

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни
"Проектування комп'ютерних мереж"
для бакалаврів спеціальності 123 "Комп'ютерна інженерія",
усіх форм навчання

Методичні вказівки до виконання курсового проекту з дисципліни "Проектування комп'ютерних мереж" для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання / Укл. Г.Г. Киричек. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 38 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 21.08.2020

Затверджено
на засіданні НМК КНТ
Протокол № 1 від 28.08.2020

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	9
1.5 Структура проекту.....	10
1.6 Завдання	11
1.7 Аналіз інформаційного трафіку	14
1.8 Планування структури об'єднаної мережі.....	15
1.9 Віддалений доступ до мережі підприємства	16
1.10 Забезпечення мережної безпеки	18
1.11 Налаштування доступу в Інтернет через cisco vpn client.....	21
2 Середовище моделювання	26
2.1 Приклад створення структури КМ в Packet Tracer	27
2.2 Моделювання потоків трафіку в Packet Tracer	28
2.3 Моделювання потоків трафіку в КМ	32
3 Загальні вимоги до оформлення курсового проекту	34
3.1 Вимоги до оформлення пояснювальної записки.....	34
3.2 Вимоги до оформлення графічних документів	35
3.3 Вимоги до виконання схем	36
Рекомендована література	37
Додаток А.....	38

1 ЗАГАЛЬНІ ВІДОМОСТІ

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

Завдання до курсового проекту передбачають розробку функціональної та структурної схеми КМ, згідно варіанту, налаштування конфігураційних параметрів мережних інтерфейсів; налагодження серверів; монтаж мережі, з'єднання окремих частин мережі за допомогою маршрутизаторів; моделювання потоків трафіку в мережі; розробку об'єднаної (корпоративної) мережі підприємства згідно з варіантом (загальна кількість кінцевих вузлів не менше 300, віддалених локальних мереж не менше 4); налаштування віддаленого доступу до мережі Internet з забезпеченням мережної безпеки.

На всіх етапах проектування необхідно проводити оцінку альтернативних варіантів побудови об'єднаної мережі та її окремих частин.

Примітка. Варіанти розподіляються між студентами згідно двом останнім цифрам залікової книжки з кратністю 25. Для прикладу, якщо дві останні цифри 03- варіант № 3, а якщо 87- варіант № 12 (87-25-25-25=12).

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 (структури підприємства, розрахунок об'єму загального трафіку та швидкості каналів зв'язку)	до 20.09
2	Розробка функціональної схеми об'єднаної мережі	21.09 – 30.09
3	Розробка структурних схем віддалених об'єктів та мережі підприємства в цілому	01.10 – 8.10
4	Опис технологій та їх стандартів для LAN і WAN мереж	09.10 – 20.10
5	Аналіз, порівняння та вибір мережного, серверного і клієнтського обладнання	21.10 – 30.10
6	Монтаж мережі	31.10 – 20.11
7	Налаштування обладнання LAN та WAN мереж підприємства	21.11 – 30.11
8	Встановлення IP-адрес мережних інтерфейсів	01.12 – 15.12
9	Організація віддаленого доступу до мережі, отримання пулу відкритих адрес	16.12 – 31.12
10	Вибір та налаштування протоколів маршрутизації об'єднаної мережі підприємства	01.01 – 31.01
12	Налаштування маршрутизаторів, згідно політики безпеки об'єднаної мережі підприємства підключення до Інтернет	01.02 – 15.02
13	Забезпечення мережевої безпеки	16.02 – 28.02
14	Оформлення графічного матеріалу (моделі, структурна схема, монтажні схеми)	01.03 – 08.03
15	Оформлення ПЗ	09.03 – 15.03
16	Захист КП	до 20.03

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 підключаємих

об'єктів (мереж), кількості та видів обладнання, фізичне середовище каналів зв'язку, мережні (LAN та WAN) технології; перелік загальних питань (4 пункт), які розглядаються (перелік основних розділів змісту) та перелік графічного (5 пункт) матеріалу (моделі, функціональна та структурні схеми, монтажні схеми, алгоритми роботи).

Календарний графік виконання курсового проекту, який складається студентом (за прикладом календарного плану) і затверджується керівником проекту, повинен відповідати етапам розробки, 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 виконаної роботи на комп'ютері в середовищі моделювання КМ (якщо це не зроблено раніше на лабораторних роботах), навести функціональну, структурні та монтажні 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 доповідача. На питання необхідно давати стислі прямі відповіді, при необхідності використовуючи середовище моделювання КМ 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 друкують без рамок, **шрифтом Times New Roman** чорного кольору прямого накреслення через **півтора міжрядкові інтервали кеглем 14**.

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 можна робити посилання на відповідну літературу. Основний зміст записки – це аналіз, порівняння, вибір та обґрунтування прийнятих рішень та проект об'єднаної мережі, згідно затвердженої назви. Треба мати на увазі, що записку складають тоді, коли розробку проекту 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 проєктант вказує мету, об'єкт та предмет проектування; технології, вид обладнання, протоколи та стандарти, які використані у розробленому проєкті. Наводить ключові слова та об'єм пояснювальної записки. Реферат рекомендовано оформити на заключному етапі (1 сторінка).

У вступі до проєкту магістр повинен обґрунтувати актуальність проектування об'єднаної (корпоративної) мережі за варіантом, навести методи та шляхи проведення досліджень, зазначити в яких розділах пояснювальної записки наведено аналіз структури організації, схема інформаційних потоків (трафіку), аналіз, порівняння та вибір технологій (локальних мереж та підключення віддалених мереж), комунікаційного обладнання. Вступ має бути коротким (1-2 сторінки) і чітким. Його не слід перевантажувати загальними фразами. Головне, щоб було зрозуміло, чому присвячені етапи проектування.

У першому розділі (4-7 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 об'єднаної мережі. Студент повинен чітко визначити коло задач, які необхідно

вирішити в курсовому проекті, а також сформулювати технічне завдання згідно діючих стандартів та оформити його окремим підрозділом.

У другому розділі (8-12 сторінок) на підставі проведеного аналізу розробляється модель (функціональна схема) та структурна схема об'єднаної мережі підприємства, виконується опис LAN\WAN-технологій окремих сегментів об'єднаної мережі. Кількість підключених робочих станцій не повинна бути меншою за 300 одиниць.

Третій розділ (8-12 сторінок) повинен містити опис апаратної та кабельної частини проекту з урахуванням попереднього вибору та можливості з'єднання через маршрутизатори окремих ЛОМ підприємства, з метою здійснення віддаленого доступу. Цей розділ містить вибір конкретних елементів реалізації функціональної та принципових електричних схем, розрахунків окремих елементів, вузлів та підсистем. Виконується налаштування загальних об'єктів.

У четвертому розділі (8-10 сторінок) розглядається підключення розробленої мережі підприємства до Internet та питання забезпечення мережевої безпеки, як у дротових так і в бездротових ЛОМ. Проектантом розкриваються питання забезпечення якості та надійності розробленої мережі, питання апаратного та програмного захисту інформації, а також захист від несанкціонованого доступу. Розглядається призначення IP-адрес та подання мережі головного офісу організації (підприємства) в Інтернеті.

У висновках (1-2 сторінки) проектанти формують основні результати, що 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), у відповідності до ГОСТ 19.701-90 (Схемы алгоритмов, программ, данных и систем). Бібліографічні описи в переліку посилань наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ ГОСТ 7.1:2006 "Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання".

До записки додаються два креслення формату А4 або А3 (структурна та монтажна схеми) та 1 плакат (алгоритм роботи мережі) того ж формату. Креслення і плакати повинні відображати проходження кабелю на всіх ділянках мережі з роз'ясненням особливостей його прокладки.

Загальний обсяг ПЗ – 35 - 40 сторінок (не рекомендовано обсяг більший за 40 стор.), причому технічна її частина, має містити не менш ніж 25 сторінок тексту з рисунками.

1.4 Теми проектів

Далі наведено теми проектів за варіантами (див. сторінку 4).

1. Розподілена комп'ютерна мережа комунального підприємства «Водоканал» м. Запоріжжя.
2. Корпоративна комп'ютерна мережа поштових відділень.
3. Розподілена комп'ютерна мережа підтримки проведення соціологічних досліджень.
4. Об'єднана комп'ютерна мережа пенсійного фонду запорізького регіону.
5. Об'єднуюча магістраль енергетичного комплексу ВАТ «УкрЕнерго».
6. Корпоративна комп'ютерна мережа торговельного підприємства.
7. Розподілена комп'ютерна мережа податкової служби області.
8. Об'єднана комп'ютерна мережа податкової служби області.
9. Корпоративна комп'ютерна мережа регіональних лікарень України.
10. Розподілена мережа забезпечення роботи банкоматів міста.
11. Корпоративна комп'ютерна мережа Укрзалізниці.
12. Об'єднана комп'ютерна мережа «Дніпровська електроенергетична система» України.
13. Розподілена комп'ютерна мережа державного підприємства «Екологія України».
14. Розподілена комп'ютерна мережа «Радіоком» міст азовського побережжя.
15. Кампусна комп'ютерна мережа мешканців мікрорайонів м.Запоріжжя.
16. Розподілена комп'ютерна мережа головних офісів банку.
17. Оптиволоконна мережа ВАТ «Дніпроспецсталь» з п'ятью філіалами.

18. Корпоративна мережа агропромислового комплексу «Україна» (4 об'єкти у різних географічних частинах України).

19. Розподілена комп'ютерна мережа концерну «Теплові мережі України».

20. Об'єднана мережа підприємства «Центромоблі».

21. Корпоративна мережа Запорізької філії ВАТ «Укртелеком».

22. Розподілена комп'ютерна мережа НУ«Запорізька політехніка» та його коледжів.

23. Корпоративна мережа металургійного підприємства.

24. Мережа ВАТ «Мотор-Січ» з віддаленими філіями.

25. Розподілена комп'ютерна супермаркетів «Сільпо» м.Запоріжжя.

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.

Монтаж та 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);

- програмна настройка 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 мережевої безпеки (налаштування обладнання, протоколів).

Висновки.

Кількість і назви розділів у проекті можуть відрізнятися 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 (об'єднаної, корпоративної) 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 (див.п.2). 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);

– 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	70	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
2	75	5	3	10BaseT, 100BaseTX	Hub, Switch	Вита пара	Статична
3	80	7	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
4	71	4	3	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Динамічна
5	76	6	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
6	59	4	1	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Статична
7	68	5	2	10BaseT, 100BaseTX	Hub Switch	Вита пара	Динамічна
8	81	4	3	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
9	79	4	1	100BaseTX WiFi	Switch	Вита пара, безпроводне	Динамічна
10	74	4	3	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична

Продовження таблиці 1.2

11	90	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Статична
12	72	5	3	10BaseT, 100BaseTX	Hub Switch	Вита пара	Статична
13	84	7	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Динамічна
14	67	5	1	100BaseTX WiFi	Switch	Вита пара, безпроводне	Динамічна
15	78	4	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
16	58	4	2	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
17	77	5	3	10BaseT, 100BaseTX	Hub Switch	Вита пара	Динамічна
18	83	6	3	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Динамічна
19	69	5	1	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Динамічна
20	85	4	2	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична
21	82	4	3	100BaseFX, WiFi	Switch	Оптичний кабель безпроводне	Динамічна
22	88	5	3	10BaseT, 100BaseTX	Switch	Вита пара	Динамічна
23	73	4	2	1000BaseSX 100BaseTX	Switch	Оптичний кабель Вита пара	Статична
24	89	7	2	100BaseTX WiFi	Hub Switch	Вита пара, безпроводне	Динамічна
25	66	4	1	1000BaseSX WiFi	Switch	Оптичний кабель безпроводне	Статична

Таблиця 1.3 – Варіанти завдань на курсовий проект

Вар. №	IP (адреси для філій)	IP (між маршру- тизаторами (3-6 мереж))	Маршрути- зація	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	172.30.2.0/24	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	MPLS

Продовження таблиці 1.3

6	192.168.0.0/25	211.2.13.0/27	Динамічна	DNS, ACL	VoIP
7	10.56.8.0/24	199.56.8.0/27	Динамічна	VLAN, NTP	IPv6
8	172.16.16.0/23	200.1.16.0/27	Статична	DNS, ACL	FrameRelay
9	10.17.2.0/25	201.17.2.0/27	Динамічна	DNS, VLAN	VoIP
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	172.31.30.0/24	228.1.30.0/27	Статична	VLAN, DNS	ACL
14	10.9.33.0/24	195.9.33.0/27	Динамічна	DNS, ACL	VPN (IPSec)
15	192.168.4.0/23	205.6.64.0/27	Динамічна	VLAN, NTP	MPLS
16	10.20.1.0/25	211.20.1.0/27	Статична	DNS, ACL	VoIP
17	172.18.84.0/24	199.8.84.0/27	Динамічна	DNS, VLAN	IPv6
18	10.4.38.0/23	214.4.38.0/27	Динамічна	DNS, ACL	FrameRelay
19	192.168.9.0/25	201.1.98.0/27	Статична	VLAN, NTP	ACL
20	172.29.19.0/24	197.9.19.0/27	Динамічна	HTTP, ACL	VPN (GRE)
21	10.2.27.0/24	223.2.27.0/27	Статична	VLAN, DNS	ACL
22	172.21.48.0/24	196.1.48.0/27	Динамічна	DNS, ACL	IPv6
23	10.3.62.0/23	201.3.62.0/27	Динамічна	VLAN, NTP	VPN (IPSec)
24	172.27.20.0/25	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.

Приклад. Нехай через зовнішній сегмент комп'ютерної мережі необхідно копіювати базу даних. Середня швидкість передачі 1 біта = 0,5 мкс, MTU=274 В. Який максимальний розмір (точно) БД можливо передати за 2 хвилини? Яка при цьому буде технічна (Rt) та

інформаційна швидкості (R_i)? Маємо заголовки каналного рівня = 26В, заголовок IP, UDP, TCP дорівнюють відповідно 24, 8, 24 В. Для спрощення вважаємо, що 1GB=1000MB, 1MB=1000KB.

Вирішення. Переводимо час в секунди $T = 120\text{с}$.

Швидкість R_t в біт/с дорівнює $1\text{ біт/с} / 0,5\text{ мкс} = 2\text{ Мб/с}$.

Об'єм даних $V_t = T * R_t = 120\text{с} * 2\text{ Мб/с} = 240\text{ Мбіт} = 30\text{ Мбайт}$.

$MSS_{UDP} = 274 - 24 - 8 = 242\text{ байти}$. $MSS_{TCP} = 274 - 24 - 24 = 226\text{ байт}$.

Знаходимо обсяг переданих даних з урахуванням тільки інформаційної складової:

- за UDP – 30 МБ - 300Б (MTU+26 В – загол.канал.рівня);
X МБ - 242 Б (MSS_{UDP}); $V_{UDP} = 24,2\text{ МБ}$;
- за TCP – 30 МБ - 300Б (MTU+26В – загол.канал.рівня);
X МБ - 226 Б (MSS_{TCP}); $V_{TCP} = 22,6\text{ МБ}$;
- максимальний розмір БД - $V = 24,2\text{ МБ}$;
- затримка на 1 кадр $300 * 8 / 2\text{ Мб/с} = 0,0012\text{ с}$;
- $R_i = MSS_{UDP} / 0,0012 = 242 * 8 / 0,0012 = 1,61\text{ Мб/с}$;
- $R_i = MSS_{TCP} / 0,0012 = 226 * 8 / 0,0012 = 1,51\text{ Мб/с}$;
- кількість кадрів - $T / 0,0012 = 120 / 0,0012 = 100000\text{ кадрів}$.

Перевірка. $UDP = 24,2\text{ МБ} / 242\text{Б} = 100000\text{ кадрів}$. $TCP = 22,6\text{ МБ} / 226\text{Б} = 100000\text{ к} [4]$.

В ході вирішення поставленого завдання треба враховувати кількість клієнтів у сегменті мережі та об'єм трафіку для кожного з них.

1.8 Планування структури об'єднаної 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, який буде використаний для монтажу мережі і підтримки її надалі. На плані треба зазначити розміщення основних компонентів мережі: кабельних ліній, комутаторів, серверів, маршрутизаторів і інших комунікаційних

пристроїв, а також комп'ютерів і периферії. Знаючи, які протоколи каналного рівня обрані для мережі, можна приступати до планування розміщення мережних ресурсів, тому що від протоколу залежить максимальна довжина кабелю і число комутаторів у мережі. Вибір протоколу каналного рівня в основному зводиться до вибору типу фізичного середовища: витої пари, оптоволоконного кабелю і частоти для бездротових каналів. Кожний тип має свої переваги та недоліки, які потрібно врахувати при виборі середовища передачі. Швидкість передачі - важливий критерій вибору протоколу каналного рівня.

Розміщення серверів повинне бути зручним для тих, хто їх підтримує та обслуговує. У кожному разі захист серверів повинен бути надійним. Їх необхідно захищати не тільки від фізичного доступу, але також від стрибків напруги та перебоїв струму. Розміщення сервера повинне враховувати розташування робочих місць користувачів, характер трафіку і бути зручним для обслуговуючого персоналу. При проектуванні рекомендовано визначитись з розміщенням обладнання з застосуванням загальних стандартів СКС, з використанням апаратних та кросових, враховуючи організацію основних підсистем СКС.

1.9 Віддалений доступ до мережі підприємства

Організація віддаленого доступу - одна з проблем комп'ютерних мереж, яка отримала назву «проблеми останньої милі» - під останньою милею мається на увазі відстань від точки присутності (POP - Point of presence) оператора зв'язку до приміщень клієнтів.

Вибір постачальника послуг Інтернету (ISP) - важливий аспект планування стратегії доступу в Інтернет для великої та середньої мережі. Основна функція ISP - надання доступу в Інтернет. ISP підтримує власну мережу, з'єднану з Інтернетом, до якої абоненти підключаються за допомогою самих різних ГОМ- технологій. Різні ISP займають різні рівні володіння мережами. Одні підключені безпосередньо до магістралей Інтернету, а інші є лише посередниками. Одні ISP орієнтовані на домашніх користувачів, а інші - на корпоративних.

Клієнти різних типів відрізняються обладнанням і вимогами до параметрів доступу. Приміщення клієнтів можуть з'єднуватись з найближчою точкою доступу оператора зв'язку різними способами: за допомогою аналогової або цифрової телефонної мережі; провідного зв'язку; телевізійного кабелю; бездротового зв'язку.

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. VPN забезпечує конфіденційність за рахунок використання механізмів інкапсуляції та шифрування. Для забезпечення цілісності даних VPN, як правило, використовують хешування. Для автентифікації VPN може використовувати паролі, цифрові сертифікати, смарт-карти і біометрію для ідентифікації на кінці мережі. 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. Використовуються три класи протоколів тунелювання:

- протоколи передачі (Carrier protocol: FRelay, ATM, MPLS);
- протоколи інкапсуляції (Encapsulating protocol: GRE, IPSec, L2F, PPTP, L2TP);
- пасажир – інкапсульований протокол (passenger protocol: IPX, AppleTalk, IPv4, IPv6).

Тунелі - створюються на різних протоколах інкапсуляції:

- універсальна інкапсуляція маршрутизації (Generic Route Encapsulation, GRE);
- протокол безпеки IP (IPSec);
- протокол переадресації 2 рівня 2 (Layer 2 Forwarding, L2F);
- протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol, PPTP);

– протокол тунелювання 2 рівня (Layer 2 TP, L2TP).

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. Організації використовують site-to-site VPN мережі, щоб зв'язати розкидані підрозділи. Оскільки більшість організацій зараз мають доступ до Інтернет, є сенс скористатися перевагами site-to-site VPN. Загалом, site-to-site VPN є продовженням класичних WAN мереж, які підключають всі мережі одну з одною. Наприклад, вони можуть зв'язати мережі філії до мережі штаб-квартири компанії. В site-to-site VPN, хости відправляють та приймають TCP/IP-трафік через VPN шлюз, яким може бути маршрутизатор або Adaptive Security Appliance (ASA).

1.10 Забезпечення мережної безпеки

Інформаційна система перебуває в стані захищеності, якщо забезпечені її конфіденційність, доступність і цілісність. Безпека забезпечується технічними засобами - системами шифрування, автентифікації, авторизації, аудита, антивірусного захисту, мережевими екранами, а також юридичними, морально-етичними нормами та адміністративними мірами.

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. До популярних протоколів захищеного каналу відносять IPSec і SSL.

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. Протокол IPSec включає криптографічні методи, які задовольняють потреби керування ключами на мережевому рівні безпеки. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет. 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. AH забезпечує перевірку достовірності і цілісності даних для IP пакетів, переданих між двома системами. Даний алгоритм перевіряє відсутність змін під час передачі повідомлення та підтверджує, що дані належать визначеним відправнику та отримувачу. AH не забезпечує конфіденційність даних шляхом шифрування пакетів. При використанні лише AH протоколу забезпечується слабкий захист. Тому він використовується з протоколом ESP, щоб забезпечити шифрування даних і захист від підробок;

- Encapsulating Security Payload (ESP) - забезпечує цілісність та конфіденційність шляхом шифрування IP-пакетів. Шифрування IP-пакетів забезпечує приховування даних та відомостей про відправника та отримувача. Хоча шифрування та автентифікація є обов'язковими для ESP, як мінімум, одна з цих функцій має бути вибрана.

IPsec реалізований на основі існуючих алгоритмів шифрування, автентифікації та обміну ключами. Деякі з стандартних алгоритмів, що використовує IPsec: DES – шифрує та розшифровує пакети даних; 3DES – забезпечує кращу ефективність шифрування ніж 56-бітний DES; AES – забезпечує кращий рівень шифрування, в залежності від довжини ключа, і більшу пропускну здатність; MD5 – автентифікація пакетної передачі даних з використанням 128-бітного спільного секретного ключа; SHA-1 – автентифікує дані, використовуючи 160-бітний спільний секретний ключ; DH – дозволяє двом сторонам створити спільний секретний ключ, що використовується для шифрування та хеш-алгоритмів, наприклад, DES та MD5, при передачі даних по незахищеному каналі.

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. В групах Діффі-Хеллмана має бути вказаний тип криптографії: DH GROUP 1 – використовується 768-бітна криптографія; DH GROUP 2 – тільки для пристроїв Cisco IOS, PIX Firewall та пристрою адаптивного захисту Cisco (ASA), використовується 1024-бітне шифрування; DH GROUP 5 – підтримується при умові виконання вимог програмної системи, використовується 1536-бітне шифрування.

GRE (англ. *Generic Routing Encapsulation* - загальна інкапсуляція маршрутів) - протокол тунелювання мережових пакетів, розроблений компанією Cisco Systems. Його основне призначення - інкапсуляція пакетів мережового рівня моделі OSI в IP пакети. Сам по собі GRE не забезпечує ніякої безпеки переданих даних - це site-to-site VPN тунель у чистому вигляді. Використовується зазвичай такий тунель, коли є специфічні завдання, пов'язані з маршрутизацією і немає вимог до безпеки. Не варто забувати, що чистий GRE тунель - не навантажує обладнання, а навантаження при шифруванні великого обсягу даних досить істотне. Протокол GRE інкапсулюється безпосередньо в IP, минаючи TCP або UDP, в IP пакеті є спеціальне поле «Protocol type», в якому міститься число, що позначає протокол, інкапсульований в даний IP пакет, для GRE код protocol type дорівнює 47. У зв'язку з цим, якщо в мережі є GRE тунелі, то варто уважно ставитися до написання розширених списків контролю доступу (ACL), так як `permit tcp any any` і `permit udp any any` приведуть до заборони на GRE через те, що він інкапсулюється безпосередньо в пакет, тому треба писати або `permit ip any any` або `permit gre any any`.

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. Для вирішення

цієї проблеми рекомендується використовувати path-mtu-discovery (визначення TCP MSS, тобто максимального розміру IP-пакетів на всьому шляху) при передачі даних через GRE-тунель.

1.11 Налаштування доступу в Інтернет через cisco vpn client

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):

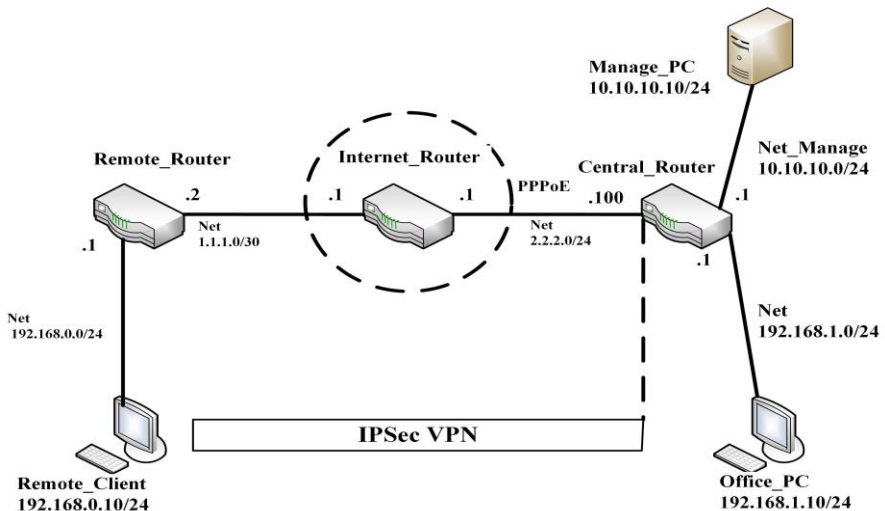


Рисунок 1.1 – Схема мережі

Пояснення до схеми. Є центральний офіс, де розташований Central_Router. Через даний пристрій співробітники отримують доступ в інтернет. На ньому є 3 інтерфейси:

- FEthernet 0/0 - підключений до інтернет. 2.2.2.100/24 - адресу він отримує від провайдера по протоколу PPPoE. Також інтерфейс використовується як outside при налаштуванні NAT, і на нього приходять запити від клієнтів на встановлення VPN тунелю;

- FEthernet 1/0 - підключений до локальної мережі з IP-адресом 192.168.1.1/24. Цей інтерфейс є inside для NAT. В даній мережі розташовані внутрішні ресурси і користувачі;

- 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). Будемо вважати що Internet_Router має публічні адреси на інтерфейсах 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

```

3 Internet_Router закінчили. Тут ми налаштували видачу конкретної IP-адреси конкретному клієнту. Можна зробити видачу IP-адрес PPPoE клієнтам більш розширено, налаштувавши або пул адрес, або DHCP.

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 V11 bound to
profile D11
*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 - включаем 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

```

Приклад повного налаштування мережі наведено у статті електронного ресурсу.

2 СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ

Курсовий проект рекомендується виконувати в середовищі моделювання Cisco Packet Tracer та GNS3.

Симулятор Cisco Packet Tracer розроблено для моделювання сучасних мереж різного призначення, емулятор GNS3 дозволяє навчитися виконанню налаштувань на реальному обладнанні.

В симуляторі Cisco Packet Tracer студенти можуть вивчати і використовувати такі мережні пристрої, як концентратори, комутатори другого і третього рівнів, сервери, маршрутизатори та робочі станції, визначати типи зв'язків між ними і з'єднувати їх.

Після того, як мережа спроектована, можна приступати до конфігурування обраних пристроїв за допомогою термінального доступу або командного рядка. Відмінною особливістю даного симулятору є наявність у ньому "Режиму моделювання" (рис. 2.1). У даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє наочно продемонструвати, з якого інтерфейсу в дані момент переміщається пакет, який протокол використовується і т.д.

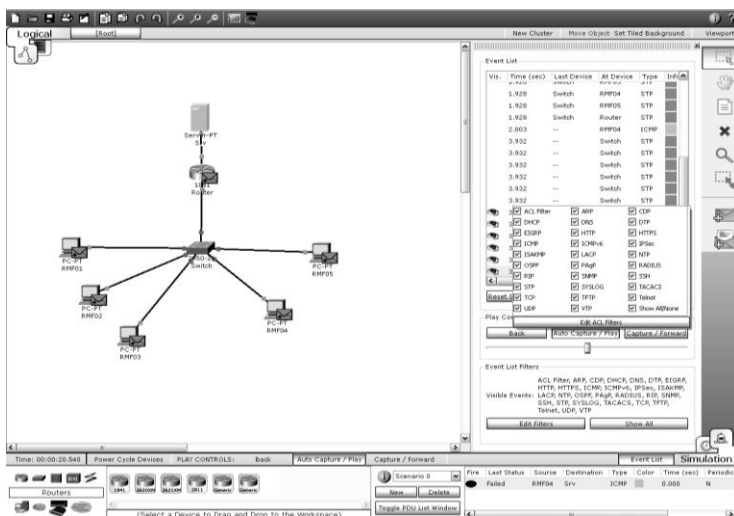


Рисунок 2.1 – Режим "Моделювання" в Cisco Packet Tracer

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, а також чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності. 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 *TFTP* 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

Розробимо у якості прикладу стандартну мережу в будь-якому середовищі моделювання (рис.2.2). Використаємо для цього нижче наведене комутаційне та кінцеве обладнання.

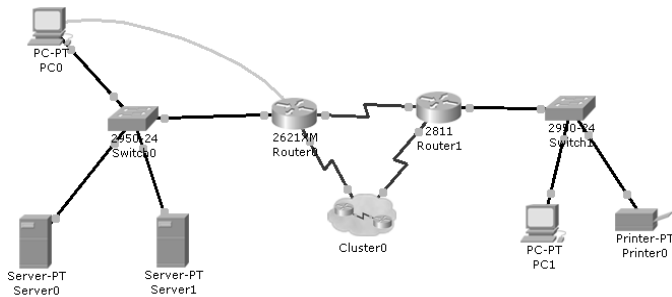


Рисунок 2.2 – Топологія мережі

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.

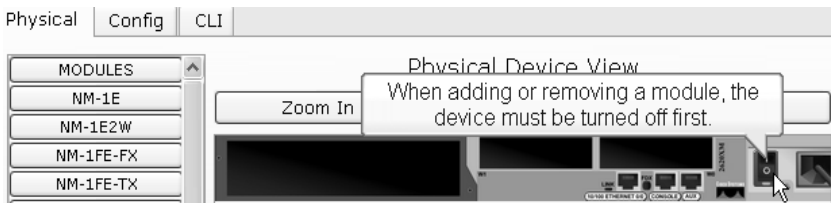


Рисунок 2.3 – Вимкнення маршрутизатора



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; увімкнути 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);

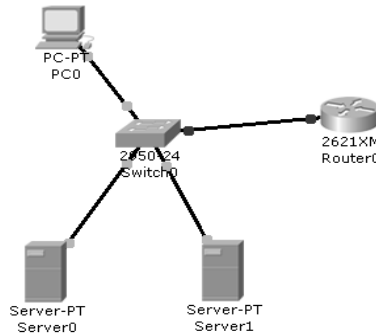


Рисунок 2.5 – Схема з'єднання вузлів

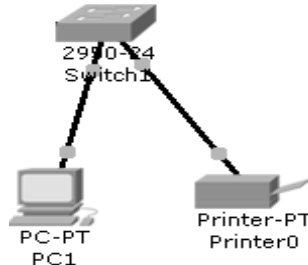


Рисунок 2.6 – Схема з'єднання обладнання

– підключить *Switch 2950-24 (1)* до маршрутизатора *2811* (за допомогою прямої витой 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.

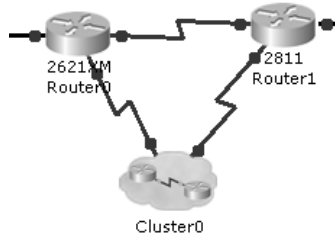


Рисунок 2.7 – Схема з'єднання кластера з маршрутизаторами

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 RIP-маршрутизації задайте, як на рисунку 2.8.

RIP Routing	
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 RIP-маршрутизації задайте, як на рисунку 2.9.

RIP Routing

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 вузлі PC-PT (PC0) виконати tracert 192.168.9.2; натиснути на кнопку Simulation панелі інструментів; обрати пакет

(Add simple PDU); в якості вузла, який буде відправляти пакети, обрати PC-PT (PC0); в якості пункту 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 пакету, протокол, номер порту (рис. 2.10);
- після моделювання обрати необхідний пакет в списку Event List, його буде відображено на структурній схемі КМ. Клацнути на ньому лівою кнопкою миші для перегляду його вмісту (наприклад, 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

Create PDU

Рисунок 2.10 – Меню створення комплексного пакету

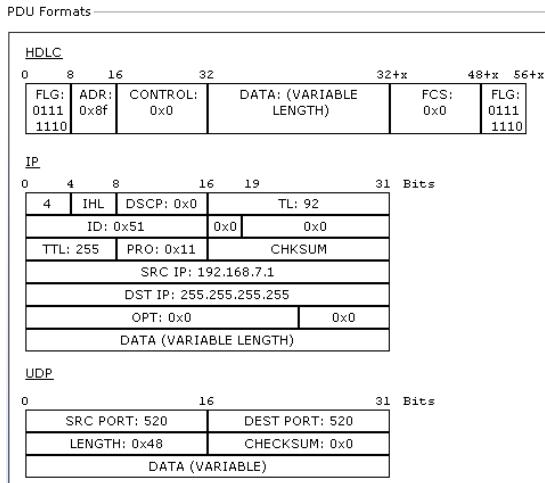


Рисунок 2.11 – Приклад вмісту PDU

3 ЗАГАЛЬНІ ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЕКТУ

3.1 Вимоги до оформлення пояснювальної записки

Пояснювальна записка курсового проекту оформлюється відповідно до діючих стандартів на оформлення програмної, текстової та графічної документації: ДСТУ 3008-95 «Документація. Звіти в сфері науки та техніки». Кожна сторінка тексту пояснювальної записки оформлюється в основній рамці (відступ зліва на 20 мм, з інших сторін на 5 мм) та з надписом (рис. 3.1), в якому визначається децимальний номер курсового проекту та номер листа (сторінки) пояснювальної записки, написаний арабськими цифрами.

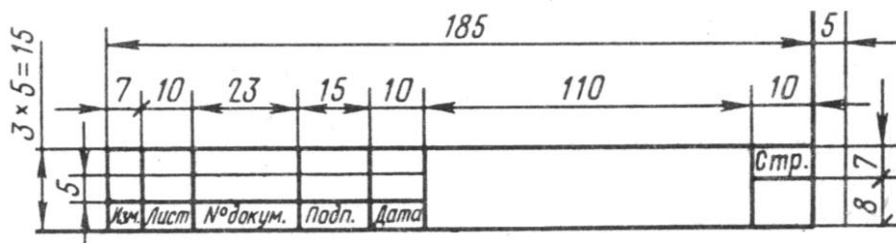


Рисунок 3.1 – Форма надпису в пояснювальній записці

Децимальний номер курсового проекту має структуру:

XX.XXXXXXXXXX.XXXXXX XX, де:

- 1 – шифр держави (для України – 13);
- 2 – шифр вищого навчального закладу (для ЗНТУ – 02070849);
- 3 – номер групи + номер теми проекту (номер варіанту);
- 4 – літерно-цифровий шифр документа.

Наприклад, для пояснювальної записки курсового проекту студента групи КНТ620 з номером варіанту – 12, децимальний номер – 13.02070849.62012 ПЗ.

Перша сторінка пояснювальної записки (титульний лист) не нумується.

3.2 Вимоги до оформлення графічних документів

Графічні документи курсового проекту пропонується виконувати на папері для креслення з нанесенням зовнішньої рамки зліва на 20 мм, з інших сторін на 5 мм. В правому нижньому куті виконують основний надпис. Графічні матеріали виконуються на папері формату А4 або А3 (210x290) та розміщуються в додатках. Кількість листів та вигляд графічних документів узгоджується студентом з керівником курсового проекту з урахуванням особливостей теми проекту. Рекомендована кількість графічних документів – 3-5 листів. Графічні документи складаються з плакатів, що мають ілюстраційний характер, та креслень, які виконуються згідно стандартів. Графічна

частина курсового проекту обов'язково повинна містити в собі два або одне креслення.

3.3 Вимоги до виконання схем

В графічній частині курсового проекту пропонується виконувати креслення або плакати на 3-5 листах формату А4 або А3. В склад графічної частини включають: модель мережі; структурні схеми мережі, яка проектується; специфікації компонентів мережі; алгоритми роботи мережі; схеми зв'язків; монтажні схеми розташування апаратних засобів. З урахуванням особливостей теми курсового проекту склад графічних документів може бути змінено.

Схеми в залежності від елементів й зв'язків між ними розділяються на такі види: 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); принципова (повна) схема Е3 (визначає повний склад елементів та зв'язків між ними та дає детальне уявлення про принципи роботи виробу); схема з'єднань (монтажна) Е4 (показує з'єднання складових частин виробів та визначає проводи, джгути, кабелі або трубопроводи, за допомогою яких виконуються ці з'єднання, а також місця їх з'єднань та виведення); схема підключення Е5 (показує зовнішні підключення виробів).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.
2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.
3. Шапорін Р.О. Моделі та методи проектування комунікаційних систем комп'ютерних мереж масштабу підприємства [Текст]: автореф. дис... канд. техн. наук: 05.13.12 / Р.О.Шапорін ; Одеський національний політехнічний ун-т. - О., 2007. - 22 с.
4. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
5. Бакланов И.Г. NGN: принципы построения и организации. – М. : Эко-Трендз, 2008. – 400 с.
6. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б.Гольдштейн, Б.С.Гольдштейн. – СПб.: БХВ, 2005. – 304 с.
7. Глотиков К. IMS (IP multimedia Subsystem). М.: Эко-трендз. 2009. – 100 с.
8. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А.Соколов, Г.Г.Яновский. – СПб. : БХВ, 2009. – 400 с.
9. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.
10. Платунова С.М. Методы проектирования фрагментов компьютерной сети – СПб: НИУ ИТМО, 2012. – 51 с.
11. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

Додаток А

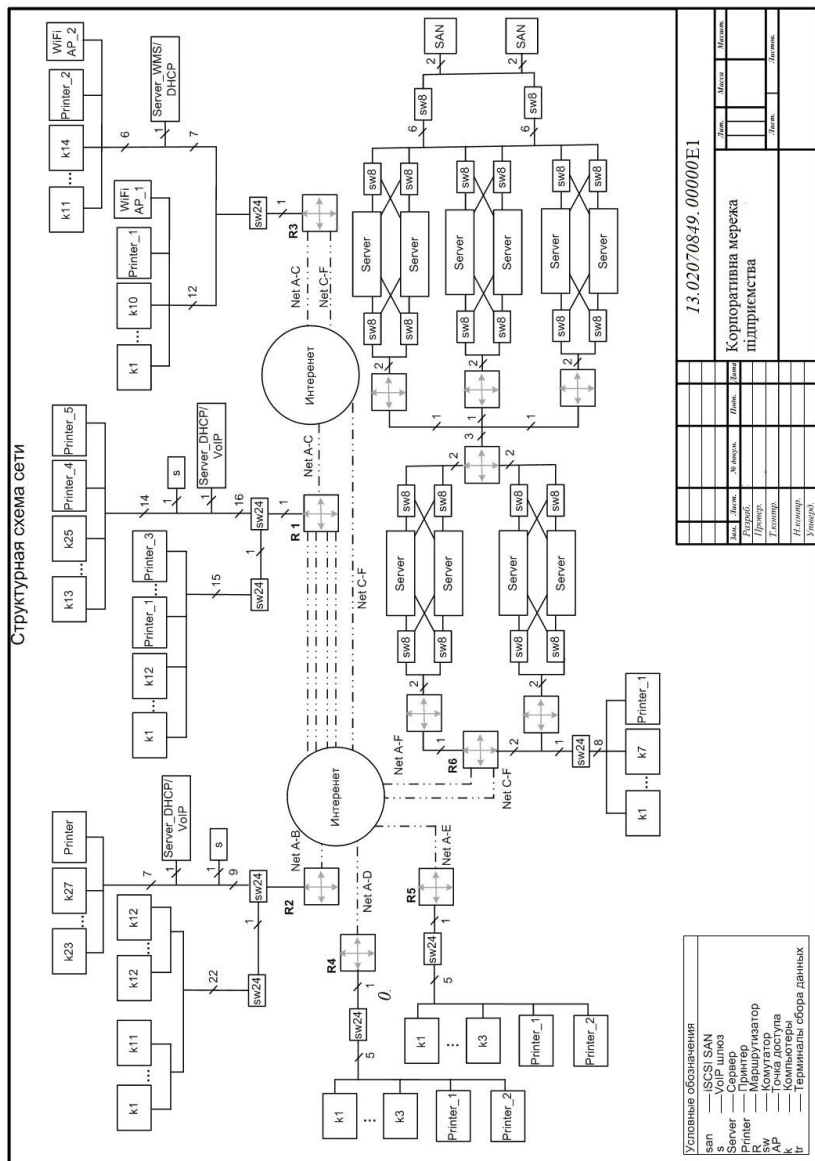


Рисунок А.1 – Структурна схема мережі