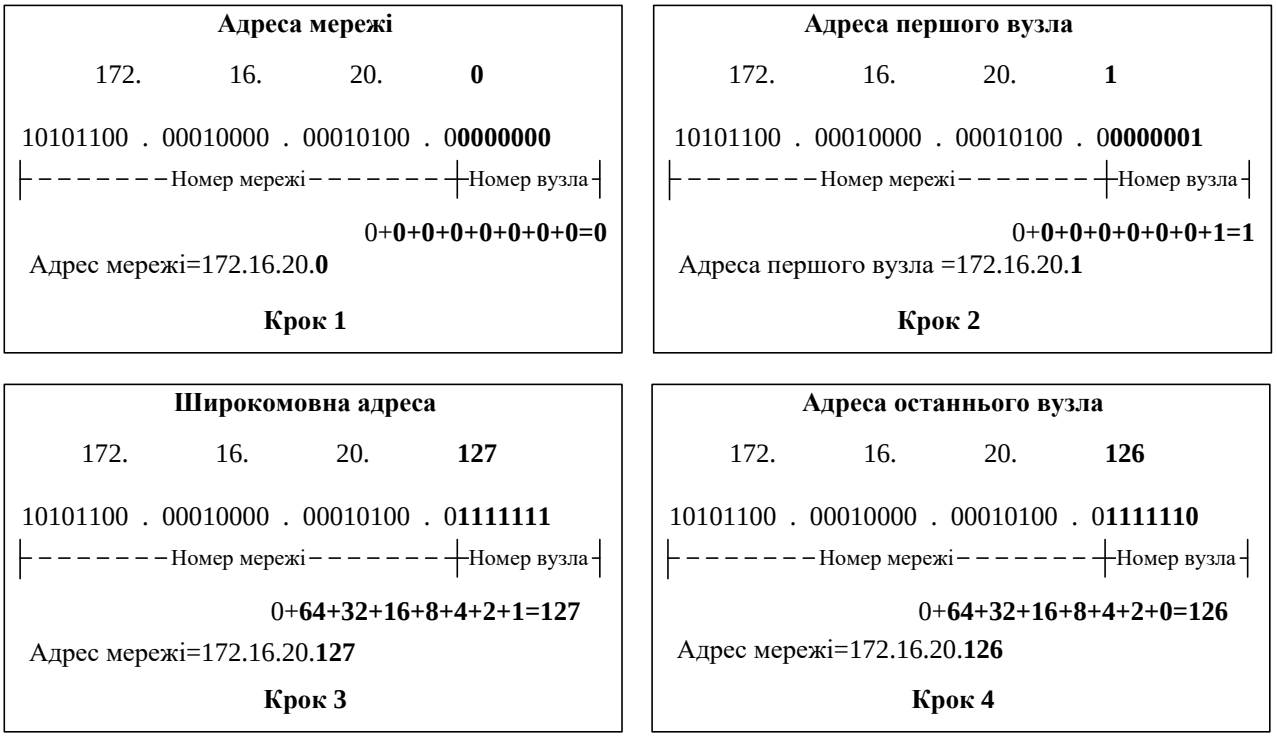


Рисунок 1 – Приклад IP-адресації

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 лабораторної 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.

Таблиця 1. 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 лабораторної 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).

Таблиця 2. Зразок таблиці

Номер підмере-жі	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.

Лабораторна робота №3

Проектування безкласової IP-адресації

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

Завдання до лабораторної 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 широкомовних 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 пласких 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?

Лабораторна робота №4

Маршрутизація й аналіз пропускної здатності мережі

Мета: навчитися розробляти алгоритми маршрутизації

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 розрізняти 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 $d(x_i)$.

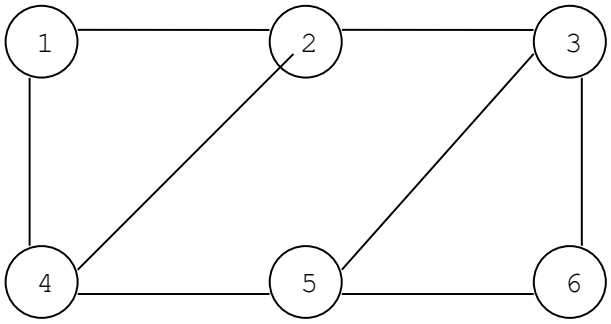
6. Встановимо $z(x_k)=1$, $P= x_k$.

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.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 1 – Приклад розрахунку найкоротших відстаней між вузлами комп’ютерної мережі

Визначення значень елементів маршрутної таблиці

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

$$M_{ij}=k, \quad \text{якщо} \quad a_{ij}= l_{ik}+ a_{kj} \qquad (1)$$

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 (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 (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.2 наведений приклад маршрутної таблиці для мережі представленої на рис.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 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 і 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.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 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}.

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

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

Rmin=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:

$$Rmax=C*N/SUM(q_{ij})$$

Де N – число каналів.

Для розглянутого прикладу: Rmax=50*8/46=8,7

Завдання до лабораторної 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:

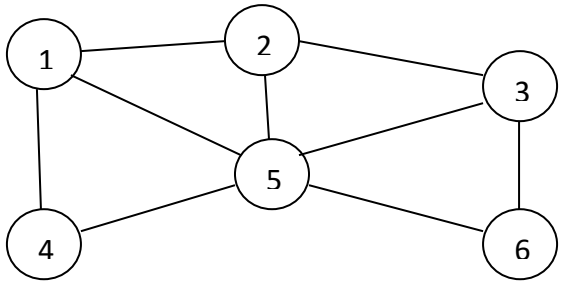
– моделювання комп’ютерної мережі у вигляді довільного графа (що генерується випадковим чином, або задається вручну),

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

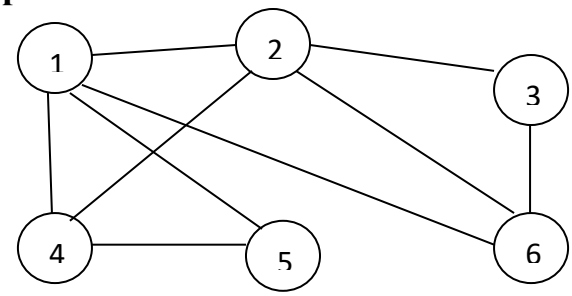
– реалізувати визначення матриці маршрутів і матриці потоків.

– реалізувати розрахунок нижньої та верхньої границі рівня трафіку.

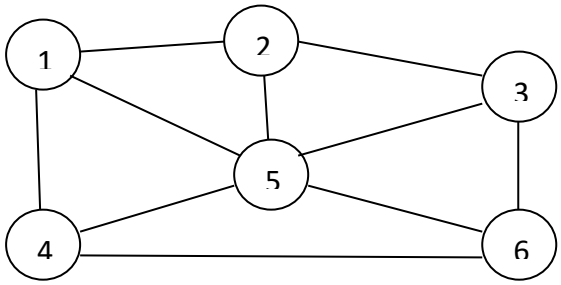
Варіант 1



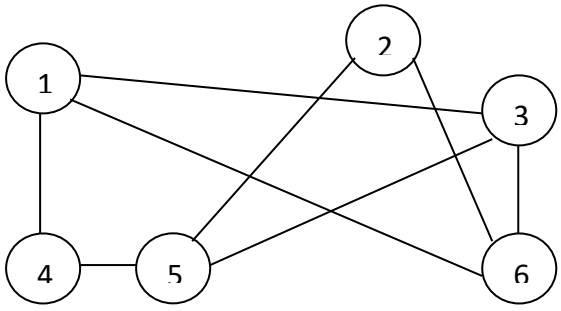
Варіант 2



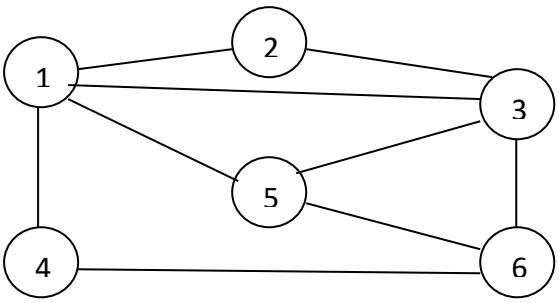
Варіант 3



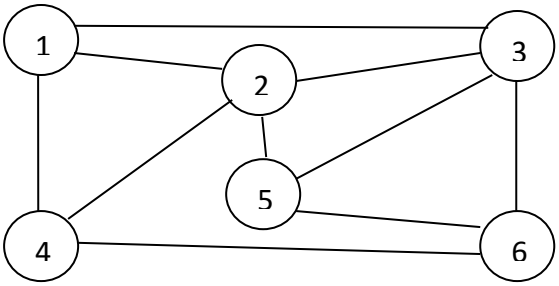
Варіант 4



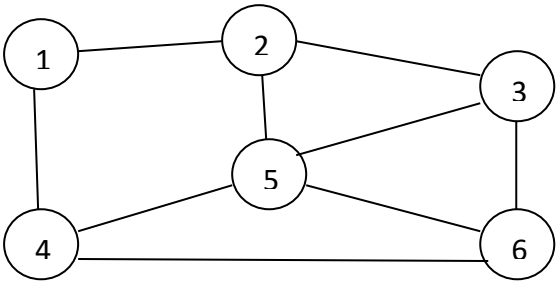
Варіант 5



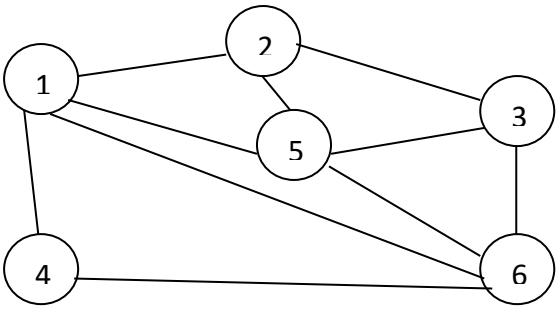
Варіант 6



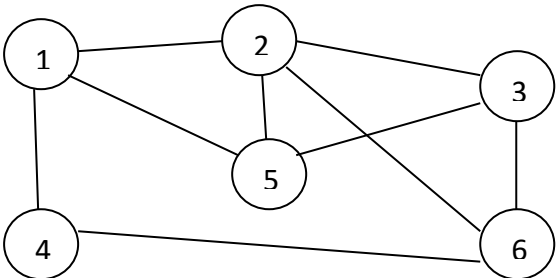
Варіант 7



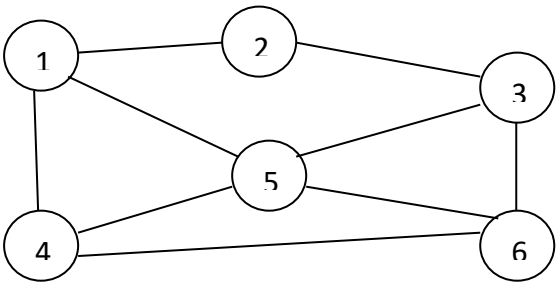
Варіант 8



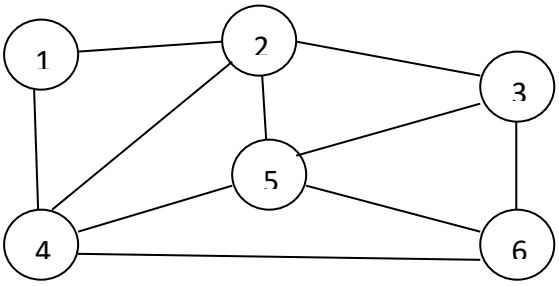
Варіант 9



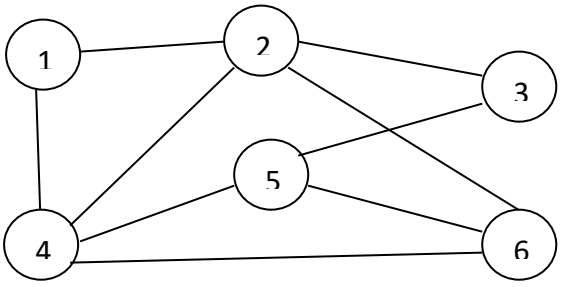
Варіант 10



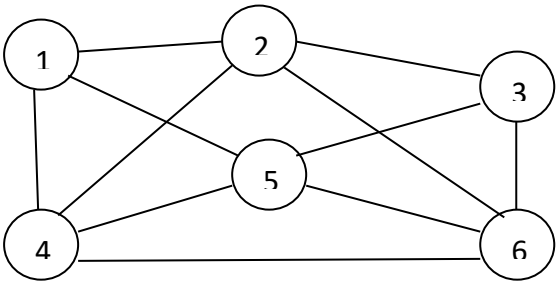
Варіант 11



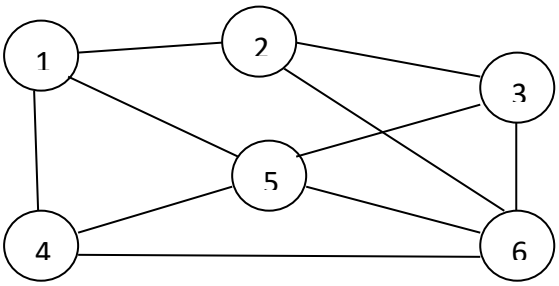
Варіант 12



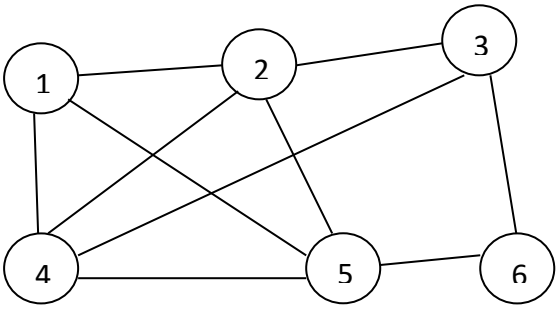
Варіант 13



Варіант 14



Варіант 15



Лабораторна робота №5

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.

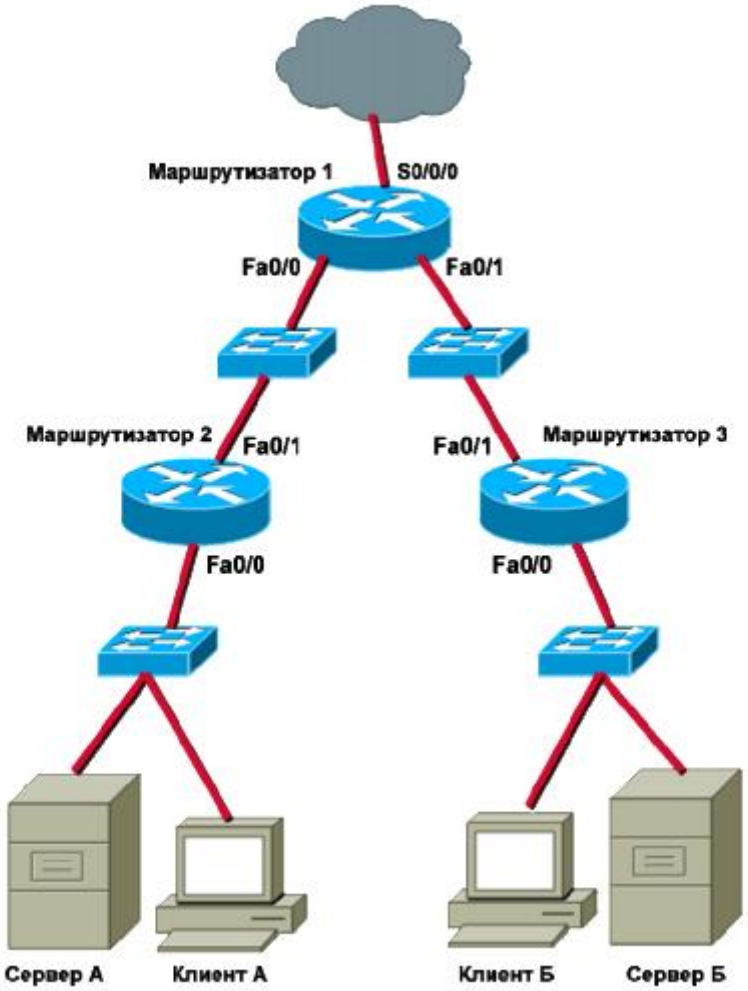


Рисунок 1 – Схема мережі корпоративного клієнта

Завдання до лабораторної 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 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?

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

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?

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

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 доступ 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?

Лабораторна робота №6-7

Збирання мережевих даних

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 лабораторній 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 лабораторії, або вдома на ПК. Вам він знадобитися 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.

Для виконання лабораторної роботи потрібні наступні ресурси:

• ПК під управлінням ОС Windows з мережею Ethernet і хоча б двома вузлами;

• програма Wireshark (версія 0.99.5 або остання версія);

• підключення до мережі Інтернет (не обов'язково, але бажано);

• доступ до командного рядка ПК;

• доступ до мережевої конфігурації TCP/IP ПК.

Завдання до лабораторної 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. 1).

Рисунок 1

1) Натисніть кнопку I Agree (прийняти) (рис. 2).

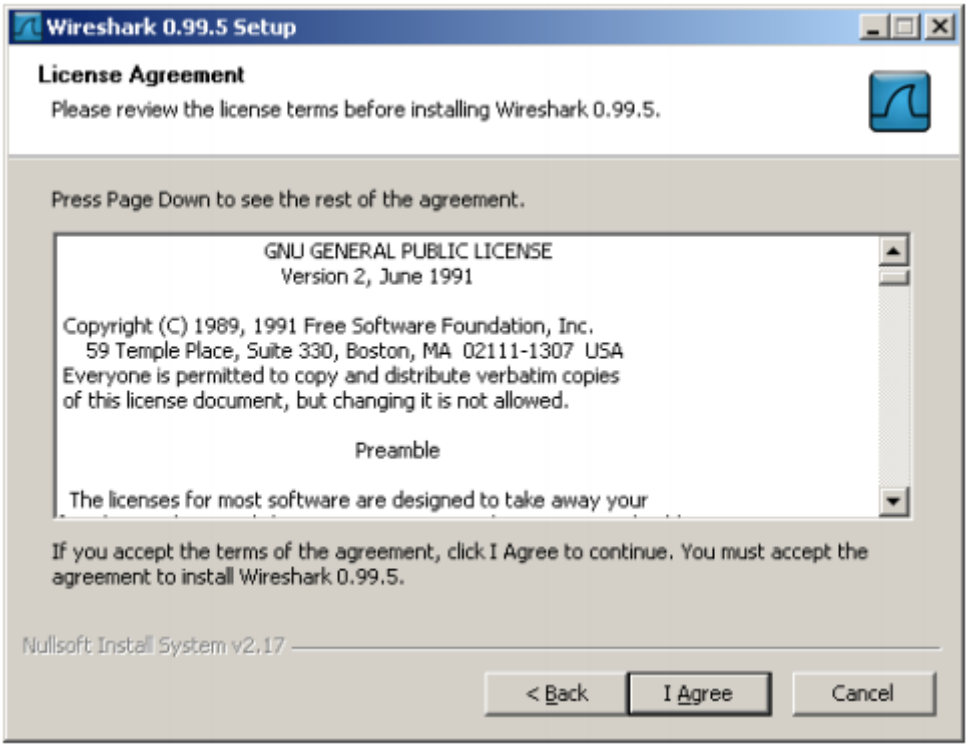


Рисунок 2

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. 3).

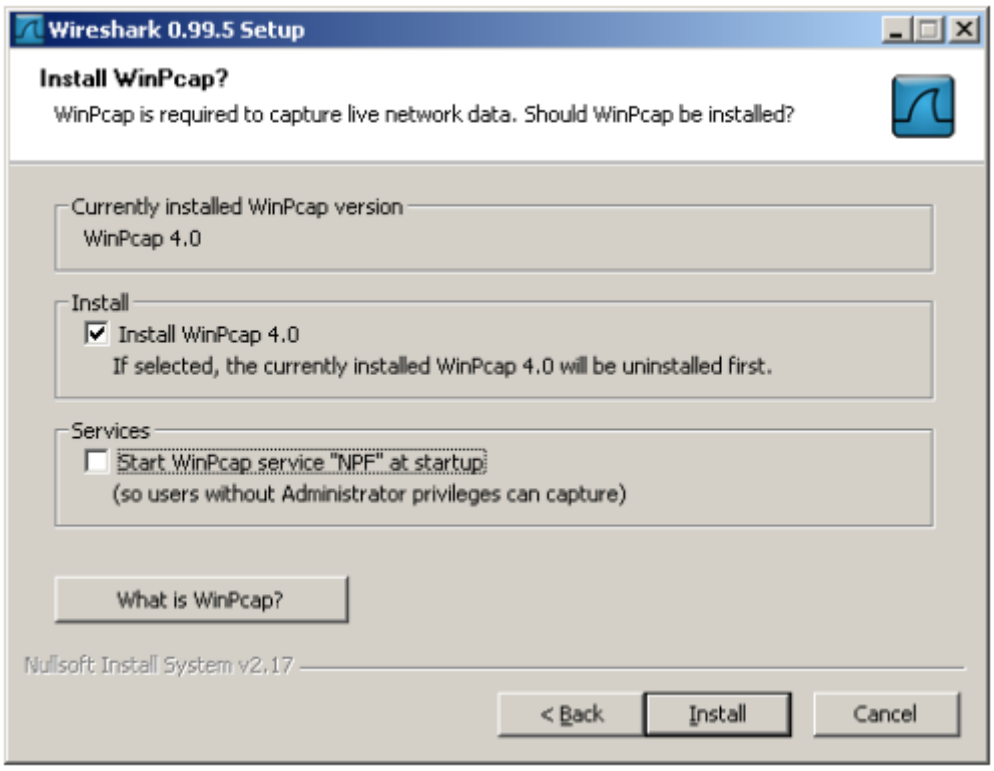


Рисунок 3

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. 4).

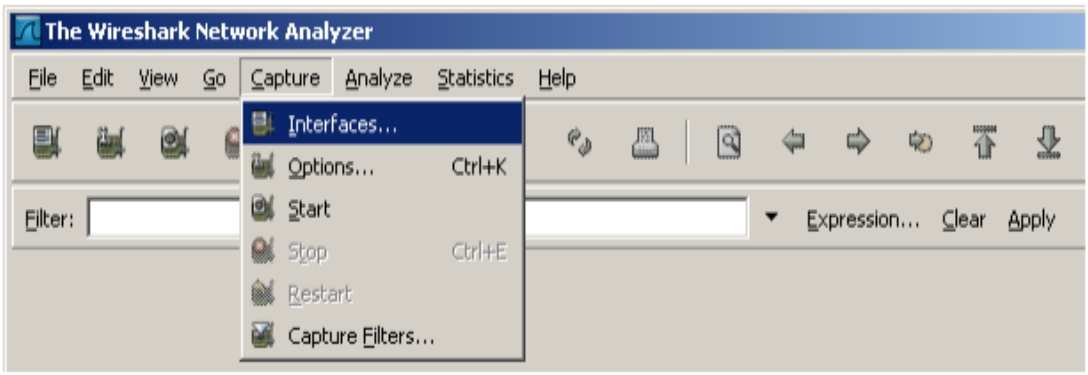


Рисунок 4

3) Натисніть кнопку Start (пуск) для інтерфейсу Ethernet (NIC), який потрібно використовувати для збору мережевого трафіку (рис. 5).

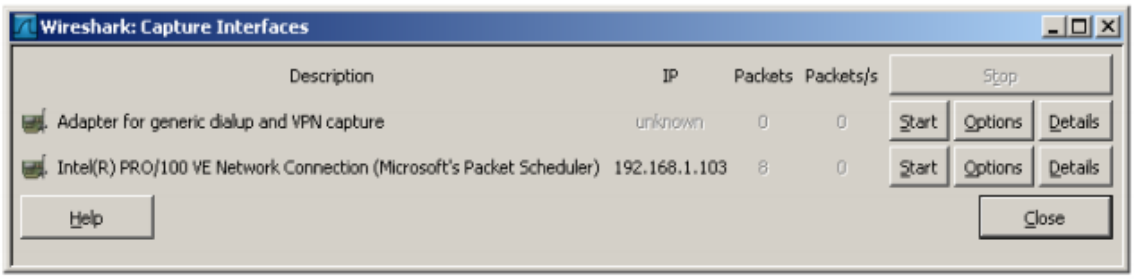


Рисунок 5

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).

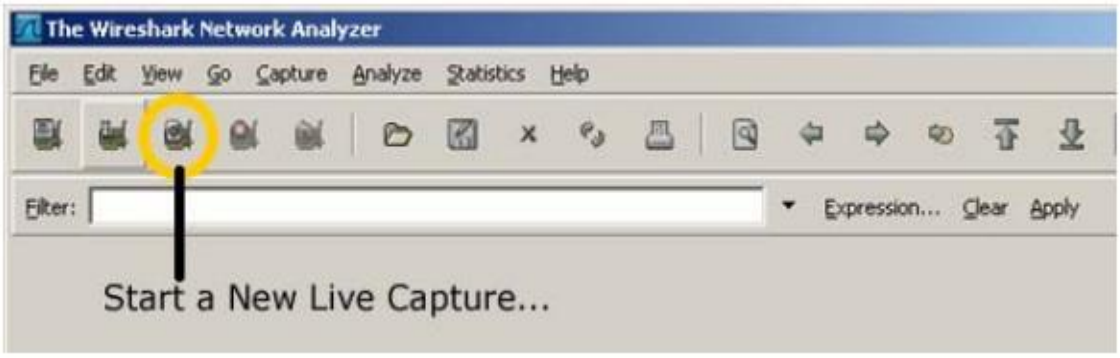


Рисунок 6

Крок 4. Аналіз відомостей про веб-трафіку

А. Якщо існує підключення до мережі Інтернет, відкрийте веб-браузер і перейдіть у вузол www.google.com. 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. 7).

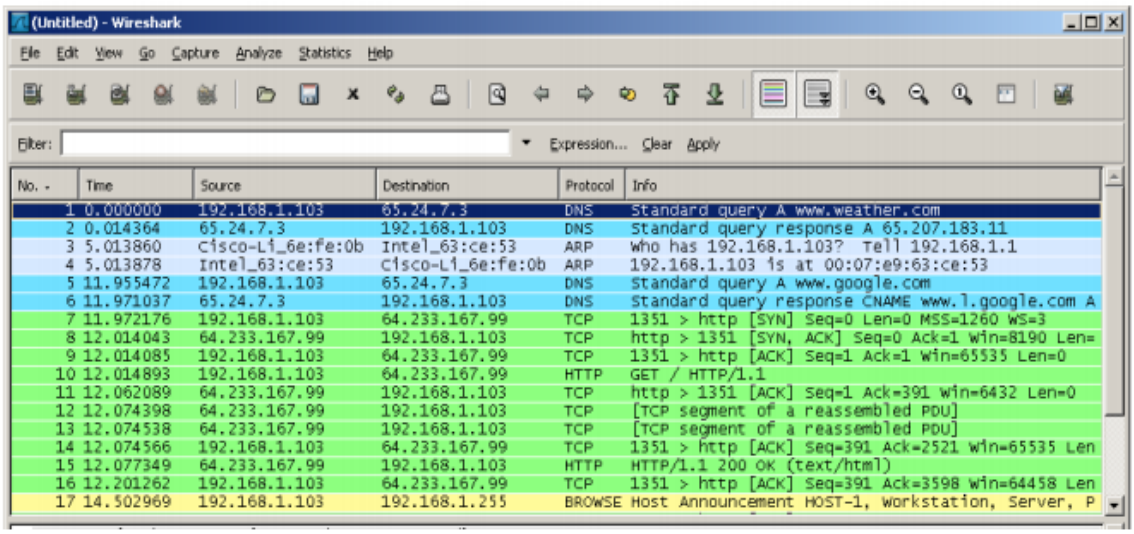


Рисунок 7

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.

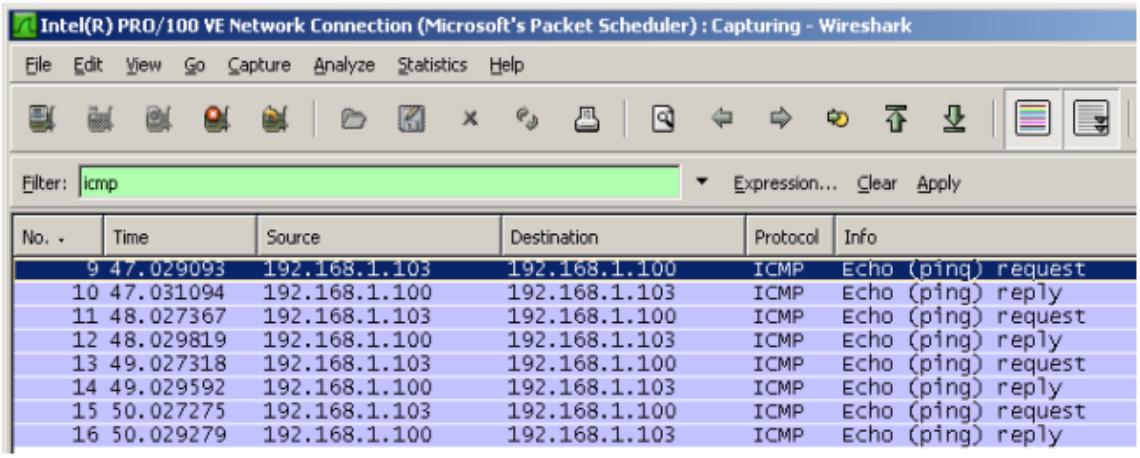


Рисунок 8

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 лабораторної 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 icmp в текстове поле Filter (фільтр)?

Список використаної літератури

1. Смірнов О.А., Конопліцька-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., Конопліцька-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., Дрєєв 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., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

5. Смірнов О.А., Євсеєв 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. 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.

8. Карпенко М. Ю. Конспект лекцій з курсу «Комп’ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп’ютерні науки, 151 – Автоматизація та комп’ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / 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

9. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп’ютерні мережі Видавництво: ВНТУ. 2013 – 374 с.

10. Комп’ютерні мережі : навчальний посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів : «Магнолія 2006», 2013. – 256 с.

11. Оліфер В.Г. Комп'ютерні мережі. Принципи, технології, протоколи. Підручник / В.Г. Оліфер, Н.А.Оліфер. – [5-е вид.]. – 2016. – 944 с.

12. Е. Таненбаум, Д. Уезеролл «Комп'ютерні мережі». – [5-е вид.]. – 2016. – 960 с.

13. Wendell Odom. «CCNA 200-301 Official Cert Guide, Volume 1». Cisco Press. 2020. – 848 p.

14. Wendell Odom. «CCNA 200-301 Official Cert Guide, Volume 2 Premium Edition eBook and Practice Test». Cisco Press. 2020. – 624 p.

15. Scott Jernigan «CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition». 2022. – 976 p.

16. Doug Lowe «Networking For Dummies 12th Edition». 2020. – 480 p.

17. Ramon Nastase «Computer Networking: The Beginner’s guide for Mastering Computer Networking, the Internet and the OSI Model». 2018. – 186 p.

18. Russ White & Ethan Banks «Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient, Modern Networks». 2017. – 832 p.

Допоміжна

19. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation 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. 2023. **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

20. 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_ru_email&txGid=1e91df71a9e62824506812d4d2f72e33

21. 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

22. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85085505335&origin=resultslist&sort=plf-f&src=s&sid=34535eee1c1d23f4f421db6a0c97e825&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm

23. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8 – 11 October 2019. P.597-601. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083682122&origin=resultslist&sort=plf-f&src=s&sid=2b6a0139fad18bb19a964441b5bded76&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm

24. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryho renko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931997&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

25. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352. **(Scopus)**. Режим

доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931008&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm

26. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-84938096221&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=6&citeCnt=33&searchTerm

27. 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»)**

28. 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»**

29. 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»)**

30. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: 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»)**

31. Смірнов О.А., Дрєєва Г.М., Дрєєв 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.

32. Дрєєва Г.М., Смірнов О.А., Дрєєв 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

33. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

34. Смирнов А.А., Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности. Безпека інформації. –Том 21, №1. – К.: НАУ – 2015. – С. 22-28. Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2015_21_1_5

35. Смирнов А.А., Мохамад Абу Таам Гани, Якименко Н.С., Смирнов С.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам. Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/4298