Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра програмування та захисту інформації

Проектування комп’ютерних систем та мереж

Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання за спеціальністю 123 “Комп’ютерна інженерія”

ЗАТВЕРДЖЕНО
на засіданні кафедри програмування та захисту інформації,
протокол № 11 від 21 грудня 2016 р.

Кропивницький
2016

Проектування комп’ютерних систем та мереж: методичні вказівки до виконання лабораторних робіт для студентів за спеціальністю. 123 “Комп’ютерна інженерія / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; [уклад. О. А. Смірнов, О. К. Конопліцька-Слободенюк] – Кропивницький: ЦНТУ, 2016. – 63 с.

Укладачі: Смірнов О. А., д-р техн. наук, професор;
Конопліцька-Слободенюк О. К., викладач.

Рецензенти: Сидоренко В. В., д-р техн. наук, професор;
Доренський О. П., канд. техн. наук.

ЗМІСТ

ВСТУП

Мета дисципліни – вивчення методології та засобів проектування комп'ютерних систем, отримання навиків моделювання комп'ютерних систем та мереж.

Методи навчання та інформаційно-методичне забезпечення

Заняття проводяться у формі лекцій та лабораторних занять. На лекціях викладається основний теоретичний матеріал. На практичних заняттях студенти навчаються застосовувати теорію до розв'язання задач. Навички, одержані студентами на заняттях, використовуються ними при розв'язанні завдань модульних контрольних робот. Засвоєння навчального матеріалу контролюється за допомогою контрольних робіт та семестрових іспитів. Щотижня надаються консультації.

Зміст дисципліни

1. Загальні принципи проектування комп'ютерних систем та мереж.
2. Проектування глобальних комп'ютерних мереж.
3. Проектування корпоративних мереж.

В методичних вказівках представлено теоретичний і практичний матеріал для роботи з комп'ютерними мережами.

Форма підсумкового контролю: іспит.

Максимальну кількість балів студент може одержати у випадку відвідування всіх лекцій, лабораторних занять, виконання і захисту виконаних самостійних завдань у встановлений термін, проходження контролю.

В якості самостійного завдання необхідно виконати теоретичну роботу, згідно обраної студентом теми.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену
90 – 100	**A**	відмінно
82-89	**B**	добре
74-81	**C**	
64-73	**D**	задовільно
60-63	**E**	
35-59	**FX**	незадовільно з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни

Вибравши предметну область, над якою ви будете працювати, ви повинні виконати завдання до лабораторних робіт, а також відповісти на питання в кінці кожної лабораторної роботи. Звіт повинен містити хід виконання завдань а також графічні матеріали, що підтверджують виконання цих завдань.

Лабораторна робота №1

Тема: 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:

–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 – 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

Тема: 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.

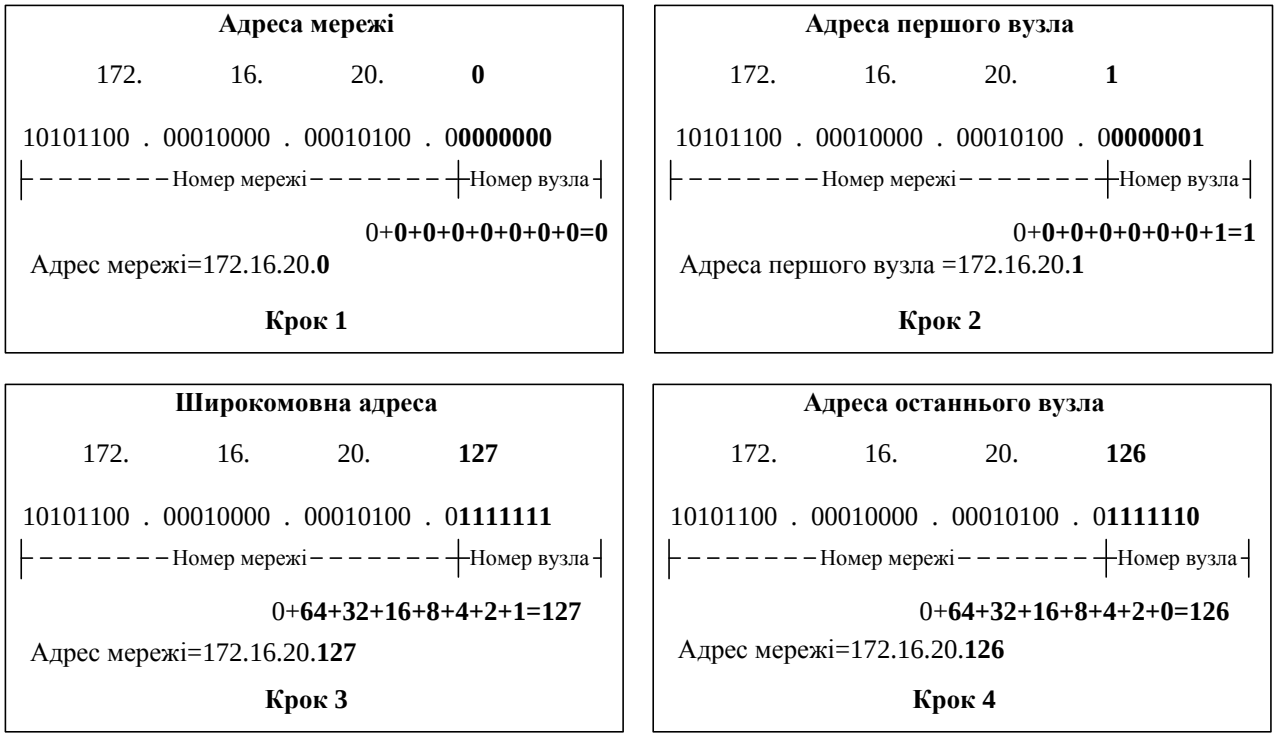


Рисунок 1 – Приклад IP-адресації

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:

1. Визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня;

2. Для кожної підмережі призначити: IP-адресу, маску підмережі, адресу широкомовного запиту;

3. Призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня;

4. У рамках підмереж для робочих станцій призначити початкову та кінцеву IP-адреси;

5. Розрахувати максимальну кількість вузлів кожної підмережі.

Результат розрахунків оформити у вигляді таблиці (див. табл.2).

Таблиця 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.

Лабораторна робота №3

Тема: Проектування безкласової IP-адресації

Мета: набути навичок для створення їєрархічної IP-адресації у великих корпоративних мережах

Теоретична частина

Впровадження комутаторів дозволяє зменшити число колізій у локальній мережі. Однак при використанні повністю комутованої мережі часто створюється єдиний домен широкомовного розсилання. У єдиному домені широкомовного розсилання (плоскій мережі) всі пристрої розташовані в одній і тій же мережі й одержують всі розсилання. У невеликих мережах використання єдиного домену широкомовного розсилання прийнятне.

При використанні великої кількості вузлів плоска мережа стає менш ефективною. У міру збільшення числа вузлів комутованій мережі збільшується число переданих і одержуваних широкомовних розсилань. Пакети широкомовних розсилань займають більшу частину смуги пропускання, що призводить до затримок при передачі трафіку і тайм-аутів.

Одне з рішень проблем великих плоских мереж – створення мереж VLAN. Мережа VLAN є власним доменом широкомовного розсилання.

Інше рішення – реалізація ієрархічної мережі з використанням маршрутизаторів (рис. 1).

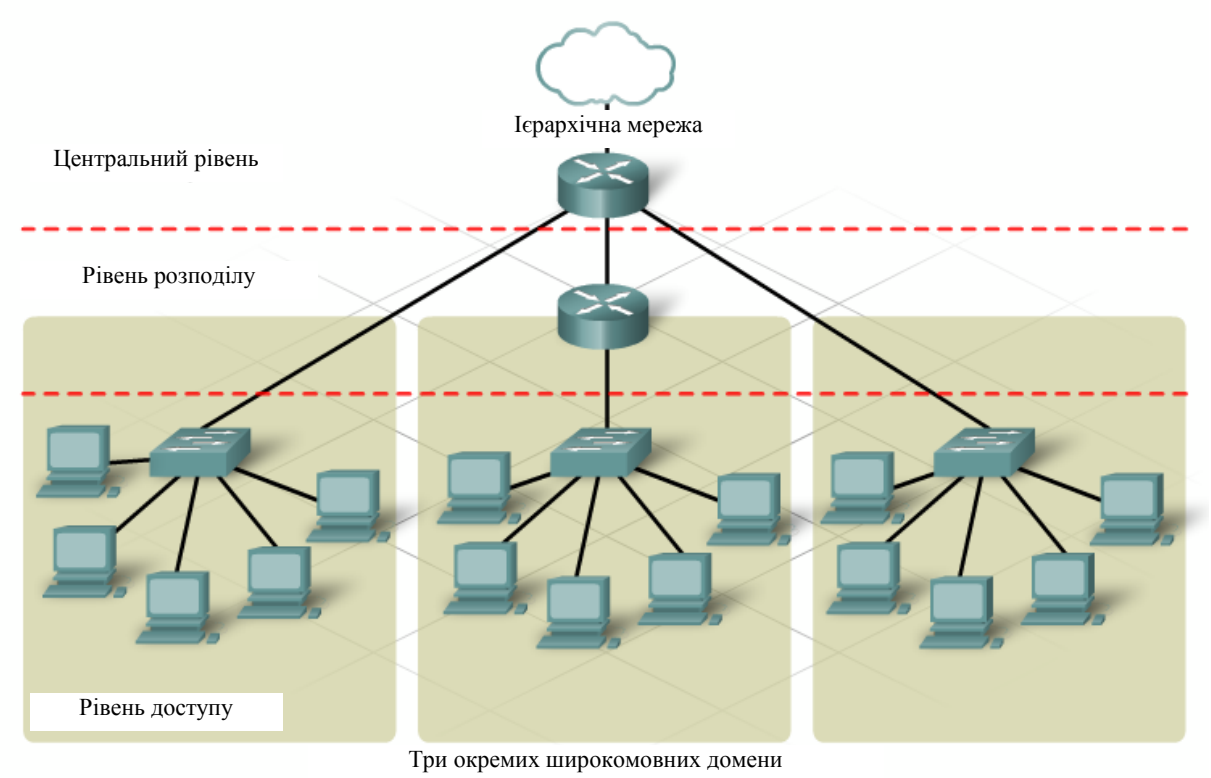


Рисунок 1 – Ієрархічна мережа

Дворівнева адресація. Мережі й підмережі. Використання масок при IP-адресації

Постачаючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити систему адресації більше гнучкою. Наприклад, якщо адресу 185.23.44.206 асоціювати з маскою 255.255.255.0, то номером мережі буде 185.23.44.0, а не 185.23.0.0, як це визначено системою класів.

У масках кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинна бути кратною 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для IP-адреси 129.64.134.5 зазначено маску 255.255.128.0, тобто у двійковому виді IP-адреса 129.64.134.5 виглядає так:

10000001. 01000000. 10000110. 00000101

А маска 255.255.128.0 так:

11111111. 11111111. 10000000. 00000000

Якщо ігнорувати маску, то відповідно до системи класів адреса

129.64.134.5 відноситься до класу B, а виходить, номером мережі є перші два байти – 129.64.0.0, а номером вузла – 0.0.134.5.

Якщо ж використовувати для визначення границі номера мережі маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, «накладені» на IP-адресу, ділять її на наступні дві частини:

	№ мережі	**№ вузла**
IP-адреса: 129.64.134.5	10000001. 01000000. 1	0000110. 00000101
Маска: 255.255.128.0	11111111. 11111111. 1	0000000. 00000000

У десятковій формі запису номер мережі – 129.64.128.0, а номер вузла – 0.0.6.5. Для стандартних класів мереж маски мають наступні значення:

клас A – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

клас B – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

клас C – 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

В 80-ті й 90-ті роки мережі розрослися, багато організацій підключили сотні й навіть тисячі вузлів. Для організації з тисячами вузлів досить мережі класу B. На жаль, виникли проблеми. Ці тисячі вузлів рідко розміщалися в тому самому місці. З метою безпеки деякі організації забажали розділити свої відділи. Для усунення цієї проблеми організації, що займаються розвитком Інтернету, вирішили розділити свої мережі на підмережі. Як розділити одну мережу класу B на декілька окремих мереж?

Стандарт RFC 917 "Підмережі в Інтернеті", передбачає використання масок підмереж як методу ізоляції підмережі від IP-адреси, виконуваної маршрутизатором. Коли маршрутизатор приймає пакет, він визначає відповідний шлях передачі на основі IP-адреси вузла призначення й маски підмережі, пов'язаної з маршрутами в таблиці маршрутизації.

Маршрутизатор побітно зчитує маску підмережі зліва направо. Якщо біт маски підмережі встановлений в 1, виходить, значення даного положення є частиною ідентифікатора мережі. Значення 0 у масці підмережі є частиною ідентифікатора вузла.

У дворівневу ієрархію адресації за класами входить ідентифікатор мережі й вузла. У підмережах, організованих за класами, ідентифікатор мережі залишається без змін, а ідентифікатор вузла ділиться на ідентифікатор підмережі й нового вузла. Наприклад, у мережі класу B є обрана за замовчуванням 16-бітна маска підмережі 11111111 11111111 00000000 00000000, або 255.255.0.0.16 біт залишається для ідентифікатора вузла.

Один зі способів розподілу класу B на декілька мереж – використання чотирьох бітів вузла як ідентифікатору підмережі. Виходить 20-бітна маска підмережі 255.255.240.0, а для ідентифікатора вузла залишається тільки 12 бітів. При такому розподілі ідентифікатора вузла виходить фіксована кількість підмереж і фіксована кількість вузлів у кожній.

Якщо в організації є мережа класу B з 4 підмережами й у деяких з них усього декілька вузлів, пропадають тисячі IP-адрес. Для більш ефективного використання IP-адрес була створена технологія безкласової міждоменної маршрутизації (CIDR).

У режимі CIDR класи мереж не використовуються. Для створення підмереж в CIDR використовуються маски підмереж змінної довжини (VLSM). Ідентифікатор мережі не обмежується рамками октету. У мережі з адресацією за класами мережа, представлена IP-адресою 192.168.5.0, відноситься до класу C. Ідентифікатор мережі повинен складатися мінімум з 24 бітів, вузлів не може бути більше 254. При використанні адресації CIDR, що іноді називають безкласовою, кількість бітів в ідентифікаторі мережі не регулюється її класом. Можна створювати мережі з адресним простором 192.168.0.0 і номером мережі, що займає менше 24 біт. Наприклад, адреса 192.168.82.174 є частиною мережі, де перші 18 бітів становлять ідентифікатор мережі. Мережа, де перебуває даний вузол, буде називатися 192.168.64.0/18, де /18 відповідає 18-бітній масці підмережі (255.255.192.0).

Мережа користувача з одним ISR жахливо перевантажена. Пропонується додати ще один мережний пристрій, більший ISR, і розділити мережу на дві більш дрібні.

З метою безпеки бездротових і дротових користувачів потрібно розділити по різних локальних мережах.

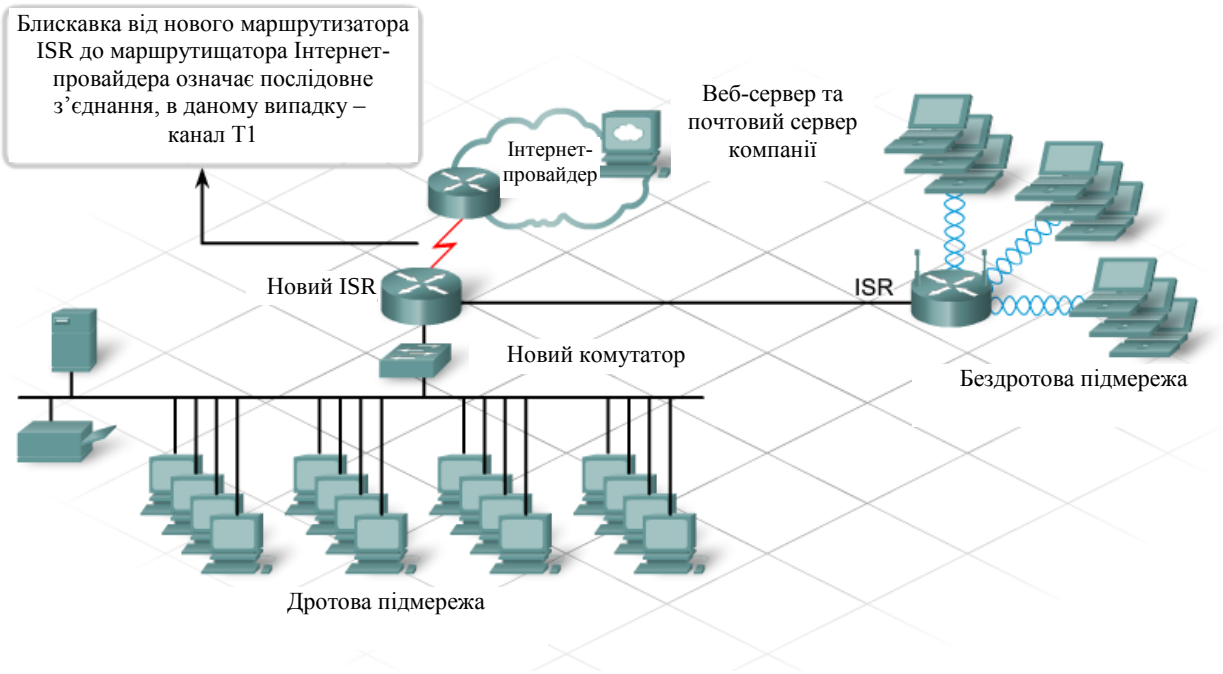


Рисунок 2 – Поділ мережі на підмережі

В 90-х роках багато мереж не мали виходу в інші мережі або Інтернет. Щоб зменшити кількість зареєстрованих організаціями унікальних IP-адрес, компанія Internet Engineering Task Force (IETF) вирішила зарезервувати частину адресного простору Інтернет для приватних мереж.

Такі блоки адрес не потрібно маршрутизувати загальнодоступній мережі Інтернет. Це означає, що всі приватні мережі можуть використовувати ті самі адреси, і поки вони не зв'язуються одна з одною, нормально обмінюватися даними.

На даний момент у більшості мереж використовується приватна структура адрес. Маршрутизуємі в Інтернеті адреси привласнюються тільки пристроям, які підключаються безпосередньо до загальнодоступної мережі. За замовчуванням більшість користувальницьких мережних пристроїв одержує приватні адреси через DHCP.

Обмін даними між підмережами

Уявіть собі підмережу у вигляді невеликої мережі. При розподілі мережі на дві підмережі фактично утворяться окремі мережі. Вони з'єднуються через маршрутизатори. Щоб пристрій з однієї підмережі зміг обмінюватися даними із пристроєм з іншої мережі, необхідний маршрутизатор.

Конфігурацію необхідно побудувати так, щоб інтерфейси маршрутизаторів, підключених один до одного, одержали IP-адреси з однієї й тої ж мережі й підмережі й щоб клієнтам були привласнені шлюзи за замовчуванням, до яких вони можуть підключатися.

Адресація в ієрархічних мережах

Великі корпоративні мережі виграють від впровадження моделі ієрархічної мережі й відповідної структури адрес. Структура ієрархічної адресації логічно ділить мережі на менш великі підмережі.

Ефективна схема ієрархічної адресації складається з адреси класової мережі на центральному рівні, що підрозділяється на менш великі підмережі на рівнях розподілу й доступу.

Можна використовувати ієрархічну мережу без використання ієрархічної адресації. Хоча мережа продовжує функціонувати, ефективність конструкції мережі знижується, а певні функції протоколу маршрутизації (наприклад, підсумовування маршрутів) працюють некоректно.

У корпоративній мережі, що охоплює безліч географічно розкиданих підрозділів, модель і структура адрес ієрархічної мережі спрощує керування мережею й усунення несправностей, а також підвищує масштабованість і ефективність маршрутизації.

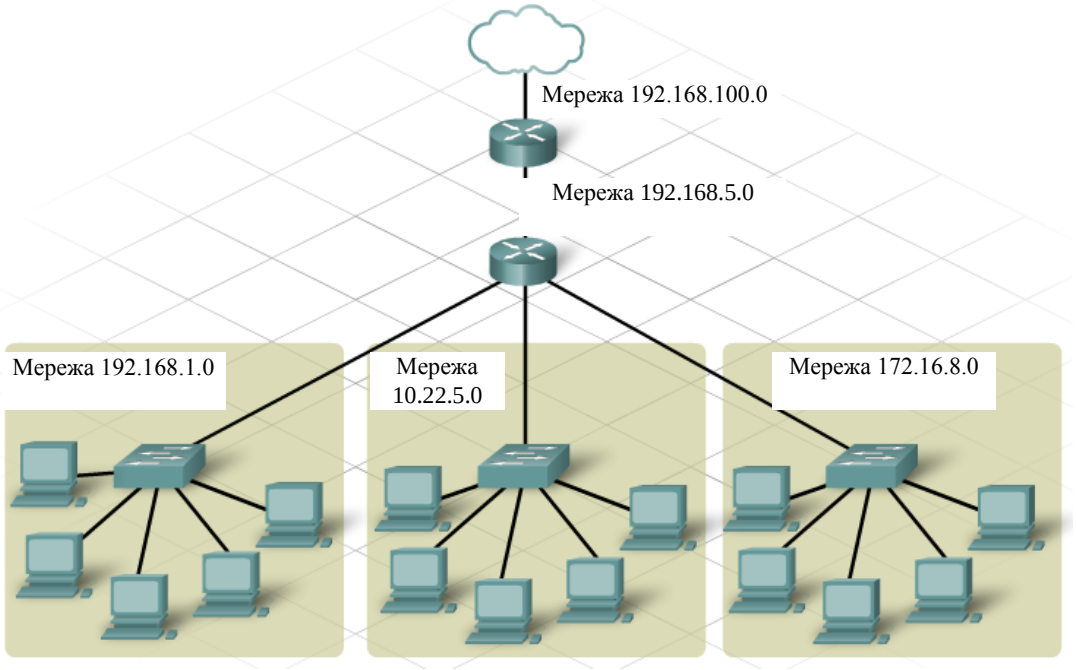


Рисунок 3 – Приклад неієрархічної мережі

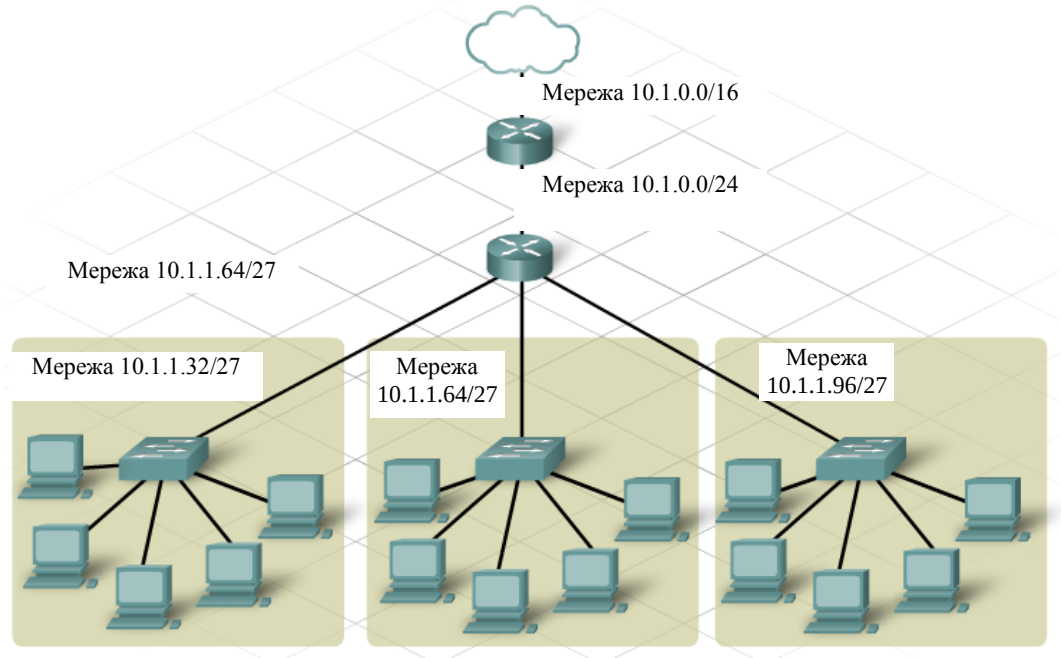


Рисунок 4 – Приклад ієрархічної мережі

Існує багато причин розділити мережу на підмережі, включаючи:

– фізичне місце розташування;

– логічне угруповання;

– безпека;

– вимоги додатків;

– обмеження широкомовного розсилання;

– модель ієрархічної мережі.

Наприклад, якщо в організації використовується мережа 10.0.0.0 для всього підприємства, можна використовувати схему адресації 10.X.Y.0, де X відповідає географічному місцю розташування, а Y – будинку або поверху в цьому місці. Ця схема адресації дозволяє використовувати:

– 255 різних географічних місць розташування;

– 255 будинків у кожному місці розташування;

– 254 вузла в кожному будинку.

Маска підмережі

Щоб використовувати поділ мережі на підмережі для створення ієрархічної моделі, необхідно чітко розуміти структуру маски підмережі.

Маска підмережі вказує, чи перебувають вузли в одній і тій же мережі. Маска підмережі – це 32-бітне значення для розрізнення бітів мережі й бітів вузлів. Вона складається з рядка одиниць, за якої треба рядок нулів. Одиниці відповідають мережі, а нулі – вузлу.

– В адресах класу А використовується маска підмережі за замовчуванням виду 255.0.0.0 або запис із косою рисою виду /8.

– В адресах класу В використовується маска за замовчуванням виду 255.255.0.0 або /16.

– В адресах класу С використовується маска за замовчуванням виду 255.255.255.0 або /24.

Запис **/x** означає число бітів у масці підмережі, що становить мережну частину адреси.

У корпоративній мережі маски підмережі розрізняються довжиною. Сегменти мережі ЛМ часто містять різне число вузлів, отже, неефективно

використовувати маску підмережі однієї й тої ж довжини для всіх створюваних підмереж.

Таблиця 1 – Представлення маски підмережі та число можливих вузлів

Крапково-десятковий вид маски підмережі	Двійкова маска під мережі	Представлення з похилою рискою	Число бітів вузла	Можлива кількість вузлів 2^{n-1}
255.0.0.0	11111111.00000000.00000000.00000000	/8	24	16777214
255.128.0.0	11111111.10000000.00000000.00000000	/9	23	8388606
255.192.0.0	11111111.11000000.00000000.00000000	/10	22	4194302
255.224.0.0	11111111.11100000.00000000.00000000	/11	21	2097150
255.248.0.0	11111111.11110000.00000000.00000000	/12	20	1048574
255.240.0.0	11111111.11111000.00000000.00000000	/13	19	524286
255.252.0.0	11111111.11111100.00000000.00000000	/14	18	262142
255.254.0.0	11111111.11111110.00000000.00000000	/15	17	131070
255.255.0.0	11111111.11111111.00000000.00000000	/16	16	65534
255.255.128.0	11111111.11111111.10000000.00000000	/17	15	32766
255.255.192.0	11111111.11111111.11000000.00000000	/18	14	16382

Крапково-десятковий вид маски підмережі	Двійкова маска під мережі	Представлення з похилою рискою	Число бітів вузла	Можлива кількість вузлів 2^{n-1}
255.255.224.0	11111111.11111111.11100000.00000000	/19	13	8190
255.255.240.0	11111111.11111111.11110000.00000000	/20	12	4094
255.255.248.0	11111111.11111111.11111000.00000000	/21	11	2046
255.255.252.0	11111111.11111111.11111100.00000000	/22	10	1022
255.255.254.0	11111111.11111111.11111110.00000000	/23	9	510
255.255.255.0	11111111.11111111.11111111.00000000	/24	8	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	7	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	6	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	5	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	4	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	3	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	2	2

Розрахунок підмереж

Для обміну даними між вузлами IP-адреса й маска підмережі вузла-відправника рівняється з IP-адресою й маскою підмережі вузла призначення. Це дозволяє визначити, чи перебувають дві адреси в одній і тій же локальній мережі.

Маска підмережі – це 32-бітне значення для розрізнення бітів мережі й бітів вузла в IP-адресі. Маска підмережі складається з рядка одиниць, за якої треба рядок нулів. Одиниці вказують число мережних битов, а нулі – число бітів вузла в IP-адресі. Рівняються мережні біти адреси відправника й адреси призначення. Якщо виявляється, що вони перебувають в одній і тій же мережі, то пакет можна доставити локально. Якщо вони не збігаються, то пакет направляється на шлюз за замовчуванням.

Наприклад, припустимо, що необхідно передати повідомлення з вузла H1, що має IP-адреса 192.168.1.44 і маску підмережі 255.255.255.0 або /24, на вузол H2, що має IP-адреса 192.168.1.66 і маску підмережі 255.255.255.0. У цьому випадку обидва вузли використовують маску підмережі за замовчуванням, рівну 255.255.255.0, що означає, що мережні біти закінчуються на границі третього октету. На обох вузлах використовуються однакові мережні біти 192.168.1, отже, вони перебувають в одній і тій же мережі.

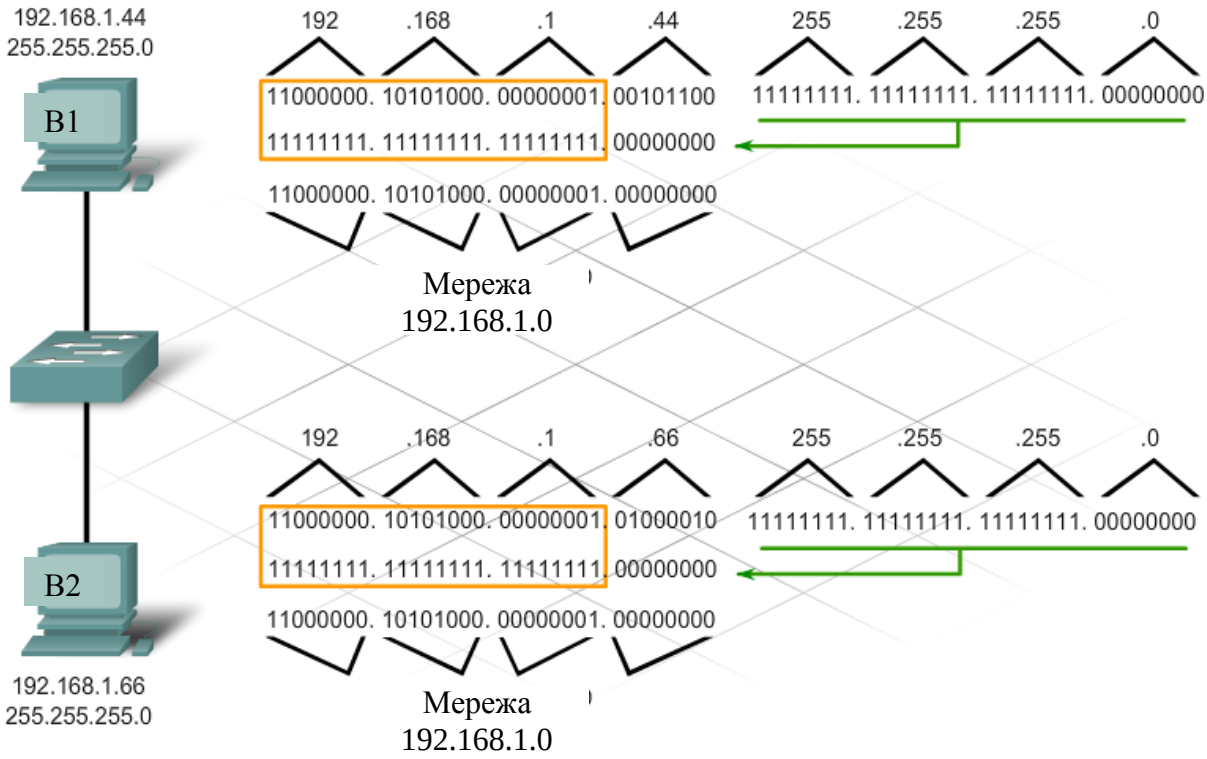


Рисунок 5 – Розрахунок підмереж з використанням двійкового представлення

Хоча досить легко визначити мережну й вузлову частини IP-адреси, коли маска підмережі закінчується на границі мережі, процес визначення мережних бітів виконується точно так само, навіть якщо мережна частина становить не цілий октет. Наприклад, IP-адреса вузла H1 – 192.168.13.21 з маскою підмережі 255.255.255.248, або /29. Це означає, що з 32 бітів 29 утворять мережну частину адреси. Мережні біти втримуються в перших трьох октетах і частині четвертого октету. У цьому випадку значення ідентифікатора мережі – 192.168.13.16.

Щоб вузол H1 з IP-адресою 192.168.13.21/29 міг обмінюватися даними з іншим вузлом, H2, з адресою 192.168.13.25/29, необхідно порівнювати мережну частину адреси цих двох вузлів, щоб визначити, чи перебувають вони в одній і тій же локальній мережі. У цьому випадку мережне значення вузла H1 становить 192.168.13.16, а мережне значення вузла H2 – 192.168.13.24. Вузли H1 і H2 розташовані в різних мережах, і для обміну даними між ними необхідно використовувати маршрутизатор.

Процес базової розбивки на підмережі

Використовуючи схему ієрархічної адресації, можна багато чого довідатися, дивлячись на IP-адресу й запис маски підмережі косою рискою (/x). Наприклад, IP-адреса 192.168.1.75 /26 містить наступні відомості:

Десяткова маска підмережі

Позначення /26 означає маску підмережі 255.255.255.192.

Число створюваних підмереж

Припустимо, що ми почали з маски підмережі за замовчуванням /24, то тоді 2 додаткових біти вузла запозичені для мережі. Це дозволяє створити 4 підмережі (2^2 = 4).

Число вузлів, придатних для використання в кожної підмережі

Шість бітів залишені для вузла, що дає 62 вузла в кожної підмережі:

(2^6 = 64 – 2 = 62).

Мережна адреса

Використовуючи маску підмережі для визначення розміщення мережних бітів, можна одержати значення мережної адреси. У цьому прикладі це значення дорівнює 192.168.1.64.

Перша застосовна адреса вузла

Серед бітів вузла не можуть утримуватися всі нулі, оскільки вони відповідають мережній адресі підмережі. Отже, першою застосовною адресою вузла в підмережі .64 буде .65.

Широкомовна адреса

Серед бітів вузла не можуть утримуватися всі одиниці, оскільки вони відповідають широкомовній адресі підмережі. У цьому випадку як адреса широкомовного розсилання використовується .127. Мережна адреса наступної підмережі починається з .128.

Підмережа	Мережна адреса	Діапазон адрес вузлів	Широкомовна адреса
0	192.168.1.0/26	192.168.1.1 – 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 – 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 – 192.168.1.254	192.168.1.255

Рисунок 6 – Приклад схеми адресації для 4-х мереж

Завдання до лабораторної роботи:

1. 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.

2. 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					

План виконання лабораторної роботи

1. Визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня;

2. Для кожної підмережі призначити: IP-адресу, маску підмережі, адресу широкомовного запиту;

3. Призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня;

4. У рамках підмереж для робочих станцій призначити початкову та кінцеву IP-адреси;

5. Розрахувати максимальну кількість вузлів кожної підмережі.

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

Тема: Маршрутизація й аналіз пропускної здатності мережі

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 розрізняти позначки вершин будемо використовувати масив Z.

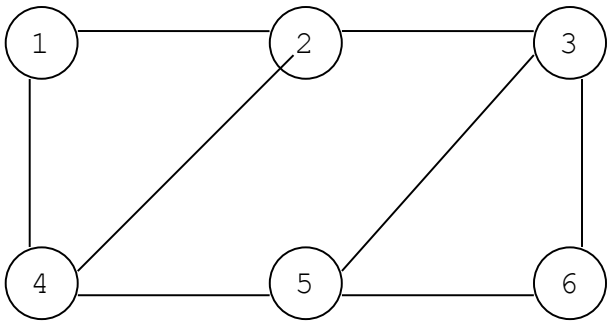
$$z(x_i)=\begin{cases} 1 - \text{якщо позначка постійна} \\ 0 - \text{якщо позначка тимчасова} \end{cases}$$

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 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.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}.

$$Rmin = \frac{C}{max(q_{ij})},$$

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:

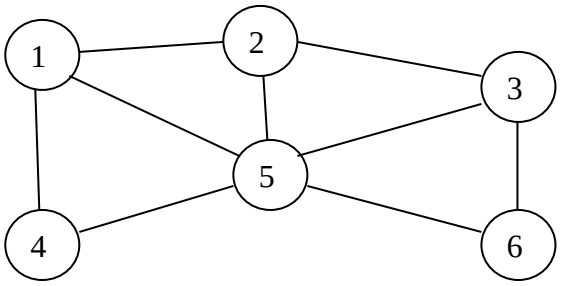
– моделювання комп’ютерної мережі у вигляді довільного графа (що генерується випадковим чином, або задається вручну),

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

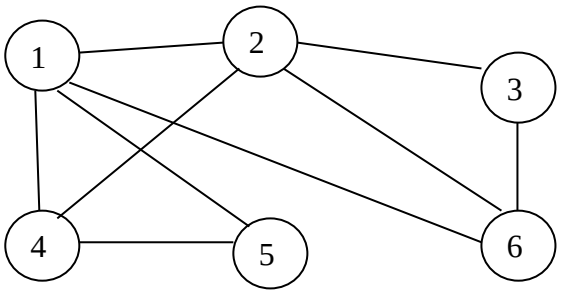
– реалізувати визначення матриці маршрутів і матриці потоків.

– реалізувати розрахунок нижньої та верхньої границі рівня трафіку.

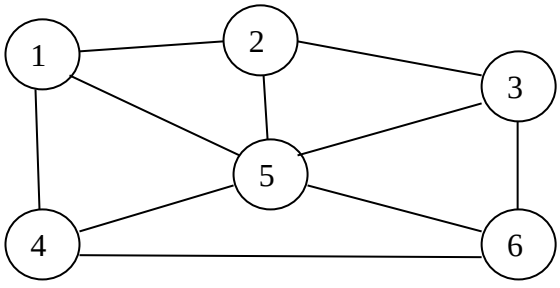
Варіант 1



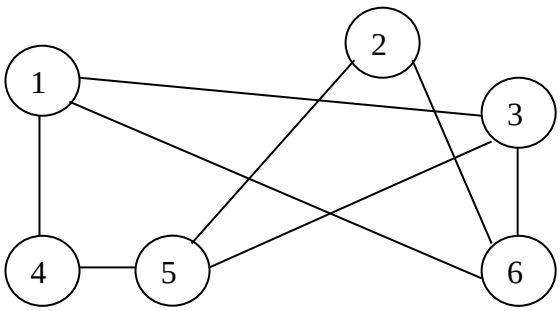
Варіант 2



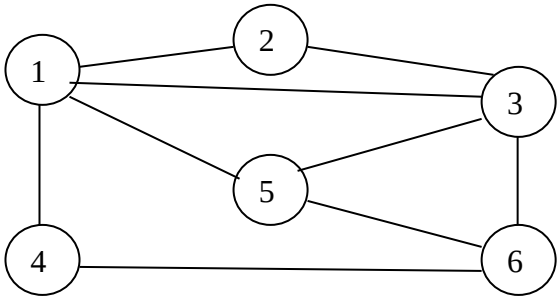
Варіант 3



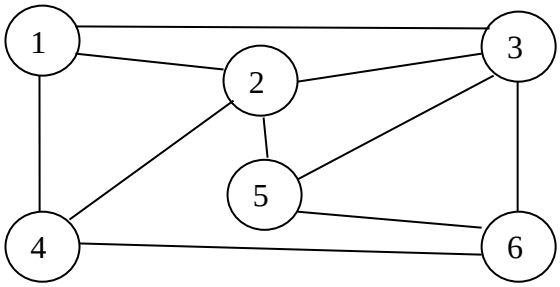
Варіант 4



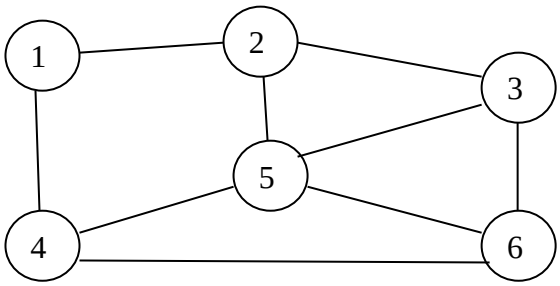
Варіант 5



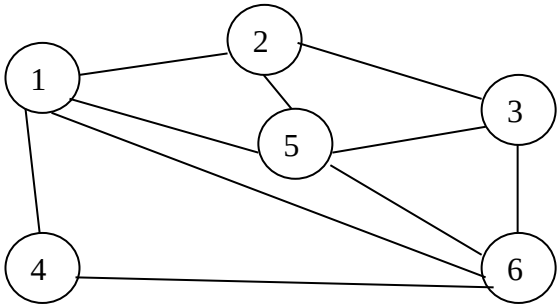
Варіант 6



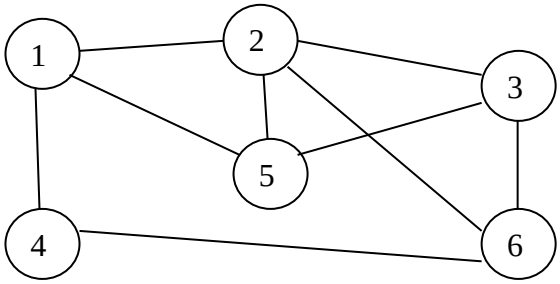
Варіант 7



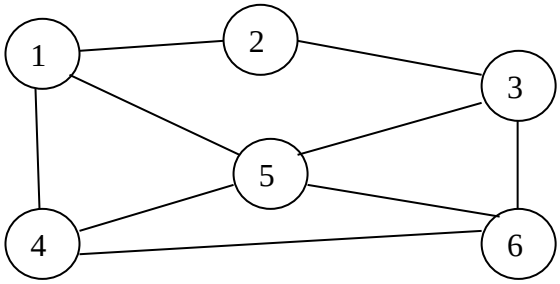
Варіант 8



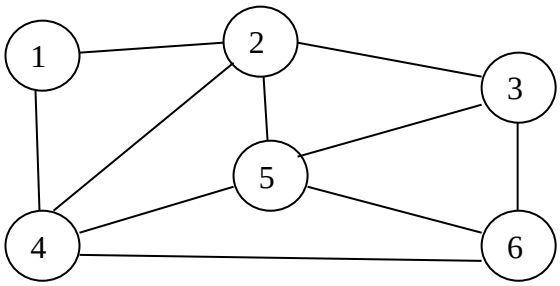
Варіант 9



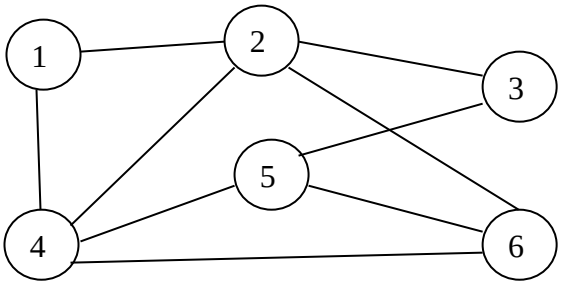
Варіант 10



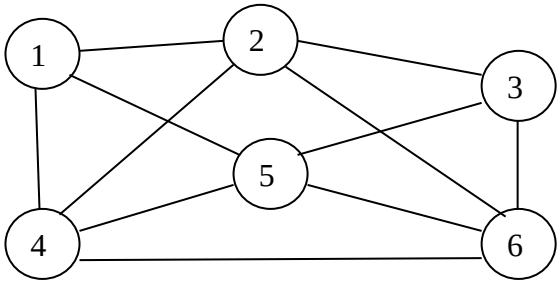
Варіант 11



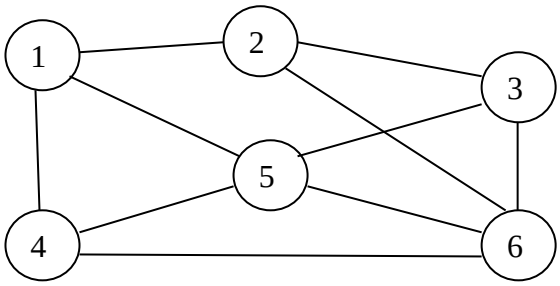
Варіант 12



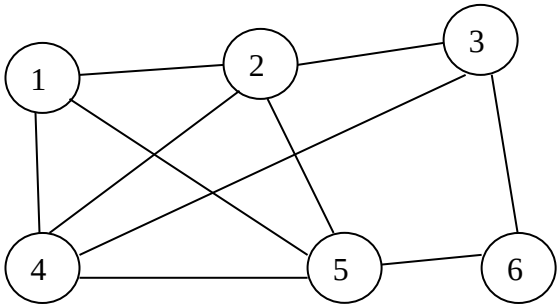
Варіант 13



Варіант 14



Варіант 15



План виконання лабораторної роботи

1. Навчитися визначати довжини найкоротших шляхів між всіма парами вузлів.

2. Визначити значення елементів маршрутної таблиці.

3. Оцінити пропускну здатність мережі.

4. Змоделювати комп’ютерну мережу у вигляді довільного графа.

Контрольні питання:

1. Що таке алгоритм Дейкстри ?
2. Як визначити значення елементів маршрутної таблиці?
3. Як зробити оцінку пропускної здатності мережі?

Лабораторна 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

Теоретичні відомості

Локальна мережа забезпечує взаємодію кожного вузла з кожним – це дуже корисна властивість, так як не потрібно робити ніяких спеціальних дій, щоб забезпечити доступ вузла А до вузла В – досить того, що ці вузли підключені до однієї і тієї ж локальної мережі. У той же час в мережі можуть виникати ситуації, коли така тотальна доступність вузлів небажана. Прикладом може служити сервер фінансового відділу, доступ до якого бажано вирішити тільки з комп'ютерів кількох конкретних співробітників цього відділу. Звичайно, доступ можна обмежити на рівні операційної системи або системи управління базою даних самого сервера, але для надійності бажано мати кілька ешелонів захисту і обмежити доступ ще й на рівні мережевого трафіку.

Багато моделей комутаторів дозволяють адміністраторам задавати додаткові умови фільтрації кадрів поряд зі стандартними умовами їх фільтрації відповідно до інформації адресної таблиці. Такі фільтри називають користувацькими.

Фільтр користувача, який також часто називають списком доступу (access list), призначений для створення додаткових бар'єрів на шляху кадрів, що дозволяє обмежувати доступ певних груп користувачів до окремих служб мережі. Фільтр користувача – це набір умов, які обмежують звичайну логіку передачі кадрів комутаторами.

Найбільш простими є користувальницькі фільтри на основі MAC-адрес станцій. Так як MAC-адреси – це та інформація, з якою працює комутатор, він дозволяє створювати подібні фільтри зручним для адміністратора способом, можливо, проставляючи деякі умови в додатковому полі адресної таблиці, наприклад умова відкидати кадри з певною адресою. Таким способом

користувачеві, який працює на комп'ютері з даними MAC-адресою, повністю забороняється доступ до ресурсів іншого сегмента мережі.

Secure Shell, **SSH** (англ. *Secure SHell* – «безпечна оболонка») – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються.

Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування. Клієнти і сервери, що підтримують цей протокол, доступні для різних платформ. Крім того, протокол дозволяє не тільки використовувати безпечний віддалений shell на машині, але і туннелювати графічний інтерфейс – X Tunnelling (тільки для Unix-подібних ОС або застосунків, що використовують графічний інтерфейс X Window System). Так само ssh здатний передавати через безпечний канал (Port Forwarding) будь-який інший мережевий протокол, забезпечуючи (при належній конфігурації) можливість безпечної пересилки не тільки X-інтерфейсу, але і, наприклад, звуку.

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

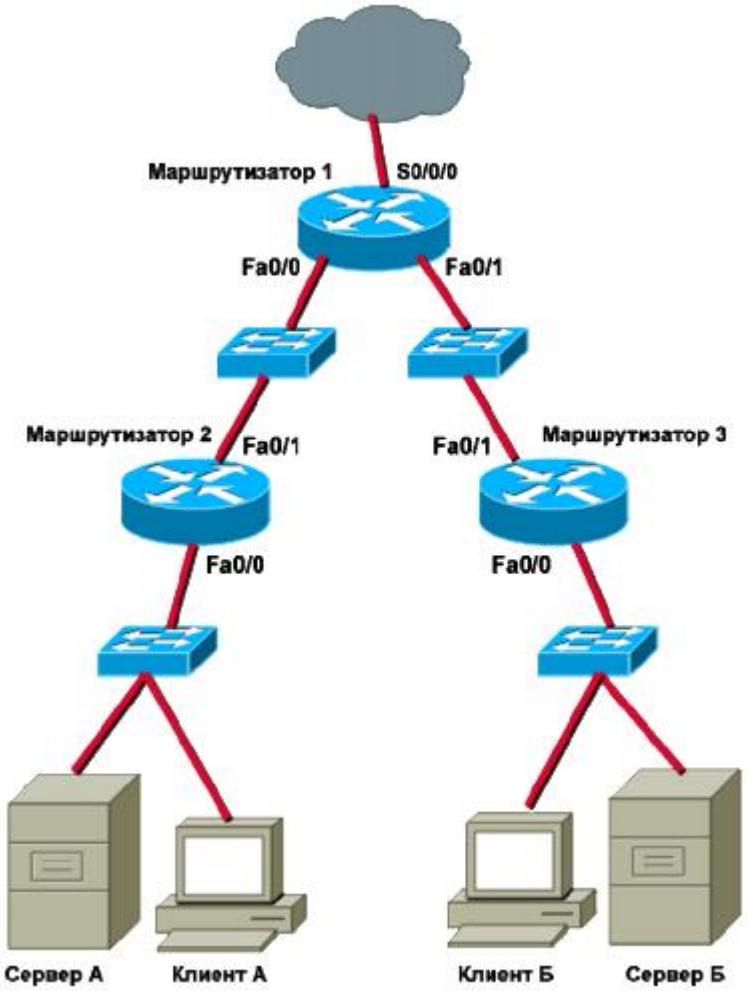


Рисунок 1 – Схема мережі корпоративного клієнта

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

План виконання лабораторної роботи:

1. Контролювати цілісності передачі даних.

2. Неуможливити зовнішні проникненння в самі мережі чи в канали зв’язку між ними.

3. Використовуючи протокол SSH, дозволити клієнту доступ до маршрутизаторів.

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

Тема: 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).

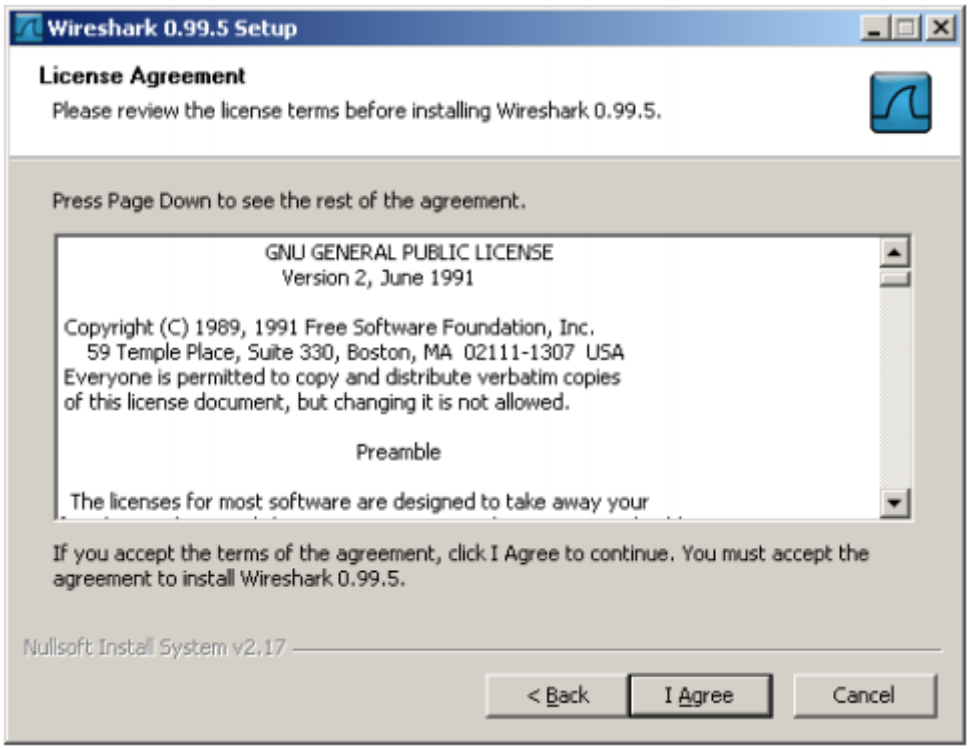


Рисунок 2

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).

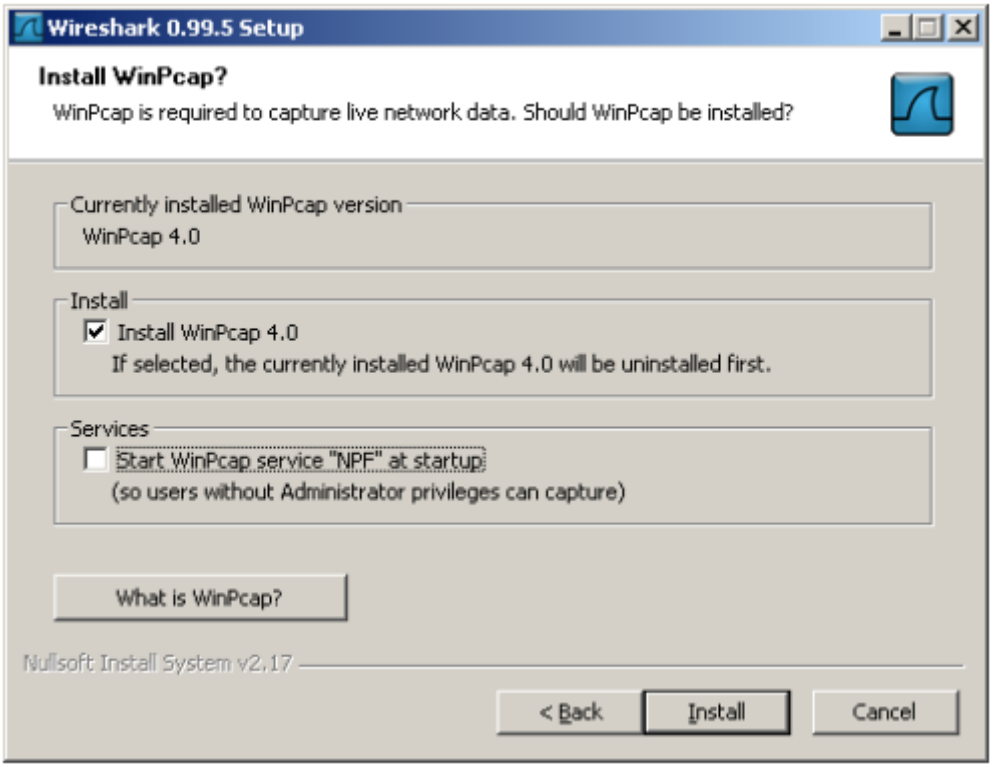


Рисунок 3

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).

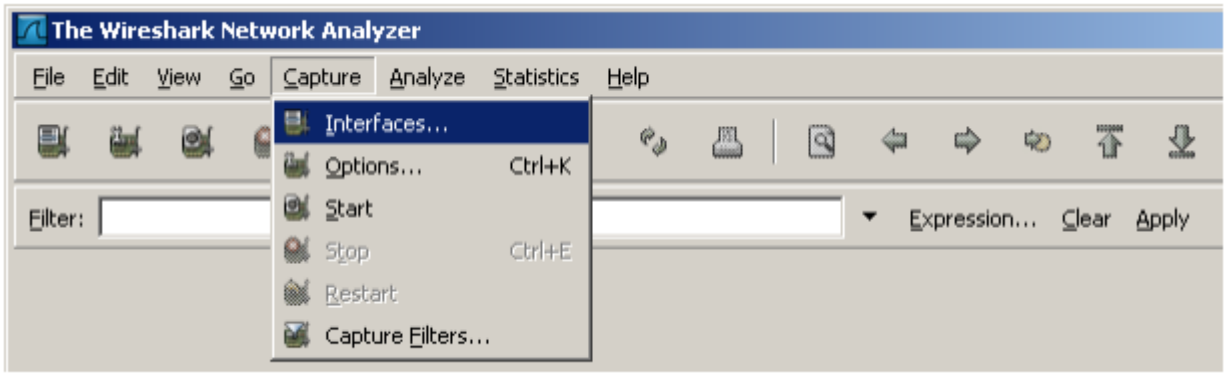


Рисунок 4

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

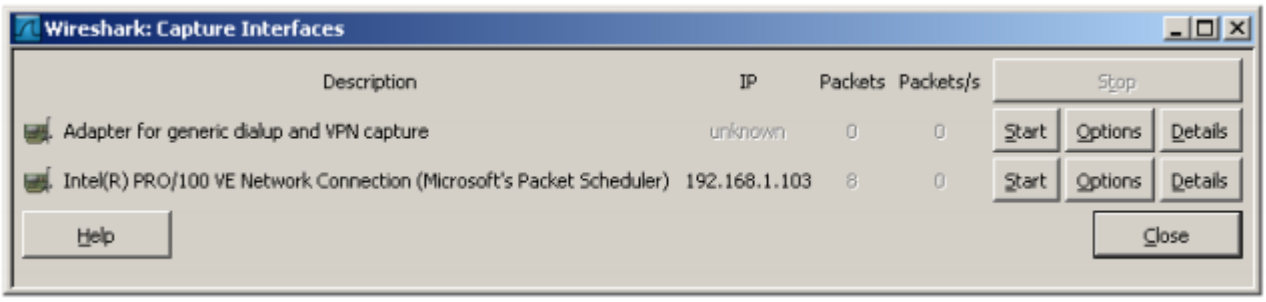


Рисунок 5

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).

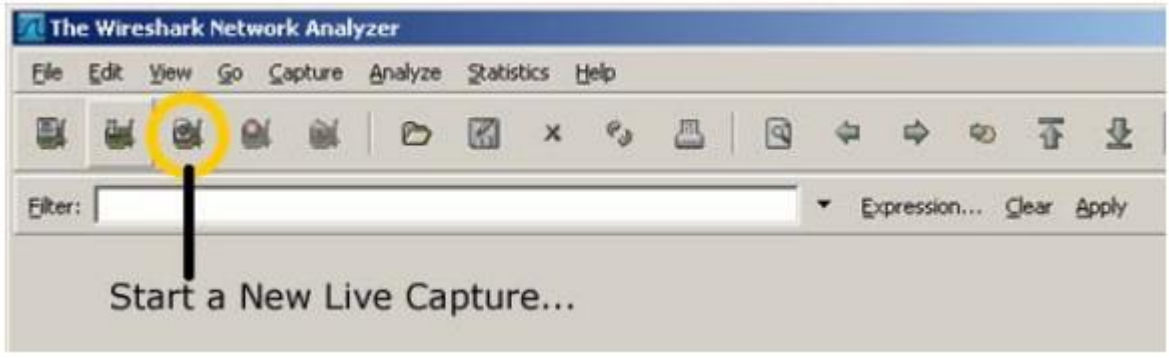


Рисунок 6

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).

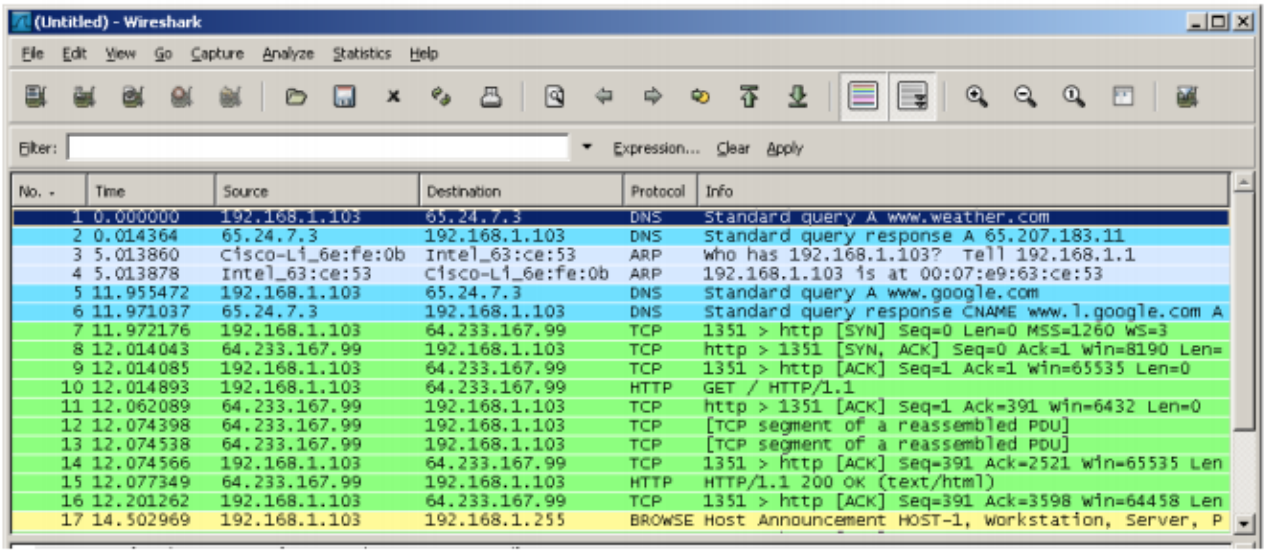


Рисунок 7

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.

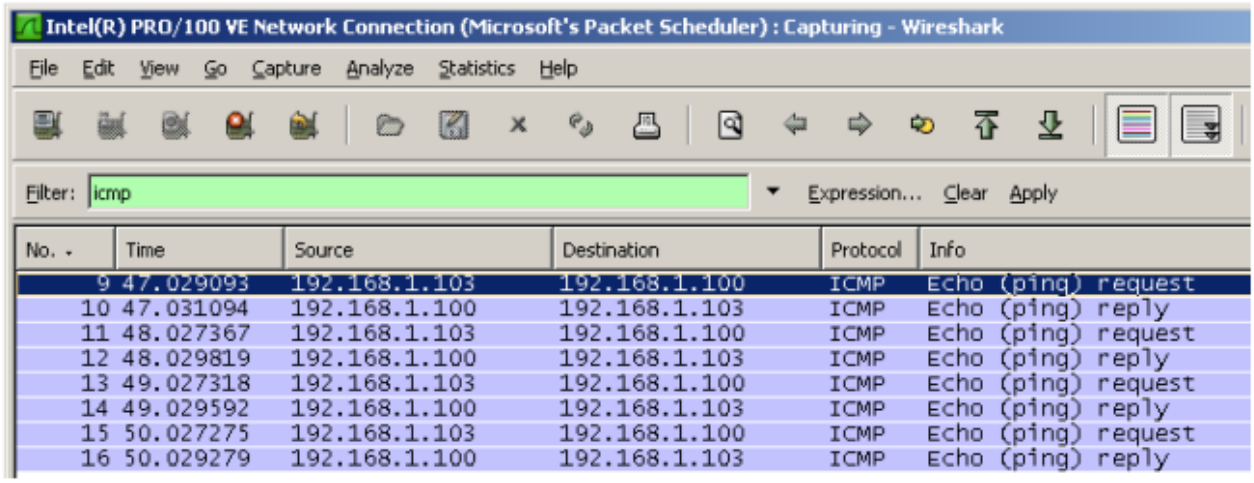


Рисунок 8

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.

План виконання лабораторної роботи:

1. Встановити на ПК (під управлінням ОС Windows з мережею Ethernet і хоча б двома вузлами) програму Wireshark (версія 0.99.5 або остання версія);

2. Використати підключення до мережі Інтернет (бажано);

3. Перевірити чи є доступ до мережевої конфігурації TCP/IP ПК.

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.Куприянов А. О. «Обеспечение защиты персональных данных в информационных системах» // Програм. инженерия и информ. безопасность. – 2013. – № 4.

2. Таненбаум Э, Уэзеролл Д. «Компьютерные сети.» – Питер, 2014. – 960 с.

3. «Абонентские сети доступа и технологии высокоскоростных сетей», Берлин А. Н. Национальный Открытый Университет «ИНТУИТ» – 2016 год – 277 страниц

4. «Администрирование сетей Microsoft Windows XP Professional»,Элсенпитер Р., Велт Национальный Открытый Университет «ИНТУИТ» – 2016 год – 650 стр.

5. «Компьютерные сети : учебно-методическое пособие по выполнению расчетно-графической работы»,Фомин Д. В. Директ-Медиа – 2015 год – 66 стр.

6. «Характеристика и особенности локальных компьютерных сетей»,Кожемяк М. Э.Лаборатория книги – 2012 год – 157 стр.

7. «Безопасность сетей», Мэйволд Э.,Национальный Открытый Университет «ИНТУИТ» – 2016 год – 572 стр.

8. «Протоколы безопасного сетевого взаимодействия», Лапонина О.Р., Национальный Открытый Университет «ИНТУИТ» – 2016 год – 462 страницы

9. «Компьютерные сети и сетевые технологии»,Николай Кузьменко,368 стр.,2013

10. «Компьютерные сети. Принципы, технологии, протоколы.», 992стр.,2016

11. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.

12. Мониторинг утечек информации. [Электронный ресурс]. – Доступный с http://www. infowatch.ru/analytics/leaks_monitoring

13. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal / Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

14. Час антивірусів пройшло: "Лабораторія Касперського" представляє корпоративну за- хист нового покоління. [Електронний ресурс]. – Доступний з http://www.infoportal.pp.ua/news/ chas_antivirusiv_projshlo_laboratorija_kasperskogo_predstavljae_korporativnu_zakhist_novogo_po kolinnja/2013-02-27-1742#.UVad0leqa70 Національний лісотехнічний університет України 328 Збірник науково-технічних праць

15. Чудінова Н.В. Особливості використання мережі Інтернет для отримання конфіден- ційної інформації / Н.В. Чудінова, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.- техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.3. – С. 337-346.

16. Nicholas Rosasco and David Larochelle. How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH. Quoting Barrett and Silverman, SSH, the Secure Shell: The Definitive Guide, O'Reilly & Associates . Dept. of Computer Science, Univ. of Virginia. Архів оригіналу за 2013-06-25.