МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

з навчальної дисципліни **«Мережеві технології»**
вибіркових компонент освітньої програми
першого(*бакалаврського*) рівня вищої освіти
125 «Кібербезпека»
«Безпека інформаційних та комунікаційних систем»

м. Харків
2023 р.

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від _30 .08.23_ № 7___

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 25 .08.23 №7

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29 .08.23_ № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій
(*протокол від* 15 .08.23_ № 8 ___)

Розробники:
1. *Професор кафедри, д.т.н., професор Семенов С.Г..*
2. *Доцент кафедри, д.т.н., Можаєв М.О.*
3. *Професор кафедри, д.т.н., професор Можаєв О.О.*

Рецензенти:
1. Доцент кафедри боротьби з кіберзлочинністю ХНУВС, к.т.н., доцент Клімушин П.С.;
2. Завідувач кафедри ЕОМ ХНУРЕ д.т.н., професор, Коваленко А.А.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Семестр 8								
Тема № 1: Основні поняття та характеристики мережі.	**22**	**2**		**2**		**6**	**1,2**	
Тема № 2: Архітектура мереж	**32**	**2**			**4**	**8**	**1,2**	
Тема № 3 Взаємодія рівнів еталонної моделі OSI	**22**	**2**		**2**		**6**	**1,2**	
ТЕМА №4. Верхні рівні моделі OSI	**22**	**2**		**2**		**6**	**1,2**	
ТЕМА №5. Нижні рівні моделі OSI	**32**	**2**			**4**	**8**	**1,2**	
ТЕМА №6. Сімейство стандартів IEEE 802	**32**	**2**			**4**	**8**	**1,2**	
ТЕМА №7. Протоколи і стеки протоколів	**22**	**2**		**2**		**6**	**1,2**	
ТЕМА №8. Архітектура стека протоколів MICROSOFT TCP/IP	**32**	**2**			**4**	**8**	**1,2**	
ТЕМА №9. Адресація в IP-мережах	**34**	**2**		**2**	**4**	**8**	**1,2**	
ТЕМА №10. Топологія локальної мережі	**32**	**2**			**4**	**8**	**1,2**	
ТЕМА №11. Методи доступу	**32**	**2**			**4**	**8**	**1,2**	
ТЕМА №12. Основні компоненти локальної мережі	**22**	**2**		**2**		**6**	**1,2**	
Всього за семестр	**150**	**24**		**12**	**28**	**86**		**екзамен**
Всього по дисципліні	**150**	**24**		**12**	**28**	**86**		**екзамен**

Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Семестр 8								
Тема № 1: Основні поняття та характеристики мережі.	**22**	**1**				**12**	**1,2**	
Тема № 2: Архітектура мереж	**32**				**2**	**12**	**1,2**	
Тема № 3 Взаємодія рівнів еталонної моделі OSI	**22**	**1**		**1**		**12**	**1,2**	
ТЕМА №4. Верхні рівні моделі OSI	**22**			**1**		**12**	**1,2**	
ТЕМА №5. Нижні рівні моделі OSI	**32**					**12**	**1,2**	
ТЕМА №6. Сімейство стандартів IEEE 802	**32**	**1**			**2**	**12**	**1,2**	
ТЕМА №7. Протоколи і стеки протоколів	**22**					**12**	**1,2**	
ТЕМА №8. Архітектура стека протоколів MICROSOFT TCP/IP	**32**					**12**	**1,2**	
ТЕМА №9. Адресація в IP-мережах	**34**			**2**		**12**	**1,2**	
ТЕМА №10. Топологія локальної мережі	**32**					**12**	**1,2**	
ТЕМА №11. Методи доступу	**32**				**2**	**12**	**1,2**	
ТЕМА №12. Основні компоненти локальної мережі	**22**	**1**		**2**		**12**	**1,2**	
Всього за семестр	**160**	**4**		**6**	**6**	**144**		**екзамен**
Всього по дисципліні	**160**	**4**		**6**	**6**	**144**		**екзамен**

2. Методичні вказівки до практичних занять

СЕМЕСТР 8

Тема № 2: Архітектура мереж

2.1 Мета роботи

Мета роботи – навчитися працювати з програмним пакетом NetCracker, v 4.1. Отримати уявлення про компоненти захищеної локальної комп'ютерної мережі. Змоделювати і дослідити основні базові топології, що застосовуються для побудови

захищених локальних мереж.

За заданими початковими умовами змоделювати захищену локальну мережу за технологією Ethernet з використанням стандартів фізичного середовища 10Base-5, 10Base-2, 10Base-T. Провести аналіз отриманої моделі і зробити висновки про її захищеність та ефективність застосування.

2.2 Завдання лабораторної роботи

– Створити моделі найпростішої локальної мережі. Змоделювати і дослідити базові топології LAN.

– Спроектувати і дослідити захищену локальну мережу за технологією ETHERNET з використанням стандартів 10BASE-5, 10BASE-2, 10BASE-T.

2.3 Методичні вказівки з організації самостійної роботи

– Вивчити теоретичний матеріал лекцій «Брандмауери, основні елементи брандмауерів» та «Програмний пакет NetCracker, v 4.1.».

– Підготувати відповіді на контрольні запитання.

– Підготувати бланк звіту з лабораторної роботи.

Допуск до виконання лабораторної роботи здійснюється за результатами письмового опитування.

2.4 Загальнотеоретичні положення

2.4.1 Загальні відомості про технологію Ethernet

Ethernet (етернет, від лат. aether – ефір – пакетна технологія комп'ютерних мереж, переважно локальних.

Стандарти Ethernet визначають дротяні з'єднання і електричні сигнали на фізичному рівні, формат кадрів і протоколи управління доступом до середовища – на канальному рівні моделі OSI. Ethernet в основному описується стандартами IEEE. Ethernet став найпоширенішою технологією локальних обчислювальних мереж у середині 90-х років минулого століття, витіснивши такі застарілі технології, як Arcnet, FDDI і Token ring.

Технологія Ethernet була розроблена разом з багатьма першими проектами корпорації Xerox PARC. Прийнято вважати, що Ethernet був винайдений 22 травня 1973 роки, коли Роберт Меткалф (Robert Metcalfe) склав доповідну записку для глави PARC про потенціал технології Ethernet. Але законне право на технологію Меткалф отримав через декілька років. У 1976 році він і його асистент Девід Боггс (David Boggs) видали брошуру під назвою «Ethernet: Distributed Packet-Switching For Local Computer Networks».

Меткалф пішов з Xerox в 1979 році і заснував компанію 3Com для просування комп'ютерів і локальних обчислювальних мереж. Йому вдалося переконати DEC, Intel і Xerox працювати спільно і розробити стандарт Ethernet (DIX). Вперше цей

стандарт був опублікований 30 вересня 1980 року.

У залежності від типу фізичного середовища стандарт Ethernet має різні модифікації :

- 10Base-5 – коаксіальний кабель діаметром 0,5 дюйма, названий «товстим» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента – 500 метрів (без повторювачів).

- 10Base-2 – коаксіальний кабель діаметром 0,25 дюйма, названий «тонким» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента – 185 метрів (без повторювачів).

- 10Base-T – кабель на основі неекранованої крученої пари (Unshielded Twisted Pair, UTP). Утворіть зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом - не більш 100 м.

- 10Base-F – волоконно-оптичний кабель. Топологія аналогічна топології стандарту 10Base-T. Є кілька варіантів цієї специфікації – FOIRL (відстань до 1000 м), 10Base-FL (відстань до 2000 м), 10Base-FB (відстань до 2000 м).

Число 10 у зазначених вище назвах позначає бітову швидкість передачі даних цих стандартів -10 Мбіт/с, а слово Base – метод передачі на одній базовій частоті 10 Мгц (на відміну від методів, що використовують кілька несучих частот, що називаються Broadband). Останній символ у назві стандарту фізичного рівня позначає тип кабелю.

Для передачі двійкової інформації з кабелю для усіх варіантів фізичного рівня технології Ethernet із пропускною здатністю 10 Мбіт/с використовується манчестерський код. Усі види стандартів Ethernet, у тому числі і Fast Ethernet і Gigabit Ethernet використовують той самий метод розподілення середовища передачі даних, так званий SCMA/CD – carrier sense multiply access with collision detection, тобто метод випадкового доступу з упізнанням несучої і виявленням колізій. Цей метод застосовується в мережах з логічною загальною шиною, у яких усі комп'ютери мають безпосередній доступ до загального середовища. Одночасно всі комп'ютери мережі мають можливість з урахуванням затримки розподілу сигналу по фізичному середовищу отримати дані, що кожен з комп'ютерів починає передавати на загальну шину.

2.4.2 Стислі відомості про стандарти фізичного середовища Ethernet

Стандарт 10Base5.

Як середовище передачі даних використовується товстий коаксіальний кабель із хвильовим опором 50 Ом, діаметром центрального мідного проводу 2,17 мм і зовнішнім діаметром близько 10 мм. Такими характеристиками володіють кабелі марок RG-8 і RG-11.

Кабель використовується як моноканал для всіх станцій. Сегмент кабелю має максимальну довжину 500 м (без повторювачів) і повинен мати на кінцях погоджувальні термінатори опором 50 Ом, що поглинають сигнали, які

поширюються по кабелю, і перешкоджають виникненню відбитих сигналів.

Станція має підключатися до кабелю за допомогою прийомо-передавача – трансівера. Трансівер установлюється безпосередньо на кабелі і живиться від мережного адаптера комп'ютера. Трансівер може приєднуватися до кабелю як методом проколювання, що забезпечує безпосередній фізичний контакт, так і безконтактним методом.

Трансівер з'єднується з мережним адаптером інтерфейсним кабелем AUI (Attachment Unit Interface) довжиною до 50 м, що складається з 4 кручених пар (адаптер повинен мати рознімання AUI). Для приєднання до інтерфейсу AUI використовується рознімання DB-15.

Допускається підключення до одного сегмента не більш 100 трансіверів, причому відстань між підключеними трансіверами не має бути менш ніж 2,5 м.

Стандарт 10Base-5 визначає можливість використання в мережі спеціального пристрою повторювача. Повторювач служить для об’єднання в одну мережу декількох сегментів кабелю і збільшення тим самим загальної довжини мережі.

Стандарт дозволяє використання в мережі не більш чотирьох повторювачів і, відповідно, не більш п’яти сегментів кабелю. При максимальній довжині сегмента кабелю в 500 м це дає максимальну довжину мережі 10Base-5 у 2500 м. Тільки 3 сегменти з 5 можуть бути навантаженими, тобто такими, до яких підключаються кінцеві вузли. Між навантаженими сегментами мають бути ненавантажені сегменти, так що максимальна конфігурація мережі являє собою два навантажених крайніх сегменти, що з’єднуються ненавантаженими сегментами ще з одним центральним навантаженим сегментом (див. рис. 2.1). На ньому показана схема фізичного рівня мережі на базі стандарту 10Base-5.

Стандарт 10Base-T.

Мережі 10Base-T використовують як середовище дві неекрановані кручені пари. Найбільш розповсюджений багатопарний кабель на основі неекранованої крученої пари категорії 3.

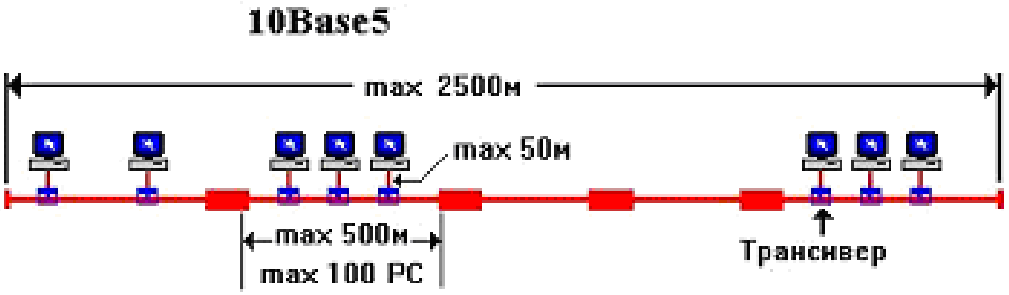


Рисунок 2.1 – Стандарт 10 Base-5

Кінцеві вузли з'єднуються за топологією «пасивна зірка» зі спеціальним пристроєм – багатопортовим повторювачем за допомогою двох кручених пар. Одна пара потрібна для передачі даних від станції до повторювача (вихід T_x мережного

адаптера), а інша – для передачі даних від повторювача до станції (вхід R_x мережного адаптера). На рис. 2.2. показано приклад мережі 10Base-T. Повторювач приймає сигнали від одного з кінцевих вузлів і синхронно передає їх на усі свої інші порти, крім того, з якого надійшли сигнали.

Багатопортові повторювачі в даному випадку звичайно називаються концентраторами. Вони здійснюють функції повторювача сигналів на усіх відрізках кручених пар, підключених до його портів, так що утвориться єдине середовище передачі даних – логічний моноканал (логічна загальна шина). Стандарт визначає бітову швидкість передачі даних 10 Мбіт/с і максимальну відстань відрізка крученої пари між двома безпосередньо зв'язаними вузлами (станціями і концентраторами) не більш 100 м за наявності крученої пари якості не нижче категорії 3. Ця відстань визначається смугою пропущення крученої пари – на довжині 100 м вона дозволяє передавати дані зі швидкістю 10 Мбіт/с при використанні манчестерського коду.

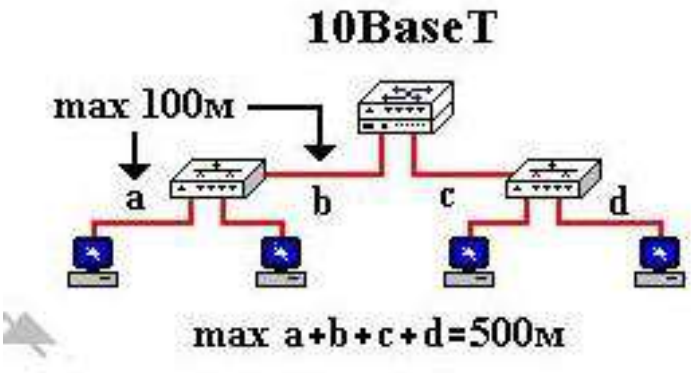


Рисунок 2.2 – Стандарт 10 Base-T

Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD і надійного розпізнавання станціями колізій у стандарті визначено максимальну кількість концентраторів між будь-якими двома станціями мережі, а саме 4. Це правило називається «правило 4-х хабів». При створенні мережі 10Base-T з великою кількістю станцій концентратори можна з'єднувати один з одним ієрархічним способом, утворюючи деревоподібну структуру.

Загальна кількість станцій у мережі 10Base-T не має перевищувати загальної межі в 1024. Кінцеві вузли потрібно підключати до портів концентраторів нижнього рівня. При цьому необхідно, щоб виконувалося правило 4-х хабів.

Стандарт 10Base-2.

Стандарт 10Base-2 використовує як передавальне середовище коаксіальний кабель з діаметром центрального мідного проводу 0,89 мм і зовнішнім діаметром близько 5 мм («тонкий» Ethernet). Кабель має хвильовий опір 50 Ом. Такими характеристиками володіють кабелі марок RG-58 /U, RG-58 AA.J, RG-58 C/U.

Максимальна довжина сегменту без повторювачів складає 185 м, сегмент повинен мати на кінцях термінатори, що походять, 50 Ом. Однак, «тонкий» коаксіал володіє гіршим захистом, гіршою механічною міцністю і більш вузькою смугою

пропущення.

Станції підключаються до кабелю за допомогою високочастотних BNC Т-конекторів, що є трійником, один відвід якого з'єднується з мережним адаптером, а два інших – із двома кінцями розриву кабелю. Максимальна кількість станцій, що підключаються до одного сегмента – 30. Мінімальна відстань між станціями – 1м.

Стандарт 10Base-2 також передбачає використання повторювачів, застосування яких також має відповідати «правилу 5-4-3». У цьому випадку мережа матиме максимальну довжину в 5х185- 925 м.

Стандарт 10Base-2 дуже близький до стандарту 10Base-5. Трансівери в ньому об'єднані з мережними адаптерами за рахунок того, що більш гнучкий тонкий коаксіальний кабель може бути підведений безпосередньо до вихідного рознімання плати мережного адаптера, встановленої в комп'ютері (рис.2.3).

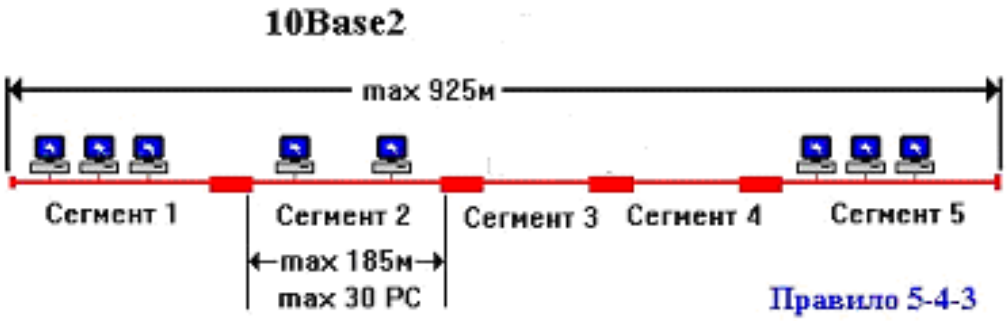


Рисунок 2.3 – Стандарт 10 Base-2

Реалізація цього стандарту на практиці призводить до найбільш простого рішення для кабельної мережі, тому що для з'єднання комп'ютерів вимагаються тільки мережні адаптери, Т-конектори і термінатори 50 Ом.

Оптоволоконний Ethernet

Оптоволоконні стандарти як основний тип кабелю рекомендують досить дешеве багатомодове оптичне волокно, що володіє смугою пропущення 500–800 Мгц при довжині кабелю 1 км. Припустимо і більш дороге одномодове оптичне волокно зі смугою пропущення в 1 Ггц, але при цьому потрібно застосовувати спеціальний тип трансівера.

Функціонально мережа Ethernet на оптичному кабелі складається з тих же елементів, що і мережа стандарту 10Base-T – мережних адаптерів, багатопортового повторювача і відрізків кабелю, що з'єднують адаптер з портом повторювача. Як і у випадку крученої пари, для з'єднання адаптера з повторювачем використовуються два оптоволокна – одне з'єднує вихід T_x адаптера з входом R_x повторювача, а інше – вхід R_x адаптера з виходом T_x повторювача.

2.4.3 Загальні відомості про систему логічного моделювання і проектування локальних та корпоративних мереж NetCracker

Призначення системи NetCracker – автоматизоване проектування і моделювання локальних і корпоративних комп'ютерних мереж для мінімізації витрат часу і засобів на розробку, верифікацію проектів.

Функції системи NetCracker:

- створення проекту мережі;
- анімаційне моделювання мережі;
- моделювання трафіку мережі і збір статистики;
- створення багаторівневих мережних проектів;
- вибір оптимальних компонентів мережі;
- використання бази даних мережних компонентів;
- інтерактивне проектування мережі.

Умови застосування системи NetCracker:

- процесор Pentium II;
- 50 Мбайт вільного простору на жорсткому диску;
- 64 Мбайт (128 Мбайт рекомендується) оперативної пам'яті;
- відеопам'ять 2 Мбайти (4 Мбайти Microsoft Direct Draw – сумісна відеоплата рекомендується);
- монітор Super VGA з розрішенням 800 × 600;
- параметри настроювання екрана мають бути встановлені High Color (16-розрядна колірна палітра, 65 536 кольорів);
- диск CD-ROM;
- звукова плата;
- Microsoft Windows NT4 або вище.

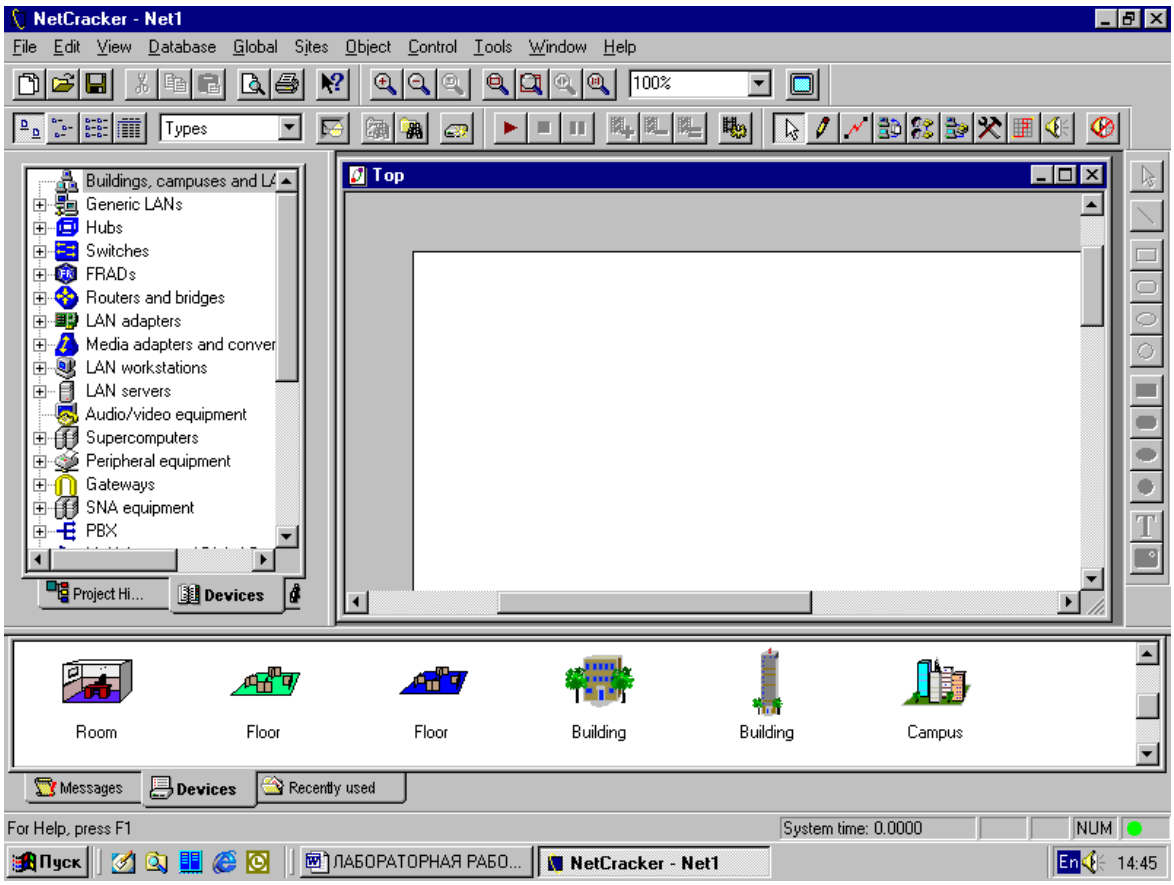
2.5 Порядок виконання лабораторної роботи

1. Вивчити теоретичний матеріал, наданий у підрозділі 2.4 цієї лабораторної роботи.

2. За допомогою системи NetCracker спроектувати найпростішу локальну комп'ютерну мережі згідно з алгоритмом:

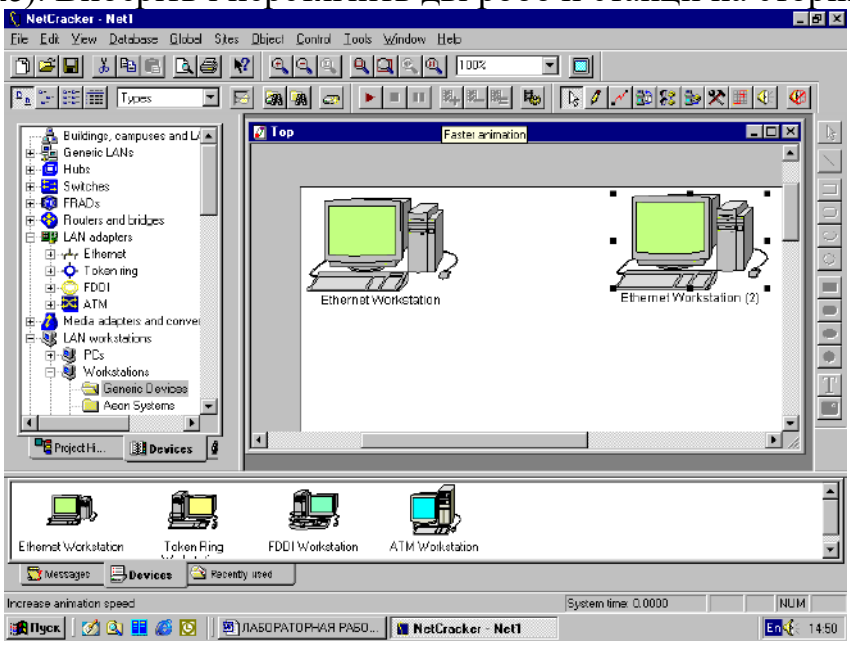
1. Відкриття нового проекту.

Натисніть *New* у меню *File*. NetCracker відкриє вікно *Top Site*.



2. Вибір робочої станції.

Перегляньте базу даних пристроїв (*Device database*), і двічі натисніть на папках у такій послідовності: *LAN workstations* → *Workstation* → *Generic device*. NetCracker відобразить робочі станції, які він розташує, в області вікна зображення виробів (*Product Image pane*). Виберіть і перетягніть дві робочі станції на сторінку проекту.



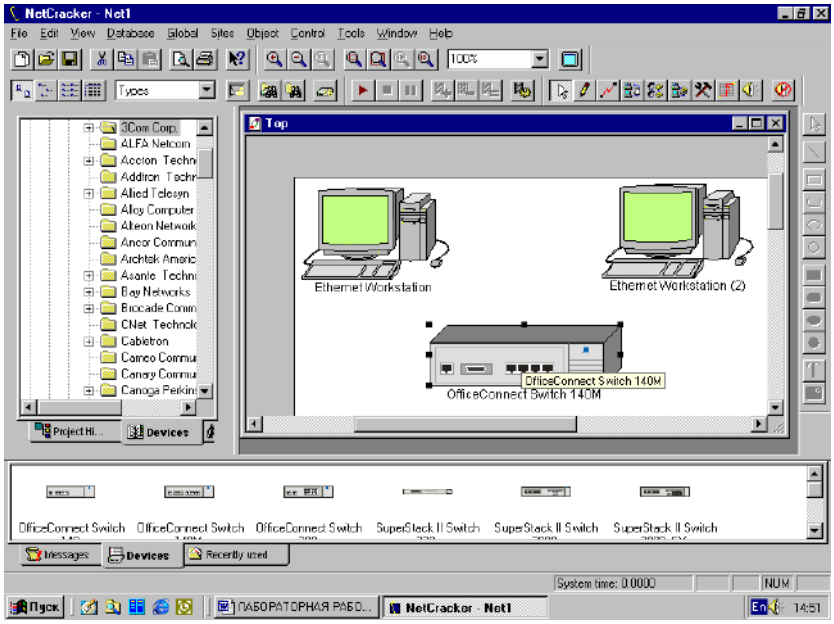
3. Вибір і додавання мережних адаптерів.

Використовуйте базу даних пристроїв (*Device database*) для пошуку мережних карт LAN (*LAN adapters*) і двічі натисніть на відповідній папці. Потім двічі

натисніть на папці Ethernet. Натисніть на папці *Generic devices*. Виберіть в області вікна зображення виробів (*Product Image Pane*) необхідний адаптер Ethernet і, перетягнувши його на сторінку проекту, розмістіть на одній з робочих станцій. Зверніть увагу, що курсор зміниться від знаку зупинки до знака "плюс", після того як Ви сполучите плату, що перетягується, з робочою станцією. Повторіть те саме для другої робочої станції.

4. Вибір і додавання комутатора.

Поверніться до *Device database*. Двічі натисніть послідовно на папках: *Switches* → *Workgroup* і перетягніть комутатор з області вікна зображення виробів (*Product Image pane*) на сторінку проекту.



5. Редагування текстових заголовків.

а. Натисніть кнопку *Standard* на інструментальній панелі *Modes* і двічі натисніть на заголовку, що редагується.

6. З'явиться діалогове вікно *Text Editor*, у якому необхідно ввести нові заголовки.

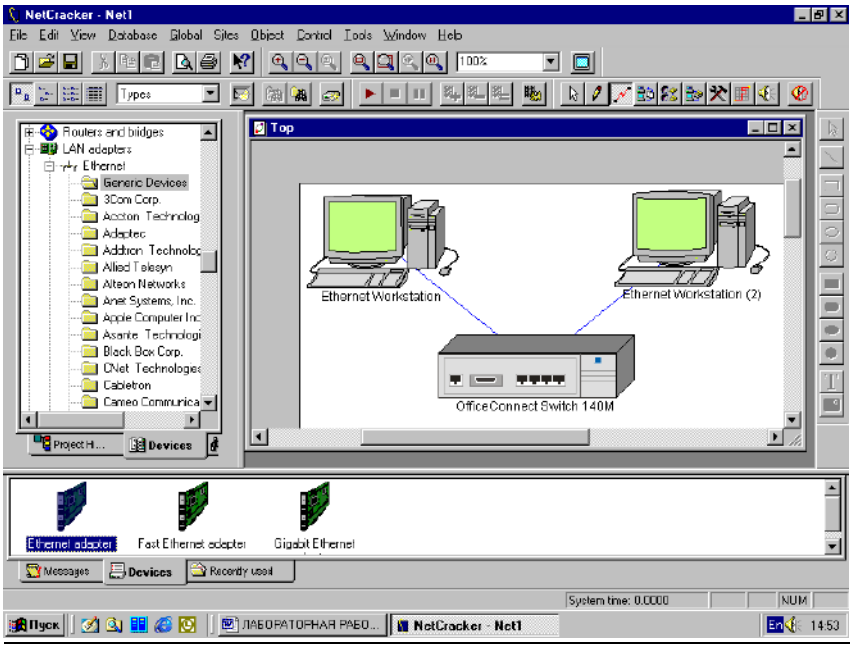
6.З'єднання робочих станцій і комутатора каналом зв'язку.

а. Натисніть кнопку *Device database* на інструментальній панелі *Modes*.

б. З покажчиком у режимі *Link*, натисніть на одній робочій станції, і потім натисніть на комутатор. NetCracker відкриє діалогове вікно *Link Assistant*.

в. Щоб прийняти задані за замовчуванням значення портів і створити зв'язок, натисніть кнопку *Link* та натисніть *Close*.

г. Використайте Швидкий Зв'язок, для цього натисніть на комутаторі і, утримуючи клавішу SHIFT, перемістіть курсор до другої робочої станції, натисніть на ній. Відпустіть клавішу SHIFT.



7. Генерація профілів.

а. Щоб згенерувати профіль між двома пристроями, натисніть кнопку *Set Traffic*.

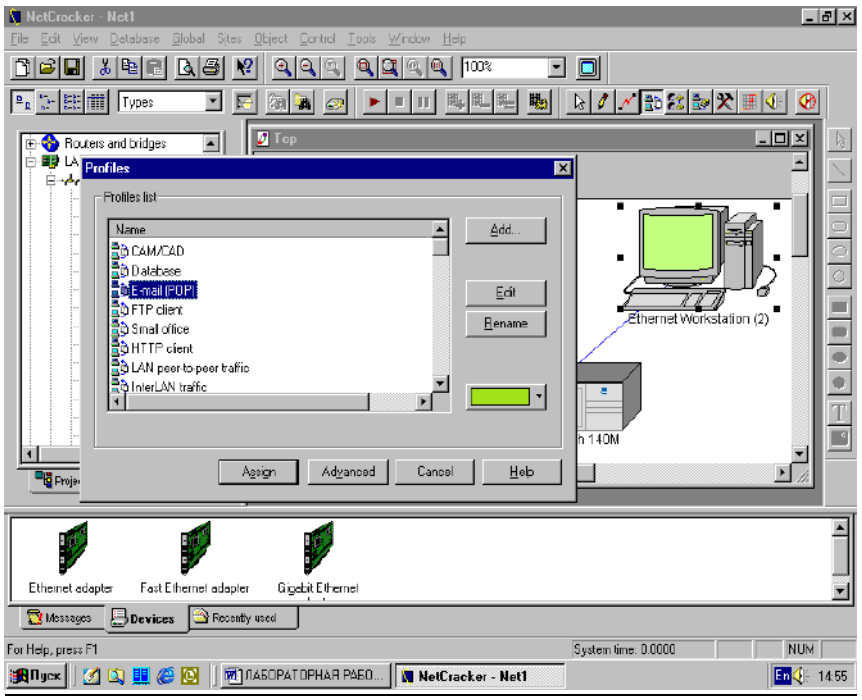
б. Натисніть на одній робочій станції, потім натисніть по іншій робочій станції. NetCracker відкриє діалогове вікно *Profiles*.

в. У вікні *Profiles list* виберіть необхідний профіль.

г. За необхідності зміни значень для обраного типу а в діалоговому вікні *Profiles* натисніть кнопку *Edit* і введіть нові значення.

д. Натисніть кнопку *Assign*, щоб призначити тип а між пристроями.

е. Закрийте діалогове вікно *Profiles*.



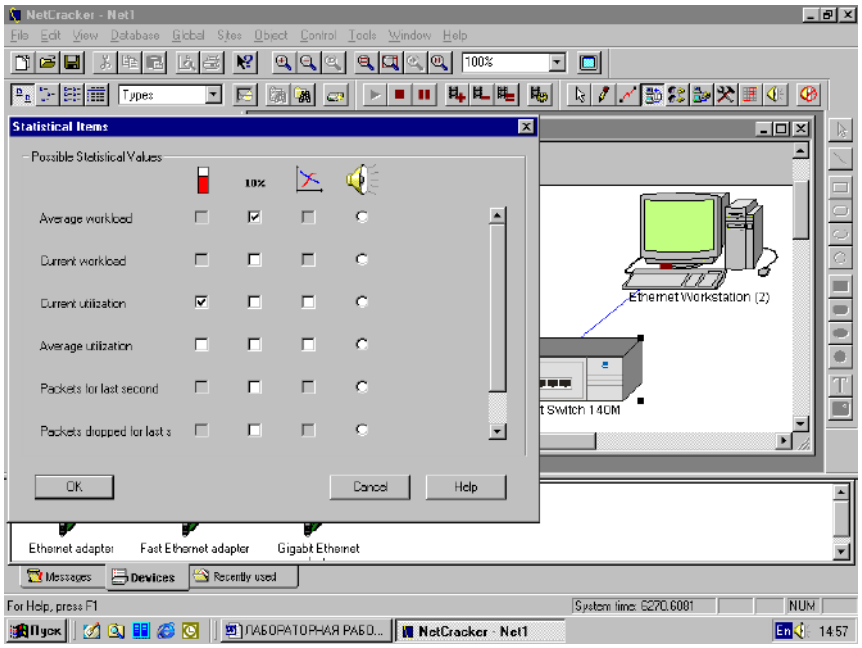
8. Запуск анімації.

Натисніть кнопку *Start* на інструментальній панелі *Control*, щоб спостерігати обраний тип а.

9. Одержання даних статистики

а. Натисніть на аналізованому мережному пристрої і з меню *Object* виберіть *Define Statistics* (чи натисніть праву кнопку мишки у меню, що з'явилося, виберіть *Statistics*).

б. У діалоговому вікні, що з'явилося, *Statistical Items* зазначено типи можливих статистичних значень.



До них зокрема відносяться:
Average workload – Середнє робоче навантаження;
Current workload – Поточне робоче навантаження;
Current utilization – Поточне використання;
Packets for last second – Пакети за останню секунду;
Packets dropped for last second – Пакети, що пропали за останню секунду;
Calls received – Отримано запитів;
Calls blocked – Блоковано запитів;
Packets received – Отримано пакетів;
Transaction received – Отримано транзакцій;
Responses received – Отримано відповідей (реакцій, відгуків);
Transaction sent – Послано транзакцій;
Completely discarded – Цілком забраковано;
Average response time – Середній час відповіді;
Average transaction length – Середня довжина транзакції;
Calls established – Встановлено запитів;
Calls requested – Необхідні запити (викликано запитів);
Average call length – Середня довжина запиту;
Average delay – Середній час очікування.

10. Збереження проекту.

а. Зупиніть анімацію, використовуючи кнопку *Stop* на інструментальній панелі *Control*.

б. У меню *File* виберіть команду *Save*. Відобразиться діалогове вікно *Save As*.

в. Виберіть директорію і введіть ім'я файла, під яким Ви хочете зберегти проект і натисніть *Save*.

3. Змоделювати роботу основних базових топологій («шина», «зірка» і «кільце»), за якими будуються локальні мережі.

4. Дослідити ефективність мережі побудованої за тією чи іншою топологією. Зробити відповідні висновки. Порівняти з теоретичними відомостями.

5. Збільшуючи інтенсивність знайти реальну продуктивність мереж, побудованих за різними топологіями. Порівняти з теоретичними даними.

6. Подивитися, що відбудеться з мережами, при виході з ладу яких-небудь мережних елементів.

7. За одним із завдань, вказаному в табл. 2.1., провести моделювання локальної мережі за технологією Ethernet з використанням різних стандартів фізичного середовища. Особливістю моделювання в даній лабораторній роботі є те, що усі без винятку завдання припускають багаторівневу архітектуру локальних мереж, наявність сервера і застосування конкретних моделей мережних пристроїв і компонентів. Під час виконання завдання необхідно приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів. Мережні пристрої в моделі мають бути з'єднані необхідними зв'язками і між ними мають бути задані різні варіанти.

Таблиця 2.1 – ІНДИВІДУАЛЬНІ ЗАВДАННЯ ДО ЛАБОРАТОРНОЇ РОБОТИ №2

Номер завдання	Зміст завдання
1	Змоделювати мережу за технологією Ethernet для РОВС, який розташований у 2-х будинках. В одному будинку працює 7 комп'ютерів, другому 3. В одному будинку три кімнати: кімната начальника (1 комп'ютер), кімната адміністратора мережі (1 комп'ютер), кімната співробітників (5 комп'ютерів). Відстань між будинками 100м. Один зі стандартів для дослідження 10Base-5. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
2	Змоделювати мережу гуртожитку. Будинок 3-х поверховий, на кожному поверсі дві кімнати, на які приходиться по одному комп'ютеру. Один з комп'ютерів виконує функції Файл і E-mail-сервера. Мережа має бути як можна простіше і дешевше. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
3	Побудувати модель банківської мережі. Банку належить три будинки. В одному з них розташований офіс. Будинки розташовані на відстані

	до 2 км. В офісі знаходиться вся база даних по клієнтурі, звідки ж здійснюється керування мережею і розподіл між підрозділами банку. В офісі 10 комп'ютерів, в інших будинках по 5. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
4	Змоделювати мережу кампуса, тобто зв'язати для початку два студентських гуртожитки між собою. Гуртожитки двоповерхові, на кожному поверсі по 3 - 5 комп'ютерів. Відстань між будинками гуртожитку близько 333м. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
5	Змоделювати мережу за технологією Ethernet для магазину, який розташований у 3-х будинках. В одному будинку працює 8 комп'ютерів, другому 4. В одному будинку 4 кімнати: кімната начальника (1 комп'ютер), кімната менеджера магазину (1 комп'ютер), кімната сервісної підтримки та реклами (6 комп'ютерів), кімната бухгалтерії (2 комп'ютери)... Відстань між будинками 100м. Один зі стандартів для дослідження 10Base-5. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
6	Змоделювати мережу фірми, яка розташована у два-х поверховому будинку, на кожному поверсі три кімнати, на які приходиться по одному комп'ютеру. Один з комп'ютерів виконує функції Файл і E-mail-сервера. Мережа має бути як можна простіша і дешевше. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
7	Побудувати модель мережі підприємства, якому належить 4 будинки. В одному з них розташований склад. Будинки розташовані на відстані до 1 км один від одного. В будинку складу знаходиться вся база даних по товару підприємства, звідки ж здійснюється керування мережею і розподіл між цехами товару. В будинку складу 7 комп'ютерів, в інших будинках по 4. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.
8	Змоделювати мережу училища, тобто зв'язати для початку три навчальних корпуси між собою. Корпуси триповерхові, на кожному поверсі по 2 - 3 комп'ютери. Відстань між корпусами училища близько 290м. Приділити особливу увагу захисту інформації на рівні мережних пристроїв і компонентів.

Алгоритм дій під час виконання другої частини лабораторної роботи.

1. Щоб визначити місце розташування пристроїв, що є сумісними з обраним пристроєм, необхідно зробити таке:

а. Натиснути на пристрої;

б. Вибрати команду Find Compatible з меню Object чи натиснути Compatible у вікні бази даних пристроїв (Device database).

2. Створення проекту з багаторівневою архітектурою. Як правильно розгорнути

«будівлю»

а. Натиснути в базі даних пристроїв (Device database) на папці Building, campuses and LAN.

б. В області вікна зображення виробів (Product Image Pane) виберіть необхідну «будівлю» і перетягніть на вікно проекту. Тепер це Ваше основне вікно багаторівневого проекту.

в. Натисніть правою кнопкою мишки на «будівлі» і у контекстному меню виберіть Expand.

г. З'явиться додаткове вікно проекту, у якому Ви можете відобразити пристрої, що входять у «будівлю» чи навпаки відобразити «будівлі», що більш докладно описують основну «будівлю». Ці «будівлі» потім можна також додатково заповнити мережними пристроями, відкривши додаткові рівні проекту.

3. Заповнення «будівлі» пристроями

а. Перетягнути необхідний мережний пристрій.

б. Щоб повторно не виконувати ту ж операцію, необхідно з меню Edit вибрати Duplicate.

4. Виділення тракту проходження даних а від одного пристрою до іншого з використанням режиму Trace на одному з рівнів проекту.

а. На інструментальній панелі Mode натиснути на кнопку Trace.

б. Натиснути на одній з робочих станцій, потім на іншій – червоним кольором виділиться шлях проходження даних між ними.

5. Виділення тракту проходження даних а від одного пристрою до іншого з використанням режиму Trace на різних рівнях проекту.

а. На інструментальній панелі Mode натиснути на кнопку Trace.

б. Натиснути на одній робочій станції в одному вікні, потім на об'єкті в іншому вікні. Червоним кольором висвітиться необхідний тракт.

6. Створення каналу зв'язку між двома будівлями.

У вікні основного проекту на інструментальній панелі Mode вибирають Link і за стандартною процедурою встановлюють канал між двома «будівлями». Між ними з'являється пунктирна лінія, що говорить про те, що зв'язок установлений не до кінця. Потім необхідно перейти у вікно будівлі і, заново вибравши Link, натиснути на конкретному пристрої, що відповідатиме, за з'єднання цього «будівлі» з іншим, а потім те саме на другій «будівлі». Установиться повноцінне з'єднання. Піктограма другої «будівлі» з'явиться в робочій області пристроїв першої «будівлі».

ЗАУВАЖЕННЯ: Якщо друга «будівля» також має вкладену архітектуру, то необхідно вибрати пристрій, що зв'язуватиме її з першою «будівлею».

7. Щоб зробити одну з робочих станцій сервером, необхідно проробити таке:

а. У вікні бази даних пристроїв (Device database) необхідно відкрити кнопку «Network and enterprise software».

б. Натиснути на кнопку «Server software». В області вікна зображення виробів (Product Image Pane) відобразяться типи серверів.

в. Перетягнути необхідний тип (чи кілька типів) серверного програмного забезпечення до робочої станції, що Ви виділили під сервер.

8. Додавання клієнт - сервер відбувається в такий спосіб:

а. На інструментальній панелі Modes вибирають Set traffic.

б. В основному вікні проекту натиснути на «будівлі» без серверного програмного забезпечення, потім у вікні іншої «будівлі» натиснути на робочій станції із серверним програмним забезпеченням.

в. Вибрати стандартним засобом необхідний профайл.

9. Контроль завдання і зміна існуючих профайлів трафіка.

а. У меню Global вибрати Data Flow.

б. З'явиться вікно Data Flow, у якому відобразяться всі типи трафіка, з зазначенням маршруту, що були задані в процесі створення проекту.

в. Для зміни конкретного типу трафіка необхідно двічі на ньому натиснути.

2.6 Зміст звіту

Звіт має містити:

– Назву, мету, стислі теоретичні відомості за досліджуваною проблемою; структурні схеми змодельованої мережі (за кожним стандартом); статистичні дані (на підставі яких проводився аналіз моделі); висновки.

– Висновки мають містити аналіз результатів, отриманих у результаті виконання лабораторної роботи і їх порівняння з теоретичними відомостями за досліджуваною проблемою.

2.7 Запитання та завдання для потокового контролю підготовленості студентів до виконання лабораторної роботи

1. Які основні механізми доступу до середовища стандарту Ethernet.
2. Розкрийте зміст механізму множинного доступу з контролем загальної шини і запобіганням колізіям.
3. Розкрийте зміст механізму множинного доступу з контролем загальної шини і виявленням колізій.
4. Надайте класифікацію стандарту Ethernet у залежності від типу фізичного середовища.
5. Розкрийте основні особливості мережного обладнання та стандартів фізичного середовища Ethernet.
6. Наведіть приклади мережного обладнання, яке забезпечує трансляцію мережних адрес у локальних комп’ютерних мережах стандарту Ethernet.
7. Наведіть приклади шифраторів, які забезпечують конфіденційність інформації, яка циркулює в локальних комп’ютерних мережах.
8. Яке основне призначення та можливості програмного середовища NetCracker 4.1.

3 ПРОЕКТУВАННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ЗМІШАНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Мета роботи

Мета роботи – одержати уявлення про основні технології канального та фізичного рівнів моделі OSI та апаратні засоби захисту інформації в комп'ютерних мережах змішаного типу.

3.2 Завдання лабораторної роботи

– За заданими початковими умовами змоделювати змішану захищену комп'ютерну мережу на основі технологій канального та фізичного рівнів (ATM, Token ring).

– За допомогою отриманих на лекціях теоретичних знань створити захищений сегмент комп'ютерної мережі та «демілітаризовану зону».

– Дослідити вплив окремих елементів захисту інформації (шифраторів, брандмауерів) на ефективність роботи комп'ютерної мережі та стан забезпечення основних послуг безпеки інформації.

3.3 Методичні вказівки з організації самостійної роботи

– Вивчити теоретичний матеріал лекцій «Брандмауери, основні елементи брандмауерів» та «Програмний пакет NetCracker, v 4.1.».

– Підготувати відповіді на контрольні запитання.

– Підготувати бланк звіту з лабораторної роботи.

Допуск до виконання лабораторної роботи здійснюється за результатами письмового опитування.

3.4 Загальнотеоретичні положення

3.4.1 Технологія ATM. Основні базові принципи

Корпоративні мережні стандарти дозволяють забезпечити ефективну взаємодію всіх станцій мережі за рахунок використання однакових версій програм і однотипної конфігурації. Проте, значні складнощі виникають при уніфікації технології доступу робочих станцій до WAN-сервісу, оскільки в цьому випадку відбувається перетворення даних з формату Token ring або Ethernet у формати типу X.25 або T1/E1. ATM забезпечує зв'язок між станціями однієї мережі або передачу даних через WAN-мережі без зміни формату кадрів - технологія ATM є універсальним рішенням для ЛВС і телекомунікацій.

Осередки ATM. Традиційним способом передачі нерівномірного навантаження є той або інший вид комутації повідомлень (пакетів).

Пакети АТМ називаються осередками (cell), оскільки всі вони мають фіксовану довжину. Довжина осередків АТМ рівна 53 байтам (октету), з яких 48 байт відводиться для передачі інформації (даних) і 5 байт для заголовка. Інформація, що міститься в 5 байтах заголовка, достатня для доставки мережею кожного осередку за призначенням.

Заголовок містить інформацію, що дозволяє передати осередок користувачу

Приклади АТМ-КОМУТАТОРІВ для локальних мереж.

Комутатори CELLplex компанії 3Com.

Комутатор CELLplex 7000 є модульним пристроєм на основі шасі, що здійснює комутацію до 16 портів АТМ (4 модулі по 4 порти). Він призначений для утворення високошвидкісної АТМ-МАГІСТРАЛІ мережі шляхом з'єднання з іншими АТМ-КОМУТАТОРАМИ чи ж для підключення високошвидкісних АТМ-ВУЗЛІВ до стягнутої в точку магістралі мережі на основі центру даних, що має порт АТМ.

Комутаційний центр забезпечує обмін даними за схемою 16 (16, використовуючи неблокуючу технологію комутації "на льоту" із загальною пропускною спроможністю 2.56 Гб/с і підтримуючи до 4096 віртуальних каналів на порт.

Пасивна внутрішня шина комутатора забезпечує передачу даних зі швидкістю до 20.48 Гб/с, забезпечуючи перехід в майбутньому на інтерфейсні модулі з великою кількістю портів або з швидкіснішими портами.

Повністю надмірне шасі із здвоєним джерелом живлення, продубльованим комутаційним центром і модульну побудову роблять комутатор CELLplex 7000 відмовостійким пристроєм, відповідним для побудови магістралі мережі і задовольняючим вимогам найбільш важливих додатків.

Є два типи інтерфейсних модулів:

– модуль з чотирма портами ОС-3с 155 Мб/с для багатомодового оптоволоконного кабелю, призначений для локальних зв'язків;

– модуль з чотирма портами DS-3 45 Мб/с – для глобальних зв'язків.

Комутатор підтримує основні специфікації технології АТМ: встановлення комутованих віртуальних каналів (SVC) за специфікаціями UNI 3.0 і 3.1, підтримку постійних віртуальних каналів (PVC) за допомогою системи управління, Interim Interswitch Signaling Protocol (IISP), емуляцію локальних мереж (LAN emulation), управління перевантаженнями (congestion management).

Управління комутатором реалізоване для стандартів: SNMP, ILMI, MIB 2, ATM MIB, SONET MIB. Використовується система управління Transcend.

Комутатор CELLplex 7200 суміщує функції АТМ-КОМУТАТОРА і Ethernet-комутатора, одночасно дозволяючи ліквідовувати вузькі місця на магістралі мережі і в мережах відділів.

CELLplex 7200 забезпечує повношвидкісні Ethernet-канали для сегментів локальних мереж, серверів і окремих робочих станцій, що вимагають підвищеної швидкодії, що розділяються. Окрім цього, комутатор може бути конфігурований з портами АТМ для з'єднання з комутаторами робочих груп, АТМ-СЕРВЕРАМИ і робочими станціями, а також для підключення до АТМ-МАГІСТРАЛІ мережі.

Комутаційний АТМ-ЦЕНТР (8(8) суміщений з процесором Ethernet/ATM комутації на мікросхемі ZipChip. ZipChip перетворить пакети даних Ethernet у стандартні осередки АТМ, а потім комутує їх з швидкістю до 780000 осередків за секунду.

На відміну від моделі CELLplex 7000 модель CELLplex 7200 має не два, а чотири типи інтерфейсних модулів:

- модуль з двома портами АТМ OC-3c;
- модуль з двома портами DS-3;
- модуль з 12 портами Ethernet і одним портом АТМ OC-3c;
- модуль з 12 портами Ethernet і одним портом АТМ DS-3.

Решта характеристик комутаторів CELLplex 7200 і CELLplex 7000 практично співпадає.

Комутатори технології АТМ LattisCell і EtherCell компанії Bay Networks

Сімейство продуктів, розроблених компанією Bay Networks для технології АТМ, складається з комутаторів LattisCell (тільки АТМ-КОМУТАЦИЯ), комутатора EtherCell (комутація Ethernet-АТМ), програмного забезпечення АТМ Connection Management System і програмного забезпечення АТМ Network Management Application.

Поставляється декілька моделей комутаторів АТМ, кожний з яких забезпечує певне поєднання фізичних рівнів, середовищ передачі і можливостей резервування джерел живлення.

Комутатор EtherCell призначений для усунення "вузьких місць" в робочих групах локальних мереж, що використовують традиційне середовище передачі даних технології Ethernet, що розділяється. За допомогою цього комутатора можна розвантажити лінії зв'язку з серверами і маршрутизаторами. Модель 10328 EtherCell має 12 портів 10Base-T і прямий доступ до мережі АТМ. Порти Ethernet можуть надавати виділену смугу пропускання 10 Мб/с за рахунок їх комутації.

Програмне забезпечення АТМ Connection Management System (CMS) розміщується на робочій станції SunSPARCStation, виконуючи функції координації і управління з'єднаннями комутатора. CMS автоматично вивчає мережну топологію і встановлює віртуальні АТМ-З'ЄДНАННЯ між взаємодіючими станціями.

Програмне забезпечення АТМ Network Management Application, працюючи спільно з CMS, забезпечує управління мережею АТМ на центральній станції управління.

Модель ATM комутатора LattisCell 10114A розроблена для використання в мережах кампусів (відстань між комутаторами до 2 км) і є пристроєм, виконаним у вигляді автономного корпусу з фіксованою кількістю портів, число яких рівне 16. Для кожного порту забезпечується пропускна спроможність в 155 Мб/с по багатомодовому оптоволоконному кабелю. Функції фізичного рівня реалізовані відповідно до стандартів SONET/SDH 155 Мб/с, а також UNI 3.0.

Архітектура FastMatrix забезпечує загальну внутрішню швидкість передачі даних 5 Гб/с, що дозволяє проводити комутацію всіх портів без блокувань. Підтримуються функції широкомовної (broadcast) і багатомовної (multicast) передачі.

Запит на встановлення з'єднання може бути виконаний для різних рівнів якості сервісу (Quality of Service, QoS):

– QoS 1 – використовується для сервісу CBR (постійна бітова швидкість);

– QoS 2 – використовується для сервісу VBR RT (змінна бітова швидкість додатків реального часу);

– QoS 3/4 – використовується для сервісу VBR, призначеного для передачі даних локальних мереж за процедурами зі встановленням з'єднань і без встановлення з'єднань;

– QoS 0 – використовується для сервісу UBR.

Управління пристроєм здійснюється також за допомогою програмної системи CMS, для якої необхідні: SunSPARCStation 2 або вище, Sun OS 4.1.3 або вище для невиділеного Ethernet-з'єднання або Solaris 2.4 для прямого ATM-З'ЄДНАННЯ.

Інші моделі комутаторів LattisCell (10114R, 10114A-SM, 10114R-SM, 10114R-SM, 10114-DS3, 10114-E3, 10115A, 10115R) розрізняються наявністю резервного джерела живлення, а також типом портів (загальна кількість портів у будь-якій моделі складає 16). Окрім багатомодових портів, комутатори можуть мати одномодові оптоволоконні порти (для мереж кампусів з відстанню до 25 км), а також порти для коаксіального кабелю з інтерфесами DS-3 (45 Мб/с) і E3 (34 Мб/с) для підключення до глобальних мереж через лінії T3/E3.

Моделі комутатора EtherCell (10328-F і 10328-SM) забезпечують комутацію Ethernet-Ethernet і Ethernet-ATM. Ці моделі мають 12 портів 10Base-T RJ-45 і один порт прямого доступу до ATM із швидкістю 10 Мб/с. Порти 10Base-T можуть використовуватися для надання повної швидкості 10 Мб/с виділеної лінії для високошвидкісних серверів чи ж для розділення її між сегментом станцій робочої групи.

Комутатор LightStream 1010 компанії Cisco

Комутатор LightStream 1010 є ATM комутатором для утворення магістралей мереж відділів або кампусів.

Комутатор володіє загальною продуктивністю 5 Гб/с і виконаний на базі 5-слотового шасі.

У центральному слоті встановлюється модуль управління комутацією ATM Switch Processor (ASP), який має пам'ять, що розділяється, із швидкістю доступу 5 Гб/с, повністю неблокуючу комутаційну матрицю, а також високопродуктивний

RISC-процесор MIPS R4600 100 MHz. Модуль ASP працює під управлінням міжмережної операційної системи IOS, як і маршрутизатори і комутатори старших моделей компанії Cisco. Програмне забезпечення модуля ASP може замінюватися "на ходу", тобто без зупинки комутатора, що важливо в умовах специфікацій, що часто змінюються, ATM Forum.

Чотири слоти, що залишилися, використовуються для установки інтерфейсних модулів CAM, у кожний з яких можна встановити до 2-х модулів адаптерів портів PAM. Отже, комутатор може мати в максимальній конфігурації до 8 модулів PAM з такого набору:

- 1 порт ATM 622 Мб/с (OC12) (одномодовий);
- 1 порт ATM 622 Мб/с (OC12) (багатомодовий);
- 4 порти ATM 155 Мб/с (OC3c) (одномодовий);
- 4 порти ATM 155 Мб/с (OC3c) (багатомодовий);
- 4 порти ATM 155 Мб/с (OC3c) (по неекранованій витій парі UTP Cat 5);
- 2 порти DS3/T3 45 Мб/с;
- 2 порти E3 34 Мб/с.

Комутатор LightStream 1010 одним з перших у галузі підтримує специфікацію маршрутизації PNNI Phase 1, необхідну для маршрутизації комутованих з'єднань (SVC) в неоднорідних ATM-МЕРЕЖАХ з урахуванням необхідної якості обслуговування.

Комутатор LightStream 1010 може виконувати роль центрального комутатора в мережі кампусу (рис. 3.1.).

3.4.2 Основні принципи забезпечення безпеки в змішаній комп'ютерній мережі, захист за допомогою брандмауерів.

При підключенні мережі організації до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів щодо її захисту.

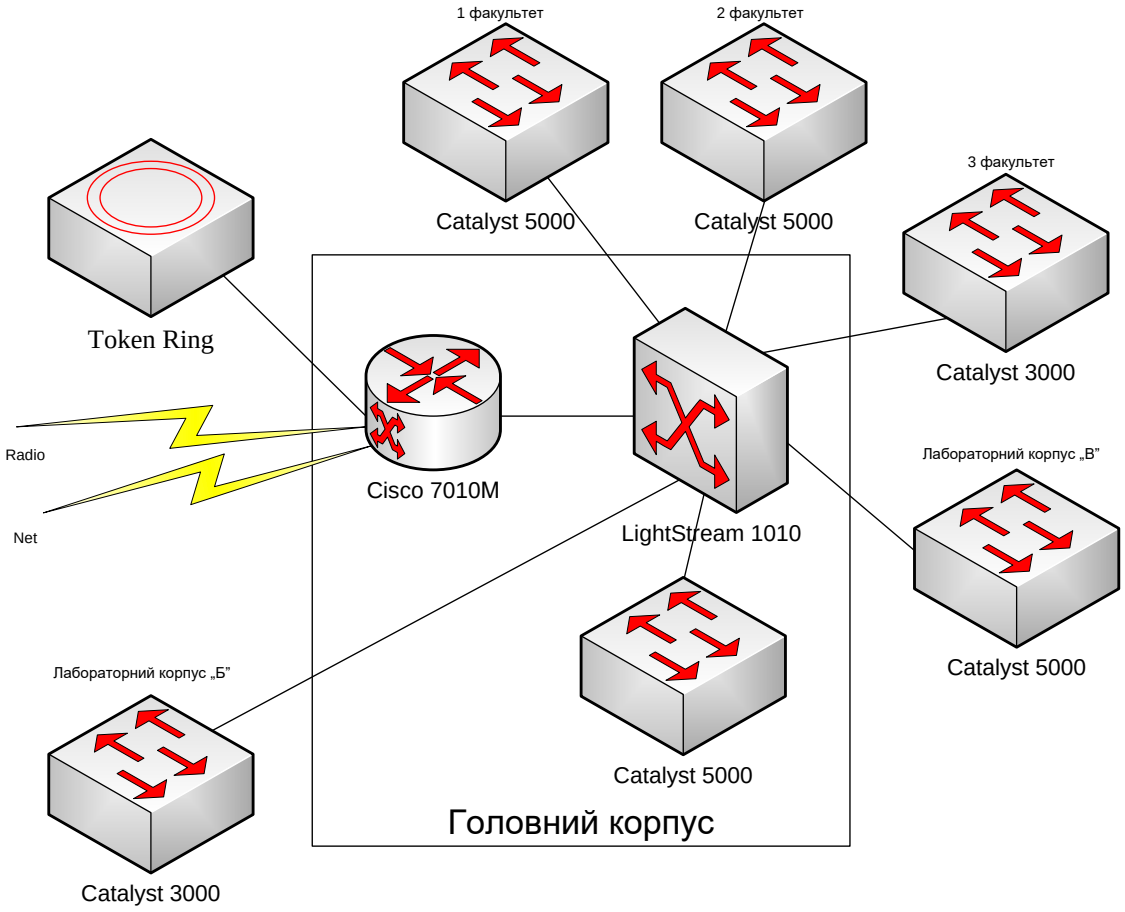


Рисунок 3.1 – Приклад мережі навчального закладу з використанням АТМ-обладнання

При побудові захисту слід виходити з того, що будь-який захист ускладнює використання системи, що захищається, за прямим призначенням, обмежує функціональні можливості, використовує обчислювальні і трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вищий захист, тим більш дорогою у створенні та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів. Тому, захищаючи мережу, слід виходити з доцільної вартості захисту. Тобто, витрати на захист мають бути пропорційні цінності ресурсу, що захищається.

Існує ряд основних принципів, що дозволяють організувати досить безпечне підключення до мережі Інтернет порівняно простими засобами.

Мабуть, основним загальновизнаним засобом такого захисту є міжмережний екран **(Брандмауер)**. Міжмережний екран встановлюється між мережею, що захищається і мережею Інтернет, і виконує роль мережного фільтра. Він настроюється так, щоб пропускати допустимий трафік від користувачів мережі, що захищається до служб Інтернет і назад, і обмежити трафік з боку Інтернет у мережу, що захищається тільки необхідними службами, наприклад: smtp, dns, ntp.

Допустимість того або іншого трафіка визначається мережним

адміністратором відповідно до політики інформаційної безпеки організації. Наприклад, може бути дозволений доступ з частини комп'ютерів мережі, що захищається до web і ftp-серверів Інтернет і двонаправлений доступ між Інтернет і поштовим сервером мережі, що захищається, але заборонені всі інші протоколи і напрями трафіка.

З огляду на те, що міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора), логічно представляється доцільним об’єднати їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і, безпосередньо, сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (називається Firewall Feature Set). Проте дане правило є необов'язковим і міжмережний екран може бути представлено окремим пристроєм.

У простому випадку виконання функцій міжмережного екрану можна організувати за допомогою мережного фільтра на основі листів доступу (access-lists). Листи доступу визначають правила, за якими вирішується або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого всередині самого маршрутизатора. IP адреса або діапазон IP адрес джерела і приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак IP-пакета можуть використовуватися як ознаки (рис. 3.2).

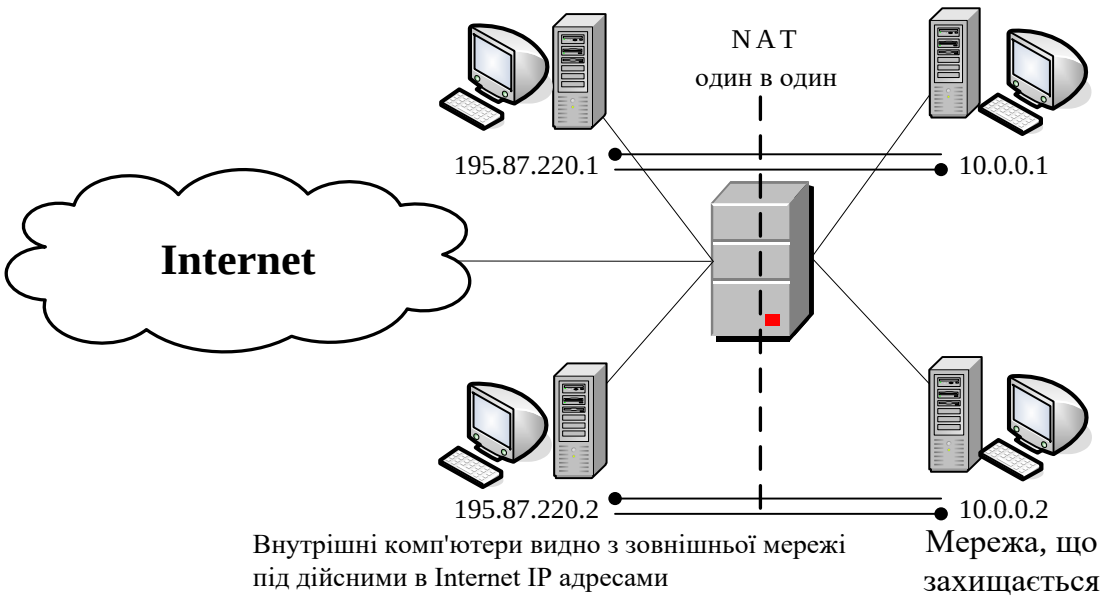


Рисунок 3.2 – Приклад побудови мережі на основі листів доступу

Відмінність і недолік листів доступу в порівнянні зі справжнім міжмережним екраном полягає в тому, що вони дозволяють створити статичний односторонній фільтр, тоді як мережне з'єднання є динамічним процесом. Листи доступу не дозволяють контролювати параметри IP-пакета, залежні від попередніх пакетів.

Звідси виникає складність застосування листів доступу для тонкої настройки фільтрації трафіка в точній відповідності з прийнятою політикою безпеки. Зокрема, з цієї причини листи доступу не в змозі захистити від такого різновиду мережної атаки, як «крадіжка з'єднання», або «хай-джекинг».

У Firewall Feature Set вказані проблеми вирішуються за допомогою того, що він відстежує кожне мережне з'єднання окремо і контролює весь процес у динаміці. При встановленні нового TCP-сеансу міжмережний екран створює для нього новий процес, який контролює правильність з'єднання до самого моменту його завершення. При цьому кожен пакет, що приходить на транспортному рівні, перевіряється на відповідність попередньому, а всі «підозрілі» пакети вибраковуються.

Таким чином, стає можливим застосування фільтра доступу внутрішнього комп'ютера до зовнішньої мережі, що не дозволяє зовнішньому комп'ютеру самостійно звернутися до внутрішнього. Іншими словами, в налаштуваннях міжмережного екрану задаються правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напряму і кожного тракту окремо. Якщо правило вирішує проходження IP-пакета від інтерфейсу внутрішньої мережі до Інтернет - інтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який вже можуть пройти у відповідь пакети від зовнішнього одержувача. Як тільки з'єднання переривається, або вичерпується час очікування, тунель закривається, і звернення ззовні до внутрішнього комп'ютера будуть виключені. З цієї ж причини екран не пропустить пакети у зворотному напрямку, якщо ініціатором з'єднання є зовнішній комп'ютер. Крім того, міжмережний екран, на відміну від листів доступу, може контролювати зміст IP пакетів у полі даних і відбраковувати пакети, що містять потенційно-небезпечні коди, наприклад java-аплети. Існують міжмережні екрани, здатні виявити в IP-пакетах ознаки відомих мережних атак і перервати таке з'єднання, але це вже достатньо дорогі системи.

Другою цеглинкою забезпечення захищеності мережі є «заміна мережної адреси» – (Network Address Translation), або NAT. Це заміна в IP-пакеті реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні її до зовнішньої мережі. Таким чином, для внутрішньої мережі стає можливим використання діапазонів адрес, які не вживаються в мережі Інтернет (10.0.0.0-10.255.255.255). Це дозволяє запобігти прямому зверненню ззовні до внутрішніх комп'ютерів і приховати структуру мережі, що захищається. Існує кілька різновидів NAT. Найбільш простою і найбільш дешевою з точки зору захисту є трансляція фіксованої внутрішньої адреси у фіксованій зовнішній. При цьому зловмисник безперешкодно «бачить» такий комп'ютер у зовнішній мережі, оскільки йому однозначно відповідає певна зовнішня адреса. Проте, вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні.

Друга форма NAT – це трансляція групи внутрішніх адрес до однієї зовнішньої. При цьому всі внутрішні комп'ютери можуть працювати з мережею

Інтернет одночасно, а маршрутизатор розрізняє, кому яку відповідь перетранслювати, за службовими даними TCP-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно ускладнює життя зловмиснику, оскільки повністю приховує внутрішні комп'ютери і перешкоджає «вирахуванню» жертви. Зловмисник, навіть побачивши звернення, що витікають з внутрішньої мережі, не зможе визначити, з якого комп'ютера вони виходять (рис. 3.3).

Крім того, це виключає можливість ініціативного звернення ззовні до внутрішнього комп'ютера, оскільки для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої адреси до внутрішньої.

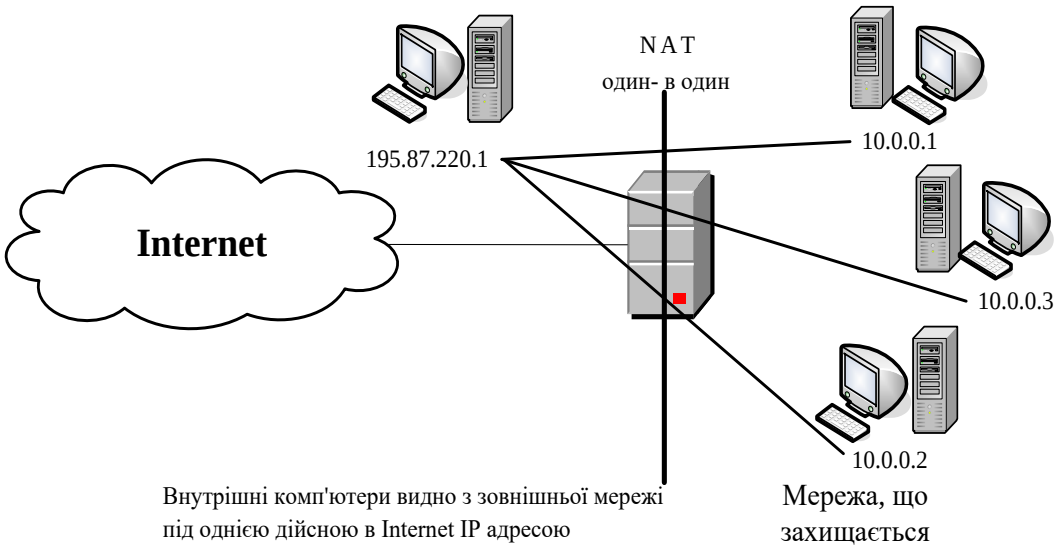


Рисунок 3.3 – Приклад побудови мережі з трансляцією групи внутрішніх адрес до однієї зовнішньої

Третя форма NAT – використання для заміни внутрішніх адрес пулу виділених адрес. Тобто, внутрішній комп'ютер, виходячи в Інтернет, отримує вільну в даний момент адресу з пулу. При цьому адреси підміняються динамічно і кожне нове TCP-з'єднання може бути встановлено з іншою IP-адресою. Це також створює додаткові труднощі зловмиснику, оскільки позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно (рис. 3.4).

Загалом, сказане відносно другої форми NAT, є справедливим і для третьої форми. Якщо запит надходить ззовні, то маршрутизатор не в змозі зв'язати адресу з пулу з адресою в мережі, що захищається. Тому, такий запит не досягне мети.

Демілітаризована зона.

Як правило, організації потрібно мати у себе деякі мережні ресурси, до яких відкрито доступ з мережі Інтернет. Зазвичай це поштовий, dns і web сервери. Механізм їх роботи припускає, можливість вільного або майже не обмеженого

звернення з мережі Інтернет. Відповідно, ймовірність їх зламу вища, ніж решти комп'ютерів мережі.

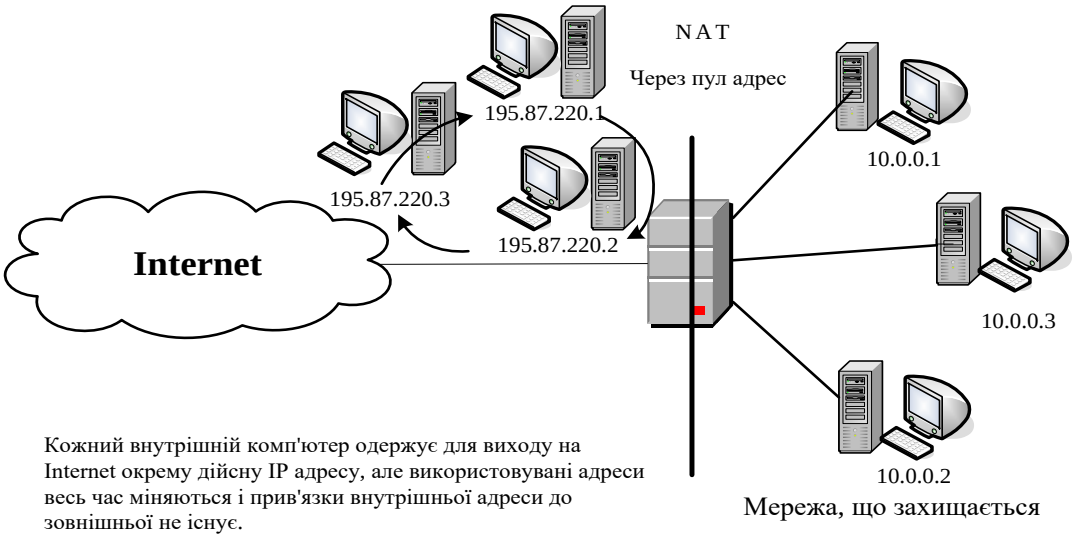


Рисунок 3.4 – Приклад побудови мережі з використанням для заміни внутрішніх адрес пулу виділених адрес

З цієї причини розміщувати їх усередині зони, що захищається, недоцільно з погляду безпеки, оскільки у разі зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів.

Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережним екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну зону їх розміщення називають «демілітаризованою зоною» (див. рис. 3.5).

З рис. 3.5 видно: що ніщо не заважає встановити другий Firewall на основному шлюзі мережі. Це є логічним рішенням і дозволяє одночасно підвищити рівень захисту внутрішньої мережі і захистити сервери «демілітаризованої зони». При правильному налагодженні обох міжмережних екранів зловмиснику буде вже набагато важче дістатися до внутрішньої мережі організації.

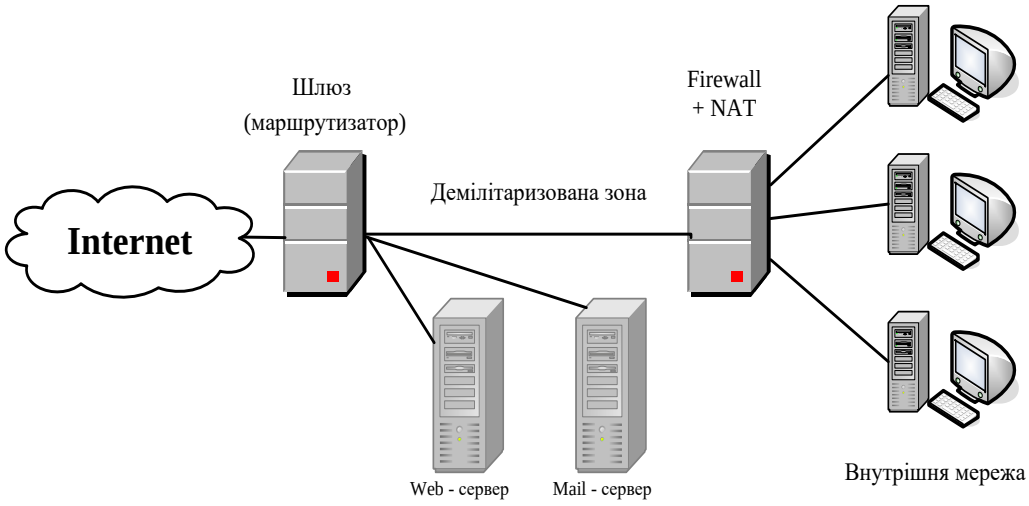


Рисунок 3.5 – Приклад побудови мережі з демілітаризованою зоною

Наявність другого міжмережного екрану (рис 3.6.) дещо ускладнює конфігурацію мережного устаткування і настройку роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використовувати Firewall'и різних виробників. Тоді, якщо в одному з них буде виявлено уразливість, інший не дозволить зловмиснику безперешкодно проникнути до мережі, як це мало б місце при використанні Firewall'ов одного типу.

Тут слід особливо підкреслити, що для унеможливлення зловмисного втручання мережний доступ до шлюзів і міжмережних екранів, має бути відключений. З погляду безпеки, пристрої, що охороняють мережу, повинні конфігуруватися і адмініструватися тільки через консольний порт локально.

Proxy-сервер. Використання proxy-сервера також підвищує рівень захищеності мережі, оскільки виключає необхідність прямого виходу в Інтернет комп'ютерів користувачів. При цьому також стає можливим більш суворий контроль за даними в IP-пакетах на рівні мережних додатків. Proxy-сервер працює як посередник між призначеним для користувача додатком і віддаленим мережним ресурсом до Інтернет. Принцип його роботи схематично показано на рис. 3.7.

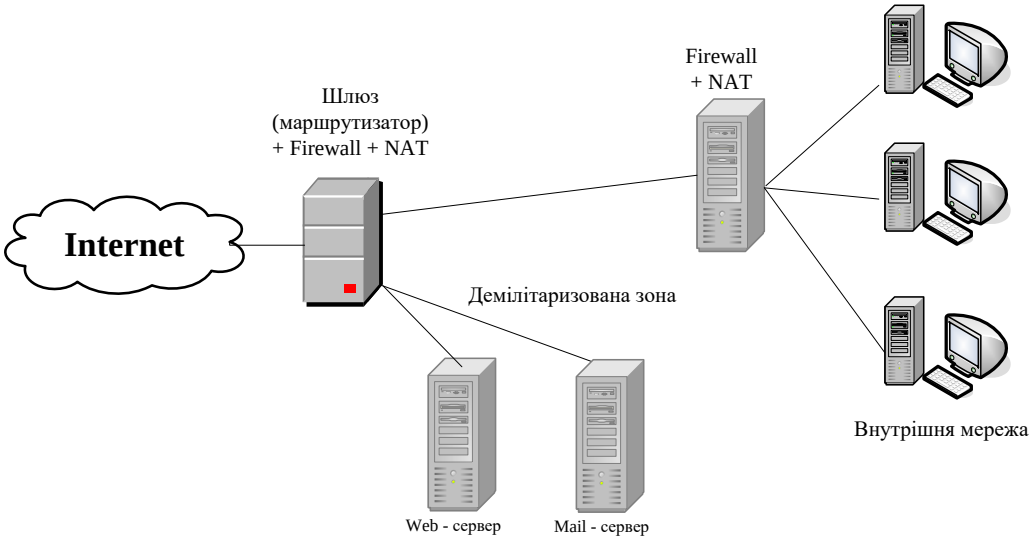


Рисунок 3.6 – Приклад побудови мережі з другим Firewall'ом (брандмауером)

Proxy-сервер складається з двох частин: клієнтської і серверної. Клієнтська частина дивиться у бік Інтернет, серверна – у бік клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до віддаленого сайту через proxy-сервер, його клієнтський мережний додаток взаємодіє з серверною частиною proxy-сервера. При цьому proxy-сервер на рівні додатка передає клієнтський запит своїй клієнтській частині і, вона, вже від імені proxy-сервера, посилає даний запит на віддалений сайт. Тобто в IP-пакеті, що відправляється, стоятиме вже адреса proxy-сервера. Потім одержана відповідь передається у зворотний бік від клієнтської частини proxy-сервера його серверної частини, з якою безпосередньо взаємодіє призначений для користувача комп'ютер.

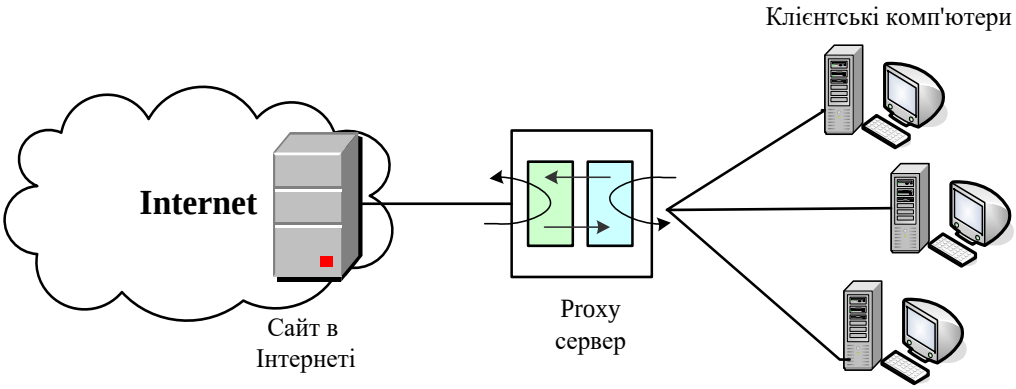


Рисунок 3.7 – Приклад побудови мережі з proxy-сервером

Таким чином, пряме з'єднання клієнтських комп'ютерів з віддаленим сайтом виключається. Усередині proxy-сервера передача даних між клієнтською частиною і

серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатку, чим забезпечується легкість контролю команд і даних на відповідність встановленим стандартам. Крім того, це дозволяє забезпечити достатньо надійний контроль над передачею ймовірних зловмисних кодів усередині даних.

Навіть у разі успішної атаки з боку Інтернет по відкритих протоколах у цьому випадку буде пошкоджено proxy-сервер, що не представляє інформаційної цінності, а призначені для користувача комп'ютери залишатимуться в безпеці ще якийсь час.

Оскільки proxy-сервер працює тільки за кількома відомими протоколами (HTTP, FTP та ін.) і не пропускає через себе решту пакетів, він дуже сильно обмежує можливості зловмисника щодо використання мережних троянських коней для закріплення на якомусь з призначених для користувача комп'ютерів.

Другий mail-сервер. Залишати mail-сервер у демілітаризованій зоні, з одного боку, небажано, оскільки на ньому фактично зберігається поштова база даних з листуванням локальних користувачів, а демілітаризована зона не може забезпечити належного рівня захисту мережним ресурсам. З іншого боку, якщо заховати mail-сервер усередині локальної мережі, то він або не зможе взаємодіяти із зовнішнім світом, або стане брамою з зовнішнього світу до внутрішньої мережі, якою потенційно зможе скористатися зловмисник.

З огляду на це, добрим рішенням є використання двох поштових серверів. Основний сервер встановлюється усередині мережі, що захищається, і не видним для зовнішнього світу. Всі локальні користувачі поштової системи реєструються на ньому і мають до нього прямий доступ. Відповідно, вся вхідна кореспонденція зберігається на ньому в поштових скриньках локальних користувачів. Відправка електронної пошти також здійснюється через нього.

Другий, або зовнішній, поштовий сервер встановлюється в демілітаризованій зоні і забезпечує взаємодію по e-mail з Інтернет. Він настроюється так, щоб всю пошту, що приходить на ім'я користувачів організації, миттєво пересилати на внутрішній поштовий сервер. Таким чином, в його поштовій базі даних немає жодного облікового запису користувачів організації і жоден лист не відправляється на довготривале зберігання. Тобто, якщо зловмисник зламає поштовий сервер, то не отримає доступу до архівів листування. Проте, після зламу, зловмисник отримує можливість перехоплення і читання транзитної пошти. Тому потрібен ретельний контроль за подібною ситуацією і негайне вживання заходів при підозрі на НСД.

Важливою перевагою такої схеми є те, що навіть із зламаного зовнішнього поштового сервера не так просто дістатися до внутрішньої мережі, що захищається. Обмін даними між зовнішнім і внутрішнім поштовими серверами відбувається через міжмережний екран з єдиним дозволеним портом (smtp) по єдиній дозволеній парі адрес. Звернення до інших комп'ютерів і по інших протоколах блокуватиметься. Тому впливати з нього безпосередньо на комп'ютери користувачів внутрішньої мережі неможливо.

Антивірусний захист поштової системи. Операційна система Windows дуже уразлива перед деякими різновидами поштових вірусів. Користувачу достатньо встановити покажчик на інфікований конверт, щоб вірус активізувався. Але набагато небезпечнішим є те, що механізм роботи поштових вірусів може бути використаний зловмисником для закидання в захищену зону мережного троянського коня. Він дозволить зловмиснику потай викачувати дані з вашої мережі і вивідати інформацію, що цікавить його. Тому забезпеченню антивірусного захисту тракту доставки пошти до внутрішньої мережі слід приділити достатньо серйозну увагу.

Існує ряд програмних засобів, призначених для контролю кореспонденції на поштових серверах на предмет наявності в ній вірусів у процесі прийому і пересилки електронної пошти. Одним з таких засобів є програма kavkeeper з пакета Антивірус Касперського для Linux Server версії 4.0 і вище.

Принцип її роботи полягає в тому, що вся пошта, що проходить через сервер, спочатку перенаправляється спеціальному користувачу, в ролі якого виступає антивірусний процес. Він сканує вміст кожного листа на наявність в ньому фрагментів відомих вірусів. Якщо лист містить щось схоже на вірус, він вилучається з процесу передачі і, залежно від настроювань антивіруса, піддається заданій обробці. Повідомлення про виявлений вірус відсилаються відправнику і одержувачу інфікованого листа, а також на ім'я вказаних адміністраторів системи. Після перевірки, листи, що не викликають підозр, відсилаються за призначенням.

Тим самим, на рівні поштового сервера ставиться надійний заслін відомим вірусам, які розповсюджуються за допомогою електронної пошти. А, оскільки kavkeeper розпізнає тільки віруси, сигнатури яких знаходяться в його базі даних, необхідно регулярно оновлювати антивірусну базу даних з офіційного сайта. Інакше мережа може стати уразливою для знову створених вірусів.

Log-сервер. Загальновідомий механізм протоколювання системних подій на серверах і клієнтських робочих станціях. Розробники ПЗ включають до своїх продуктів фрагменти коду, які на ту чи іншу подію генерують відповідні текстові повідомлення. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем з метою з'ясування, які події відбувалися в системі якийсь час тому. Це дозволяє, наприклад, з'ясувати, чому не запускається та або інша програма або перестав функціонувати певний сервіс. Дуже корисні log-файли для пошуку слідів зламу системи і відвідувань її несанкціонованими гостями. А, оскільки злам, як правило, супроводжується безліччю заборонених дій, це викликає велику кількість системних повідомлень, що осідають в log-файлах.

З цієї причини зловмисник завжди прагне стерти сліди своєї присутності, видаливши, або вичистивши log-файли. В обох випадках адміністратору буде дуже важко зрозуміти, що саме відбулося в системі: яким чином до неї проникли, як довго знаходилися, що встигли використати. Або навіть просто переконатися, що все гаразд. Тому обов'язковою умовою для мережі, підключеної Інтернет, є наявність в

ній окремого log-сервера. Принцип його роботи полягає в тому, що кожна операційна система може посилати повідомлення про системні події по UDP протоколу на віддалений сервер. Це можуть робити також маршрутизатори і міжмережні екрани. Збираючи такі повідомлення на спеціально виділеному сервері, ми забезпечуємо їм збереження від рук зловмисника. Тому, для мінімізації імовірності зламу, log-сервер має бути призначений тільки для збору log-повідомлень. Він не повинен виконувати будь-яких інших функцій і виконувати інші мережні додатки, окрім syslogd. У цьому випадку після зламу комп'ютерів мережі, на log-сервері залишаться відповідні повідомлення, знищити які зловмисник вже не зможе.

Таким чином, як приклад підключення локальної мережі установи (організації) до мережі Інтернет для захисту інформації і системних ресурсів можливо (а у ряді випадків й доцільно) використання схеми, наведеної на рис. 3.8.

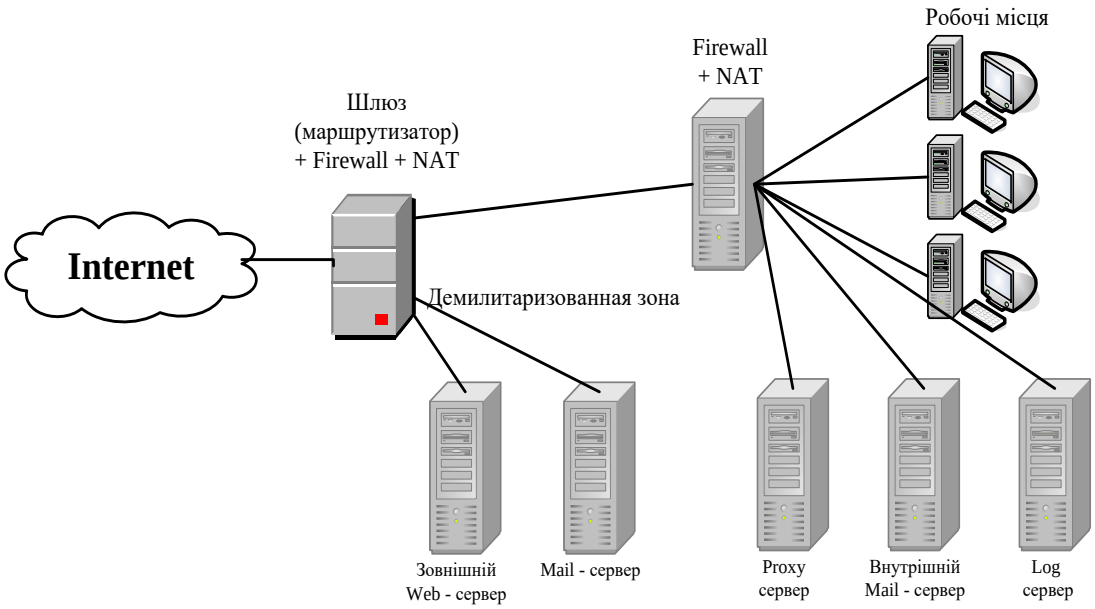


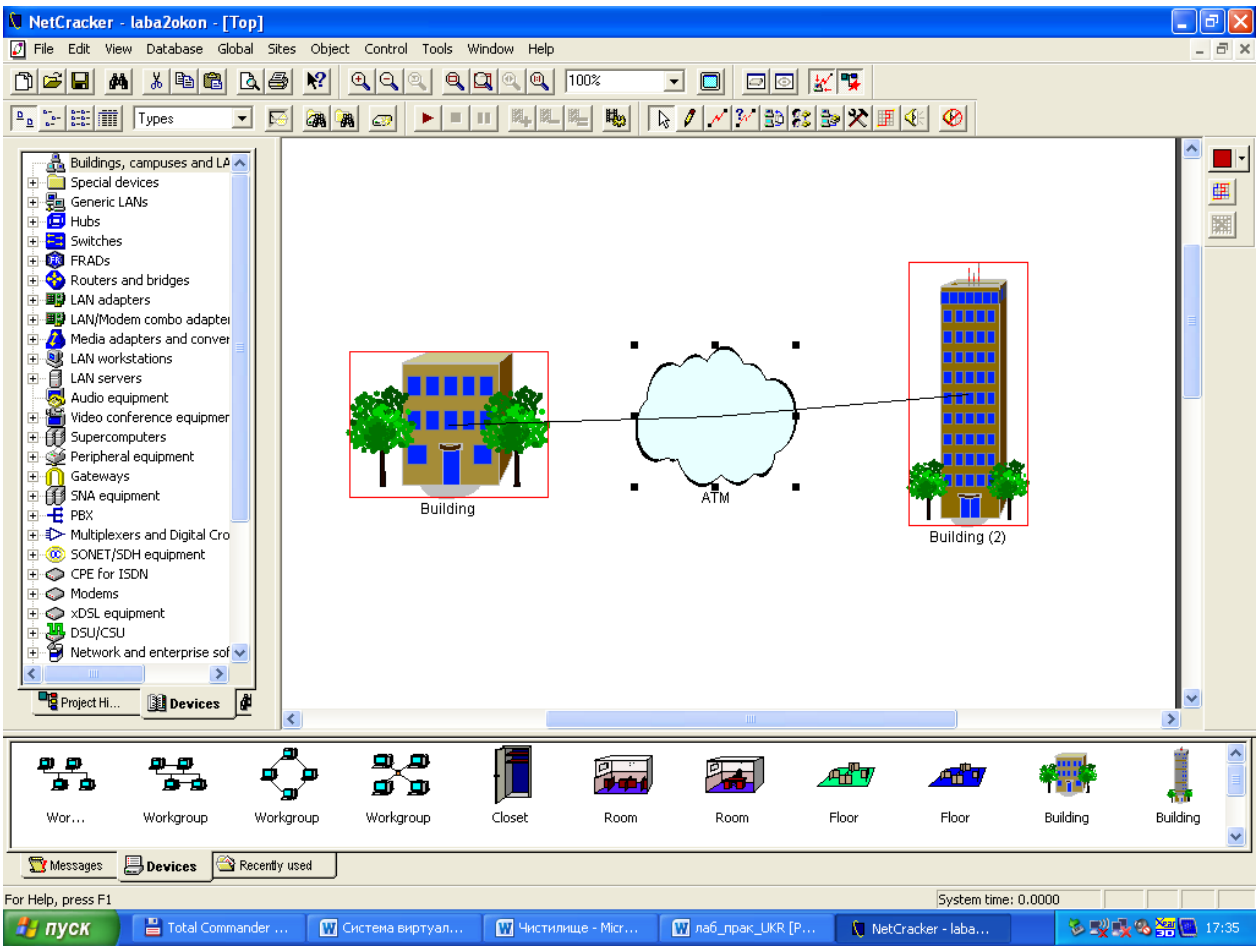
Рисунок 3.8 – Приклад побудови локальної мережі при підключенні до мережі Інтернет

3.5 Порядок виконання лабораторної роботи

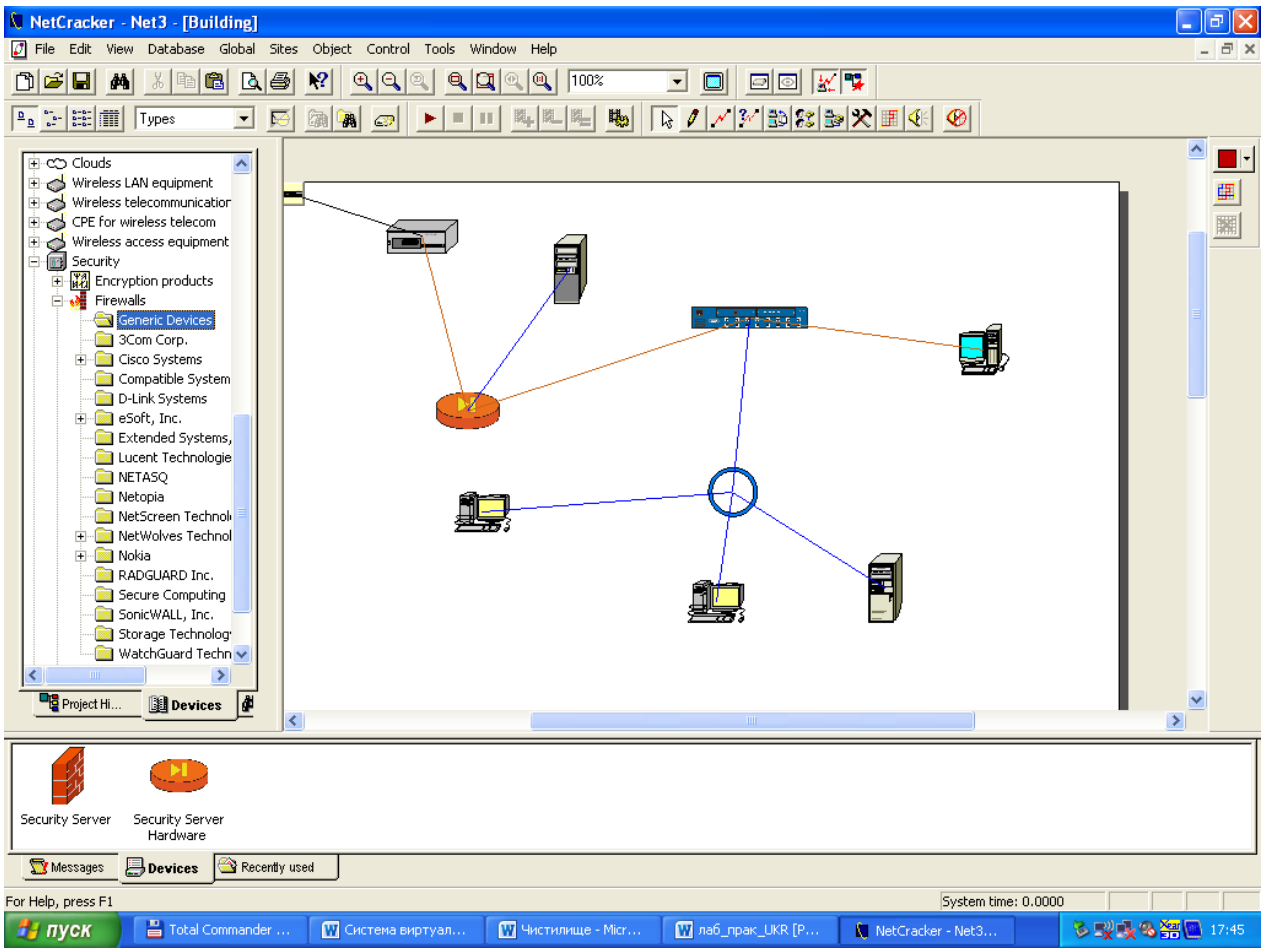
1. Вивчити теоретичний матеріал, наданий у підрозділі 3.4 цієї лабораторної роботи.

2. За допомогою системи NetCracker спроектувати змішану захищену комп’ютерну мережу на основі технологій канального та фізичного рівнів (ATM, Token ring) згідно з алгоритмом:

а. Вибрати в панелі бази даних пристроїв два будинки та об’єднати їх між собою, використовуючи ATM-пристрої.



б. В одному із будинків, використовуючи технологію Token ring, розгорнути захищену локальну комп'ютерну мережу з двох комп'ютерів та сервера. Безпосередньо до мережного обладнання необхідно підключити комп'ютер з мережною картою ATM. При створенні локальної мережі особливу увагу необхідно приділити створенню демілітаризованої зони, та вибору приладів для захисту локальної мережі. Весь інформаційний обмін між створеними будинками має забезпечуватися механізмами шифрування та автентифікації.

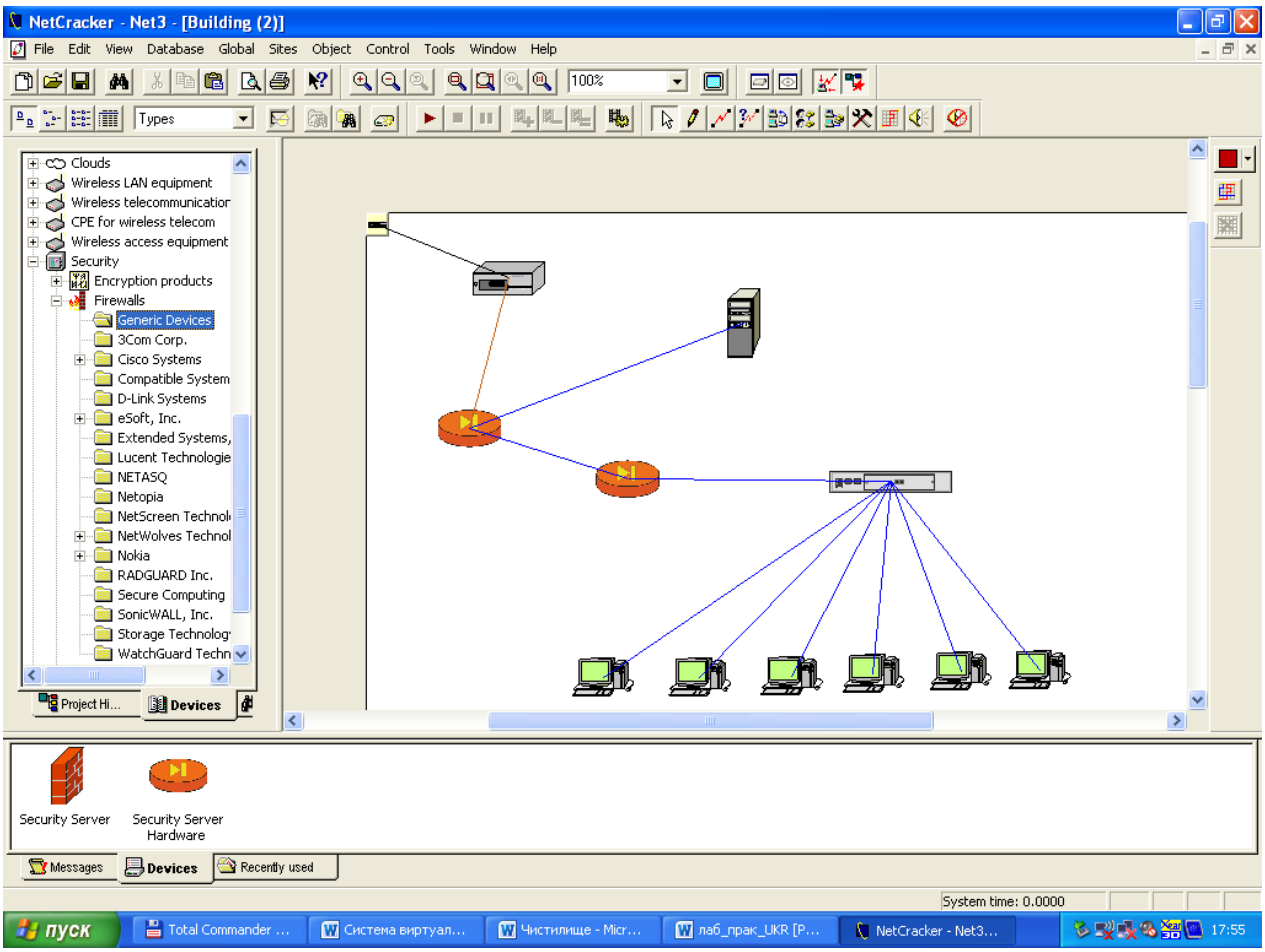


в. У другому будинку, використовуючи технологію Ethernet, розгорнути захищену локальну комп'ютерну мережу з шістьох комп'ютерів. При створенні локальної мережі особливу увагу необхідно приділити створенню демілітаризованої зони, та вибору приладів для захисту локальної мережі. Весь інформаційний обмін між створеними будинками має забезпечуватися механізмами шифрування та автентифікації.

г. Згенерувати обмін між компонентами локальних мереж різного інформаційного трафіка (відповідно до призначень приладів та компонентів).

д. Дослідити вплив окремих елементів захисту інформації (шифраторів, брандмауерів) на загальну ефективність роботи комп'ютерних мереж та стан забезпечення основних послуг безпеки інформації (конфіденційності, автентичності, цілісності та ін.).

е. Оцінити можливості захисту інформації окремих приладів, які є в базі даних приладів.



3.6 Зміст звіту

Звіт має містити:

– Назву, мету, стислі теоретичні відомості за досліджуваною проблемою; структурні схеми змодельованої мережі (за кожним стандартом); статистичні дані (на підставі яких проводився аналіз моделі); висновки.

– Висновки повинні містити аналіз результатів, отриманих у результаті виконання лабораторної роботи і їх порівняння з теоретичними відомостями за досліджуваною проблемою.

3.7 Питання для потокового контролю підготовленості студентів до виконання лабораторної роботи

1. Призначення та основні особливості технології канального рівня ATM.
2. Основні базові принципи обміну інформації при використанням технології ATM.
3. Вид та основні особливості осередків технології ATM.
4. Наведіть приклади та надайте основні тактико-технічні характеристики ATM-комутаторів для локальних і глобальних мереж.
5. Надайте класифікацію стандарту Ethernet у залежності від типу фізичного середовища.

6. Розкрийте основні особливості мережного обладнання та стандартів фізичного середовища Ethernet.

7. Наведіть приклади мережного обладнання, яке забезпечує трансляцію мережних адрес в локальних комп'ютерних мережах стандарту Ethernet.

8. Надайте класифікацію стандарту Token ring.

9. Розкрийте основні особливості мережного обладнання Token ring.

10. Призначення та основні особливості створення «демілітаризованої зони» локальної комп'ютерної мережі.

11. Функції, завдання, та різновиди систем захисту інформації на основі трансляції мережних адрес. Призначення та види трансляторів (NATів), їх порівняльна характеристика.

12. Призначення, функції та основні служби безпеки брандмауер-систем. Особливості практичної реалізації брандмауер-систем.

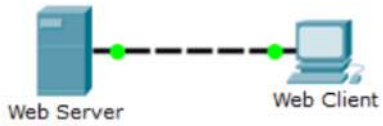
13. Наведіть приклади шифраторів, які забезпечують конфіденційність інформації, яка циркулює в локальних комп'ютерних мережах.

14. Основне призначення та можливості програмного середовища NetCracker 4.1.

Лабораторна робота №2

ВИВЧЕННЯ МОДЕЛЕЙ TCP/IP І OSI У ДІЇ

Топологія:



Завдання:

1. Вивчення HTTP-трафіку
2. Відображення елементів пакета протоколів TCP/IP

Загальні відомості:

Дана вправа по симуляції - перший крок на шляху до розуміння принципів роботи пакета проколів **TCP / IP** і його взаємозв'язку з моделлю **OSI**. Режим симуляції дозволяє переглядати вміст даних, що переміщаються по мережі на кожному з рівнів.

При передачі даних по мережі вони розбиваються на більш дрібні фрагменти і ідентифікуються таким чином, щоб їх можна було з'єднати по прибуттю в пункт призначення. Кожен фрагмент отримує власне ім'я (**protocol data unit** - PDU) і асоціюється з конкретним рівнем моделей TCP / IP і OSI. Режим симуляції програми **Packet Tracer** дозволяє переглядати всі рівні і пов'язані з ними PDU. Нижче описана послідовність кроків користувача для запиту веб-сторінки з веб-сервера за

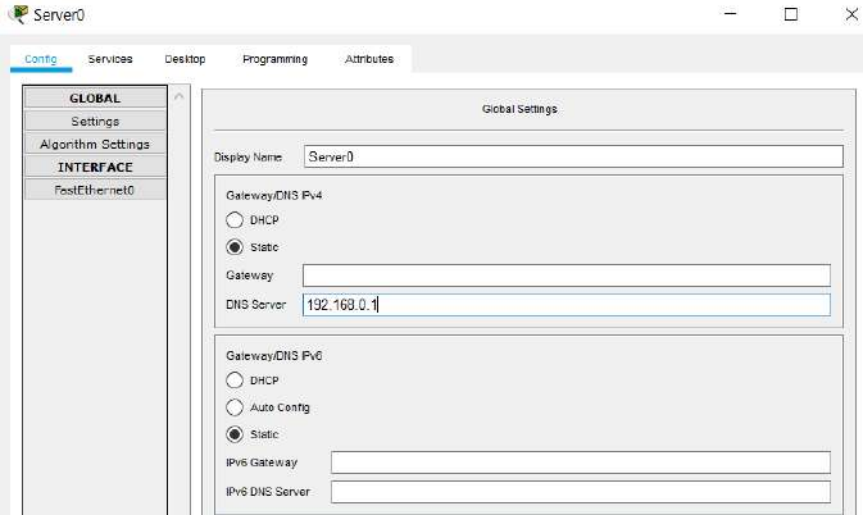
допомогою встановленого на клієнтському ПК веб-браузера.

Дана лабораторна робота дасть вам можливість ознайомитися з можливостями програми **Packet Tracer**, а також наочно розглянути процес інкапсуляції.

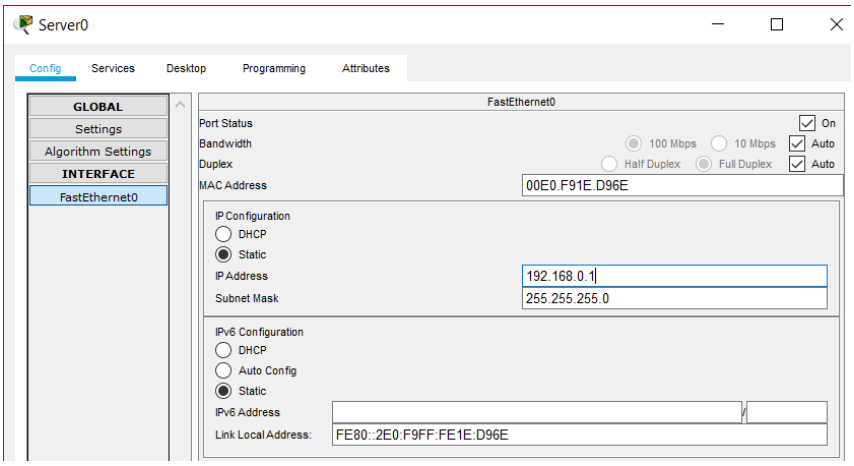
Для виконання лабораторної роботи потрібно спочатку створити систему, що відповідає наведеній вище топології, а потім – додати наступні налаштування:

•Для веб-сервера:

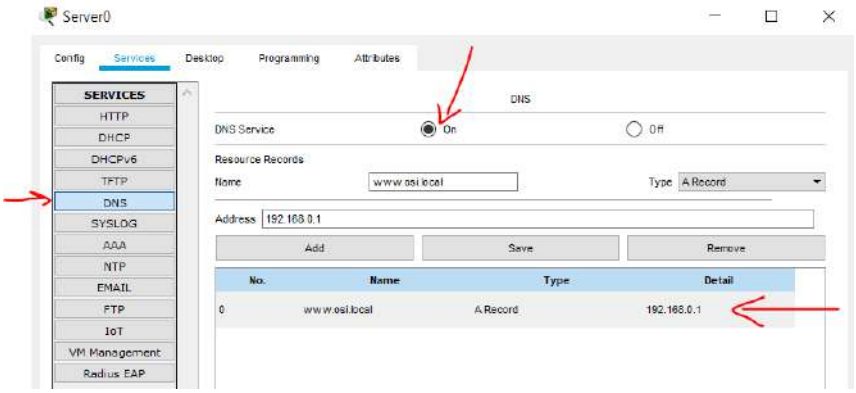
1. на вкладці **Config,** розділ **Settings** в полі **DNS Server** задати будь-яку **IP-адресу** (наприклад, 192.168.0.1);



2. цю саму IP-адресу задати в полі **IP-Address** на вкладці **Config**, розділ **FastEthernet0** (після цього поле **Subnet Mask** має автоматично заповнитись);

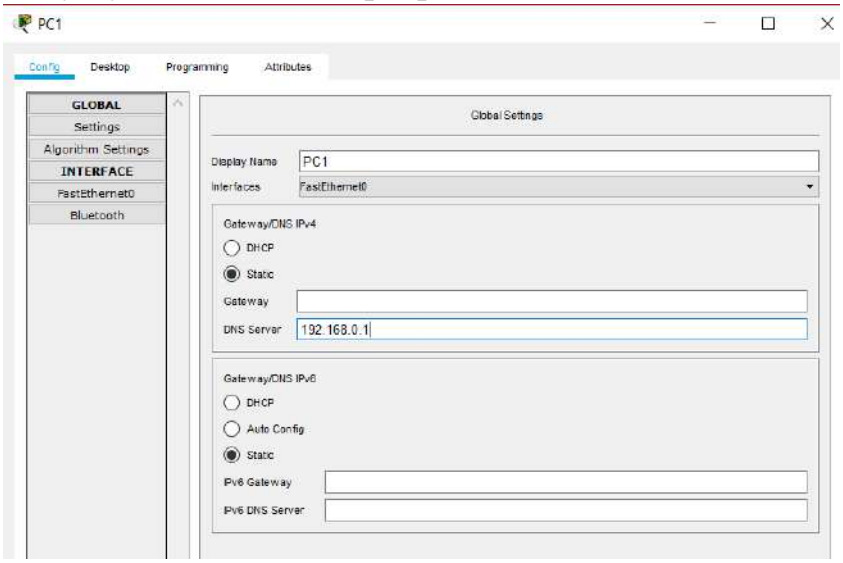


3. на вкладці **Services** в розділі **DNS** потрібно увімкнути **DNS Service** (On) та додати новий домен з ім’ям **www.osi.local** та адресою, що була задана в першому пункті.

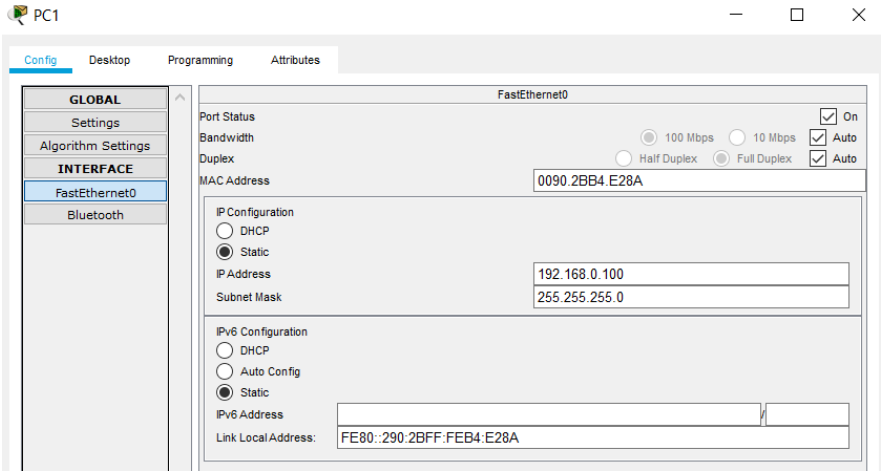


•Для веб-клієнта:

1. на вкладці **Config,** розділ **Settings** в полі **DNS Server** задати адресу, що було додана у першому пункті для веб-сервера;



2. задати будь-яку адресу (наприклад 192.168.0.100), відмінну від адреси DNS Сервера, в полі **IP-Address** на вкладці **Config**, розділ **FastEthernet0** (після цього поле **Subnet Mask** має автоматично заповнитись).



ЧАСТИНА 1. ВИВЧЕННЯ HTTP-ТРАФІКУ

У першій частині лабораторної роботи ви будете використовувати програму

Packet Tracer (PT) в режимі симуляції для генерування веб-трафіку і вивчення протоколу HTTP.

Крок 1: Перейдіть з режиму реального часу в режим симуляції

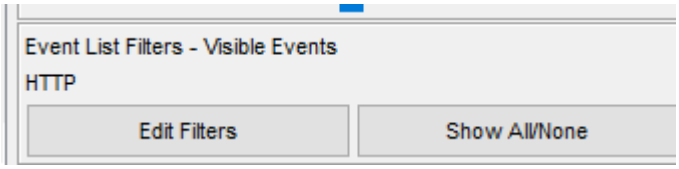
У правому нижньому кутку інтерфейсу **Packet Tracer** знаходяться вкладки для перемикання між режимами **Realtime** (режим реального часу) і **Simulation** (режим симуляції). PT завжди запускається в режимі **Realtime**, в якому мережеві протоколи працюють з реальними значеннями часу. Однак широкі можливості **Packet Tracer** дозволяють користувачеві «Зупинити час», переключившись в режим симуляції. У режимі симуляції користувачі можуть покроково переходити від одної мережевої події до іншої.

a. Натисніть на значок режиму **Simulation** для перемикання з режиму реального часу в режим симуляції.

b. Виберіть в списку **Event List Filters** (Фільтри списку подій) пункт **HTTP**

1) HTTP в цей момент вже може бути єдиною видимою подією. Натисніть кнопку **Edit Filters** (Змінити фільтри), і Ви побачите видимі події. Встановіть або зніміть прапорець **Show All / None** (Показати всі / нічого) і зверніть увагу на те, як зміниться стан встановлених і знятих прапорців.

2) Натискайте на прапорець **Show All / None** до тих пір, поки всі прапорці не будуть зняті, а потім виберіть **HTTP**. Натисніть на будь-яке місце за межами поля **Edit Filters**, щоб приховати його. У розділі видимих подій тепер відображається тільки HTTP.



Крок 2: Згенеруйте веб-трафік (HTTP).

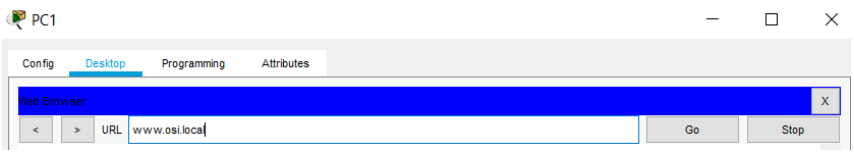
На даний момент панель симуляції порожня. У верхній частині панелі симуляції видно найменування п’яти стовпців списку подій. У міру генерації і просування трафіку в списку будуть з'являтися події.

Примітка. Веб-сервер і веб-клієнт показані на лівій панелі. Розмір панелі можна змінити, якщо навести покажчик на смугу прокрутки і, коли він набуде вигляду двобічної стрілки, перетягнути його вліво або вправо.

a. Натисніть **Web Client** (Веб-клієнт) на крайній лівій панелі.

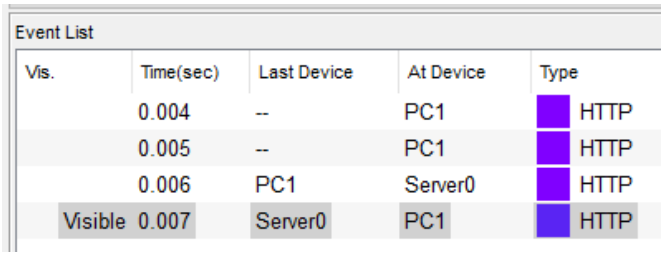
b. Натисніть вкладку **Desktop** (Робочий стіл), потім клацніть на значок **Web Browser**, щоб відкрити веб-браузер.

c. У полі **URL** введіть адресу **www.osi.local** і натисніть кнопку **Go**.



Оскільки час в режимі симуляції прив'язаний до подій, то для відображення подій в мережі необхідно використовувати кнопку **Capture / Forward** (Захоплення / вперед).

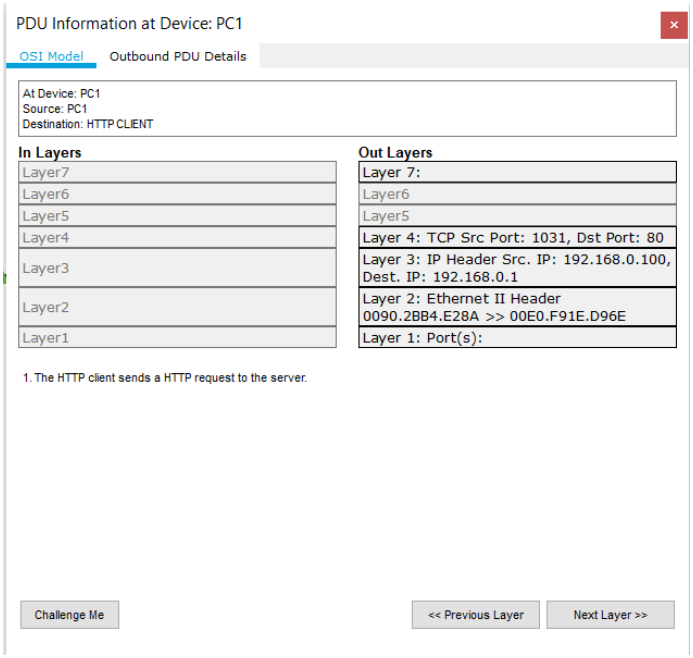
d. Натисніть кнопку **Capture / Forward** чотири рази. У списку подій повинні бути чотири події.



Подивіться на сторінку веб-клієнта в веб-браузері. Що-небудь змінилося?

Крок 3: Вивчення змісту HTTP-пакету

a. Натисніть на перший кольоровий квадрат в списку подій **Event List**. Вам може знадобитися розгорнути панель симуляції або використовувати смугу прокрутки безпосередньо під списком подій **Event List**.



Відкриється вікно PDU **Information at Device: Web Client** (Інформація про PDU на пристрої: веб-клієнт). У цьому вікні є тільки дві вкладки: **OSI Model** (Модель OSI) і **Outbound PDU Details** (Відомості про вихідну PDU), оскільки це тільки початок передачі. По мірі вивчення нових подій стануть видні три вкладки, включаючи нову вкладку **Inbound PDU Details** (Відомості про вхідну PDU). Коли подія є останньою в потоці трафіку, відображаються тільки вкладки **OSI Model** і **Inbound** PDU **Details**.

a. Переконайтеся, що обрана вкладка **OSI Model**. Переконайтеся, що в стовпці **Out Layers** (Вихідні рівні) виділено поле **Layer** 7 (Рівень 7).

Яка інформація перерахована в пронумерованих кроках безпосередньо під полями **In Layers** (Вхідні рівні) і **Out Layers** (Вихідні рівні)?

b. Натисніть кнопку **Next Layer** (Наступний рівень). Має бути виділений 4 рівень. Яке призначення Має параметр **DST Port** (Порт призначення)?

c. Натисніть **Next Layer** (Наступний рівень). Має бути виділений 3 рівень. Яке призначення Має параметр **Dest. IP** (IP-адреса призначення)?

d. Натисніть **Next Layer** (Наступний рівень). Яка інформація відображається на цьому рівні?

e. Натисніть на вкладку **Outbound PDU Details** (Відомості про вихідну PDU).

Відомості на вкладці **PDU Details** (Відомості про PDU) відображають рівні моделі TCP / IP.

Примітка. Відомості в розділі **Ethernet II** містять ще більш докладні дані, ніж показані в розділі рівня 2 на вкладці **OSI Model**. Вкладка **Outbound PDU Details** містить більш описові і докладні відомості. Значення **DEST MAC** (MAC-адресу призначення) і **SRC MAC** (MAC-адресу джерела) в розділі **Ethernet II** на вкладці **PDU Details** відображаються на вкладці **OSI Model** в розділі Layer 2**,** але не вказані в якості таких.

- Якщо порівняти відомості в розділі **IP** вкладки **PDU Details** з відомостями на вкладці **OSI Model**, яка інформація є для них загальною? До якого рівня вона відноситься?

- Якщо порівняти відомості в розділі **TCP** вкладки **PDU Details** з відомостями на вкладці **OSI Model**, яка інформація є для них загальною і до якого рівня вона відноситься?

f. Натисніть на наступний кольоровий квадрат в списку **Event List**. Активний тільки рівень 1 (не відображається сірим кольором). Пристрій витягує кадр з буфера і поміщає його в мережу.

g. Перейдіть до наступного поля в списку подій **Event List** і натисніть на кольоровий квадрат. У цьому вікні є два стовпці: **In Layers** і **Out Layers**. Зверніть увагу на напрямок стрілки безпосередньо під стовпцем **In Layers**. Вона дивиться вгору, показуючи напрямок переміщення даних. Прокрутіть ці рівні, звертаючи

увагу на переглянуті раніше елементи. У верхній частині стовпчика стрілка вказує вправо. Це означає, що сервер тепер відправляє дані назад клієнту.

Порівняйте дані в стовпці **In Layers** з даними в стовпці **Out Layers** і скажіть, в чому полягає основна відмінність між ними.

ЧАСТИНА 2. ВІДОБРАЖЕННЯ ЕЛЕМЕНТІВ ПАКЕТУ ПРОТОКОЛІВ TCP/IP

У другій частині лабораторної роботи ви будете використовувати режим симуляції Packet Tracer для спостереження і вивчення роботи деяких протоколів, що входять в пакет TCP/IP.

Крок 1: Продивіться додаткові події

a. Закрийте всі вікна з відомостями про PDU.

b. У розділі **Event List Filters > Visible Events** (Фільтри списку подій > Видимі події) натисніть на кнопку **Show All** (показати все).

Які додаткові типи подій з’явилися в **Event List**?

Ці додаткові записи грають різні ролі в пакеті протоколів **TCP / IP**. Якщо в списку вказано **ARP** (Address Resolution Protocol), то цей протокол здійснює пошук MAC-адреси. Протокол **DNS** відповідає за перетворення імен (наприклад, www.osi.local) в IP-адреси.

Додаткові події TCP пов'язані з встановленням з'єднань, узгодженням параметрів зв'язку і роз'єднанням сеансів зв'язку між пристроями.

В даний час Packet Tracer дозволяє охоплювати більше 35 протоколів (типів подій).

c. Натисніть на першу подію DNS в **Event List**. Перегляньте вкладки **OSI Model** і **PDU Details** і зверніть увагу на процес інкапсуляції. На вкладці **OSI Model** з виділеним полем **Layer 7** безпосередньо під стовпцями **In Layers** і **Out Layers** відображається опис того, що відбувається. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клієнт відправляє DNS-запит на DNS-сервер]) Це дуже корисна інформація, яка допомагає зрозуміти, що відбувається під час процесу зв'язку.

d. Клацніть вкладку **Outbound PDU Details** (Відомості про вихідну PDU). Які відомості показані в полі **NAME**: в розділі DNS QUERY?

e. Натисніть на останній кольоровий квадрат DNS у списку подій. Який пристрій відображений та чому?

Яке значення показано біля поля **IP:** у розділі DNS ANSWER на вкладці **Inbound PDU Details?**

f. Знайдіть першу подію **HTTP** у списку і натисніть на кольоровий квадрат події **TCP** відразу після цієї події. Виділіть **Layer** 4 на вкладці OSI **Model**. Які відомості відображаються під пунктами 4 і 5 в пронумерованому списку безпосередньо під стовпцями **In Layers** і **Out Layers**?

TCP поміж іншого управляє підключенням і відключенням каналу зв'язку. Ця конкретна подія показує, що канал зв'язку був встановлений.

g. Натисніть на останню подію TCP. Виділіть Layer 4 на вкладці **OSI Model.** Перевірте дії, перечисленні безпосередньо під стовпцями **In Layers** і **Out Layers.** Яка дія наведена в останньому пункті списку (4).

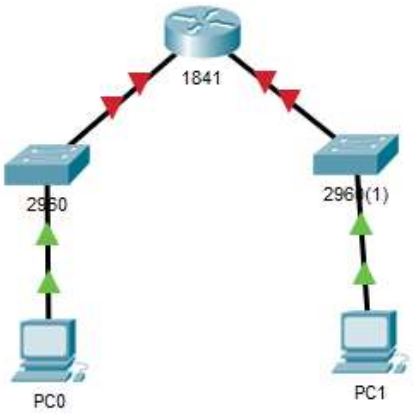
Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: в даній лабораторній роботі ми познайомились з такими мережевими протоколами як TCP/IP, DNS, HHTP, з рівнями моделі OSI, з хедерами та їхнім вмістом для кожного рівня моделі OSI, а також поспостерігали за рухом пакетів в мережі.

Лабораторна робота №3

ПОБУДОВА МЕРЕЖІ. ВИЗНАЧЕННЯ MAC- ТА IP-АДРЕС

Топологія:



Завдання:

1. Побудова простої мережі
2. Визначення MAC- та IP-адрес під час тестування з'єднання

Загальні відомості:

У даній роботі навчимося створювати просту мережу: з'єднувати між собою кінцеві та проміжні пристрої та налаштовувати їх так, щоб можна було надсилати дані. Після цього, за допомогою простої команди **ping**, ми будемо спостерігати за рухом пакета по мережі та визначимо **MAC**- та **IP**-адреси, зазначені в хедері пакета даних на кожному етапі його руху по мережі.

IP-адреса – це логічна адреса мережевого рівня (**network layer**), яка необхідна для доставки пакету даних до місця призначення.

IP-адреса складається з мережевої частини (ліва частина адреси, яка визначає, до якої мережі належить ця IP-адреса) і вузлової частини (права частина адреси, яка визначає конкретний пристрій в мережі). Мережева частина однакова для всіх пристроїв в межах однієї мережі, в той час як вузлова частина є унікальною.

Маска підмережі (**Subnet Mask**) відділяє мережеву частину адреси від вузлової. За допомогою маски підмережі здійснюється поділ на підмережі, що дозволяє «економити» IP-адреси.

Наприклад, є IP-адреса та її маска: 168.192.0.1 255.255.255.0. В даному випадку 192.168.0 визначає мережу (це мережева частина), а 1 – унікальна адреса пристрою в цій мережі (вузлова частина).

Окрім того, IP-адреса може бути статичною та динамічною. Статична адреса задається вручну, в той час як динамічна призначається автоматично DHCP сервером. Зазвичай використовується саме динамічне присвоєння адреси, проте в лабораторних роботах ми будемо користуватися статичним присвоєнням. Це полегшить навчання і допоможе уникнути певних можливих плутанин.

MAC-адреса (Media Access Control) – фізична адреса мережевої інтерфейсної

плати.

Під час руху по мережі, якщо пристрої знаходяться в одній локальній мережі, пошук і транспортування здійснюється саме по MAC-адресі. IP-адреса використовується, коли пристрої знаходяться в різних мережах. У такому випадку пакет даних спочатку автоматично доправляється до маршрутизатора, а вже звідки відправляється далі. IP-адреси протягом всього руху по мережі залишаються сталими, в той час як MAC-адреси відправника і отримувача змінюються на кожній окремій ділянці транспортування.

ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте свою першу робочу мережу.

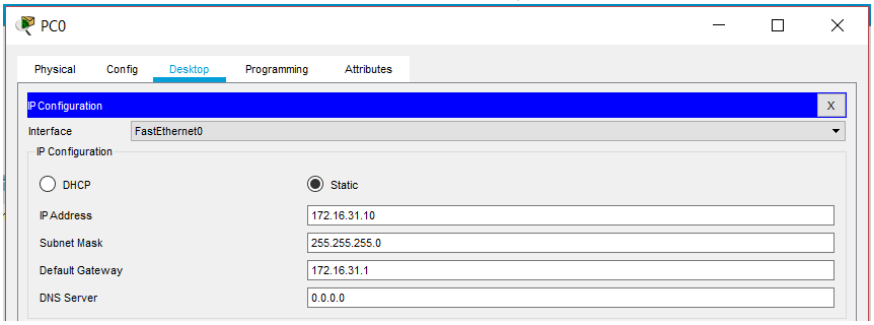
Крок 1: Створіть систему за наданою вище топологією

Зверніть увагу: обирайте саме такі маршрутизатор і комутатори, які вказані на топології, тобто маршрутизатор 1841 та комутатори 2960. Це допоможе уникнути складнощів з портами (на різних пристроях присутні різні порти. Їх можна додавати і забирати, проте це не є метою лабораторної роботи).

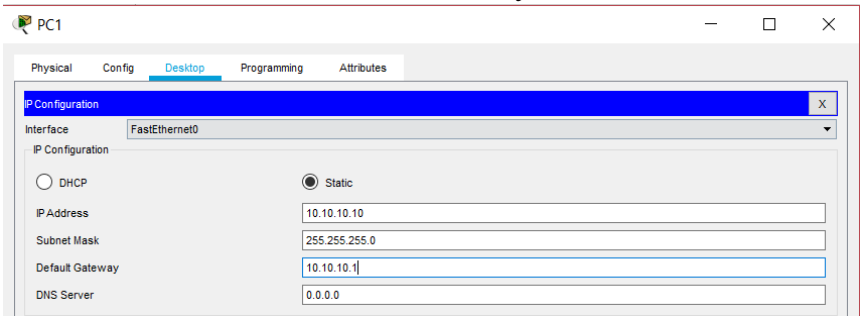
Крок 2: Налаштуйте мережу.

На даний момент, якщо ви спробуєте надіслати дані з одного ПК на інший, у вас нічого не вийде, так як ні в одного з пристроїв мережі немає адрес. Для того, щоб можна було передавати дані між пристроями, необхідно присвоїти кожному з них унікальну **IP-адресу**.

a. Клікніть на PC0. Налаштуйте його відповідно до рисунку



b. Клікніть на PC1. Налаштуйте його відповідно до рисунку



Зверніть увагу: ви щойно налаштували IP-адреси для обох ПК. Але окрім того ви приписали кожному з них адресу шлюзу за замовчуванням (**default gateway**). Це адреса інтерфейсу маршрутизатора, яка відповідає даній підмережі. Саме сюди

будуть відправлятися дані, якщо адреси отримувача не знайдено в локальній мережі. Тоді це вже буде справа маршрутизатора – перенаправити пакет даних у правильному напрямку.

c. Налаштуйте комутатори. Для цього під'єднайте один з ПК до кожного з комутаторів по черзі за допомогою консольного кабелю **Console** (як ви це робили в першій лабораторній роботі). Тепер потрібно налаштувати віртуальний інтерфейс, тобто присвоїти йому адресу. Для цього з режиму глобальної конфігурації вам потрібно перейти в режим конфігурації даного інтерфейсу. Це можна зробити за допомогою команди **interface vlan 1.** Тепер призначимо адреси за допомогою наступних команд: **ip address 172.16.31.100 255.255.255.0** та **ip address 10.10.10.100 255.255.255.0** для комутатора 2960 та 2960(1) відповідно. Далі потрібно активувати інтерфейс. Це робить за допомогою команди **no shutdown** (це потрібно зробити для обох комутаторів).

```
Switch(config)#int vl 1
Switch(config-if)#ip ad 172.16.31.100 255.255.255.0
Switch(config-if)#no sh
```

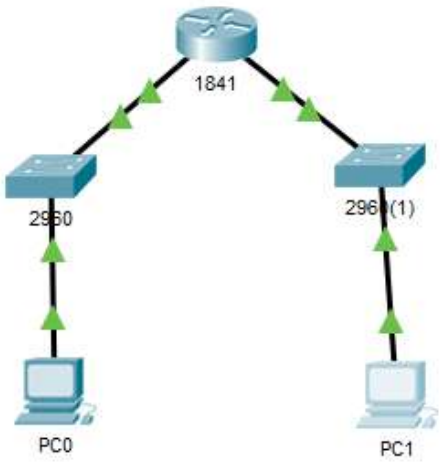
```
Switch(config)#int vl 1
Switch(config-if)#ip ad 10.10.10.100 255.255.255.0
Switch(config-if)#no sh
```

d. Налаштуйте маршрутизатор. Це робиться ідентично до налаштування комутатора, тільки тепер замість введення адреси до віртуального інтерфейсу ми будемо це робити для кожного порту окремо. Під'єднайтесь за допомогою консолі до маршрутизатора та введіть наступні команди (у вас можуть відрізнятися порядкові номери інтерфейсів, все залежить від того, до якого порту який комутатор ви підключили. Головне – прослідкуйте за тим, щоб інтерфейс, якому ви назначаєте IP-адресу, що починається на 172, був під'єднаний до комутатора, в якого IP-адреса віртуального інтерфейсу починається на 172. Ідентично з іншого боку – інтерфейс з початковими цифрами 10 у адресі має бути «повернутий» в сторону підмережі, в якій всі пристрої мають адреси, що починаються на 10).

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface f 0/0
Router(config-if)#ip address 172.16.31.1 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface f 0/1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

Тепер мережа повністю налаштована і має виглядати так:



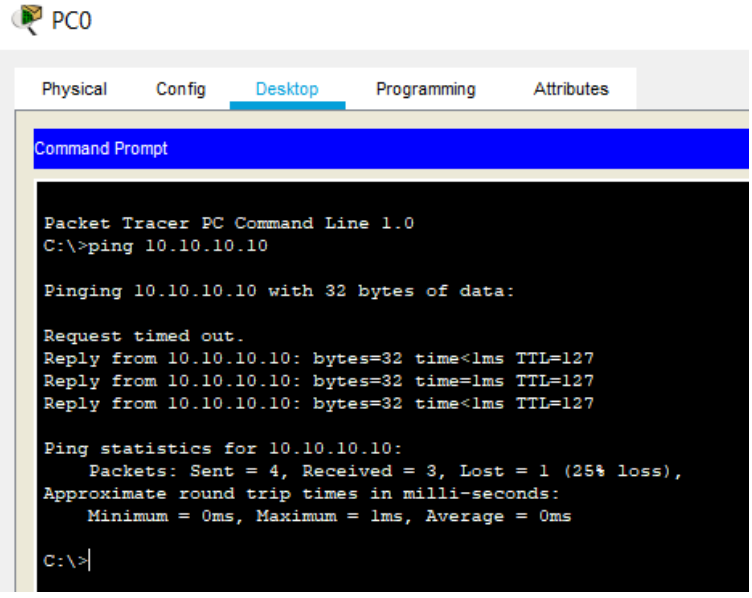
ЧАСТИНА 2. ВИЗНАЧЕННЯ MAC- ТА IP-АДРЕС

У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як пересуватиметься пакет даних по мережі та визначите адреси на кожному етапі транспортування.

Крок 1: Пропінгуйте один комп'ютер з іншого

a. Клікніть на **PC0** та відкрийте вікно **Command Prompt** (Командний рядок)

b. Введіть команду **ping 10.10.10.10** та дочекайтесь відповіді. Вона має мати наступний вигляд



Таким чином ми перевірили з'єднання між двома комп'ютерами (так як пакет, відправлений одним ПК, досяг іншого і повернувся). Тепер можна перейти до збирання інформації про **MAC**- та **IP**-адреси.

c. Перейдіть в режим симуляції та повторіть команду пінгування. Поряд з **PC0** має з'явитися одиниця даних протоколу (**PDU**). Натисніть на **PDU** та запишіть

в таблицю, наведену в кінці лабораторної роботи, наступні дані на вкладці **Outbound PDU Layer**.

- MAC-адреса призначення
- MAC-адреса відправника
- IP-адреса призначення
- IP-адреса відправника

d. Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Зберіть тут аналогічні дані. Повторюйте цю процедуру до тих пір, поки **PDU** не досягне **PC1**.

Команда «ping 10.10.10.10 » з PC0	Пристрій	MAC-адреса призначення	MAC-адреса відправника	IP-адреса призначення	IP-адреса відправника
	PC0				
	2960				
	1841				
	2960(1)				
	PC1				

e. Дайте відповіді на наступні запитання:

•Чому IP-адреси залишались сталими, в той час як MAC-адреси постійно змінювались?

•Чому на етапі комутаторів MAC-адреси залишились такими ж, як і на попередньому етапі?

•Навіщо потрібна MAC-адреса?

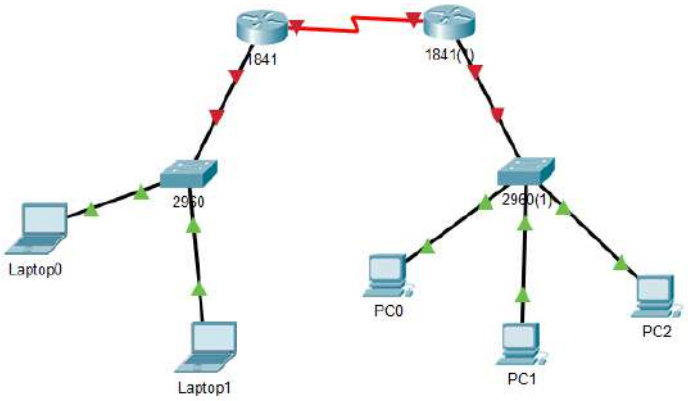
Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему, заповнену таблицю та відповіді на запитання.

Підсумок: у даній лабораторній роботі ми побудували свою першу мережу, протестували її, а також поспостерігали за рухом пакету даних в ній. На основі спостережень визначили IP-адреси та MAC-адреси пристроїв в мережі, а також розібрались, в чому між ними різниця.

Лабораторна робота №4

ВИВЧЕННЯ ТАБЛИЦІ ARP

Топологія:



Завдання:

1. Побудова складної мережі
2. Аналіз ARP-запиту

Загальні відомості:

У даній лабораторній роботі ми навчимося створювати вже складнішу мережу: тут вже будуть присутні два маршрутизатора, що ускладнює рух по мережі. Навчимося настроювати пристрої, щоб вони могли відправляти та отримувати дані в такій мережі, окрім того, на прикладі маршрутизатора дізнаємося, як можна змінювати фізичний стан пристрою, додаючи до нього нові потрібні нам порти. Після цього, за допомогою простої команди ping, ми будемо спостерігати за процесом **ARP-запиту**, дізнаємось, як відбувається вивчення пристроями **MAC-адрес** інших пристроїв та вивчимо **таблицю ARP**.

ARP (address resolution protocol) – протокол, який пристрої використовують для визначення **MAC-адреси** отримувача. У цього протоколу є дві основні функції: співставлення IP-адрес з MAC-адресами та створення таблиці співставлень. Ця таблиця називається **ARP-таблицею**. Вона створюється поступово кожним пристроєм окремо по мірі відправлень пакетів даних цим пристроєм до інших пристроїв. Тобто MAC-адресу кожен пристрій дізнається при першому надсиланні даних. Цей процес називається **ARP-запитом**. Коли відповідне значення вже існує в таблиці, пристрій одразу може відправляти пакет з даними. Якщо ж отримувача немає в даній локальній мережі, дані перенаправляються на шлюз за замовчуванням (**default gateway**).

ARP-запит в своєму заголовку окрім IP-адреси призначення, MAC-адреси відправника та типу повідомлення (яке інформує, що це ARP-запит) містить MAC-адресу призначення, яка є загальною, тобто призначається для всіх інтерфейсів Ethernet в мережі. Кожен пристрій, який отримав такий ARP-запит, мусить його обробити. Для цього він звіряє свою власну IP-адресу з тою, яка міститься в запиті, і якщо вони однакові, відправляє свою MAC-адресу пристрою, який відправив запит.

Після отримання MAC-адреси, пристрій поміщає її в свою ARP-таблицю і тепер може використовувати ці дані в майбутньому. Варто відмітити, що дані в ARP-таблиця не є постійними і мусять постійно оновлюватись.

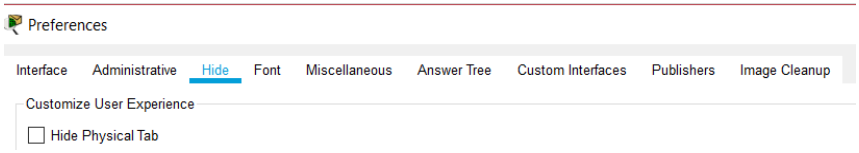
ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте мережу.

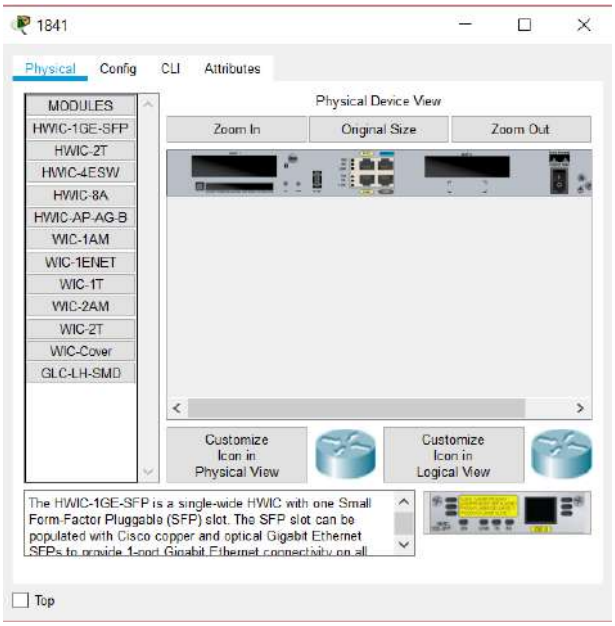
Крок 1: Створіть систему за наданою вище топологією

Зверніть увагу: обирайте саме такі маршрутизатор і комутатори, які вказані на топології, тобто маршрутизатори **1841** та комутатори **2960**. Для того, щоб з'єднати між собою два маршрутизатори необхідно використати **Serial DTE** підключення. Проте маршрутизатори за замовчуванням можуть не мати потрібних нам портів. Треба їх додати вручну. Для цього:

•Клікніть на маршрутизатор та перейдіть на вкладку **Physical** (ця вкладка може бути прихована, відкрити її можна, забравши галочку з **Hide Physical Tab** в **Options-Preferences-Hide**)



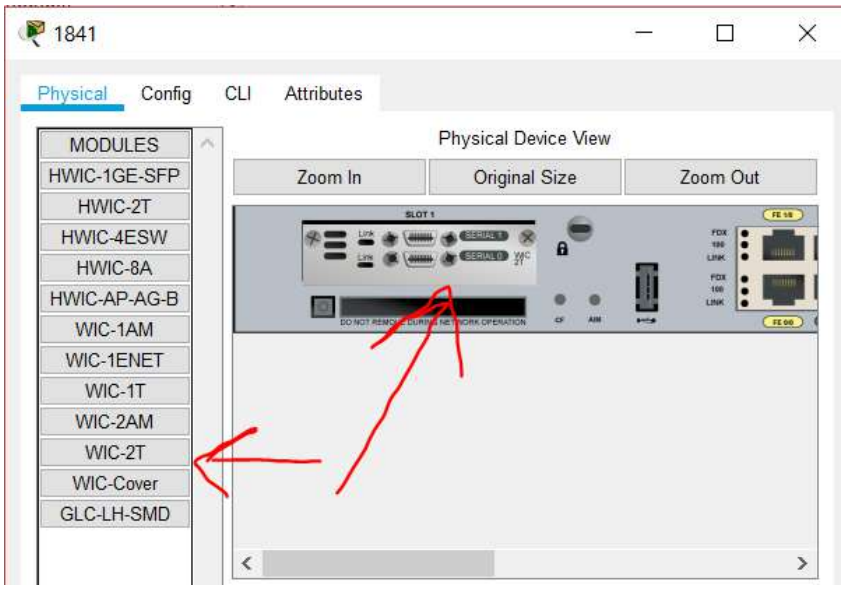
•Коли ви клікнули на вкладку **Physical**, ви можете побачити реальний фізичний вигляд маршрутизатора зі всім портами, що на ньому є. Нам потрібно додати порт **Serial**, щоб ми мали змогу використати необхідний кабель для передачі даних.



•Ви можете приближати та віддаляти рисунок для зручності, використовуючи кнопки **Zoom in** і **Zoom out**.

•Для того, щоб додати необхідні порті, треба для початку вимкнути живлення. Для цього просто натисніть на перемикач. Погасне зелений світлодіод, що розташований під ним.

•Тепер, власне, додамо порти: перенесіть модуль **WIC-2T** зі списку модулів, що розташований зліва від рисунку на рисунок маршрутизатора. Цей модуль містить два **Serial** порти (можна використати також модуль **WIC-1T**, який має лише один такий порт).



•Увімкніть живлення

Крок 2: Налаштуйте мережу.

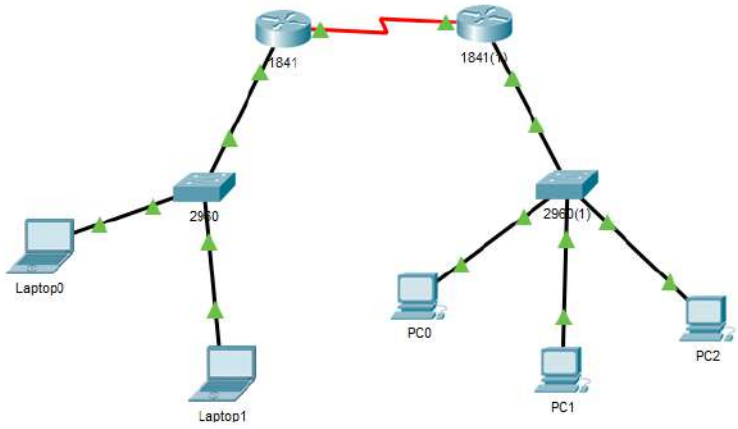
Використовуючи знання, набуті в попередніх лабораторних роботах, налаштуйте пристрої в мережі відповідно до наступної таблиці.

Пристрій	Порт (для проміжних пристроїв) / IP-адреса шлюзу за замовчуванням (для кінцевих пристроїв)	IP-адреса
1841	Serial	192.168.0.2

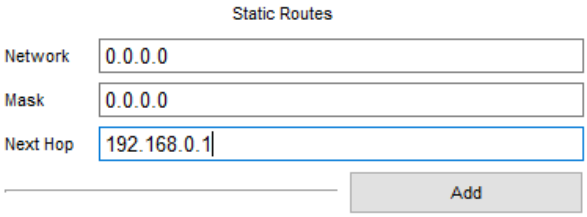
		255.255.255.0
	FastEthernet0/0	172.16.31.1 255.255.255.0
1841(1)	Serial	192.168.0.1 255.255.255.0
	FastEthernet0/0	10.10.10.1 255.255.255.0
2960	Vlan 1	172.16.31.100 255.255.255.0
2960(1)	Vlan 1	10.10.10.100 255.255.255.0
Laptop0	172.16.31.1	172.16.31.10 255.255.255.0
Laptop1	172.16.31.1	172.16.31.11 255.255.255.0
PC0	10.10.10.1	10.10.10.10 255.255.255.0
PC1	10.10.10.1	10.10.10.11 255.255.255.0
PC2	10.10.10.1	10.10.10.12 255.255.255.0

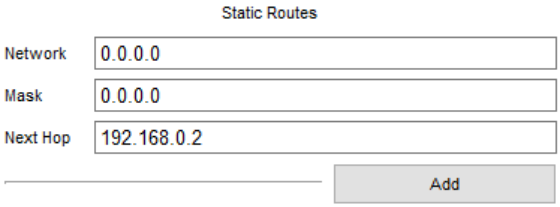
Увага: не забудьте активувати інтерфейс після присвоєння йому IP-адреси (команда **no shutdown**). Окрім того, у вас необов'язково порт на маршрутизаторі буде саме 0/0. Ви можете обрати будь-який порт **FastEthernet**.

Тепер ваша мережа має мати такий вигляд (зверніть увагу: усі позначення на з'єднаннях мають зелений колір, тобто сигнал присутній):



Залишився один крок – вказати маршрутизаторам, що робити, коли до них приходить пакет, який потрібно передати комусь з іншої мережі. Для цього необхідно клікнути на маршрутизатор та обрати вкладку **Config**. Далі переходимо на пункт **Static** в розділі **Routing**. Вказуємо наступні значення для маршрутизаторів 1841 та 1841(1) відповідно:





Далі натискаємо кнопку **Add** і закриваємо налаштування маршрутизатора. Готово! Тепер наша мережа є абсолютно дієспроможною. Це можна перевірити за допомогою, наприклад, команди **ping.**

ЧАСТИНА 2. АНАЛІЗ ARP-ЗАПИТУ

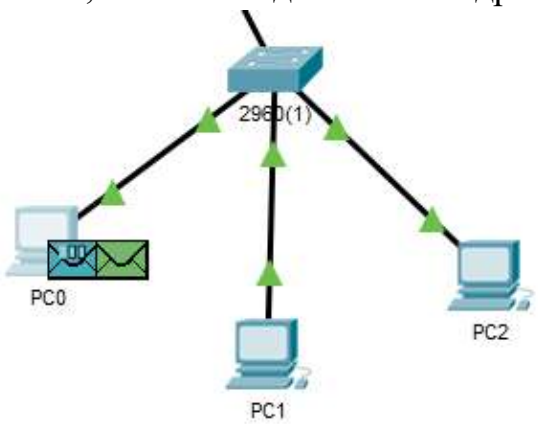
У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як працює протокол **ARP**, як здійснюється **ARP-запит** та як виглядає **ARP-таблиця**.

Крок 1: Пропінгуйте один комп'ютер з іншого

a. Клікніть на PC0 та відкрийте вікно **Command Prompt** (Командний рядок).

b. Введіть команду **arp -d**, щоб очистити **ARP**-таблицю.

c. Перейдіть в режим симуляції та введіть команду **ping 172.16.31.10**. Мають з'явитися дві одиниці даних: протоколу **ARP** та протоколу **ICMP**. **ICMP**-пакет не може бути відправлений, так як невідома MAC-адреса.



d. Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Як бачимо, ARP-пакет перемістився далі, в той час як ICMP-пакет зник. Насправді він просто очікує, поки повернеться ARP-пакет з потрібною MAC-адресою.

e. Натисніть кнопку **Capture/Forward** на панелі симуляції для переміщення до наступного пристрою. Скільки копій запиту створив комутатор та чому?

f. Натискайте кнопку **Capture/Forward** поки пакет не повернеться до відправника. До якого пристрою дійшов запит? Скільки копій пакету зробив комутатор цього разу?

g. Зверніть увагу, що знову з’явився **ICMP** пакет. Натисніть на **ARP**-пакет, зайдіть у вкладку **Inbound PDU Details** та подивіться на **Source Mac.** А тепер натисніть на маршрутизатор, вкладка **Config,** та оберіть серед інтерфейсів той, до якого підключений комутатор. Чи співпадає MAC-адреса цього інтерфейсу з з тою, яка зазначена у відповіді **ARP**-запиту? Що це означає?

h. Поверніться назад в режим реального часу – команда **ping** завершиться. Натисніть на ПК, з якого був відправлений запит та виконайте в командному рядку команду **arp -a**. IP- та MAC-адреси якого пристрою містяться у виведеній таблиці?

i. Тепер виконайте команду **ping 10.10.10.11,** а потім знову **arp -a.** Що змінилося в таблиці?

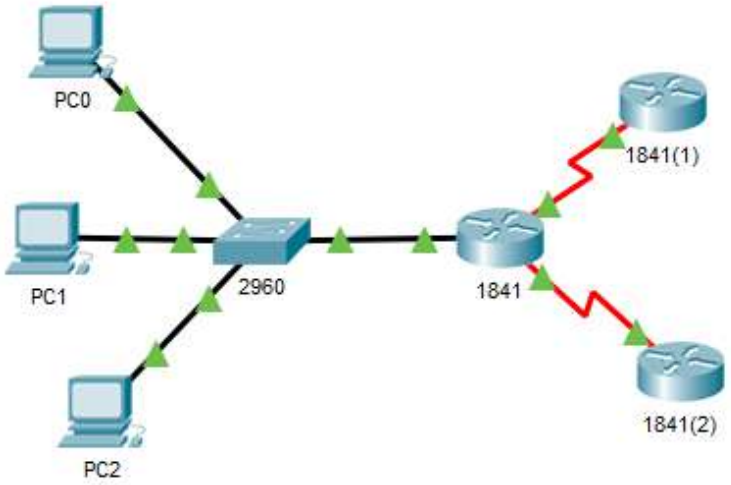
Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: у даній лабораторній роботі ми побудували мережу, що складається з кількох підмереж та протестували з’єднання між пристроями з різних мереж. У процесі тестування ми познайомилися з **ARP** протоколом та вивчили навіщо він потрібен і як працює.

Лабораторна робота №5

АНАЛІЗ ТРАФІКУ ОДНОАДРЕСНОЇ ТА ЗАГАЛЬНОЇ РОЗСИЛКИ

Топологія:



Завдання:

1. Побудувати мережу
2. Генерація трафіку одноадресної розсилки
3. Генерація трафіку загальної розсилки

Загальні відомості:

В даній роботі ми дізнаємось, що таке одноадресна, багатоадресна та загальна розсилка та проаналізуємо перші дві з них. Ми навчимося генерувати комплексні пакети даних та за допомогою одного такого створимо загальну розсилку.

Пристрої в мережі можуть обмінюватись даними один з одним трьома різними способами:

- Одноадресною розсилкою
- Багатоадресною розсилкою
- Загальною розсилкою

Одноадресна розсилка (**Unicast**) – процес відправлення пакету з одного вузла на інший конкретний вузол. Використовується для самої звичайної передачі даних між двома вузлами.

Багатоадресна розсилка (**Multicast**) – процес відправлення пакету з одного вузла групі вузлів, які можуть знаходитись в різних мережах. В якості отримувача вказується IP-адреса групи, для якої зарезервовані адреси від 224.0.0.0 до 239.255.255.255, з яких з 224.0.0.0 до 224.0.0.255 – для багатоадресної розсилки в межах однієї мережі. Вузол отримує пакет, адресований на групову адресу, якщо підписується на відповідну групу.

Загальна розсилка (**Broadcast**) – процес відправлення пакету з одного вузла всім іншим вузлам в мережі. Для цього в якості адреси отримувача використовується 255.255.255.255. Маршрутизатори за замовчуванням не пересилають загальні розсилки.

ЧАСТИНА 1. ПОБУДОВА МЕРЕЖІ

У першій частині лабораторної роботи ви побудуєте та налаштуєте мережу.

Крок 1: Створіть та налаштуйте систему

Використовуючи отримані в минулих лабораторних роботах знання, побудуйте та налаштуйте систему відповідно до топології та наступної таблиці адрес:

Пристрій	Порт (для проміжних пристроїв) / IP-адреса шлюзу за замовчуванням (для кінцевих пристроїв)	IP-адреса
1841	Serial 0/1/0	10.0.2.1 255.255.255.0
	Serial 0/1/1	10.0.3.1 255.255.255.0
	FastEthernet0/0	10.0.1.1 255.255.255.0
1841(1)	Serial 0/1/0	10.0.2.2 255.255.255.0
1841(2)	Serial 0/1/1	10.0.3.2 255.255.255.0
2960	Vlan 1	10.0.1.100 255.255.255.0
PC0	10.0.1.1	10.0.1.2 255.255.255.0
PC1	10.0.1.1	10.0.1.3 255.255.255.0
PC2	10.0.1.1	10.0.1.4 255.255.255.0

Увага: не забудьте активувати інтерфейси після присвоєння їм IP-адреси (команда **no shutdown**). Окрім того, у вас необов'язково порти на маршрутизаторах будуть мати саме наведені у таблиці номери. Ви можете обрати будь-які доступні порти. Окрім того, не забудьте вказати для маршрутизаторів дані про наступну зупинку, як це було показано в попередній лабораторній роботі (частина 1 крок 2).

ЧАСТИНА 2. АНАЛІЗ ОДНОАДРЕСНОЇ ТА ЗАГАЛЬНОЇ РОЗСИЛОК

У другій частині лабораторної роботи ви протестуєте створену мережу, намагаючись пропінувати один ПК з іншого. Окрім цього, ви вивчите, як працює протокол ARP, як здійснюється ARP-запит та як виглядає ARP-таблиця.

Крок 1: Проаналізуйте одноадресну розсилку

a. Клікніть на PC0 та відкрийте вікно **Command Prompt** (Командний рядок).

b. Введіть команду **ping 10.0.3.2**. Виконання має закінчитися успішно.

c. Перейдіть в режим симуляції, у фільтрі (**Edit Filters**) на панелі симуляції оберіть **ICMP** та введіть на PC0 команду **ping 10.0.3.2**. Натискайте кнопку **Capture/Forward** поки пакет не повернеться до відправника. Через які пристрої пройшов пакет? Натисніть на пакет та подивіться інформацію про нього. З якого рівня починається передача (які рівні моделі **OSI** є доступними) та чому?

d. Натисніть кнопку **Reset Simulation**.

Крок 2: Проаналізуйте загальну розсилку

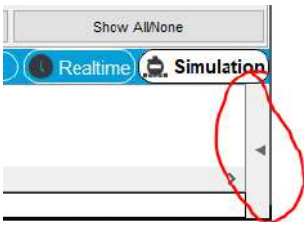
a. Додамо складну **PDU**. Для цього натисніть кнопку **Add Complex PDU** в панелі інструментів зверху.

b. Натисніть на PC0, відкриється діалогове вікно **Create Complex PDU.**

c. У вікні, яке відкриється, введіть наступні значення:

- IP-адреса призначення (**Destination IP Address**): 255.255.255.255
- Порядковий номер (**Sequence Number**): 1
- Час одноразової події (**One Shot Time**): 0

d. Натисніть **Create** PDU. Вікно зачиниться, а біля ПК з'явиться пакет даних. Окрім цього цей пакет повинен з'явитися в **Event List** та у вікні **PDU List** (якщо у вас такого вікна немає, його можна відкрити за допомогою стрілки в нижньому лівому краю)



e. Двічі натисніть кнопку **Capture/Forward.** Спочатку пакет переміститься на комутатор, а потім утвориться три копії, кожна з яких піде в різному напряму: на два ПК та на маршрутизатор. Вивчіть дані третього рівня для всіх подій. Якою є IP-адреса отримувача у кожного з них та чому?

f. Ще раз натисніть кнопку **Capture/Forward.** Чи пересилається пакет на інші маршрутизатори? Чому?

g. Видалити пакет після його вивчення можна, натиснувши на **Delete** під **Scenario 0** в **PDU List.**

Завдання: повторити кроки, описані вище. Як результат виконання роботи продемонструвати побудовану систему та відповіді на запитання.

Підсумок: у даній лабораторній роботі згенерували одноадресну та загальну розсилку та вивчили як і навіщо вона використовується. Окрім того, ми навчилися створювати складні **PDU** в **Cisco Packet Tracer.**

Лабораторна робота №6

МЕРЕЖЕВІ СТАНДАРТИ І ПРОТОКОЛИ

Загальні відомості:

Система імен

- DNS (Система (або служба) доменних імен) - Перетворює доменні імена (наприклад «kpi.ua») в IP-адреси.

Конфігурація імен

- DHCP (Протокол динамічної конфігурації мережного вузла) - Динамічно привласнює IP-адреси клієнтським станціям при запуску, дозволяє повторно використовувати непотрібні адреси.

Електронна пошта

- SMTP (Протокол простої передачі електронної пошти) - Дозволяє клієнтам відправляти електронні повідомлення на поштовий сервер, Дозволяє серверам відправляти електронні повідомлення на інші сервера.

- POP (Поштовий протокол версії 3 (POP3) - Дозволяє клієнтам отримувати електронні повідомлення з поштового сервера, завантажує електронні повідомлення з поштового сервера на комп'ютер.

- IMAP (Протокол доступу до повідомлень в Інтернеті) - Дозволяє клієнтам отримувати доступ до електронних повідомлень, які зберігаються на поштовому сервері, зберігає електронні повідомлення на поштовому сервері.

Передача файлів

- FTP (Протокол передачі файлів) - Встановлює правила, які дозволяють користувачеві отримувати доступ з одного вузла на інший і обмінюватися файлами по мережі, надійний і загальновизнаний протокол доставки файлів з встановленням з'єднання.

Веб

- HTTP (Протокол передачі гіпертексту) - Задає правила обміну в Інтернеті текстом, графічними зображеннями, звуковими, відео-та іншими файлами мультимедіа.

- HTTPS (Безпечний Протокол передачі гіпертексту) — Більш надійна версія HTTP, яка використовує SSL для більш безпечного з’єднання.

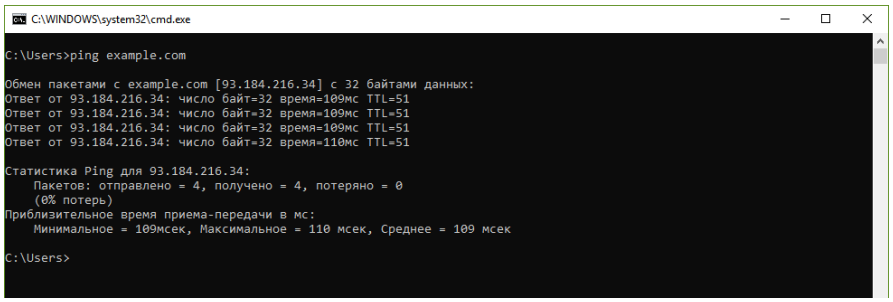
Хід виконання робіт:

- Визначити IP-адрес певного сайту, використовуючи команду *ping*

Команда: *ping /IP/*

(де замість /змінна/ треба підставити необхідні параметри)

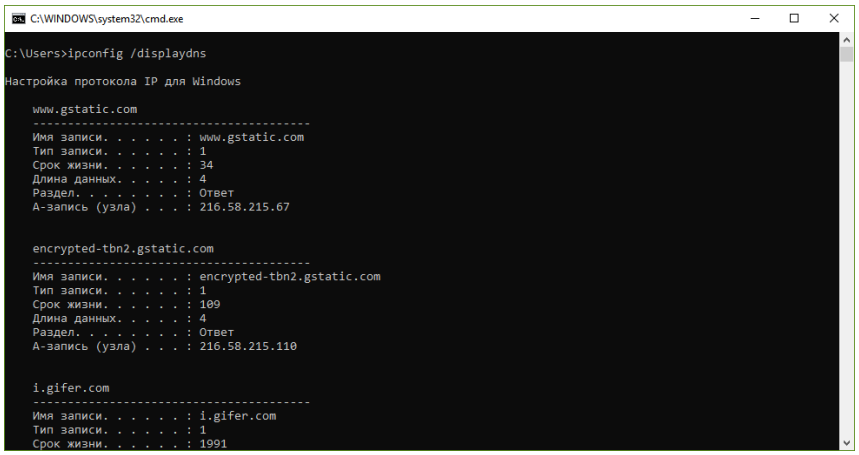
Приклад



•Визначити усі DNS записи з кешу

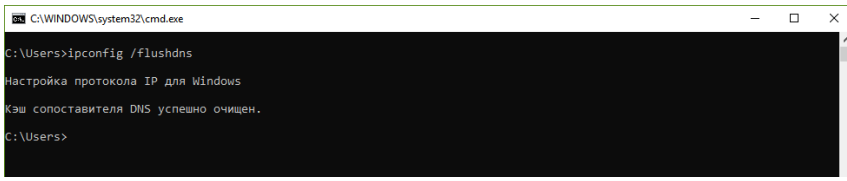
Команда: *ipconfig /displaydns*

Приклад



•Видаліть DNS кеш

Команда: *ipconfig /flushdns*

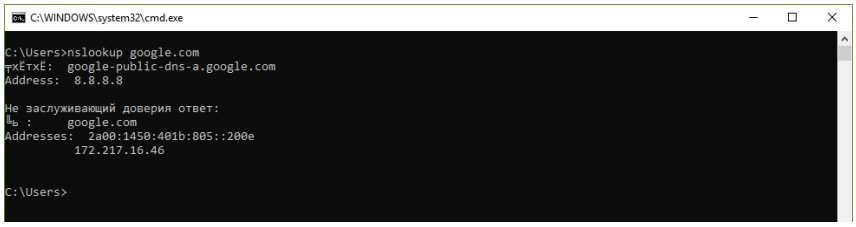


Приклад

•Визначити IP-адрес та DNS-сервер за замовчуванням

Команда: *nslookup /Певний домен/*

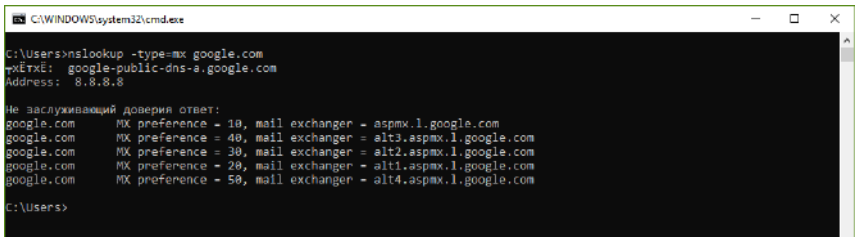
Приклад



•Визначити які MX-записи використовуються для домена google.com

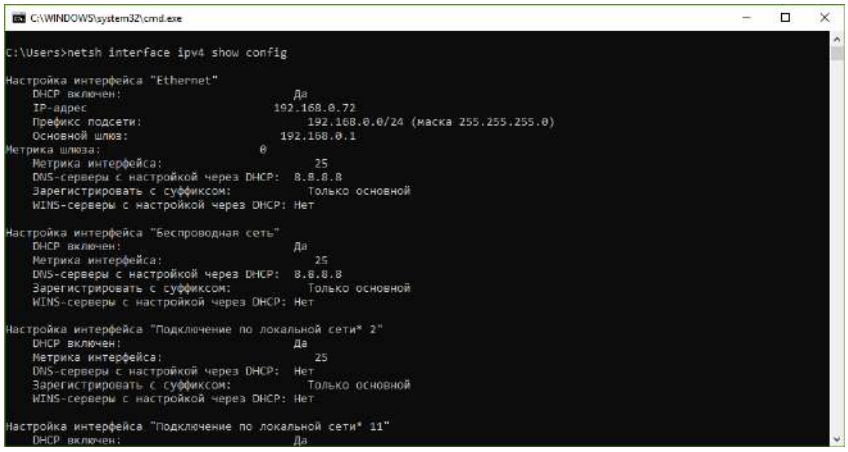
Команда: *nslookup -type=mx /Певний домен/*

Приклад



•Відтворити повну інформацію про всі адаптери та параметри з'єднань
Команда: *ipconfig /all*
Приклад

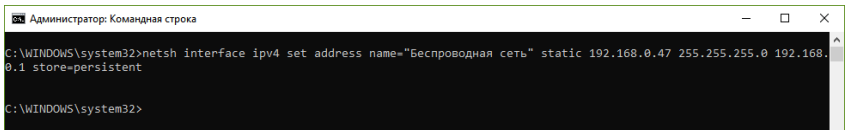
•Вивести конфігурацію усіх мережевих інтерфейсів
Команда: *netsh interface ipv4 show config*



Приклад

•Змінити адресу у визначеного інтерфейса на статичний IP з маскою підмережі та шлюзом

Команда: *netsh interface ipv4 set address name="/Ім'я інтерфейсу/" static /Локальний IP/ /Маска підмережі/ /Основний шлюз/ store=persistent*



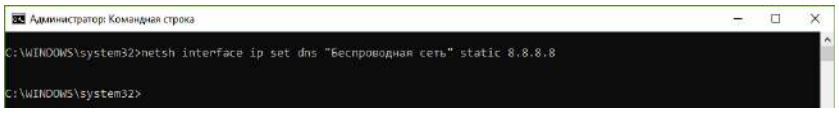
Приклад

Команду треба запускати від імені адміністратора.

•Змінити DNS

Команда: *netsh interface ip set dns "/Ім'я інтерфейсу/" static /DNS/*

Приклад

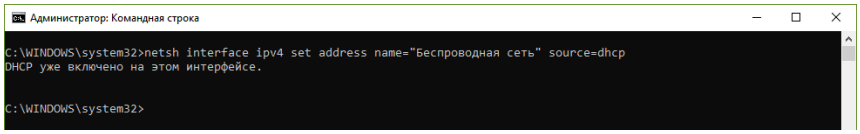


Команду треба запускати від імені адміністратора.

• Встановити DHCP на поточний інтерфейс

Команда: *netsh interface ipv4 set address name="/Ім'я інтерфейсу/" source=dhcp*

Приклад



Команду треба запускати від імені адміністратора.

• Приєднатися до FTP-серверу

Команда: *ftp /IP/*

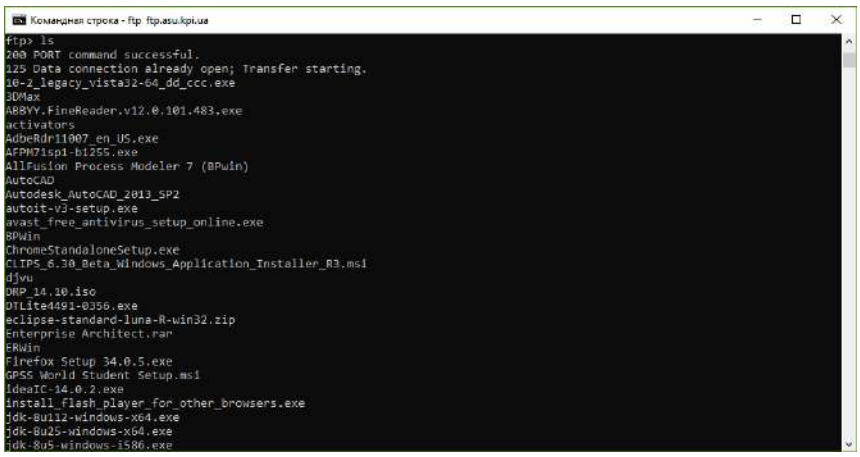
Приклад

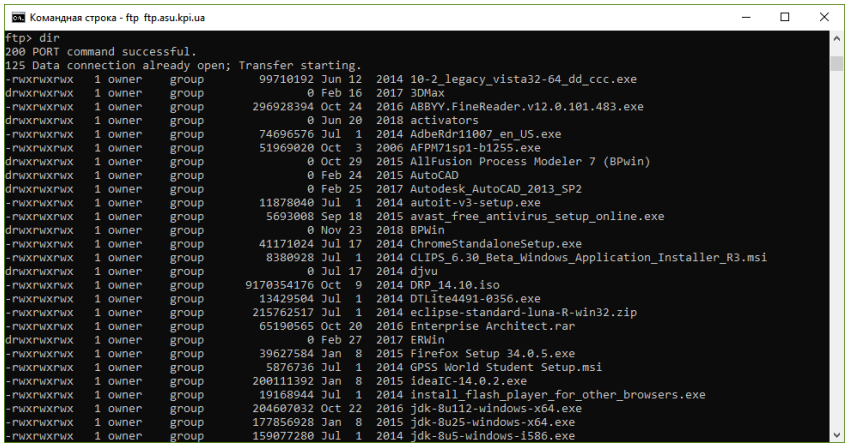
Може знадобитися автентифікація.

• Переглянути поточку директорію

Команда: *dir* або *ls*

Приклад

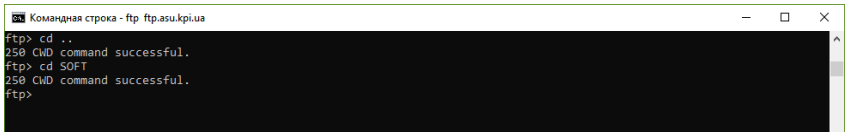




• Перейти у інший каталог або повернення назад у батьківський каталог.

Команда: *cd /Точка переходу/*

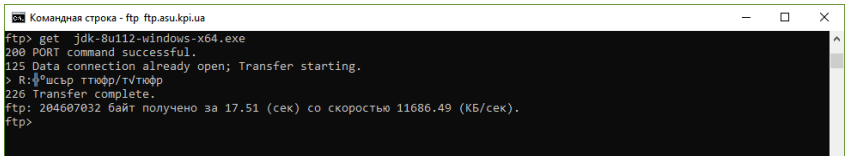
Приклад

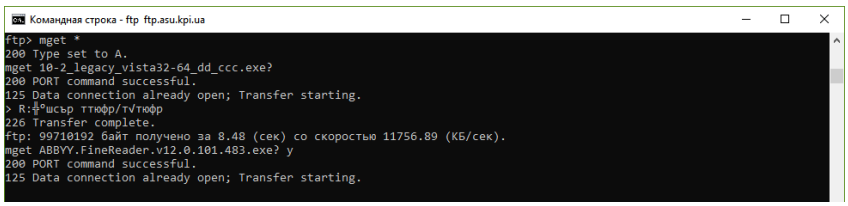


• Скачати файл або декілька з папки

Команда: *get /Назва файлу/* або *mget /Назва папки/*

Приклад





Можливо знадобиться підтвердження y/n (y – так, n – ні).

Завдання для самостійного опрацювання

1) За допомогою командного рядка та команди *ping* з’ясувати IP-адреси сайтів kpi.ua і asu.kpi.ua.

2) За допомогою команди *ipfconfig* вивести на екран усі DNS записи з кешу.

3) Видалити DNS кеш та знову вивести DNS записи.

4) За допомогою команди *nslookup* з’ясувати IP-адреси сайтів kpi.ua і asu.kpi.ua, визначити який DNS-сервер використовується за замовчуванням.

5) За допомогою команди *nslookup* і флагу *type=mx* визначити які MX-записи використовуються для домена kpi.ua.

6) Дізнатися поточну конфігурацію завдяки *ipconfig /all.*

7) За допомогою *netsh interface* вивести конфігурацію усіх мережевих інтерфейсів. Визначитись з інтерфейсом, який ви будете конфігурувати у наступних завданнях.

8) Змінити адресу у визначеного інтерфейса на статичний IP *192.168.5.50* з маскою підмережі *255.255.255.0* та шлюзом *192.168.5.1*

9) Задати новий DNS *8.8.4.4.*

10) Вивести поточну конфігурацію через *ipconfig* або *netsh interface.*

11) Установити DHCP на цей інтерфейс.

12) Знову вивести конфігурацію.

13) За допомогою команди *ftp* зайдіть на ftp-сервер кафедри (використовуючи ваш логін та пароль).

14) За допомогою команд *cd, dir* та *get* (або *mget*) скачайте будь-який файл та продемонструйте його у локальній папці.

Лабораторна робота №7

ТРАНСПОРТНИЙ РІВЕНЬ, TCP, UDP

Загальні відомості:

TCP

TCP вважається надійним транспортним протоколом, а це значить, що він використовує процеси, які забезпечують надійну передачу даних між додатками за допомогою підтвердження доставки. Передача з використанням TCP аналогічна відправці пакетів, які відслідковуються від джерела до одержувача. Якщо замовлення служби KPI Express розбивається на кілька відправлень, замовник може зайти на веб-сайт компанії і переглянути порядок доставки.

TCP використовує такі три основні операції для забезпечення надійності:

- відстеження переданих сегментів даних
- підтвердження отриманих даних
- повторна відправка всіх непідтверджених даних

TCP розбиває повідомлення на фрагменти меншого розміру, які називаються сегментами. Цим сегментам присвоюються порядкові номери, після чого вони передаються IP-протоколу, який збирає їх в пакети. TCP відстежує кількість сегментів, відправлених на той чи інший вузол тим чи іншим додатком. Якщо відправник не одержує підтвердження протягом певного періоду часу, то TCP розглядає ці сегменти як втрачені і повторює їх відправку. Повторно відправляється тільки втрачена частина повідомлення, а не всі повідомлення цілком. Протокол TCP на приймаючому вузлі відповідає за повторне складання сегментів повідомлень і їх передачу відповідним додатком. Протокол передачі файлів (FTP) і протокол передачі гіпертексту (HTTP) - це приклади додатків, які використовують TCP для доставки даних.

Такі процеси забезпечення надійності підвищують навантаження на мережеві ресурси, що пов'язано з необхідністю підтвердження, відстеження та повторної відправки даних. Для підтримки перерахованих вище процесів між відправляють і отримують вузлами пересилаються додаткові керуючі дані. Ця контрольна інформація міститься в заголовку TCP**.**

UDP

У той час як функції надійності TCP забезпечують більш стабільне взаємодію між додатками, вони також споживають більше ресурсів і можуть стати причиною затримок при передачі даних. Є певний компроміс між надійністю і тим навантаженням, яке вона представляє для мережевих ресурсів. Додаткове навантаження для забезпечення надійності деяких додатків може знизити корисність самого додатку і навіть негативно позначитися на його продуктивності. У таких випадках використання протоколу UDP більш переважно.

UDP забезпечує тільки основні функції для відправки сегментів даних між відповідними додатками, при цьому незначно використовуючи ресурси і перевірку даних. UDP відомий як протокол негарантованої доставки даних. Стосовно до

комп'ютерних мереж негарантована доставка вважається ненадійною, оскільки при цьому немає підтвердження про отримання відправлених даних на вузлі призначення. UDP не використовує процеси транспортного рівня, які повідомляють відправнику про успішну доставку даних.

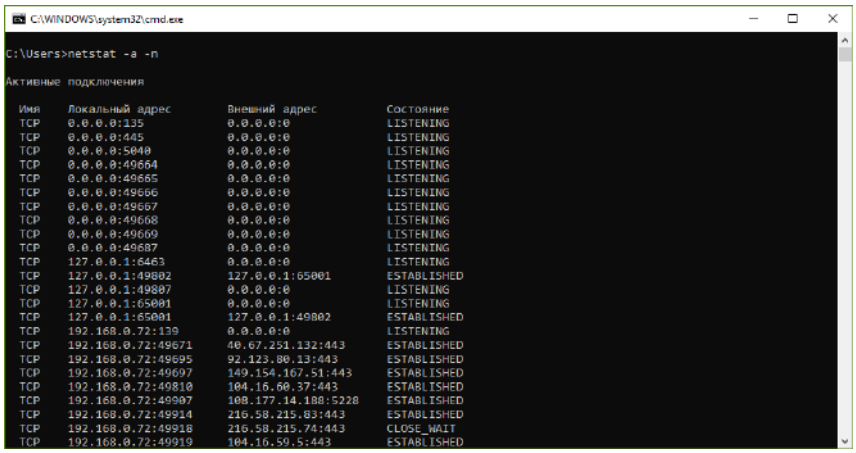
Протокол UDP подібний до того, як якщо б поштою відправляли звичайне незареєстровану лист. Відправник не знає, чи зможе адресат отримати лист, а поштове відділення не несе відповідальності за відстеження листи або інформування відправника про те, доставлено чи лист за адресою.

Хід виконання роботи:

•Вивести усі мережеві з'єднання

Команда: *netstat -a -n*

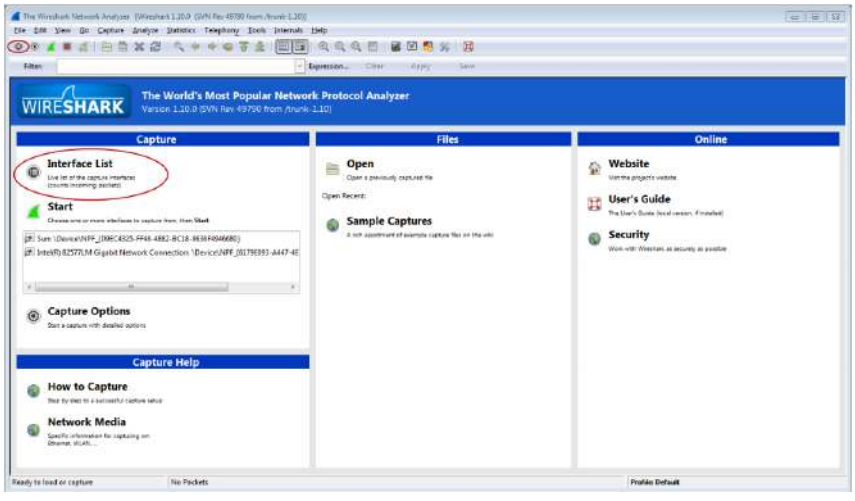
Приклад

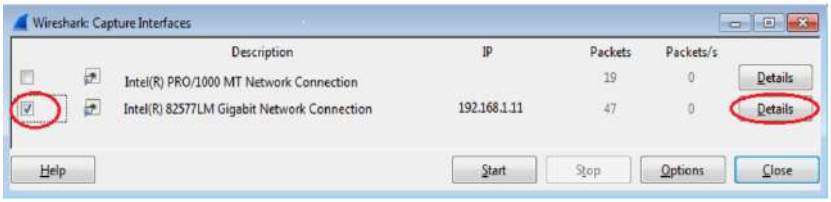


Аналіз тристороннього рукостискання TCP

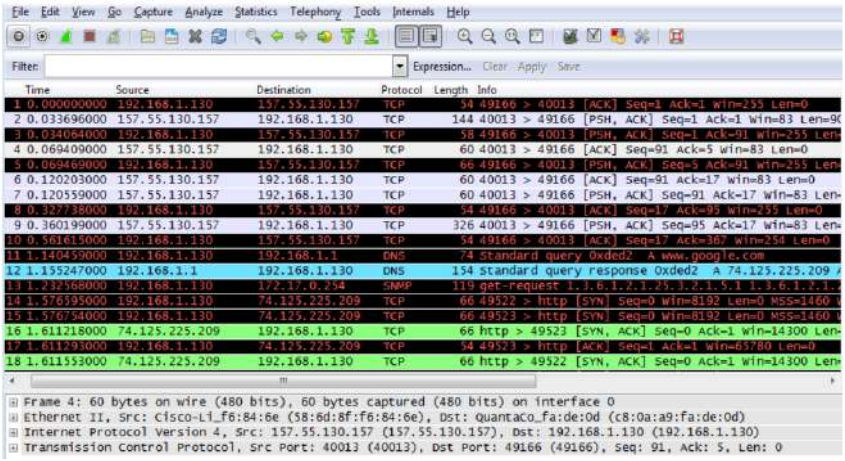
a. Вам потрібно встановити програму

b. Нажміть на параметр *Interface List*



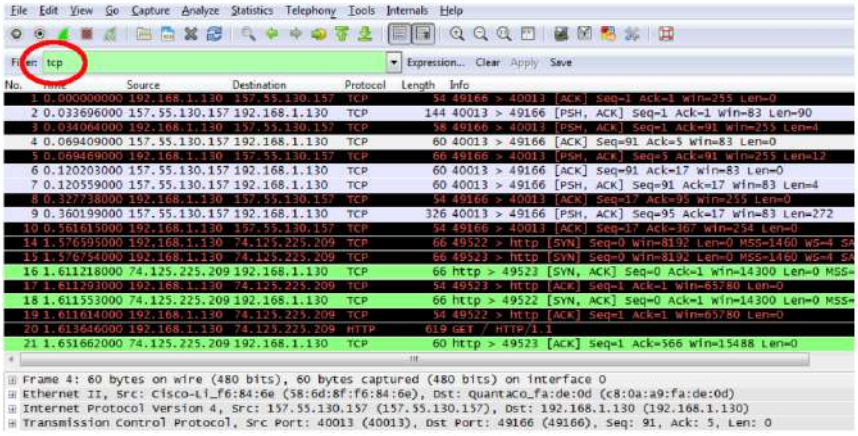


c. Установіть флажок напроти інтерфейсу вашої мережі



d. Зайдіть у браузері на певний сайт. Зупиніть процес захвату даних, ви побачите захвачений трафік, як на скріншоті. Знайдіть стовчики Time (час), Source (джерело), Destination (пункт призначення), Protocol (протокол), Length (довжина), Info (інформація).

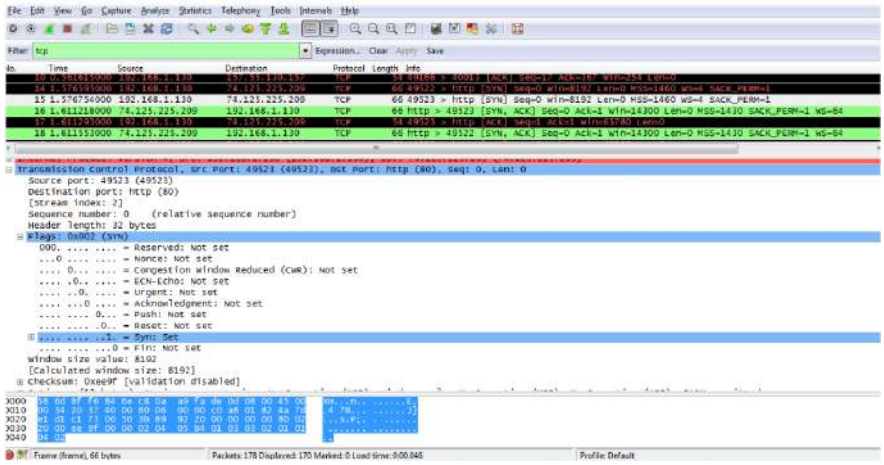
d. Профільтруйте TCP пакети, ввівши “tcp” у вікно фільтру



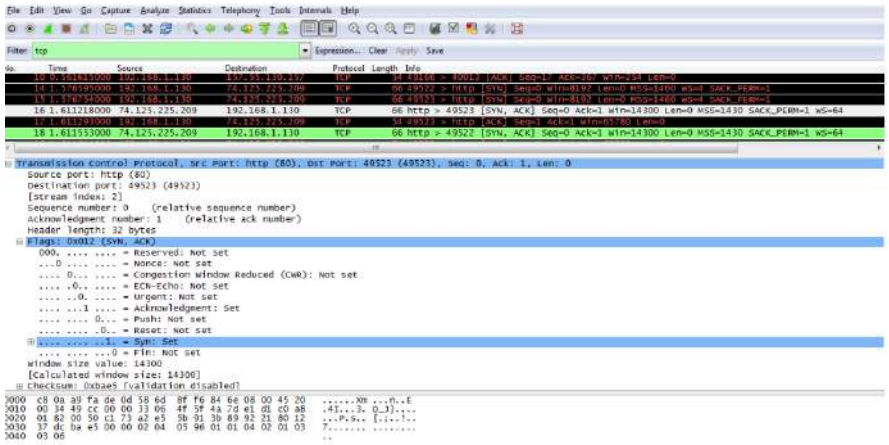
e. У наведеному прикладі кадр 15 показує початок тристороннього рукостискання між ПК і веб-сервера сайту. На панелі списку пакетів (верхній розділ основного вікна) виберіть кадр. Після цього буде виділений рядок і відображена зашифрована інформація з пакету в двох нижніх панелях. Перевірте дані TCP в панелі відомостей про пакети (середній розділ основного вікна).

На панелі натисніть на значок + зліва від рядка Transmission Control Protocol (Протокол управління передачею даних), щоб побачити детальну інформацію про TCP. Зліва від прапорців натисніть на значок +. Зверніть увагу на порти джерела і призначення,

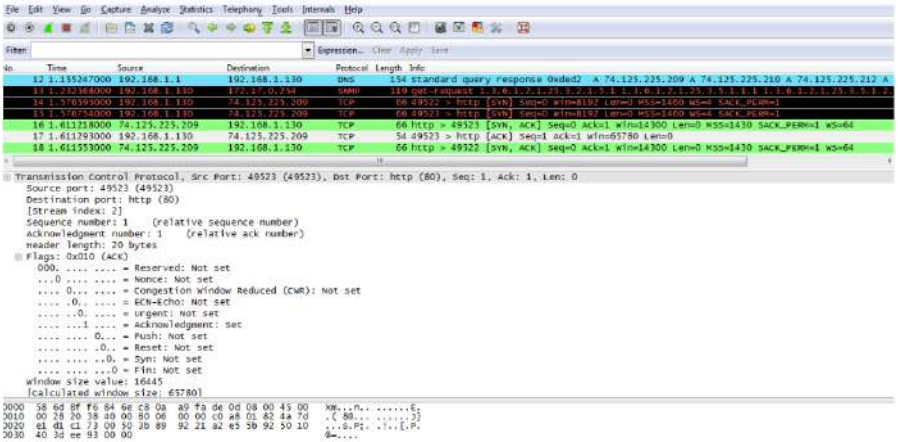
а також на встановлені прапорці.



f. Щоб вибрати наступний кадр в тристоронньому рукостисканні, в меню програми Wireshark виберіть параметр Go (Перейти), а потім Next Packet In Conversation (Наступний пакет комунікації). В даному прикладі це кадр 16. Це відповідь веб-сервера сайту на вихідний запит для початку сеансу.



І, нарешті, вивчіть третій пакет тристороннього рукостискання в даному прикладі. натиснувши на кадр 17 в верхньому вікні, ви побачите наступну інформацію в даному прикладі.



Завдання

•Визначити, до якого способу доставки (TCP, UDP або до обох) треба віднести наступні протоколи та обгрунтуйте відповідь:

- HTTP
- Telnet
- SMTP
- FTP
- DHCP
- VoIP
- IPTV
- TFTP
- DNS
- SNMP

•За допомогою команди *netstat* вивести усі мережеві з'єднання. Виписати порти, які мають зареєстроване IANA застосування та їх опис.

•Тристороннє рукостискання TCP.

•Зайдіть у браузері на google.com. Зупиніть процес захвату даних та проаналізуйте перехвачені пакети.

•Знайдіть пакет, який ініціював тристороннє рукостискання TCP.

•Випишіть IP-адрес сайту. Назвіть порт джерела TCP, якби ви класифікували порт джерела? Назвіть порт призначення, якби ви його класифікували? Які флажки встановлені?

•Перейдіть на наступний кадр в тристоронньому рукопотисканні та проаналізуйте пакет даних так само, як і в попередньому пункті. Аналогічно проробіть з останнім 3 пакетом даних.

Основна література

1. Навчальний посібник з дисциплін "Комп'ютерні мережі" для студентів / Коган А. В., Роковий О. П., Алєнін. О. І. – Київ: КПІ, 2020. – 77 с.
2. Організація комп'ютерних мереж: підручник: для студ. / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. — Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

Допоміжна література

3. Жураковський Ю.П., Полторак П. Теорія інформації та кодування : Підручник. К.: Вища шк., 2011. 255 с.

Інформаційні ресурси в Інтернеті

Закордонні електронні наукові інформаційні ресурси: European Library. Вільний доступ до ресурсів 47 Національних бібліотек Європи, Австралії, Білорусії, Великої Британії, Німеччини, бібліотека коледжу Лондонського університету.
http://www.irbis-nbuv.gov.ua/
https://elibrary.kubg.edu.ua