

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни

"Проектування комп'ютерних мереж"

для студентів спеціальності 123 Комп'ютерна інженерія,
усіх форм навчання

2024

Методичні вказівки до виконання курсового проекту з дисципліни "Проектування комп'ютерних мереж" для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання / Укл. Г.Г. Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 30 с.

Укладач:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 1 від 06.08.2024

Рекомендовано до видання
НМК ФКНТ
Протокол № 1 від 04.09.2024

ЗМІСТ

1 Загальні відомості.....	4
1.1 Календарний план та отримання завдання.....	4
1.2 Вимоги до захисту	6
1.3 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки.....	6
1.4 Теми проектів.....	8
1.5 Структура проекту.....	9
1.6 Завдання.....	11
1.7 Аналіз інформаційного трафіку	14
1.8 Планування структури мережі	14
1.9 Віддалений доступ до мережі підприємства.....	15
1.10 Забезпечення мережної безпеки.....	16
1.11 Налаштування доступу в Інтернет через cisco vpn client.....	17
2 Середовище моделювання.....	21
2.1 Приклад створення структури КМ в Packet Tracer.....	22
2.2 Моделювання потоків трафіку в Packet Tracer	23
2.3 Моделювання потоків трафіку в КМ.....	27
2.4 Вимоги до оформлення пояснювальної записки	29
Рекомендована література	30

1 ЗАГАЛЬНІ ВІДОМОСТІ

Мета роботи – закріплення теоретичних і практичних навичок із: проектування, моделювання, налаштування та розрахунку параметрів локальних комп'ютерних мереж (КМ) та проектування мереж рівня підприємства; проведення аналізу їх функціонування у сучасному середовищі; адміністрування, конфігурування локальних мереж та мереж рівня підприємства; організації їх доступу до мережі Internet.

Об'єктом є процес проектування мережі рівня підприємства, згідно індивідуального варіанту.

Предметом є моделі, технології, стандарти, програмні засоби та імітаційне середовище моделювання проектованої мережі.

Завдання до курсового проекту передбачають розробку функціональної моделі мережі підприємства та її структурної схеми, згідно варіанту; визначення кількості та видів обладнання; опис технологій і стандартів, згідно варіанту; налаштування конфігураційних параметрів мережних інтерфейсів обладнання мережі та серверів; з'єднання в єдину мережу локальних мереж підприємства за допомогою маршрутизаторів (загальна кількість кінцевих вузлів та віддалених локальних мереж вказана в таблиці 1.2); моделювання потоків трафіку в мережі та налаштування віддаленого доступу до Internet із забезпеченням мережної безпеки.

Примітка. Варіанти, згідно списку студентів по групах, розміщуються в системі moodle.

1.1 Календарний план та отримання завдання

Систематичне і своєчасне виконання роботи – запорука одержання якісного результату і високої оцінки.

Рекомендований графік роботи наведено в таблиці 1.1. Студент може корегувати графік в межах наведених дат, не змінюючи дати захисту.

Таблиця 1.1- Етапи виконання курсового проекту

№ п/п	Назва етапів курсового проекту	Термін виконання
1	Аналіз технічного завдання та оформлення ТЗ на проектування	до 28.02
2	Розробка функціональної моделі, проектованої мережі	01.03 – 10.03
3	Розробка структурної схеми проектованої мережі підприємства	11.03 – 20.03
4	Опис технологій та їх стандартів для LAN і WAN сегментів мережі підприємства	21.03 – 25.03
5	Аналіз та вибір мережного, серверного і клієнтського обладнання	26.03 – 31.03
6	Налаштування обладнання LAN та WAN мереж підприємства	01.04 – 10.04
7	Встановлення IP-адрес мережних інтерфейсів	11.04 – 15.04
8	Організація віддаленого доступу до мережі, отримання пулу відкритих адрес	16.04 – 20.04
9	Вибір методів та налаштування маршрутизації мережі підприємства	21.04 – 25.04
10	Налаштування маршрутизаторів, згідно політики безпеки мережі підприємства, підключення до Інтернет	26.04 – 30.04
12	Оформлення графічного матеріалу (моделі, структурна схема)	01.05 – 10.05
13	Оформлення ПЗ	11.05 – 19.05
14	Захист КП (згідно графіку захисту)	до 25.05

У відповідності до теми, студент оформлює (заповнює основні розділи з вказівкою термінів виконання окремих етапів та всього проекту в цілому) технічне завдання (ТЗ) до проекту та затверджує його у **керівника проекту**.

У ТЗ треба чітко визначити такі данні: назва проекту; вихідні данні до проектування (3 пункт) із зазначенням кількості об'єктів, які підключаються (мереж), кількості і видів обладнання, фізичне середовище каналів зв'язку; технології (LAN та WAN) мереж; перелік загальних питань (4 пункт), які розглядаються (зверніть увагу, що це є переліком основних розділів змісту) та перелік графічного (5 пункт) матеріалу

(моделі, функціональна та структурні схеми (обов'язкові), монтажні схеми, алгоритми роботи мережі).

Календарний графік виконання курсового проекту, який складається студентом (за прикладом календарного плану, табл.1.1) і затверджується керівником проекту, повинен відповідати етапам проектування, аналізу та вирішенню загальних питань стосовно до всього об'єкту проектування в цілому.

1.2 Вимоги до захисту

Захист курсового проекту відбувається за затвердженим викладачем графіком (останній тиждень теоретичного навчання). На доповідь дається 5 хвилин. За цей час необхідно продемонструвати результати виконання проекту в середовищі моделювання Cisco Packet Tracer (якщо це не зроблено раніше на лабораторних роботах), навести функціональну та структурну схеми мережі, стисло викласти суть прийнятих рішень та довести працездатність мережі.

Після закінчення доповіді викладач може задавати питання, призначення яких – уточнити рівень кваліфікації і ступень самостійності виконання проекту студентом. На питання необхідно давати стислі прямі відповіді, при необхідності використовуючи середовище моделювання та презентацію проекту за темою.

1.3 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки

Теми роботи, наведені у розділі 1.4 та виконуються кожним студентом, згідно персональних варіантів (розділ 1.6).

Звіт виконують без рамок, **шрифтом Times New Roman** чорного кольору прямого креслення через **півтора міжрядкові інтервали** кеглем **14 пт**, з **абзацем** для основного тексту **1,25 см** та полями: **нижнє та верхнє 2 см, ліве 2,5 см та праве 1,5 см**.

До пояснювальної записки необхідно включати матеріал, який безпосередньо відноситься до розробки конкретної мережі, яка підлягає проектуванню, у відповідності до технічного завдання. Не рекомендується робити великі реферативні огляди. При необхідності потрібно робити посилання на відповідну літературу. Основний зміст записки – це аналіз, порівняння, вибір та обґрунтування прийнятих

рішень та проект мережі підприємства, згідно затвердженої назви. Треба мати на увазі, що звіт складають тоді, коли проектування завершено, всі рішення прийнято, всі деталі є відомими, є кінцевий результат, і саме його необхідно привести разом з аргументацією вибору рішень, необхідними розрахунками, графіками, таблицями, рисунками, матеріалами, які обґрунтовують прийняті рішення.

Приблизний рекомендований обсяг кожного розділу наведено нижче. Назви розділів у конкретній роботі можуть відрізнятися від наведених далі, послідовність розташування розділів може бути іншою, але в цілому у пояснювальній записці рекомендовано висвітлити всі питання.

У рефераті проектант вказує мету роботи, об'єкт та предмет проектування; технології, вид обладнання, протоколи та стандарти, які використані у розробленому проекті. Наводить ключові слова та об'єм пояснювальної записки, кількість рисунків, таблиць та джерел. Реферат рекомендовано оформити на заключному етапі (**1 сторінка**).

У вступі до проекту проектант повинен обґрунтувати актуальність проектування мережі підприємства за варіантом, навести методи та шляхи проведення досліджень, зазначити в яких розділах пояснювальної записки наведено: аналіз структури організації; схеми інформаційних потоків (трафіку); опис технологій (LAN та WAN мереж) та комунікаційного обладнання; налаштування, тощо. Вступ має бути коротким (1-2 сторінки) і чітким, не перевантаженим загальними фразами, зрозумілим, чому присвячені етапи проектування.

У першому розділі (4-5 сторінок) ПЗ необхідно провести аналіз технічного завдання, розглянути структуру підприємства в цілому та проаналізувати загальний обсяг трафіку, визначити необхідну швидкість каналів зв'язку та яке обладнання потребує заміни і яке необхідно придбати додатково для підключення віддалених об'єктів мережі підприємства. Студент повинен чітко визначити коло задач (перелік основних задач наведено на стор. 4), які необхідно вирішити в курсовому проекті.

У другому розділі (6-8 сторінок) на підставі проведеного аналізу наводиться модель (функціональна схема) та структурна схема мережі підприємства, виконується опис LAN\WAN-технологій окремих сегментів мережі. Кількість мереж та підключених робочих станцій визначається варіантом.

Третій розділ (6-8 сторінок) повинен містити опис апаратної та кабельної частини проекту з урахуванням технологій та можливості з'єднання через маршрутизатори окремих LAN підприємства, з метою налаштування віддаленого доступу. Цей розділ містить вибір конкретних елементів реалізації монтажних схем, розрахунок окремих елементів, вузлів та підсистем. Виконується налаштування загальних об'єктів.

У четвертому розділі (до 6 сторінок) розглядається підключення мережі підприємства до Internet та питання забезпечення мережевої безпеки, як у дротових так і бездротових LAN. Проектантом розкриваються питання забезпечення якості та надійності мережі, питання апаратного та програмного захисту інформації. Розглядається призначення IP-адрес та подання мережі головного офісу організації (підприємства) в Інтернеті.

У висновках (1 сторінка) студент формулює основні результати, які отримані під час виконання курсового проекту.

Оформлення записки здійснюється у відповідності до діючих стандартів ДСТУ 3008-95 “Документація. Звіти в сфері науки і техніки”, Єдиної Системи Конструкторської Документації (ЄСКД). Бібліографічні описи в переліку посилань наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання». До записки обов'язково додається креслення формату А4 або А3 (структурна схема) та 1 плакат (функціональна схема мережі) того ж формату.

Загальний обсяг ПЗ – 25 - 30 сторінок (не рекомендовано обсяг більший за 35 стор.), причому технічна частина ПЗ, має містити не менш ніж 15-20 сторінок тексту з налаштуванням обладнання.

1.4 Теми проектів

Далі наведено теми проектів за варіантами.

1. Розподілена комп'ютерна мережа транспортного підприємства.
2. Розподілена комп'ютерна мережа офісів оператора мобільного зв'язку.
3. Розподілена комп'ютерна мережа коледжів.
4. Розподілена комп'ютерна мережа металургійного підприємства.

5. Розподілена комп'ютерна мережа спорткомплексів.
6. Розподілена комп'ютерна мережа поштових відділень.
7. Розподілена комп'ютерна мережа багатоквартирного будинку.
8. Розподілена комп'ютерна мережа авіаційного підприємства.
9. Розподілена комп'ютерна мережа баз відпочинку.
10. Розподілена комп'ютерна мережа мешканців мікрорайону.
11. Розподілена комп'ютерна мережа офісів банку.
12. Розподілена комп'ютерна мережа пенсійного фонду.
13. Розподілена комп'ютерна мережа агропромислового комплексу.
14. Розподілена комп'ютерна мережа комунального підприємства.
15. Розподілена комп'ютерна мережа супермаркетів.
16. Розподілена комп'ютерна мережа енергетичного комплексу.
17. Розподілена комп'ютерна мережа торгівельного підприємства.
18. Розподілена комп'ютерна мережа податкової служби.
19. Розподілена комп'ютерна мережа лікарень.
20. Розподілена комп'ютерна мережа вузів міста.
21. Розподілена комп'ютерна мережа банкоматів.
22. Розподілена комп'ютерна мережа залізниці.
23. Розподілена комп'ютерна мережа готелів.
24. Розподілена комп'ютерна мережа салонів краси.
25. Розподілена комп'ютерна мережа промислового підприємства.

1.5 Структура проекту

В процесі проектування мережі рівня підприємства студенту рекомендовано розглянути наведені нижче питання, тримаючись загального плану проекту за варіантом. Основні етапи проектування можуть включати.

Вступ.

Аналіз технічного завдання:

– дослідження та аналіз структури підприємства (з описом основних підрозділів і філій, з урахуванням їх віддаленості);

- аналіз інформаційних потоків (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку);
- аналіз (для модернізації) наявних апаратних і мережних пристроїв; побудова моделі мережі;

– постановку завдань, пов'язаних з проведенням досліджень, аналізом, порівнянням та вибором методів за засобів проектування.

Вибір технологій, апаратних і мережних пристроїв:

– проведення аналізу, наявних LAN і WAN технологій, порівняння та вибір технологій (певних специфікацій) для конкретних каналів зв'язку у LAN мережах підприємства та WAN між мережами вашої організації, з урахуванням підключення філій;

– дослідження, аналіз технічних характеристик та вибір мережних пристроїв з визначенням кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування;

– аналіз технічних характеристик та вибір апаратних пристроїв (сервери, ПК, ноутбуки, термінали, планшети, IP-телефони та ін.) З описом характеристик кожного пристрою або групи пристроїв, опис призначення та особливості застосування.

Налаштування мережі:

– визначення основних LAN і WAN сегментів, проектування структурної схеми мережі;

– побудова монтажної схеми (розміщення мережових і апаратних пристроїв (в будівлях, на поверхах, в кімнатах));

– розрахунок потужності антен; підключення (фізичне об'єднання мережних і апаратних пристроїв єдиної мережі);

– вибір принципу адресації та маршрутизації для LAN і WAN сегментів (мереж);

– програмне налаштування всього мережного обладнання (з урахуванням адресації і маршрутизації).

Адміністрування мережі:

– опис налаштування віддаленого доступу до філій (технології створення тунелів між LAN підприємства (див. методичні вказівки до лабораторних робіт));

– моделювання потоків трафіку;

– підключення до Інтернет та забезпечення мережової безпеки (налаштування обладнання, протоколів).

Висновки.

Кількість і назви розділів у проекті можуть відрізнятись від наведених але це не повинно впливати на загальну мету проектування.

1.6 Завдання

Практична частина проекту передбачає наступні завдання:

- розробити функціональну та структурну схему розподіленої мережі підприємства, згідно варіанту завдання (табл. 1.2, 1.3), де PC – кількість комп'ютерів; N – загальна кількість локальних мереж (підмереж); S – кількість серверів; IP – тип ір-адресації та адреса мережі для розбиття на N мереж;
- налаштувати стандарти локальних мереж, враховуючи запропоноване мережне обладнання і фізичне середовище (табл. 1.2);
- налаштувати додаткові технології LAN мереж (табл. 1.3);
- налаштувати IP-адреси локальних та відкритих мереж підприємства з урахуванням типу адресації (табл. 1.3);
- налаштувати додаткові технології WAN мереж та маршрутизацію, з урахуванням її виду (табл. 1.3);
- виконати моделювання потоків трафіку в мережі в середовищі моделювання. Для цього відправити комплексні пакети від клієнта до серверів за відповідними протоколами (згідно варіанту) та між мережами підприємства. Переглянути їх маршрути, навести маршрут та вміст пакетів після кожного хопу (переходу);
- налаштувати підключення до Інтернет;
- за бажанням, виконати монтажні схеми мережі підприємства.

Таблиця 1.2 – Варіанти завдань на курсовий проект

Вар. №	PC	N	S	Стандарти локальних мереж	Мережне обладнання	Фізичне середовище	Тип IP адресації
1	150	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
2	170	5	3	10BaseT, 100BaseTX	Hub, Switch	Вита пара	Статична
3	180	7	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
4	171	4	3	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Статична

Продовження таблиці 1.2

5	176	6	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
6	159	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Статична
7	168	5	2	10BaseT, 100BaseTX	Hub Switch	Вита пара	Динамічна
8	181	4	3	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
9	179	4	2	100BaseTX WiFi	Switch	Вита пара, безпроводне	Динамічна
10	174	4	3	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
11	190	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Статична
12	172	5	3	10BaseT, 100BaseTX	Hub Switch	Вита пара	Статична
13	184	7	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Динамічна
14	167	5	2	100BaseTX WiFi	Switch	Вита пара, безпроводне	Динамічна
15	178	4	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
16	158	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
17	177	5	3	10BaseT, 100BaseTX	Hub Switch	Вита пара	Статична
18	183	6	3	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Динамічна
19	169	5	2	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Статична
20	185	4	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Динамічна
21	182	4	3	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
22	188	5	3	10BaseT, 100BaseTX	Switch	Вита пара	Динамічна
23	173	4	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
24	189	7	2	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Статична
25	166	4	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Динамічна

Таблиця 1.3 – Варіанти завдань на курсовий проєкт

Вар. №	IP (адреси для філій)	IP (між маршрутизаторами (3-6 мереж))	Маршрутизація	LAN технології	WAN технології
1	192.168.2.0/24	212.3.25.0/27	Статична	DNS, VLAN	FrameRelay
2	10.5.16.0/23	193.5.16.0/27	Статична	DNS, ACL	VPN (GRE)
3	172.30.2.0/23	222.32.2.0/27	Динамічна	VLAN, NTP	ACL
4	10.1.14.0/24	195.1.14.0/27	Статична	HTTP, ACL	VPN (IPSec)
5	172.23.40.0/23	212.3.40.0/27	Динамічна	VLAN, DNS	IPv6
6	192.168.0.0/24	211.2.13.0/27	Динамічна	DNS, ACL	FrameRelay
7	10.56.8.0/23	199.56.8.0/27	Статична	VLAN, NTP	VPN (GRE)
8	172.16.16.0/24	200.1.16.0/27	Статична	DNS, ACL	ACL
9	10.17.2.0/24	201.17.2.0/27	Динамічна	DNS, VLAN	VPN (IPSec)
10	10.9.11.0/24	210.9.11.0/27	Динамічна	DNS, ACL	IPv6
11	172.17.13.0/24	200.3.13.0/27	Статична	VLAN, NTP	FrameRelay
12	10.5.18.0/23	199.5.18.0/27	Статична	HTTP, ACL	VPN (GRE)
13	172.31.30.0/23	228.1.30.0/27	Статична	VLAN, DNS	ACL
14	10.9.33.0/23	195.9.33.0/27	Динамічна	DNS, ACL	VPN (IPSec)
15	192.168.4.0/24	205.6.64.0/27	Динамічна	VLAN, NTP	IPv6
16	10.20.1.0/24	211.20.1.0/27	Статична	DNS, ACL	FrameRelay
17	172.18.84.0/23	199.8.84.0/27	Динамічна	DNS, VLAN	VPN (GRE)
18	10.4.38.0/23	214.4.38.0/27	Динамічна	DNS, ACL	ACL
19	192.168.9.0/23	201.1.98.0/27	Статична	VLAN, NTP	VPN (IPSec)
20	172.29.19.0/24	197.9.19.0/27	Динамічна	HTTP, ACL	IPv6
21	10.2.27.0/23	223.2.27.0/27	Статична	VLAN, DNS	ACL
22	172.21.48.0/23	196.1.48.0/27	Динамічна	DNS, ACL	IPv6
23	10.3.62.0/24	201.3.62.0/27	Динамічна	VLAN, NTP	VPN (IPSec)
24	172.27.20.0/23	217.7.20.0/27	Статична	DNS, ACL	FrameRelay
25	192.168.8.0/24	194.5.81.0/27	Статична	DNS, VLAN	VPN (GRE)

1.7 Аналіз інформаційного трафіку

При проведенні аналізу інформаційного трафіку (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку) скористайтесь рішенням подібних завдань. Загальний об'єм трафіку за 10 хвилин:

- для підприємств з інформаційним трафіком 20 ГБайт;
- для підприємств з відео трафіком 100 ГБайт;
- для підприємств із різним видом трафіком 50 ГБайт;

Приклад постановки завдання та його вирішення. Яку мінімальну швидкість у каналі зв'язку в бітах/сек. необхідно забезпечити у сегменті мережі, яка включає 100 користувачів, при одночасній передачі ними файлів обсягом по 100 Мбайт. За умови: час передачі кожного користувача не більше 10 хвилин; MTU = 1000 байт (B); заголовки канального рівня = 20 B; заголовки IP = 15 B, UDP, TCP по 25 B.

Для спрощення вважаємо, що 1 GB = 1000 MB, 1 MB = 1000 KB.

Вирішення.

1. Знайдемо загальний обсяг корисних даних, який потрібно передати за 10 хвилин та час у секундах:

$V_k = 100 * 100\text{MB} = 10 \text{ GB}$ - загальний обсяг корисних даних

$T = 10 * 60 = 600 \text{ сек.}$ - час у секундах

2. Визначимо MSS:

$MSS = MTU - IP - TCP = 1000 - 15 - 25 = 960 \text{ байт корисних даних}$

3. **Кількість пакетів:** $10\text{Гбайт}/960\text{байт} = 10\,416\,667 \text{ пакетів}$

4. **Обсяг заголовків:** $10\,416\,667 * (20 + 15 + 25) = 625\,000\,020 \text{ байт} \approx 625\text{Мбайт} + \text{до } 10\text{Гбайт}.$

5. $V = 10\,625 \text{ Мбайт} * 8 = 85\,000 \text{ Мбіт} = 85 \text{ Гбіт}$ – загальний обсяг даних, який потрібно передати за 10 хвилин.

6. **Швидкість** $R(t) = V/T = 85 \text{ Гб}/600\text{с} = 141,7 \text{ Мб/с}$

Розрахунки виконуються для всіх підключень з метою визначення пропускну здатності каналів зв'язку.

1.8 Планування структури мережі

Створення плану мережної інфраструктури - найважливіша частина проектування мережі. Як правило, не всі елементи

інфраструктури мережі доводиться проектувати "з нуля", деякі з них успадковуються від інших елементів.

Планування інфраструктури набагато складніше інших етапів побудови мережі, оскільки припускає створення плану, що використовується для монтажу і підтримки мережі. На плані задають розміщення основних компонентів мережі: кабельних ліній, комутаторів, серверів, маршрутизаторів і інших комунікаційних пристроїв, а також комп'ютерів, тощо. Маючи протоколи каналного рівня для реалізації мережі, можна приступати до планування розміщення мережних ресурсів, тому що від протоколу залежить максимальна довжина кабелю і число комутаторів у мережі. Описуємо фізичне середовище: вита пара, оптоволоконо, частоти для бездротових каналів. Швидкість передачі - важливий критерій вибору протоколу каналного рівня. Розміщення сервера повинне враховувати розташування робочих місць користувачів та характер трафіку. При проектуванні рекомендовано визначитись з розміщенням обладнання з застосуванням загальних стандартів СКС.

1.9 Віддалений доступ до мережі підприємства

Організація віддаленого доступу та вибір постачальника послуг Інтернету (ISP) - важливий аспект планування стратегії доступу в Інтернет для великої та середньої мереж. Основна функція ISP - надання доступу в Інтернет. ISP підтримує власну мережу, з'єднану з Інтернетом, до якої абоненти підключаються за допомогою різних технологій. Оператор зв'язку може мати різну спеціалізацію: постачальник телефонних послуг; постачальник послуг Інтернету; оператор кабельного телебачення; універсальний оператор, який надає весь спектр послуг і володіє власними мережами всіх типів.

Технологія VPN використовує передові технології шифрування і тунелювання для створення безпечного з'єднання через Інтернет. Основою для безпеки VPN є конфіденційність даних, цілісність даних та автентифікація. Використання можливостей конфіденційності даних в VPN гарантує, що тільки визначені відправники та отримувачі здатні інтерпретувати оригінальний вміст повідомлення. Тунелювання дозволяє використовувати публічні мережі для передачі даних для користувачів так, ніби користувачі мали доступ до приватної мережі.

Тунелювання інкапсулює весь пакет в інший пакет і посилає новий, композитний пакет по мережі.

Мережа VPN імітує канал точка-точка та інкапсулює дані, у заголовку яких міститься інформація про маршрутизацію. Даний формат дозволяє даним проходити через публічну мережу, щоб досягнути призначення. Сам по собі тунель не може забезпечити безпеку, а лише створює розширення локальної мережі в рамках WAN чи публічної мережі. Тунелі можуть передавати як зашифровані, так і незашифровані дані.

1.10 Забезпечення мережної безпеки

Технологія захищеного каналу – захист трафіку між двома підключеннями у відкритій транспортній мережі (Інтернет). Захищений канал виконує три основних функції: автентифікація абонентів при встановленні з'єднання; шифрування переданих повідомлень; підтвердження цілісності повідомлень.

IPSec - архітектура або набір концепцій, які використовуються для захисту мереж IP (скорочена версія найменування в RFC (RFC +4301; архітектура безпеки Інтернет-протоколу - Security Architecture for the Internet Protocol), для якої вживається назва "IPSecurity" або скорочена версія - "IPSec"). IPSec - набір протоколів для забезпечення IP комунікацій, який забезпечує шифрування, цілісність та автентифікацію. Протоколи IPSec можна розділити на два класи: протоколи, які відповідають за захист потоку пакетів та протоколи обміну криптографічними ключами. На даний момент визначений тільки один протокол обміну криптографічними ключами – IKE (Internet Key Exchange) – та два протоколи, які забезпечують захист потоку інформації, що передається:

- Authentication Header (AH) - використовується коли конфіденційність не потрібна, або не вимагається;
- Encapsulating Security Payload (ESP) - забезпечує цілісність та конфіденційність шляхом шифрування IP-пакетів.

IPSec реалізований на основі існуючих алгоритмів шифрування, автентифікації та обміну ключами. Для виконання шифрування та дешифрування за допомогою алгоритмів, які використовують симетричний секретний ключ колективного використання, необхідно його створити та роздати. Налаштування ключів може здійснюватися

вручну мережевим адміністратором, або за допомогою методу обміну ключами. Погодження ключа Діффі-Хеллмана (DH) – це публічний метод обміну ключами, який дозволяє двом сторонам встановлювати секретний ключ, що використовується при передачі даних по незахищеному каналі.

GRE (англ. *Generic Routing Encapsulation* - загальна інкапсуляція маршрутів) - протокол тунелювання мережних пакетів, розроблений компанією Cisco Systems. Його основне призначення - інкапсуляція пакетів мережевого рівня моделі OSI в IP пакети. У зв'язку зі службовим заголовком розмір переданих даних усередині IP пакета через GRE-тунель зменшується при збереженні загального розміру пакета. У IP-пакеті передбачено наявність біта DF (do not fragment), який забороняє поділ пакета на декілька частин при передачі через середовище з меншим розміром MTU.

1.11 Налаштування доступу в Інтернет через cisco vpn client

Для прикладу, виконаємо налаштування доступу в інтернет через cisco VPN client і корпоративний cisco router, підключений до провайдера по PPPoE. Необхідно організувати IPsec VPN між корпоративним мережним пристроєм і в інтернет виходити через нього. З'явиться реальна можливість безпечно використовувати внутрішні ресурси корпоративної мережі. Для цього досить мати router з підтримкою VPN. Схема наступна (рис.1.1):

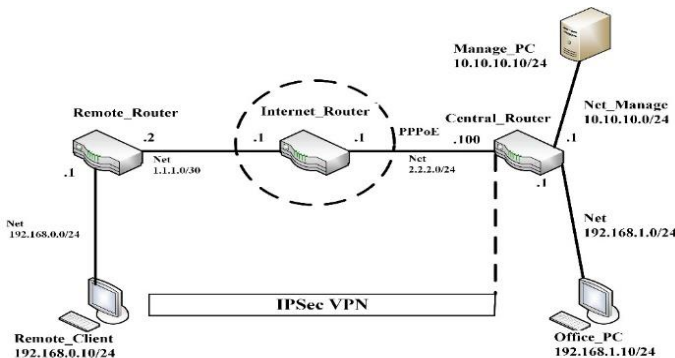


Рисунок 1.1 – Схема мережі

Маємо центральний офіс, де розташований Central_Router. Через нього робітники отримують доступ в інтернет. Він має 3 інтерфейси:

- FEthernet 0/0 - підключений до інтернет. 2.2.2.100/24 - адресу він отримує від провайдера;
- FEthernet 1/0 - підключений до локальної мережі з IP-адресом 192.168.1.1/24. Цей інтерфейс є inside для NAT;
- FEthernet 2/0 - підключений до мережі управління (Manage). IP-адреса 10.10.10.1/24. У цій мережі розташована консоль (Manage_PC 10.10.10.10/24) для налаштування роутера.

Далі є Internet_Router. За допомогою нього емулюється мережа Internet і він налаштовується як PPPoE Server, для обслуговування підключення центрального офісу (Central_Router). Internet_Router має публічні адреси і видає їх клієнту (2.2.2.100/24 - публічна IP-адреса).

Далі Remote_Router, використовуємо в якості доступу до Internet віддалених клієнтів. На ньому є два інтерфейси:

- FEthernet0/0 - підключений до ЛОМ з адресою 192.168.0.1/24, де знаходиться віддалений клієнт. Адреса є inside для NAT;
- FEthernet1/0 - підключений до мережі Internet. IP-адреса 1.1.1.2/24 Цей інтерфейс є outside для NAT;

Для перевірки є два комп'ютера:

- перший (Office_PC) в ЛОМ офісу (192.168.1.10/24);
- другий (Remote_Client) розташовується у віддаленій мережі (192.168.0.10/24) з cisco VPN client для побудови VPN тунелю.

Почнемо з віддаленого роутера. Заходимо на Remote_Router:

```
R1#conf t
R1(config)#hostname Remote_Router - задаємо ім'я;
Remote_Router(config)#int fa 0/0
Remote_Router(config-if)#ip address 192.168.0.1 255.255.255.0
- встановлюємо IP-адресу;
Remote_Router(config-if)#no cdp enable - вимикаємо CDP;
Remote_Router(config-if)#ip nat inside - вказуємо, що
інтерфейс буде inside для NAT;
Remote_Router(config-if)#no shutdown - вмикаємо інтерфейс;
Remote_Router(config-if)#exit
Remote_Router(config)#int fa 1/0
Remote_Router(config-if)#ip address 1.1.1.2 255.255.255.252
Remote_Router(config-if)#ip nat outside - вказуємо, що
інтерфейс буде outside для NAT;
Remote_Router(config-if)#no shutdown
Remote_Router(config-if)#exit
Remote_Router(config)#ip access-list extended FOR_NAT -
```

створюємо список доступу для NAT;

```
Remote_Router(config-ext-nacl)#permit ip 192.168.0.0
0.0.0.255 any
Remote_Router(config-ext-nacl)#deny ip any any
Remote_Router(config-ext-nacl)#exit
Remote_Router(config)#ip nat inside source list FOR_NAT
interface fa 1/0 overload - вмикаємо NAT на роутері;
Remote_Router(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1 -
прописуємо маршрут за замовченням;
Remote_Router(config)#exit
Remote_Router#wr - зберігаємо конфігурацію.
```

Переходимо на роутер Internet_Router:

```
R2#conf t
R2(config)#hostname Internet_Router
Internet_Router(config)#int fa 0/0
Internet_Router(config-if)#ip address 1.1.1.1 255.255.255.252
Internet_Router(config-if)#no shutdown
Internet_Router(config-if)#exit
Internet_Router(config)#interface virtual-template 1 -
заходимо в налаштування шаблону інтерфейсу користувача для
PPPoE клієнтів;
Internet_Router(config-if)#ip address 2.2.2.1 255.255.255.0 -
вказуємо IP-адресу, яка буде gateway для PPPoE клієнтів;
Internet_Router(config-if)#ip virtual-reassembly
Internet_Router(config-if)#ip unnumbered fastEthernet 1/0 -
визначаємо інтерфейс, на який будуть приходити запити на
встановлення PPPoE з'єднань;
Internet_Router(config-if)#ppp authentication chap ms-chap -
визначаємо вид аутентифікації для PPPoE клієнтів;
Internet_Router(config-if)#exit
Internet_Router(config)#bba-group pppoe global - вмикаємо
підтримку PPPoE на роутері;
*Mar 1 00:24:45.303: %LINK-3-UPDOWN: Interface Virtual-
Access2, changed state to up
*Mar 1 00:24:46.303: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access2, changed state to up
Internet_Router(config-bba-group)#virtual-template 1 -
прив'язуємо до цієї групи раніше створений шаблон;
Internet_Router(config-bba-group)#sessions max limit 100 -
обмежуємо кількість сесій;
Internet_Router(config-bba-group)#sessions per-mac limit 1 -
одна mac-адреса на сесію;
Internet_Router(config-bba-group)#sessions auto cleanup -
вмикаємо автоматичне очищення сесій;
Internet_Router(config-bba-group)#exit
Internet_Router(config)#int fa 1/0
Internet_Router(config-if)#pppoe enable group global -
```

```

вмикаємо PPPoE на потрібному інтерфейсі;
Internet_Router(config-if)#no shutdown
Internet_Router(config-if)#exit
Internet_Router(config)#aaa new-model - вмикаємо функцію aaa на роутері;
Internet_Router(config)#aaa authentication ppp default local
- вказуємо, що процес аутентифікації PPPoE клієнтів буде використовувати локальну базу користувачів;
Internet_Router(config)#aaa authorization network default local - процес авторизації PPPoE клієнтів також буде використовувати локальну базу;
Internet_Router(config)#aaa attribute list PPPOE - створюємо перелік атрибутів (далі прив'яжемо його до конкретного клієнта, щоб отримувати конкретну IP-адресу);
Internet_Router(config-attr-list)#attribute type addr 2.2.2.100 service ppp protocol ip - прописуємо конкретний IP-адрес, який нам потрібен;
Internet_Router(config-attr-list)#exit
Internet_Router(config)#username PPPOE_User privilege 0 password cisco - створюємо PPPoE користувача;
Internet_Router(config)#username PPPOE_User aaa attribute list PPPOE - прив'язуємо до нього перелік атрибутів (тепер цей клієнт отримає конкретну IP-адресу, вказану в атрибутах);
Internet_Router(config)#exit
Internet_Router#wr

```

З Internet_Router закінчили, налаштували видачу конкретної IP-адреси конкретному клієнту. Тепер переходимо до Center_Router.

```

R3#conf t
R3(config)#hostname Center_Router
Center_Router(config)#int fa 1/0
Center_Router(config-if)#ip address 192.168.1.1 255.255.255.0
Center_Router(config-if)#ip nat inside
Center_Router(config-if)#no cdp enable
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#int fa 2/0
Center_Router(config-if)#ip address 10.10.10.1 255.255.255.0
Center_Router(config-if)#no cdp enable
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#interface dialer 1 - створюємо спеціальний інтерфейс Dialer, який і підніме PPPoE;
Center_Router(config-if)#ip address negotiated - вказуємо, що IP-адреса буде прийматися від провайдера;
Center_Router(config-if)#ip mtu 1492 -вказуємо mtu для PPPoE;
Center_Router(config-if)#ip nat outside - цей інтерфейс буде

```

```

outside і через нього користувачі будуть виходити в інтернет;
Center_Router(config-if)#encapsulation ppp - інкапсуляція;
Center_Router(config-if)#dialer pool 1 - задаємо № пулу для
прив'язки на фізичному інтерфейсі;
Center_Router(config-if)#ppp chap hostname PPPOE_User -
вказуємо ім'я користувача на Internet_Router (дає провайдер);
Center_Router(config-if)#ppp chap password cisco - вказуємо
пароль користувача;
Center_Router(config-if)#exit
Center_Router(config)#int fa 0/0
Center_Router(config-if)#pppoe-client dial-pool-number 1 -
прив'язуємо фізичний і Dialer через раніш заданий пул;
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#
*Mar 1 00:07:45.407: %DIALER-6-BIND: Interface Vi1 bound to
profile Di1
*Mar 1 00:07:45.463: %LINK-3-UPDOWN: Interface Virtual-
Access1, changed state to up
*Mar 1 00:07:46.591: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access1, changed state to up - це означає,
що інтерфейс піднявся;
Center_Router(config)#ip access-list extended FOR_NAT -
створюємо список доступу для NAT;
Center_Router(config-ext-nacl)#permit ip 192.168.1.0
0.0.0.255 any
Center_Router(config-ext-nacl)#deny ip any any
Center_Router(config-ext-nacl)#exit
Center_Router(config)#ip nat inside source list FOR_NAT
interface dialer 1 overload - включаєм NAT на роутері;
Center_Router(config)#ip route 0.0.0.0 0.0.0.0 dialer 1 -
прописуємо маршрут за замовчуванням через інтерфейс Dialer 1;
Center_Router(config)#exit
Center_Router#wr

```

2 СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ

Курсовий проект рекомендується виконувати в середовищі моделювання Cisco Packet Tracer або GNS3. Після того, як мережа спроектована, приступайте до конфігурування обраних пристроїв за допомогою термінального доступу або командного рядка. Відмінною особливістю симулятору є наявність у ньому "Режиму моделювання" (рис. 2.1). У даному режимі всі пакети, які пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє наочно

продемонструвати, з якого інтерфейсу в даний момент передається пакет, який протокол використовується, тощо.

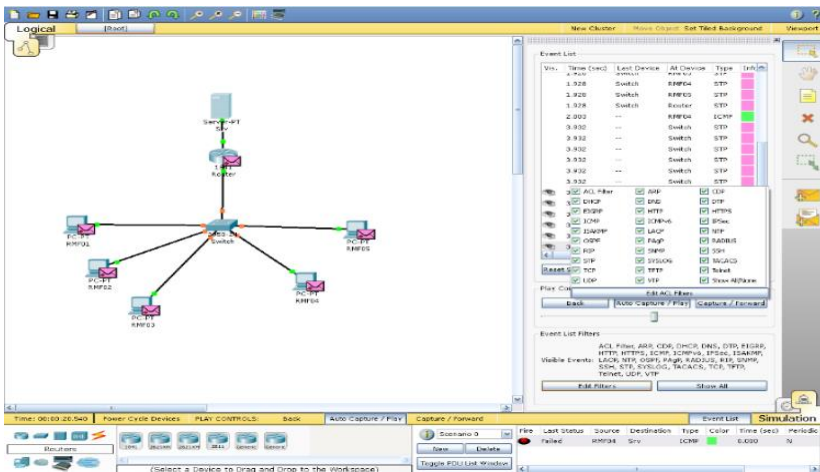


Рисунок 2.1 – Режим "Моделювання" в Cisco Packet Tracer

У "Режимі моделювання" можна не тільки відслідковувати протоколи, що використовуються, а й бачити, на якому з семи рівнів моделі OSI даний протокол працює. Packet Tracer здатний моделювати велику кількість пристроїв різного призначення. Протоколи, які можна відстежувати: ARP; CDP; DHCP; EIGRP; ICMP; TCP; UDP.

2.1 Приклад створення структури КМ в Packet Tracer

Для ПК в області моделей (лівого нижнього кута) вибрати *End Devices* → *PC-PT* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі комп'ютера. На вкладці *Config* вибрати пункт *FastEthernet*. В меню *IP Configuration* вибрати *Static* та задати статичну IP-адресу 10.0.32.1 з маскою підмережі 255.255.255.0. В пункті *Settings* в графі *Display Name* задати доменне ім'я *PC1*. В меню *Gateway/DNS* вибрати *Static* та задати IP-адресу шлюза (інтерфейс за допомогою якого комп'ютер зможе зв'язуватися з комп'ютерами з інших мереж) 10.0.32.50, IP-адресу DNS-сервера 10.0.32.100.

Для сервера з області моделей вибрати *End Devices* → *Server-PT* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі сервера. На вкладці *Config* вибрати пункт *Fast Ethernet*. В меню *IP Configuration* задати IP-адресу 10.0.32.100 з маскою підмережі 255.255.255.0. В пункті *Settings* в графі *Display Name* задати доменне ім'я *Server1*, шлюз – 10.0.32.50. В пункті *HTTP* вимкнути підтримку сервером *HTTP* та *HTTPS*. В пункті *DHCP* вимкнути підтримку цієї служби. В пункті *TFPT* вимкнути підтримку цієї служби.

Для комутатора в області моделей вибрати *Switches* → *Switch-PT-Empty* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі комутатора. На вкладці *Physical* вимкнути пристрій за допомогою візуального перемикача. Вибрати пункт *PT-SWITCH-NM-1CFE* та перенести його у "пустий" порт моделі п'ять разів (три комп'ютери, сервер, маршрутизатор), увімкнути комутатор.

Для маршрутизатора з області моделей вибрати *Routers* → *Router-PT-Empty* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі маршрутизатора. На вкладці *Physical* вимкнути пристрій за допомогою візуального перемикача. Вибрати пункт *PT-ROUTER-NM-1CFE* та перенести його у "пустий" порт два рази (кожний інтерфейс для кожної мережі), увімкнути пристрій. На вкладці *Config*, вибрати пункт *FastEthernet8/0*. Ввести IP-адресу 10.0.32.50 з маскою підмережі 255.255.255.0, увімкнути порт за допомогою прапорця у відповідному полі. Вибрати пункт *FastEthernet9/0*. Ввести IP-адресу 10.0.2.1 з маскою підмережі 255.255.255.0, увімкнути порт.

Для налаштування зв'язків вибрати *Server1* на вкладці *Config* в меню *DNS* задати *Name* – *my.com*, *Address* – 10.0.2.2 та натиснути кнопку "Add". В таблицю DNS буде доданий запис відповідності доменного імені реальної IP-адресі. З області моделей вибрати *Connections* → *Copper Straight-Trough* та з'єднати комп'ютери з комутатором, *Server1* з комутатором, комутатор з восьмим портом маршрутизатора. З області моделей вибрати *Connections* → *Copper Cross-Over* та з'єднати сервер *my.com* з дев'ятим портом маршрутизатора. Протестуйте роботу мережі командою *ping*.

2.2 Моделювання потоків трафіку в Packet Tracer

Наведемо стандартну мережу в середовищі моделювання (рис.2.2). Використаємо комутаційне та кінцеве обладнання.

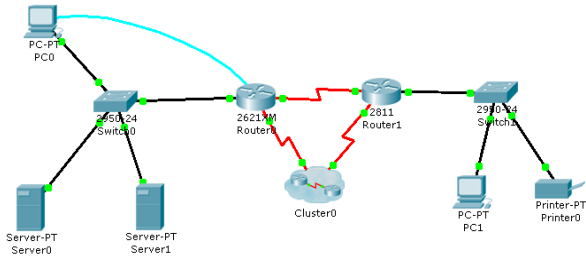


Рисунок 2.2 – Топологія мережі

Примітка. Це обладнання повинно відповідати вашому варіанту (мати стандарти і порти, які потрібні для виконання умов підключення ваших кінцевих вузлів, сегментів та мереж).

Для створення мережі заданої топології треба перенести на робочу область моделі наступних компонентів: server-PT (2 шт); PC-PT (2 шт); printer-PT (1 шт); switch 2950-24 (2 шт); router 2621XM (1 шт); router 1841 (1 шт); router 2811 (1 шт); cluster (1 шт).

Для маршрутизатора 2621XM виконати наступні дії: вимкнути маршрутизатор (рис. 2.3); додати до маршрутизатора модуль NM-8A/S (рис. 2.4); увімкнути маршрутизатор 2621XM.

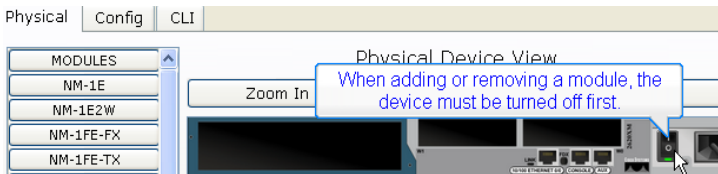


Рисунок 2.3 – Вимкнення маршрутизатора



Рисунок 2.4 – Додавання модулів до маршрутизатора

Для маршрутизаторів 2811 та 1841 виконати наступні дії: вимкнути маршрутизатори 2811 та 1841; додати до маршрутизаторів модуль послідовних інтерфейсів WIC-2T; ввімкнути маршрутизатор.

Для створення зв'язків виконайте наступне:

- з'єднайте 2 сервери *Server-PT*, 1 ПК *PC-PT* (*PC0*) та маршрутизатор 2621XM з комутатором *Switch* 2950-24 (0). Для з'єднання використовувати пряму виту пару та порти *Fast Ethernet*. Результат повинен мати вигляд, як на рисунку 2.5;

- підключить до комутатора *Switch* 2950-24 (1) один ПК *PC-PT* (*PC0*) та принтер *Printer-PT*. Для з'єднання використовувати пряму виту пару та порти *Fast Ethernet*. Результат повинен мати вигляд як на рисунку 2.6 (або може бути інакше, якщо у вас інше обладнання, стандарт та умови підключення);

—

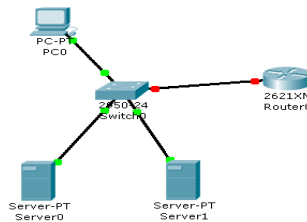


Рисунок 2.5 – Схема з'єднання вузлів

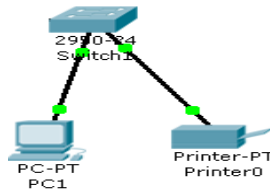


Рисунок 2.6 – Схема з'єднання обладнання

- підключить *Switch* 2950-24 (1) до маршрутизатора 2811 (за допомогою прямої вити пари);

- з'єднайте послідовні інтерфейси маршрутизаторів 2621XM та 2811.

Для додавання кластера треба: виділити маршрутизатор 1841; натиснути на кнопку "New Cluster", яка розташована над робочою областю; з'єднати кластеризований маршрутизатор 1841 з маршрутизаторами 2621XM та 2811 за допомогою послідовних портів, використовуючи тип з'єднання *Serial DCE*. Отриманий фрагмент мережі повинен виглядати, як на рисунку 2.7.

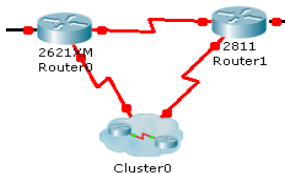


Рисунок 2.7 – Схема з'єднання кластера з маршрутизаторами

Етапи конфігурування мережі включають конфігурування портів маршрутизатора 2621XM: на порту Fast Ethernet 0/0 задати IP та MASK (192.168.4.1 / 255.255.255.0); на порту Serial 1/0 задати IP та MASK (192.168.5.1 / 24); на порту Serial 1/1 задати IP та MASK (192.168.6.1 / 24); при цьому задіяні порти мають бути увімкнені.

Таблицю маршрутизації задайте, використовуючи налаштування з лабораторних робіт, або як на рисунку 2.8.

Network	
	Add
Network Address	
192.168.4.0	
192.168.5.0	
192.168.6.0	

Рисунок 2.8 – Таблиця маршрутизації 2621XM

Етапи конфігурування мережі включають конфігурування портів маршрутизатора 2811: на порту Fast Ethernet 0/0 задати IP та MASK (192.168.9.1 / 24); на порту Serial 1/0 задати IP та MASK (192.168.5.2 / 24); на порту Serial 1/1 задати IP та MASK (192.168.7.1 / 24); задіяні порти мають бути увімкнені.

Таблицю маршрутизації задайте, як на рисунку 2.9.

Network	Add
Network Address	
192.168.5.0	
192.168.7.0	
192.168.9.0	

Рисунок 2.9 – Таблиця маршрутизації 2811

Інші налаштування:

- конфігурування портів кластеризованого маршрутизатора 1841: на порту Serial 1/0 задати IP та MASK (192.168.6.2/24); на порту Serial 1/1 задати IP та MASK (192.168.7.2/24); задіяні порти мають бути ввімкнені;
- з'єднати порт RS-232 вузла PC-PT (PC0) з консоллю маршрутизатора 2621XM; конфігурувати вузол PC-PT (PC0): gateway – 192.168.4.1; IP – 192.168.4.2; mask – 255.255.255.0;
- конфігурувати Server PT (0): gateway – 192.168.4.1; IP – 192.168.4.3; mask – 255.255.255.0;
- конфігурувати Server PT (1): gateway – 192.168.4.1; IP – 192.168.4.4; mask – 255.255.255.0;
- конфігурувати вузол PC-PT (PC1): gateway – 192.168.9.1; IP – 192.168.9.2; mask – 255.255.255.0;
- конфігурувати мережний принтер Printer-PT: gateway – 192.168.9.1; IP – 192.168.9.3; mask – 255.255.255.0;

Результатом є мережа, відповідної конфігурації (рис. 2.2).

2.3 Моделювання потоків трафіку в КМ

Виконаємо моделювання потоків трафіку в отриманій мережі. Для цього вам потрібно скористатися наступною схемою та порядком виконання нижче наведених кроків:

- виконати трасування маршруту від вузла PC-PT (PC0) до вузла PC-PT (PC1): на PC-PT (PC0) виконати tracert 192.168.9.2; натиснути кнопку Simulation; обрати пакет (Add simple PDU); в якості вузла, що відправляє пакети, обрати PC-PT (PC0); пунктом призначення обрати PC-PT (PC1); запустити моделювання (Auto Capture / Play); виконати покрокове моделювання (Capture Forward);
- послідовність моделювання описується в списку Event List;

- інформація про передані пакети (їх вміст та призначення) описується у стовпці Info списку Event List;
- для точної настройки протоколів, за допомогою яких відправляються пакети додати комплексний пакет (Add complex PDU);
- вибрати адресу призначення, протокол, порт (рис. 2.10);
- після моделювання обрати необхідний пакет в списку Event List, його буде відображено на схемі. Клацнути на ньому лівою кнопкою миші для перегляду вмісту (як показано на рисунку 2.11).

При виконанні моделювання потоків трафіку у ваших власних мережах, згідно варіанту, ви повинні кратко описати отримані результати та відмінності у отриманих звітах. Вказати, які показники (адреси змінились), а які залишились не змінними.

Create Complex PDU

Source Settings
 Source Device: RMF04
 Outgoing Port: FastEthernet ☒ Auto Select Port

PDU Settings
 Select Application: HTTP
 Destination IP Address:
 Source IP Address:
 TTL: 32
 TOS: 0
 Source Port:
 Destination Port: 80
 Size: 0

Simulation Settings
☐ One Shot Time: Seconds
☒ Periodic Interval: 120 Seconds

Рисунок 2.10 – Меню створення комплексного пакету

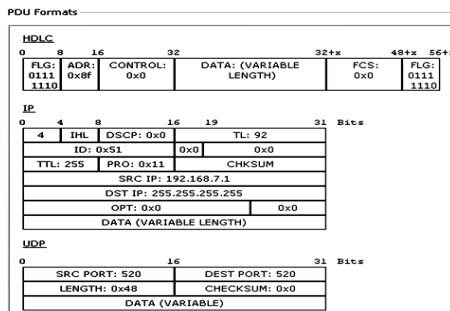


Рисунок 2.11 – Приклад вмісту PDU

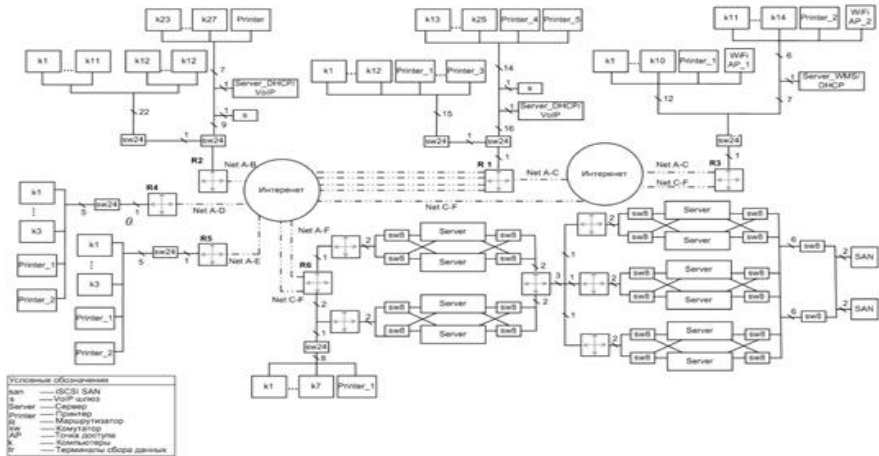


Рисунок 2.12 – Приклад структурної схеми

2.4 Вимоги до оформлення пояснювальної записки

Пояснювальна записка оформлюється відповідно до стандартів на оформлення програмної, текстової та графічної документації: ДСТУ 3008-95 «Документація. Звіти в сфері науки та техніки». Номер сторінки арабськими цифрами у верхньому куті сторінки. Звіт друкують без рамок, шрифтом Times New Roman чорного кольору прямого накреслення через півтора міжрядкові інтервали кеглем 14. Поля: відступ зліва 2,5 см.; справа 1,5 см.; зверху та знизу по 2 см. Колонтитули до верхнього 1 см., до нижнього 0 см. Абзац 1,25 см. Графічні документи курсового проекту пропонується виконувати на папері форматом A4 або A3. Рекомендована кількість графічних документів – 2-3 листа. Графічна частина курсового проекту обов'язково повинна містити в собі одне креслення. Схеми є такі: структурна схема Е1 (додаток А) визначає основні функціональні частини виробів, їх значення та взаємозв'язки; функціональна схема Е2 (служить для роз'яснення процесів, які протікають в окремих функціональних колах виробу або у виробі в цілому); схема з'єднань (монтажна) Е4 (показує з'єднання складових частин виробів та визначає кабелі за допомогою яких виконуються ці з'єднання); схема підключення Е5 (показує зовнішні підключення).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
3. Киричек Г.Г. Конспект лекцій з дисципліни Комп'ютерні мережі. 2024. 58 с.
4. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
5. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.
6. Tulloch M., Team WS Introducing Windows Server 2012 R2. - Microsoft press, 2013.
7. Krause J. Mastering Windows Server 2016. - Packt Publishing Ltd, 2016.
8. ІТ Блог Тараса Кучинського. Знайомство з програмою "Cisco packet tracer". URL: <https://kychinskiy.blogspot.com/2017/12/cisco-packet-tracer.html>.
9. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 1. 2024. 30 с.
10. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 2. 2024. 30 с.
11. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 3. 2024. 30 с.
12. Киричек Г. Г. Лабораторні роботи із застосування мережевих сервісів та протоколів. 2024.
13. Киричек Г. Г. Сервіси та служби Windows Server. 2024.