Міністерство освіти і науки України
Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра комп’ютерної інженерії

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту

з дисципліни

«Комп'ютерні мережі»

для студентів освітнього ступеню «бакалавр»
спеціальності 123 Комп’ютерна інженерія

Покровськ – 2020

УДК 004

Методичні вказівки до виконання курсового проекту за дисципліною «Комп'ютерні мережі» для студентів освітнього ступеню «бакалавр» спеціальності 123 Комп’ютерна інженерія / Укладачі С.О. Цололо, Ю.Л. Дікова. – Покровськ: ДонНТУ, 2020. – 96 с.

Метою курсового проекту є реалізація повного циклу проектування, розрахунку, вибору обладнання та моделювання локальної обчислювальної мережі підприємства.

Укладачі: _____ Цололо Сергій Олексійович, доц. каф. КІ, к.т.н., доц.
(підпис)

_____ Дікова Юлія Леонідівна, доц. каф. КІ
(підпис)

Рецензент: _____ Назарова Ірина Акопівна, доц. каф. ПМІ, к.т.н., доц.
(підпис)

Відповідальний
за випуск: _____ Святний Володимир Андрійович, зав. каф. КІ, д.т.н., проф.
(підпис)

Розглянуто на засіданні кафедри комп’ютерної інженерії
Протокол № 10 від 14 квітня 2020 р.

Затверджено навчально-методичним відділом ДонНТУ
Протокол № ___ від ___ _____ 20___ р.

ЗМІСТ

Вступ

Метою курсового проекту з дисципліни "Комп’ютерні мережі" є формування знань та навиків студентів щодо алгоритмів роботи вузлів мережі та мережі в цілому шляхом розробки проекту та моделі функціонування комп’ютерної мережі для вказаного підприємства. Модель повинна включати відображення топології мережі та її вузлів, обґрунтування вибору характеристик, розрахунок працездатності, з урахуванням враховуючи топології і стандартів фізичного середовища передачі даних а також характеристик інтелектуальних вузлів мережі як то концентратор, комутатор, шлюз і маршрутизатор.

В результаті виконання курсової роботи студенти повинні:

- вміти аналізувати потреб підприємства щодо вибору топології та логічної схеми мережі;
- виконувати розрахунок характеристик мережі та розподіляти мережеві адреси;
- планувати структуровану кабельну система підприємства, обирати тип кабелю для підсистем та активне обладнання;
- обирати мережеву операційну систему та стратегію адміністрування у мережі;
- налагоджувати мережеві екрани та антивірусне програмне забезпечення;
- організовувати зберігання даних та резервне копіювання;
- забезпечувати спільний доступ до елементів мережі та інтернету;
- розробляти та перевіряти працездатність моделі мережі перед безпосереднім впровадженням
- вміти складати кошторис на кабелі, обладнання та програмне забезпечення, необхідних для функціонування мережі;
- оцінювати можливі шляхи вдосконалення мережі.

. Вимоги і список завдань до курсового проекту

1.1 Мета і загальні вимоги

Метою курсового проекту (КП) є організація обчислювальної локальної мережі, відповідно до вибраного варіанта, яка дозволить організовувати процеси керування документами, та спільного використання ресурсів підприємства.

Основні вимоги до процесу виконання КП:

1. Перед виконанням КП необхідно оформити технічне завдання відповідно до варіанту і підписати його у керівника проекту.
2. У завданнях до КП наведені мінімальні вимоги до роботи, тому вітається прояв ініціативи в рамках заданої теми.
3. Локальна обчислювальна мережа (ЛОМ) повинна бути спроектована таким чином, щоб забезпечити належну ступінь захищеності даних. Треба пам'ятати, що це не повинно вплинути на зручність роботи користувачів і адміністраторів мережі.
4. У разі найменшого відступу від технічного завдання обґрунтувати вибір мережевої архітектури для комп'ютерної мережі, метод доступу, топологію, тип кабельної системи, операційної системи, додатків, протоколів тощо.
5. Якщо проект повністю відповідає технічному завданню, привести переваги і недоліки названих характеристик мережі, в тому числі:
   - вибір способу управління мережею;
   - конфігурацію мережевого устаткування – кількість серверів, концентраторів, мережевих принтерів;
   - управління мережевими ресурсами та користувачами мережі;
   - заходи забезпечення безпеки мережі.
6. Провести розрахунок і планування середнього трафіку і коефіцієнта використання мережі.
7. Розробити і обґрунтувати схему розміщення вузлів – структурну схему мережі підприємства, опрацювати питання забезпечення необхідного рівня захисту даних.
8. Виконати розрахунок працездатності розробленої конфігурації.
9. Раціонально розподілити IP-адреси з використанням масок змінної довжини. Обґрунтувати своє рішення.
10. Розробити модель мережі в пакеті PacketTracer і виконати її тестування.

1.2 Варіанти завдань

Завдання до КП формується згідно з табл. 1.1., планом та описом приміщення, а також додатковими умовами щодо особливостей ЛОМ.

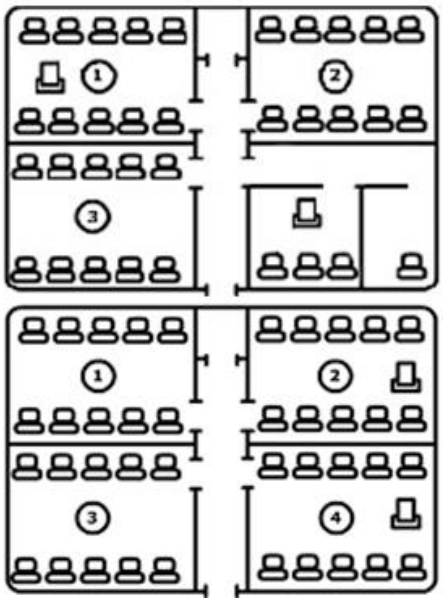
Таблиця 1.1 – Параметри ЛОМ для проектування

(N) mod		Призначення IP-адрес	Служба шлюзу	Обов'язкова складова
(N) mod 4	*0*	вручну	PAT	VLAN
	1	автоматично	статичний NAT	WI-FI
	2	вручну	динамічний NAT	VLAN
	3	автоматично	PAT	WI-FI

Плани та описи приміщень відповідно до номеру варіанту:

Варіант 1.

Організація локально-обчислювальної мережі комп’ютерного клубу



1-й поверх: три класи, адміністрація і кабінет системного адміністратора

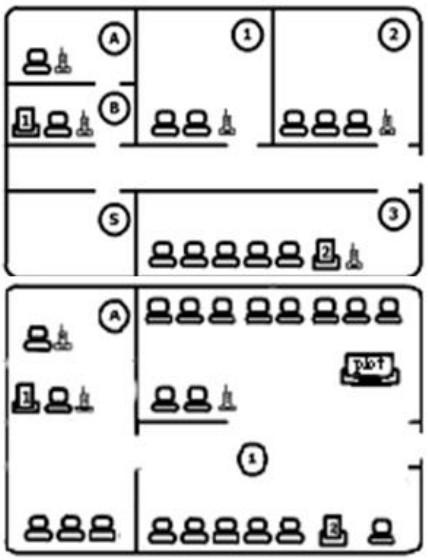
2-й поверх: чотири класи персональних комп'ютерів по 10 од. в кожному, а також два принтера.

Необхідно: організувати повноцінну ЛОМ з виходом в інтернет, а також передбачити можливість спільного використання мережевих ресурсів (принтерів) для 1 поверху для всіх, для другого поверху принтер адміністрації доступний тільки для адміністрації і системного адміністратора. Ці чотири комп'ютери (3 – адміністрації та 1 один системного адміністратора) не доступні іншим користувачам.

Параметри будівлі 70 *30 * 9 м

Варіант 2.

Організація локально-обчислювальної мережі агентства нерухомості



На 1-му поверсі будівлі агентство нерухомості має три підрозділи в кабінетах 1, 2 і 3. Кабінет директора і секретаря розташовані в кабінетах А і В відповідно. Серверну передбачається розмістити в кабінеті S. На другому поверсі будівлі знаходяться бухгалтерія та -видавничий центр агентства.

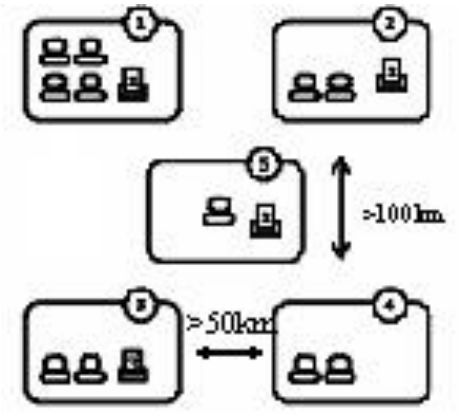
Організувати мережу з виходом в інтернет та підтримкою власного веб-ресурсу, електронною поштою, а також:

- організувати резервування даних;
- забезпечити можливість виведення на принтер 2 (1 пов) всім працівникам агентства, на принтер 1 – директору і секретарю (1 пов);
- передбачити можливість розвитку мережі за рахунок збільшення кількості комп'ютерів;
- передбачити ізоляцію мережі бухгалтерії від інших співробітників;
- спільне користування плотером і принтером працівникам видавничого центру агентства.

Параметри будівлі 50 * 40 * 9 м.

Варіант 3.

Аналіз можливих рішень при об'єднання мережі магазинів.



Мережа магазинів 1 (3 поверхи), 2, 3, 4 (2 поверху), розташованих в різних містах (на великій відстані один від одного), і склад 5.

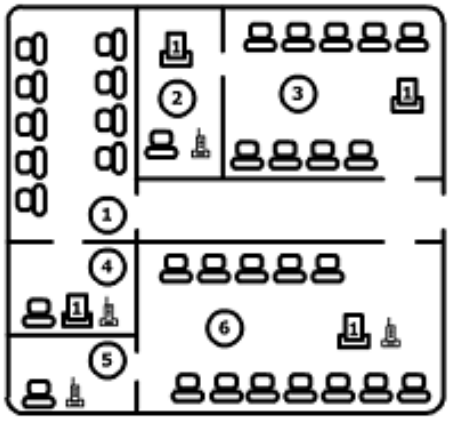
Необхідно визначити найбільш ефективне рішення по організації повноцінної взаємодії між усіма магазинами і складом:

- забезпечити динамічне оновлення даних про товари в кожному магазині;
- організувати можливість отримання статистичної інформації в центральному магазині 1 усіма повноважними користувачами мережі, а також введення інформації на складі.
- забезпечити можливість використання електронної пошти в усіх магазинах.

Параметри будівлі 1: 60 * 50 * 15 м.

Параметри будівель 2,3,4: 40 * 12 * 6 м.

Варіант 4.
Організація локально-обчислювальної мережі фірми

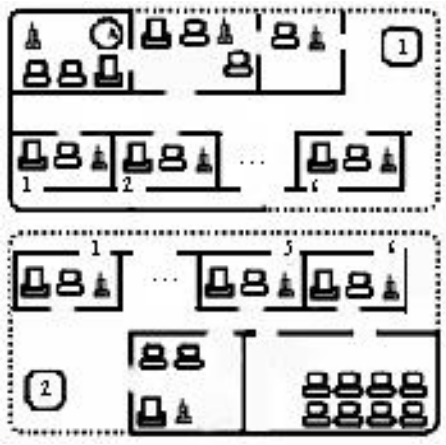


Фірма з розробки ПЗ займає поверх будівлі і має три відділи: веб-програмісти, розробники баз даних і дизайнери (1, 3 і 6 відповідно). Керівники відділів розташовані в кабінетах 2, 4 і 5.
Необхідно запропонувати шляхи побудови ЛОМ з наступними параметрами:

- вихід в інтернет (підтримка власного веб-ресурсу), електронна пошта;
- організувати підтримку поновлення розділу веб-ресурсу уповноваженим представником відділу;
- забезпечити спільний доступ до принтера веб-програмістів і розробників баз даних;
- в кожному з відділів зарезервувати по 7 додаткових робочих місць (2 з яких – WI-FI);
- програмістам БД виділити сервер із встановленою СУБД;
- запропонувати варіанти і засоби обслуговування і забезпечення безпеки ЛВС.

Параметри поверху 70 * 45 * 3 м.

Варіант 5.
Проектування ЛОМ в організації з продажу квитків (вокзал)

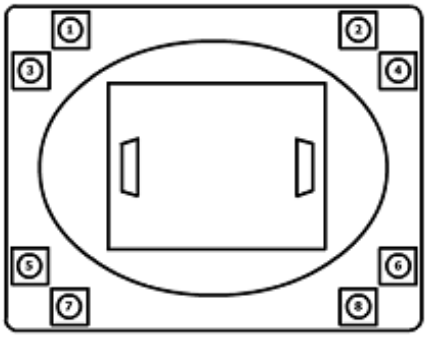


Організація займає перший і другий поверх 3-х поверхового будинку. Залізничні каси (6 кабінетів по 1 робочому місцю в кожному) розташовуються на першому поверсі. Офіс адміністратора, бухгалтера і директора організації (3 робочих місця) так само знаходиться на першому поверсі.
На другому поверсі знаходяться каси попереднього продажу (3) і каси для пільговиків (3), довідкове відділення і зал очікування з інтернет-доступом (адміністратор і 5 робочих місць).
У мережі будуть використовуватися:

- сервер баз даних;·
- вихід в інтернет (окрім кас).
- забезпечення можливість резервного копіювання даних з сервера БД;
- принтери в кожній касі.

Параметри будівлі: 170 * 130 * 7 м

Варіант 6.
Автоматизація діяльності спортивного комплексу на основі ЛОМ

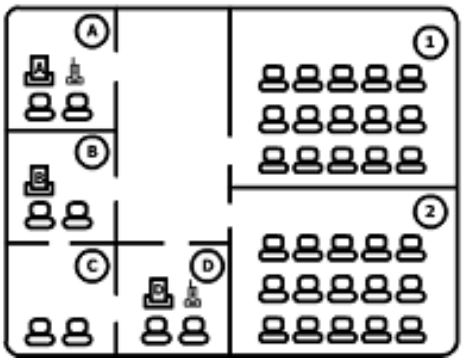


Спортивний комплекс реалізує квитки на спортивні заходи в 8-ми касах (1-8). На другому рівні по периметру (тільки уздовж коротких сторін) розташовані по два приміщення для тренерів на два робочих місця для аналізу матчів.
Необхідно запропонувати план побудови ефективної мережевої системи управління продажами і отримання статистики. Також передбачити:

- підтримку веб-ресурсу власними можливостями,
- установку сервера для обробки потокового відео (на 2-му поверсі)
- резервне зберігання даних (backup).
- відеокамери для трансляції відео.

Параметри будівлі: 200 * 100 * 8 м (висота вказана для першого рівня).

Варіант 7.
Організація локально-обчислювальної мережі навчального центру



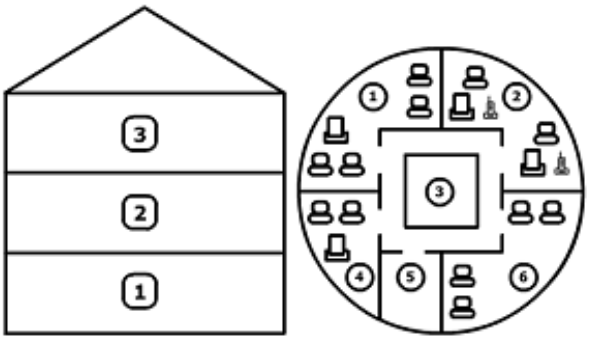
На кожному поверсі 3-поверхової будівлі навчальний центр має по два класи 1 і 2 для проведення занять і по чотири кабінети викладачів A, B, C і D.
Необхідно організувати загальну мережу для спільного використання мережевих ресурсів та забезпечити вихід в інтернет, а також:

- передбачити можливість збільшення кількості комп'ютерів у класах 1 і 2;
- забезпечити можливість обміну інформацією між викладачами (трафік ізольований від студентів);
- організувати резервування даних на сервері (розмістити сервер);
- забезпечити можливість виведення на принтер D всім викладачам, а на принтер A і B – тільки з кабінетів A і B відповідно (на кожному поверсі).

Параметри будівлі: 80 * 70 * 12 м.

Варіант 8.

Побудова структурованої кабельної системи банку



Будівля має три поверхи з однотипною плануванням. Діаметр будівлі 60м. Необхідно запропонувати схему побудови СКС і ЛОМ на її базі.

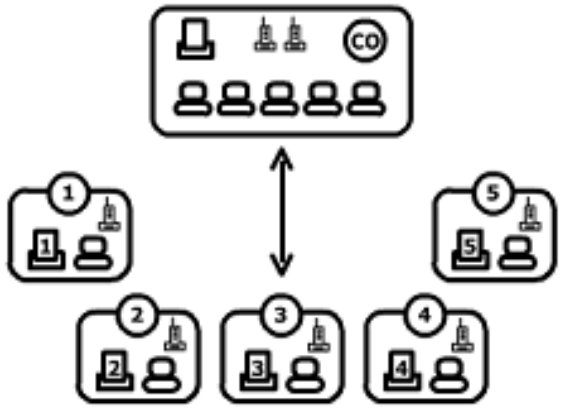
Приміщення 3 – 1 поверх хол; 2 поверх конференц-зал з комп'ютеризованими 25-ма місцями, на 3-му поверсі – дирекція (3 робочих місця із загальним доступом до всієї банківської інформації).

Визначити місце під серверну. Наприклад, кімната №5 вільна, але необхідно мотивувати вибір поверху. Передбачити:

- можливість спільного використання принтерів на поверхах 2 і 3.
- можливість розвитку мережі за рахунок збільшення кількості комп'ютерів;
- можливість обміну службовою інформацією між співробітниками відділів;
- резервування даних;
- особливу увагу до політики безпеки та системного адміністрування.

Варіант 9.

Консолідація потоків підприємства мобільного телефонії

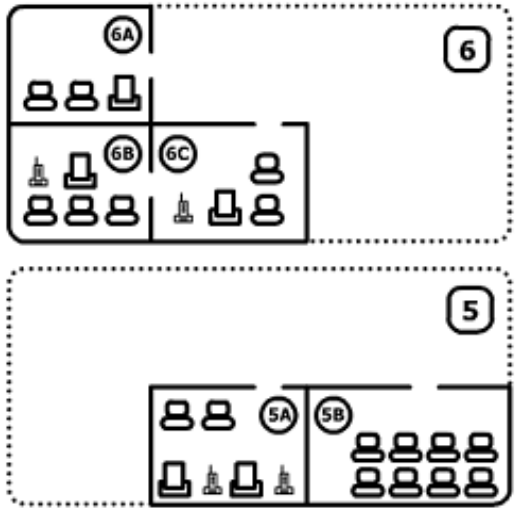


Центральний офіс (central office – CO, три поверхи, 100 *70 *12 м) і мережу його представництв 1, 2, 3, 4, 5 (50 * 40 * 8 м, по 2 поверхи), розташованих на великій відстані один від одного (50-100 км) з однотипним набором технічних засобів .

Необхідно визначити найбільш ефективне рішення, з точки зору ціна / якість, щодо забезпечення передачі інформації з усіх представництв центральний офіс CO.

У центральному офісі організувати ЛОМ з виходом в інтернет. Та передбачити наявність відділів для: 1) керуючого, 2) секретаря, 3) бухгалтерії, відділу роботи з клієнтами.

Варіант 10.
Організація локально-обчислювальної мережі офісного центру

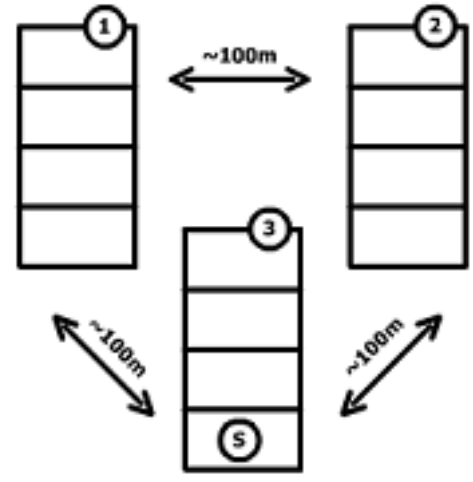


Офісний центр розташований на 1-му (5А і 5В) і 8-му (6А, 6В і 6С) поверхах будівлі.
Необхідно запропонувати шляхи побудови ЛОМ з наступними параметрами:

- вихід в інтернет і електронна пошта;
- забезпечити можливість обміну інформацією між співробітниками кімнат 5А і 6С;
- трафік 6А і 6В – ізолювати від усіх;
- організувати резервування даних; виділити сервер для установки на нього 1С Бухгалтерія;
- передбачити можливість розвитку мережі за рахунок збільшення кількості комп'ютерів на випадок збільшення займаної площі;
- забезпечити можливість спільного доступу до електронної пошти.

Параметри поверху: 60 * 40 * 3 м

Варіант 11.
Організація локально-обчислювальної мережі студентського містечка

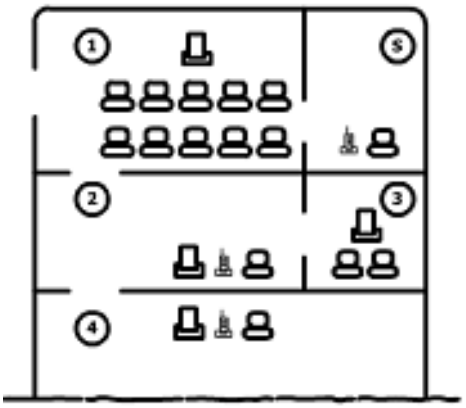


Три 4-х поверхових (5 кімнат на кожному поверсі) будівлі студентського містечка віддалених на відстань близько 100 м один від одного (1, 2, 3). Серверна S знаходиться вбудівлі №3 на першому поверсі.
Необхідно запропонувати план організації мережі ,що покриває всі кімнати 3-х корпусів, а також:

- організувати можливість доступу до інтернету;
- передбачити можливість включення гетерогенних підмереж в створювану мережу (в будівлі 2 на першому, другому і третьому поверхах ПК об'єднані в мережу Ethernet 100Base-TX, а на четвертому поверсі Ethernet 10Base-2).

Параметри будівель: 1 і 2 – 70 * 40 * 12 м та 3 – 60 * 300 * 12 м.

Варіант 12.
Автоматизація роботи бібліотеки на базі ЛОМ



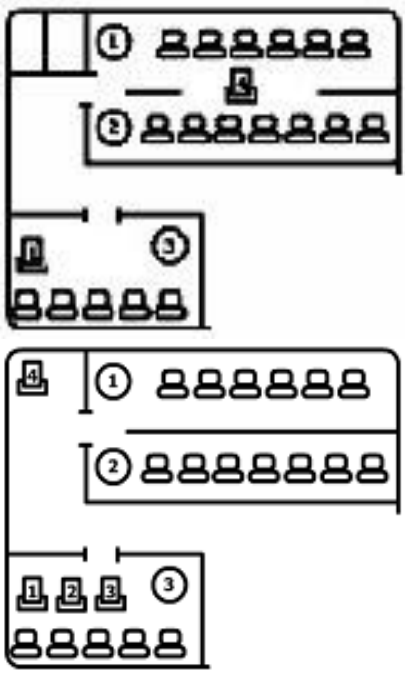
Бібліотека має на 1-му поверсі такі відділи:
- відділ пошуку літератури 1;
- відділ видачі / приймання книг 2;
- відділ інвентаризації бібліотечних фондів 3;
- сховище книг 4;
- серверна S.

на 2-му поверсі 3 комп'ютеризованих зали:
- для викладачів на 30 місць;
- студентів на 50 місць;
- зал для роботи з дисертаціями на 30 місць (без підключення до інтернету і принтерів).

Запропонувати план ЛОМ з доступом до інтернету. Передбачити можливості:
- відділу інвентаризації бібліотечних фондів проводити поповнення/списання книг;
- резервування баз даних;
- організувати спільне використання принтерів.

Параметри будівлі: 100* 50 * 10 м

Варіант 13.
Організація локально-обчислювальної мережі інтернет-кафе



1-й поверх: два класи комп'ютерів по 6 шт. (№1) та 7 шт. (№2), каса та обслуговуючий персонал №3.

2-й поверх: два класи комп'ютерів по 6 шт. (№1) та 7 шт. (№2), поліграфічний центр №3 з 5 ПК, а також 4 принтери.

Необхідно організувати повноцінну ЛОМ з виходом в інтернет, а також передбачити можливість спільного використання мережевих ресурсів (принтерів) всіма повноважними користувачами мережі.

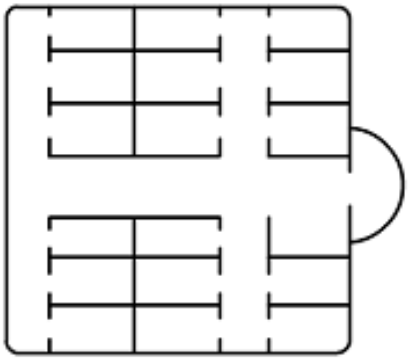
Каси і поліграфічний центр - ізольовані підмережі.

Організація планує мати власний веб-сервер.

Параметри будівлі: 60 * 40 * 10 м

Варіант 14.

Підвищення ефективності роботи медичного центру за рахунок ЛОМ



Медичний центр складається з 10 лікарських кабінетів в двох поверхах і реєстратури.

Необхідно запропонувати план підвищення ефективності роботи медичного центру за рахунок впровадження в його роботу ЛОМ.

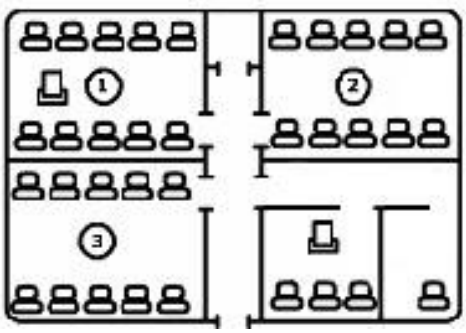
Передбачити:

- підтримку веб-ресурсу,
- доступ до інтернету,
- можливість віддаленої реєстрації на прийом до лікаря і отримання результатів аналізів,
- резервування даних;
- мережевий друк документів.

Параметри будівлі: 100 *80 *8 м.

Варіант 15.

Автоматизація роботи підприємства



Підприємство збирається переїжджати в триповерховий будинок. Кожен поверх буде займати три відділи (мінімум по 15 р.м. + резерв 6 р.м.) і кабінети начальників відділів.

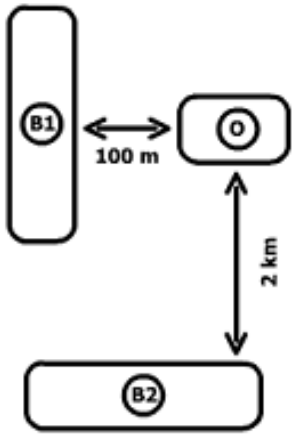
Необхідно:

- організувати в будівлі ЛОМ, що зв'язує всі відділи, і забезпечити їм вихід в інтернет;
- передбачити наявність мережевих розеток у кожній кімнаті, мережевого принтера на кожному поверсі;
- врахувати, що кожен поверх працює зі своєю базою даних, і що співробітники одного поверху будівлі не повинні мати доступ до ресурсів іншого поверху;
- передбачити наявність загальних для всіх відділів мережевих ресурсів.

Параметри будівлі: 50 * 30 * 12 м.

Варіант 16.

Підприємство з розробки, впровадження і підтримки різних видів ПЗ



Підприємство займає три будівлі.

Офіс «О» (20 * 15 * 8 м, 2 поверхи) включає кабінет директора (1 р.м.) і секретаря (1 р.м), бухгалтерію (5 р.м.) і відділ прийому замовлень і роботи з клієнтами (10 р.м.).

Будівля В1 (40 * 25 * 8 м, 2 поверхи) включає по дві групи розробників (15 люд + резерв) і по два керівника проектів на кожному поверсі.

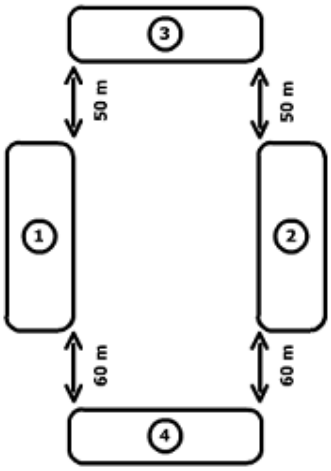
Будівля В2 (50 *30 * 4 м, 1 поверх) включає три групи впровадження та підтримки по 5 люд + керівник.

Необхідно:

- зв'язати будівлі В1 і В2 з офісом О.
- забезпечити ЛОМ вихід в інтернет;
- визначити місце розміщення БД і дати до неї доступ всім об'єктам (О, В1, В2) та адміністратору мережі;
- врахувати, що кожен відділ має загальний принтер і кілька мобільних робочих місць.

Варіант 17.

Проектування домашньої локальної мережі



4 житлових будинки (розташованих квадратом):

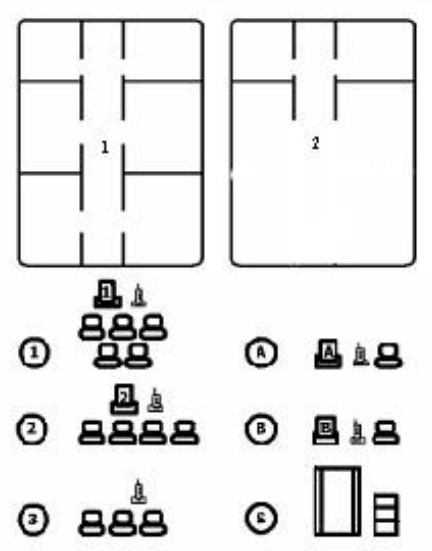
- 1 і 2 – два 9-поверхові будинки з чотирма під’їздами (довжина 80 м, поверх – 3 м);
- 3 і 4 – два 12-поверхові будинки з шістьма під'їздами (довжина 80 м, поверх – 3 м).

Відстань між будівлями наведена на рисунку. В кожному будинку на поверсі знаходиться чотири квартири. Необхідно:

- спроектувати ЛОМ, що об'єднує всі будинки так, щоб житель будь-якої квартири міг при бажанні до неї підключитися
- забезпечити вихід в інтернет;
- врахувати, що число квартир, яких потрібно буде підключати до локальної мережі, заздалегідь невідомо
- розрахувати приблизну вартість створення мережі без урахування витрат на підключення кожної квартири.

Варіант 18.

Розробка моделі розвитку кабельної системи підприємства



Задана двоповерхова будівля представленої планування, а також передбачуване для використання обладнання (1-й поверх):

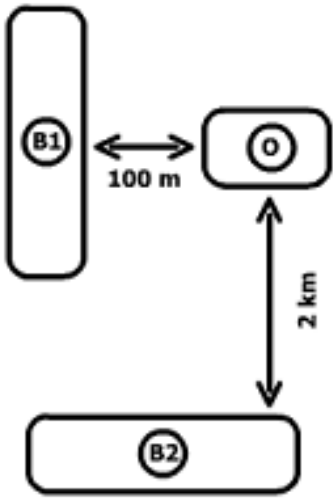
- A і B – для кабінету директора і секретаря;
- S – обладнання для серверної (серверна стійка);
- 1, 2, 3 – для відділів №№ 1, 2, 3 відповідно.

На другому поверсі передбачається розмістити 20 робочих місць для рекламно-видавничого центру підприємства з плотером і принтером в загальному доступі, серверну і кабінет системного адміністратора.

Необхідно запропонувати оптимальне рішення для розміщення обладнання і побудови структурованої кабельної системи, а також розвитку на її базі ЛОМ.

Варіант 19.

Автоматизація роботи автомайстерні



Задано:

- офіс мережі автомайстерень О (2 поверхи, 70 * 50 * 6 м, 8 раб. місць);
- бокси 1 (В1), розташовані на відстані 100 метрів від офісу (50 * 20 * 4 м, 1 поверх);
- бокси 2 (В2), розташовані на відстані 2 км від офісу (50 * 20 * 4 м, 1 поверх).

Необхідно:

- організувати зв'язок ремонтних боксів В1 і В2 з офісом;
- визначити місце розміщення БД і забезпечити до неї доступ всіх об'єктів (О, В1, В2).
- забезпечити офіс виходом в інтернет;
- врахувати, що число робочих місць (точок підключення до локальної мережі) в боксах В1 і В2 заздалегідь не відомо.

Варіант 20.

Проектування комп'ютерної мережі в організації з постачання та обслуговування комп'ютерної техніки

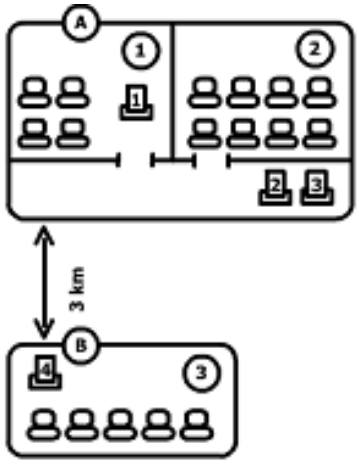
Фірма пропонує послуги з постачання комп'ютерної техніки:

- роздрібний продаж комп'ютерної техніки, консультації по вибору комп'ютерних і програмних рішень для конкретної сфери бізнесу або будинку (торговий зал А в двох поверхах, 12 роб. місць)
- діагностика та налаштування обладнання (1) – 5 роб. місць.
- гарантійне і післягарантійне обслуговування (2) – 10 роб. місць.
- мережеві рішення (3) – 7 роб. місць.
- В – серверна;
- С – секретар;

Необхідно організувати повноцінну ЛОМ з виходом в інтернет, а також передбачити можливість спільного використання мережевих ресурсів.

Варіант 21.

Аналіз можливих рішень при об'єднання основного офісу і філії підприємства в єдину інформаційну мережа



Фірма з основним офісом А (2 поверхи) і віддаленим на 3 км філією В (3 поверхи).

Параметри будівель:

- А – 100 * 80 * 10 м;
- В – 50 * 40 * 12 м.

Необхідно:

- організувати загальну повноцінну мережу для спільного використання мережевих ресурсів (принтерів) і баз даних усіма повноважними користувачами мережі,
- забезпечити вихід в інтернет;
- передбачити додаткові мобільні робочі місця для користувачів офісу В.

1.3 Технічне завдання

У технічному завданні (ТЗ) до КП формулюються такі вимоги до обчислювальної мережі підприємства:

- план приміщення, в якому буде організована;
- середовище передачі даних (коаксіальний кабель / кручена пара / оптоволокно);
- метод призначення IP-адрес (автоматично / вручну);
- спосіб та/або протокол маршрутизації (статична / динамічна / RIP / OSPF);
- служба шлюзу (статичний NAT / динамічний NAT / PAT);
- обов'язкова складова (VLAN/WI-FI).

Крім того, в ТЗ вказуються:

- розділи пояснювальної записки, що підлягають розробці;
- зміст графічної частини КП;
- графік виконання курсової роботи;
- дати здачі КП на перевірку та дата захисту.

Шаблон технічного завдання наведений у додатку А.

1.4 Реферат та вступ

В рефераті фіксуються основні статистичні дані щодо змісту пояснювальної записки, формулюються мета і основні задачі роботи. Також наводиться перелік ключових слів, що найбільш точно характеризують тематику та зміст курсового проекту. Сторінка з рефератом друкується на листі зі стандартним штампом заголовного листа.

Вступ містить загальний опис курсового проекту, докладний перелік усіх етапів роботи із вказівкою проміжних результатів та визначення результату, який очікується у результаті виконання роботи.

1.5 Структура та зміст ПЗ

Загальний обсяг пояснювальної записки – від 40 до 50 аркушів, графічний матеріал – 4 листа відповідно до технічного завдання. Значна частина пояснювальної записки повинна бути присвячена розділу 6 – розробці, налагодженні і тестування моделі мережі.

Пояснювальна записка до КП повинна мати такі розділи та підрозділи:

Титул

Технічне завдання

Реферат

Зміст

Вступ

1. *Логічна схема та характеристики мережі*
   - *1.1. Аналіз потреб підприємства і вибір топології*
   - *1.2. Розробка логічної схеми мережі*
   - *1.3. Розрахунок ефективного трафіку*
   - *1.4. Пропускна здатність та коефіцієнт використання мережі*
   - *1.5. Розподіл мережевих адрес*
2. *Планування кабельної системи та вибір обладнання*
   - *2.1. Структурована кабельна система*
   - *2.2. Вибір типу кабелю для підсистем*
   - *2.3. Вибір активного обладнання*
   - *2.4. Розробка фізичної схеми*
   - *2.5. Складання кошторису на кабелі та обладнання*
3. *Програмне забезпечення та адміністрування мережі*
   - *3.1. Вибір мережевої операційної системи*
   - *3.2. Стратегія адміністрування у мережі*
   - *3.3.Спільний доступ до зовнішніх мереж*
   - *3.4. Мережеві екрани та антивірусне програмне забезпечення*
   - *3.5. Організація зберігання даних та резервне копіювання*
   - *3.6. Складання кошторису на програмне забезпечення*
4. *Моделювання мережі у середовищі Cisco Packet Tracer*
   - *4.1. Розробка та налаштування моделі мережі*
   - *4.2. Перевірка працездатності моделі*
   - *4.3. Оцінка шляхів вдосконалення*

Висновок

Література

Додатки

Графічна частина

1.6 Висновок, література і додатки

У висновках перелічуються отримані навички і вміння, отримані підчас виконання курсового проекту, узагальнюються основні результати та здобутки роботи.

В переліку літератури вказуються джерела, які були використані при написання пояснювальної записки. Джерела нумеруються в порядку появі в тексті, відповіді номери посилань за текстом пояснювальної записки надаються в квадратних дужках («[]»).

В окремому додатку обов’язково наводиться конфігурація усіх пристроїв моделі локальної мережі в середовищі Cisco Packet Tracer (див. розділ 5 вказівок).

1.7 Графічна частина

Графічна частина КП повинна містити два креслення, що виконуються на листах формату А3:

1. Логічна схема мережі.
2. Фізична (топологічна) схема мережі.

Під логічною топологією мережі мається на увазі структура зв'язку кінцевих вузлів в локальній мережі, яка підтримує потрібні напрямку передачі даних, тобто мова йде про організацію організація на 3-му і вище рівнях моделі OSI - мережеві протоколи, адресація, взаємодія робочих станцій з серверами.

На логічної схемою повинна бути представлені така інформація:

- підмережі -–VLAN ID (усі), назви VLAN'ов, мережеві адреси і маски (префікси);
- L3-пристрої – маршрутизатори, міжмережеві екрани, VPN-шлюзи, найбільш значущі сервери (наприклад, DNS і ін.), IP-адреси цих серверів, логічні інтерфейси;
- інформація протоколів маршрутизації.

Приклад логічної схеми наведений в додатку Б.

Під фізичною топологією розуміється схему, по якій прокладаються кабельні лінії зв'язку, встановлюються мережеві короби, розміщуються розетки тощо.

На фізичній схемі повинна бути представлена така інформація:

- план всіх приміщень будівлі з дотриманням масштабу;

- активне і пасивне устаткування, сервери і хости в місцях їх фізичного розміщення;
- мережеві розетки в межах приміщення;
- всі кабельні з'єднання між обладнанням мережі (СКС).

Приклад фізичної схеми наведений в додатку В.

Логічна схема та характеристики мережі

2.1 Аналіз потреб підприємства

Планування проекту ЛОМ починається з аналізу інформаційних потреб підприємства. Вивчення найбільш поширених ланцюжків діяльності та процесів, що відбуваються на підприємстві, дозволяють найбільш точно сформулювати вимоги до ЛОМ підприємства .

Важливість цього етапу пов'язана як з необхідністю впорядкування вимог до створюваної ЛОМ і її окремих складових для забезпечення можливості прийняття в майбутньому зважених конкретних рішень, так і з її обґрунтуванням.

Передбачити всі можливі фактори, врахувати всі потреби, які можуть виникнути в майбутньому, практично неможливо. Однак загальні підходи до проектування локальних комп'ютерних мереж все-таки можуть бути сформульовані. При плануванні ЛОМ підприємства необхідно враховувати такі фактори [1]:

- необхідний розмір мережі (в даний час, в найближчому майбутньому і за прогнозом на перспективу);
- структура, ієрархія і основні частини мережі (по підрозділах підприємства, а також по кімнатах, поверхах і будівлям підприємства);
- основні напрямки та інтенсивність інформаційних потоків в мережі (в даний час, в найближчому майбутньому і в далекій перспективі).
- характер інформації, що передається по мережі інформації (дані, оцифрована мова, зображення), який безпосередньо позначається на необхідної швидкості передачі (до декількох сотень Мбіт/с для телевізійних зображень високої чіткості);
- технічні характеристики обладнання (комп'ютерів, адаптерів, кабелів, репітерів, концентраторів, комутаторів) і його вартість;
- можливості прокладки кабельної системи в приміщеннях і між ними, а також заходи забезпечення цілісності кабелю;
- обслуговування мережі і контроль її безвідмовності і безпеки;
- вимоги до програмних засобів по допустимому розміру мережі, швидкості, гнучкості, розмежування прав доступу, вартості, за можливостями контролю обміну інформацією тощо;
- необхідність підключення до глобальних або до інших ЛОМ.

Результатом даного етапу є підтвердження та уточнення ТЗ до КП.

2.2 Вибір топології та розробка логічної схеми

Після аналізу виконується попередній вибір базової мережної технології для проектованої локальної мережі на підставі технічних вимог, експертних даних, результатів аналізу потреб підприємства й плану будинку. У табл. 2.1 наведені найпоширеніші технології сучасних локальних мереж.

Таблиця 2.1 – Різновиди Ethernet та їх фізичні характеристики

Стандарт	*Фізична специфікація*	*Кабелі, роз'єми*	*Обмеження на довжину фізичного сегмента, м*	*Макс. кількість повторювачів*	*Макс. кількість станції*	*∅ мережі, м*
Ethernet (802.3i)	10Base5 (Thicknet)	Товстий коаксіал RG-8/11, роз'єми AUI	500 min 2,5 м	4 (2 сегменти без вузлів)	100	2500
	10Base2 (Cheapernet)	Тонкий коаксіал RG-58A/U, роз'єми BNC	185 (200) min 0,5 м		30	925
	10BaseTX	2КП UTP3-4-5, RJ-45	100	4	1024	500
	10BaseF	ОМ ОВ / ММ ОВ 62.5, роз'єми ST	1000/5000	-	2	1000/ 5000
Fast Ethernet (802.3u)	100BaseTX	2КП UTP, STP Type 1, роз'єми RJ-45	100	1 класу I / 2 класу II (кабель між повторювачами – до 5 м)	1024	200-320
	100BaseFX	БМ ОВ 62.5, 125 мкм, роз'єми ST, SC	160 / 412 (полудуплекс)/ 2000 (повнодуплексн.)			
	100BaseT4	4КП UTP3-4-5, RJ-45	100			
Gigabit Ethernet (802.3z)	1000BaseLX	БМ ОВ / ОМ ОВ, роз'єми ST, SC	316 (550/3000)	-	2	550/ 3000
	1000BaseSX	БМ ОВ 62.5/50 мкм, роз'єми ST, SC	275 (300/550)	-		300/ 550
	1000BaseCX	коаксіал, (КП-7 STP), RJ-45	25	-		25
(802.3ab)	1000BaseT	КП STP5-6 RJ-45	200	1		100

Умовні скорочення:

– 2КП – 2-жильна кручена пара, 4КП – 4-жильна кручена пара;

– ОВ – оптоволокно, БМ – багатомодове, ОМ – одномодове.

Згідно з вихідним розташуванням комп'ютерів і обраної мережної технології обирається мережева топологія. Будується топологічна схема локальної мережі із вказівкою номерів робочих станцій, видів серверів та іншого обладнання, типу й пропускної здатності каналів зв'язків.

Далі будується логічна схема ЛОМ, приклади якої наведені на рис 2.1 та в додатку Б.

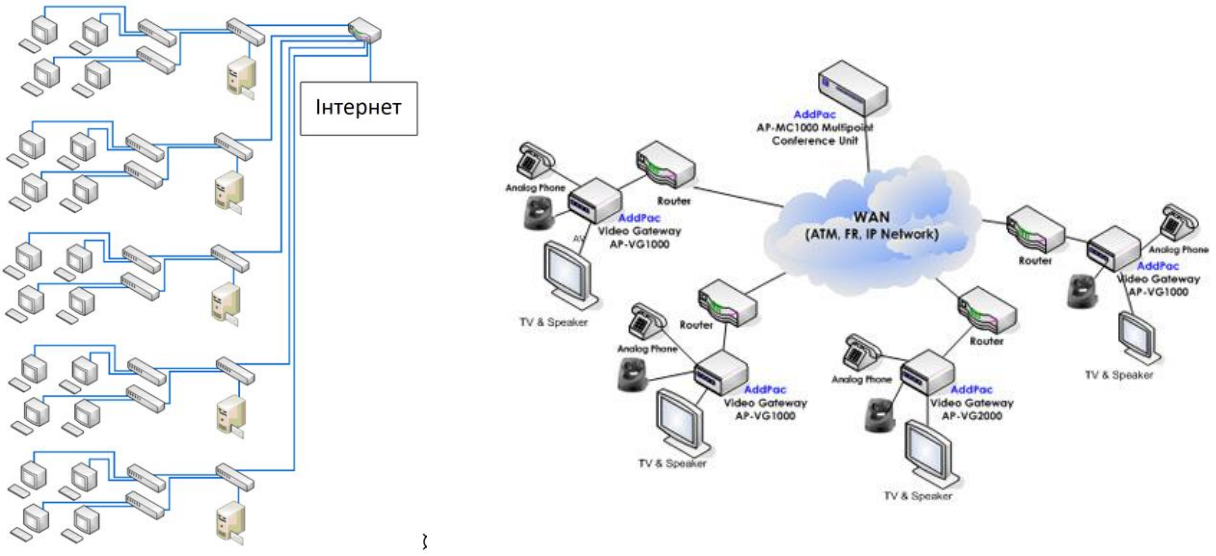


Рисунок 2.1 – Приклади логічних схем ЛОМ

2.3 Розрахунок характеристик мережі

Для кожної робочої станції визначається ефективний трафік $П_{ei}$ як сума навантажень по всіх додатках (табл. 2.1). Потім виконується розрахунки навантаження на мережу [2].

Таблиця 2.2 – Мережні задачі, що використовуються в локальних мережах

Завдання	*Навантаження на одного абонента, Mb/c*	*Серверна частина*	*Клієнтська частина*
Обмін файлам	0,002-0,005 Mb/c	Мережева ОС	Мережева ОС
Файловий сервер	0,002-0,005 Mb/c	Серверна мережева ОС	Клієнтська мережева ОС
Резервування інформації	0,06-0,08 Mb/c на 1 станцію 0,5 Mb/c на 1 сервер	Мережева ОС	Мережева ОС
Мережевий друк	0,08-0,1 Mb/c	Мережева ОС	Мережева ОС
Служба терміналів	0,002-0,008 Mb/c на 1 станцію (трафік 1 Мбіт/с)	Серверна мережева ОС	Клієнтська мережева ОС
СУБД	0,04-0,07 Mb/c	Сервер БД	Додаток БД
Дистанційний доступ	0,02-100 Mb/c на модем	Сервер віддаленого доступу	Клієнт віддаленого доступу
Інтернет	0,002-0,005 Mb/c	Проксі-сервер	Браузер
Електронна пошта	0,5-2 на 1 клієнта	Поштовий сервер	Поштовий клієнт

Завдання	*Навантаження на одного абонента, Mb/c*	*Серверна частина*	*Клієнтська частина*
Інтранет	0,04-0,07 Mb/c на 1 клієнта	Веб-сервер	Браузер
Інтерактивні повідомлення	0,002 на 1 станцію	різні	різні
Голосовий зв'язок (IP-телефонія)	0,2-0,8 Mb/c на 1 станцію (трафік 1 Mb/c)	різні	різні
Відеоконференції	0,4-2 Mb/c на 1 станцію (трафік 10 Мбіт/с)	різні	різні
Служби мережевої безпеки	0,02-0,05 Mb/c на 1 сервер + 0,002-0,005 Mb/c на 1 клієнта	Серверна мережева ОС	Клієнтська мережева ОС

Навантаження на мережу – це обсяг даних, реально переданий по мережі в одиницю часу. Розрахунки навантаження на мережу здійснюється по формулі:

$$П_{\Sigma e.} = n*П_{ei+} m*П_{серв} \quad (2.1)$$

де n – число комп'ютерів у мережі,

m – кількість серверів,

$П_{ei}$ – навантаження на один комп'ютер у мережі,

$П_{серв}$ – навантаження на один сервер.

Значення $П_{\Sigma e}$ помножується на коефіцієнт запасу $k_з=(1,2÷2,0)$ для урахування майбутнього розвитку мережі.

Пропускна здатність – це максимально можлива для даної мережі швидкість передачі даних, яка визначається бітовою швидкістю та деякими іншими обмежуючими факторами (тривалість інтервалів між переданими блоками даних, обсяг переданої по мережі службової інформації тощо). Значення пропускної здатності для мережевих технологій відомі і наводяться в стандарті. У більшості випадків можна прийняти пропускну здатність рівної бітової швидкості.

Розрахуємо теоретичну корисну пропускну здатність Fast Ethernet без обліку колізій і затримок сигналу в мережному встаткуванні.

Відмінність корисної пропускної здатності від повної пропускної здатності залежить від довжини кадра. З урахуванням того, що частка службової інформації завжди та сама, то чим меншим є загальний розмір кадра, тем вище є «накладні витрати». Службова інформація в кадрах Ethernet становить 18 байт (без преамбули і стартового байта), а розмір поля даних кадра змінюється від 46 до 1500 байт. Сам розмір кадра змінюється від 46 + 18 = 64 байт до 1500 + 18 = 1518 байт. Тому для кадра мінімальної довжини корисна інформація $V_к$ становить усього лише 46/64 ≈ 0,72 від загальної переданої інформації, а для кадра максимальної довжини $V_к$=1500/1518 ≈ 0,99 від загальної інформації.

Щоб розрахувати корисну пропускну здатність мережі для кадрів максимального і мінімального розміру, необхідно врахувати різну частоту проходження кадрів. Природно, що, чим меншим є розмір кадрів, тим більше таких кадрів буде проходити по мережі за одиницю часу, несучи із собою більшу кількість службової інформації і меншу кількість корисної.

Так, для передачі кадра мінімального розміру, який разом із преамбулою має довжину 72 байти, або 576 біт, буде потрібен час, рівне 576 bt, а якщо врахувати міжкадровий інтервал в 96 bt, то отримаємо період проходження кадрів у розмірі 672 bt. При швидкості передачі в 100 Мбіт/с це відповідає часу 6,72 мкс. Тоді частота проходження кадрів, тобто кількість кадрів, що проходять мережею за 1 секунду, складе f_{min} = 1/6,72 мкс ≈ 148 810 кадрів/с.

При передачі кадра максимального розміру, який разом із преамбулою має довжину 1526 байтів або 12 208 біт, період проходження становить 12 208 bt + 96 bt = 12 304 bt, а частота кадрів при швидкості передачі 100 Мбіт/с складе f_{max} = 1/123,04 мкс = 8 127 кадрів/с.

Знаючи частоту проходження кадрів f і розмір корисної інформації $V_к$ у байтах, що переноситься кожним кадром, можна розрахувати корисну пропускну здатність мережі:

$$П_к \text{ (біт/с)} = V_к \cdot 8 \cdot f. \qquad (2.2)$$

Для кадра мінімальної довжини (46 байт) теоретична корисна пропускна здатність дорівнює

$$П_{к\,min} = 46*8*148\,810 \text{ кадрів/с} = 54{,}76 \text{ Мбіт/с}, \qquad (2.3)$$

що становить лише трохи більше половини від загальної максимальної пропускної здатності мережі.

Для кадра максимального розміру (1500 байт) корисна пропускна здатність мережі дорівнює

$$Пк_{\,max} = 1500*8*8127 \text{ кадрів/с} = 97{,}52 \text{ Мбіт/с}, \qquad (2.4)$$

Таким чином, у мережі Fast Ethernet корисна пропускна здатність може мінятися залежно від розміру переданих кадрів від 54,76 до 97,52 Мбіт/с.

Оскільки для розрахунків ми користувалися відносною величиною бітового інтервалу bt, яка для Ethernet в є в 10 разів меншою, то можна аналогічно розрахувати усі значення для мережі Ethernet 10 Мбіт/с.

Коефіцієнт використання мережі дорівнює відношенню навантаження на мережу до пропускної здатності. Коефіцієнт використання мережі розраховується за формулою:

$$k_{вик} = П_{\Sigma e} / П_{к\,max}, \qquad (2.5)$$

Наприклад, для $П_{Σe}$ =60 Мбіт/с $k_{вик}$ = 60.0/97,52 = 0.615.

Незважаючи на те, що швидкість передачі даних у мережі певної технології завжди та сама, продуктивність мережі зменшується зі збільшенням обсягу переданих даних. По-перше, обсяг переданих даних (трафік) ділиться між усіма комп'ютерами мережі. По-друге, навіть та частка пропускної здатності поділу сегменту, що розділяється, яка повинна припадати на один вузол, дуже часто йому не дістається через особливості роботи механізму доступу до загального середовища передачі даних. Після певної межі збільшення коефіцієнта використання мережі приводить до різкого зменшення реальної швидкості передачі даних. Втрати часу, пов'язані з роботою механізму доступу до середовища, що розділяється, залежать від характеру звернень комп'ютерів до мережі і не можуть бути точно розраховані, тому для забезпечення достатньої продуктивності задається граничне значення коефіцієнта використання мережі, при якому мережа буде швидко реагувати на звернення користувачів.

За отриманим значенням $П_{Σe}$ уточнюється обрана технологія ЛОМ таким чином, щоб коефіцієнт використання мережі $k_{вик}$ був не більш за 0,65. Якщо необхідно, виконується сегментація підмережі за допомогою комутаторів або мостів з метою зменшення трафіка, або вибирається інша мережева технологія.

У випадку перевищення трафіка мережа розбивається на логічні сегменти за допомогою комутаторів. Сумарний трафік перераховується для кожного логічного сегмента. Для кожного логічного сегмента уточнюється коефіцієнт використання мережі, як зазначено вище.

У випадку високого широкомовного і службового трафіка при наявності більш 150-300 станцій необхідна розбивка локальної мережі на підмережі за допомогою маршрутизаторів.

У якості результату планування проекту ЛОМ записується найменування обраної технології, пропускна здатність мережі й усереднений по логічних сегментах коефіцієнт використання мережі.

2.3 Розподіл мережевих адрес

Сучасні маршрутизатори використовують форму IP-адресації звану безкласової междоменной маршрутизацією (Classless Interdomain Routing, CIDR), яка ігнорує класи. У системах, що використовують класи, маршрутизатор визначає клас адреси і потім розділяє адресу на октети мережі і октети хоста, базуючись на цьому класі. У CIDR маршрутизатор використовує біти маски для

визначення в адресі мережної частини і номера хоста. Межа розподілу адреси може проходити посеред октету.

CIDR дозволяє маршрутизаторів агрегувати або підсумовувати інформацію про маршрутах. Вони роблять це шляхом використання маски замість класів адрес для визначення мережної частини IP-адреси. Це скорочує розміри таблиць маршрутів, так як використовується лише одна адреса і маска для подання маршрутів до багатьох подсетям. Без CIDR і агрегації маршрутів маршрутизатор повинен містити індивідуальну інформацію для всіх підмереж.

Виходячи із запису CIDR легко з'ясувати маску підмережі. Наприклад, для IP-адреси 213.45.64.123 з CIDR / 27 необхідно виконати наступні дії:

- кількість біт з CIDR перетворити в бінарний вигляд – «/ 27» → 11111111111111111111111111100000;
- розбити на 4-ри октети –11111111.11111111.11111111.11100000;
- перевести в десяткову систему – 255.255.255.224.

Також за записом CIDR легко визначити адресу мережі, широкомовну адреса (broadcast) і число хостів у мережі. Наведемо приклад для 213.45.64.123/27:

- 32-27 = 5 біт;
- 25 = 32, а значить робочих IP-адрес в цій мережі 30-ть (1-а адреса – адреса мережі, а остання – широкомовна);
- дивимося на останній октет IP-адреси (213.45.64.**123**) – в 123-х цілих 32-ек укладається 3 рази, а значить адреса мережі 213.45.64.96 (32х3 = 96);
- широкомовною адресою буде 213.45.64.127 (32х4-1 = 127).

Розглянемо, як по хосту і масці підмережі визначити адресу мережі, широкомовна адреса, число хостів у мережі. Як приклад використаємо IP-адресу 192.168.32.48 з маскою підмережі 255.255.255.192:

- 256-192 = 64, де 192 – це останній октет з маски (255.255.255.**192**), а 64 – загальна кількість хостів в мережі, 1-а адреса – це адреса мережі, а остання – широкомовна; отримуємо 62 робочих хоста в мережі;
- дивимося останній октет IP-адреси (192.168.32.48), в 48 цілих 64-рок укладається нуль – отримуємо адресу мережі 192.168.32.0 (0 × 64 = 0);
- широкомовною адресою буде 192.168.32.63 (64 × 1-1 = 63).

Таким чином, після побудови логічної схеми ЛОМ підприємства в КП необхідно виконати розбиття адресного простору підприємства на підмережі. Логіка розбиття повинна відповідати логічній схемі та враховувати можливості

майбутнього розширення мережі. Результатом повинна бути адресна таблиця, приклад якої наведений у табл. 2.3, а також текстовий опис процесу та логіки розбиття адресного простору.

Таблиця 2.3 – Приклад розподілу адресів у мережі

Відділ	*Кількість хостів*	*Адреса підмережі*	*Перша доступна адреса хоста*	*Остання доступна адреса хоста*	*Широкомовна адреса*
Дизайнери	14 + 7	192.168.10.0/27	192.168.10.1	192.168.10.30	192.168.10.31
Розробники баз даних	11 + 7	192.168.10.32/27	192.168.10.33	192.168.10.62	192.168.10.63
Веб-програмісти	9 + 7	192.168.10.64/27	192.168.10.65	192.168.10.94	192.168.10.95
Веб-програмісти (керівник)	3	192.168.10.96/29	192.168.10.97	192.168.10.102	192.168.10.103
Розробники баз даних (керівник)	3	192.168.10.104/29	192.168.10.105	192.168.10.110	192.168.10.111
Дизайнери (керівник)	2	192.168.10.112/29	192.168.10.113	192.168.10.118	192.168.10.119

3 Планування кабельної системи та вибір обладнання

3.1 Структурована кабельна система

Структурована кабельна система (СКС, Structured Cabling System, SCS) – набір комутаційних елементів (кабелів, роз’ємів, конекторів, кросових шаф), а також методика їх спільного використання, яка дозволяє створювати регулярні, легко розширювані структури зв'язків в обчислювальних мережах. СКС є свого роду «конструктором», за допомогою якого проектувальник мережі будує потрібну йому конфігурацію зі стандартних кабелів, з'єднаних стандартними роз’ємами, що комутуються у стандартних кросових (мережевих) шафах. При необхідності конфігурацію зв'язків можна легко змінити – додати комп'ютер, сегмент, комутатор, вилучити непотрібне обладнання, а також поміняти з'єднання між комп'ютерами чи концентраторами.

При побудові СКС мається на увазі, що кожне робоче місце на підприємстві повинне бути оснащене розетками для підключення телефону та комп'ютера, навіть якщо в цей момент цього не потрібно. Тобто гарна СКС будується надлишковою – у майбутньому це може заощадити кошти, тому що зміни в підключенні нових пристроїв можна робити за рахунок перекомутації вже встановленого обладнання та прокладених кабелів.

СКС планується і будується ієрархічно, з головною магістраллю і численними відгалуженням від неї. Ця система може бути побудована на базі вже існуючих сучасних телефонних кабельних систем. Кабелі, що представляють собою набір кручених пар, прокладаються в кожному будинку, розводяться між поверхами, на кожному поверсі використовується спеціальна кросова шафа, від якої кабелі в трубах і коробах підводять до кожної кімнати і розводять по розетках. На жаль, у нашій країні далеко не у всіх будинках телефонні лінії прокладаються крученими парами, тому вони непридатні для створення комп'ютерних мереж, і кабельну систему в такому випадку потрібно будувати заново [3].

Типова ієрархічна структура СКС (рис. 3.1) включає:

- горизонтальні підсистеми (у межах поверху);
- вертикальні підсистеми (усередині будинку);
- підсистему кампуса (у межах однієї території з декількома будинками).

Можна також доповнити список підсистем СКС ще підсистемами робочої групи й адміністративною підсистемою.

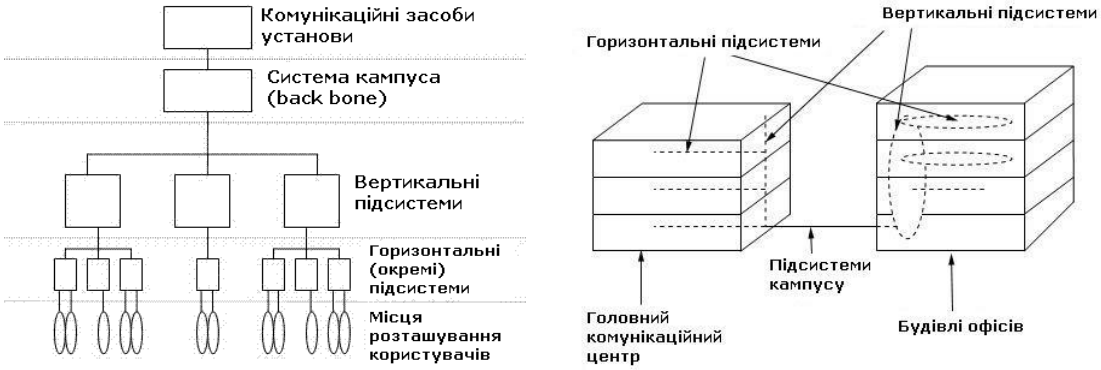


Рисунок 3.1 – Ієрархія СКС

Підсистеми робочої групи не завжди збігаються з горизонтальною підсистемою, особливо на об'єктах, що стрімко розвиваються та розбудовуються. А на проектування адміністративної підсистеми накладають свою специфіку деякі апаратні комплекси дистанційного керування, розмежування доступу, безпеки тощо, а також "погляди на життя" системних адміністраторів і керівників, що випадають із загальної ідеології проектування кабельних підсистем у рамках конкретного об'єкта. Практика показує, що якщо не виділити ці дві підсистеми із загального проекту, то процес ухвалення рішення замовником майже напевно затягнеться на невизначений термін.

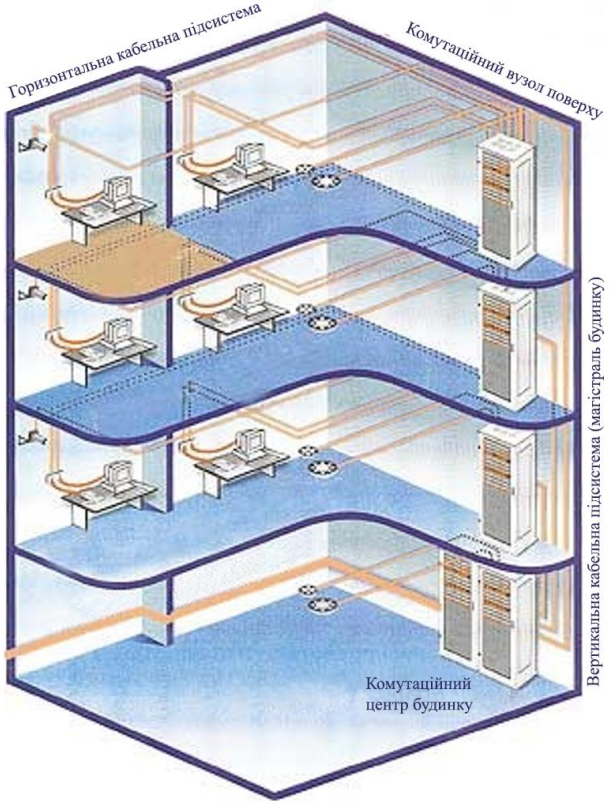


Рисунок 3.2 – Приклад типової схеми організації СКС

Горизонтальна підсистема з'єднує кросову шафу поверху з розетками користувачів. Підсистеми цього типу відповідають поверхам будинку. Вертикальна підсистема з'єднує кросові шафи кожного поверху із центральною апаратною будинку. Наступним кроком ієрархії є підсистема кампуса, яка з'єднує кілька будинків з головної апаратній усього кампуса. Ця частина кабельної системи звичайно називається магістраллю (backbone) або Basic Subsystem.

СКС дає можливість інтегрувати в одну кабельну систему ЛОМ, системи відеоспостереження і охоронно-пожежну сигналізацію, телефонні мережі, системи керування та диспетчерізації. СКС у порівнянні нестандартизованими та хаотично створюваними мережами має ряд переваг:

1. *Модульність структури*, що дозволяє швидко переходити на резервні лінії при позаштатних ситуаціях і забезпечує гнучкість у розміщенні обладнання.
2. *Універсальність.* СКС може стати єдиним середовищем для передачі комп'ютерних даних в ЛОМ, організації локальної телефонної мережі, передачі відеоінформації і навіть передачі даних і сигналів від датчиків пожежної безпеки або охоронних систем. Це дозволяє автоматизувати багато процесів контролю, моніторингу і керування господарськими службами та системами життєзабезпечення підприємства.
3. *Збільшення терміну служби*. Строк морального старіння добре структурованої кабельної системи може становити 10-15 років.
4. *Зменшення вартості додавання нових користувачів і зміни їх місць розміщення*. Відомо, що вартість кабельної системи є значною та визначається в основному не вартістю кабелю, а вартістю робіт з його прокладання. Тому більш вигідно провести однократну роботу із прокладки кабелю, можливо, з більшим запасом по довжині, ніж кілька раз виконувати прокладання, нарощуючи довжину кабелю. При такому підході всі роботи з додавання або переміщення користувача зводяться до підключення комп'ютера до вже наявної розетки.
5. *Можливість легкого розширення мережі*. СКС є модульної, тому її легко розширювати. Наприклад, до магістралі можна додати нову підмережу, ніяк не впливаючи на існуючі підмережі. Можна замінити в окремій підмережі тип кабелю незалежно від іншої частини мережі. СКС є основою для розподілу мережі на легко керовані логічні сегменти, тому що вона сама вже розділена на фізичні сегменти.

6. *Уніфікація.* СКС передбачає використання будь-якого стандартного мережного встаткування, одночасне використання декількох різнотипних мережних протоколів та дозволяє скоротити працезатрати на обслуговування завдяки простоті експлуатації й адміністрування.
7. *Стандартизація* та масове поширення СКС забезпечує зниження цін на конструктивні елементи й комплектуючі. Усі компоненти СКС відповідають міжнародним технічним стандартам (TIA/EIA-568-B1,TIA/EIA-568-B2,TIA/ EIA-568-B).

3.2. Вибір типу кабелю для підсистем

3.2.1 Горизонтальні підсистеми

Горизонтальна підсистема характеризується дуже більшою кількістю відгалужень кабелю (рис. 3.3), тому що його потрібно провести до кожної користувацької розетки, причому й у тих кімнатах, де комп'ютери в мережу поки не поєднуються.

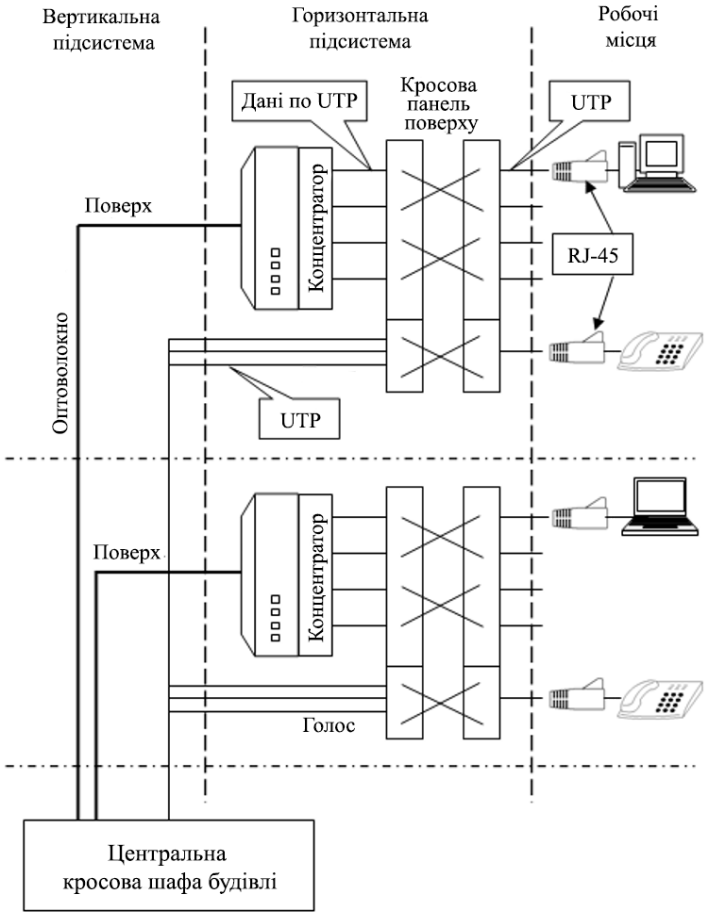


Рисунок 3.3 – Структура кабельної системи будинку

Тому до кабелю, що використовується в горизонтальній проводці, пред'являються підвищені вимоги до зручності виконання відгалужень, а також зручності його прокладки в приміщеннях. На поверсі звичайно встановлюється кросова панель, яка дозволяє за допомогою коротких відрізків кабелю, оснащеного розніманнями, провести перекомутацію з'єднань між користувацьким устаткуванням і концентраторами/комутаторами (рис. 3.4).

Рисунок 3.4 – Панелі горизонтальної підсистеми СКС

Синій колір гнучких кабелів передбачений системою адміністрування і означає підключення до портів СКС устаткування, що забезпечує роботу інформаційних додатків.

Підсистема робочої групи і адміністративна підсистема, як правило, є складовими частинами горизонтальної СКС. Залежно від характеристик об'єкта, на якому вона встановлюється (виробничий цех, поверх адміністративного будинку, спортивний стадіон, морський порт, виставковий павільйон тощо), цю підсистему доводиться проектувати з використанням оптоволокна, захищеної або незахищеної крученої пари. Звичайно застосовують кручену пару (найчастіше категорії 5) або волоконно-оптичний кабель.

Таблиця 3.1 – Хронологічна таблиця прийняття категорій СКС

Категорія СКС	*Діапазон частот*	*Застосунки, під які розроблялися категорії*	*Рік прийняття стандарту*
Категорія 3	16 МГц	Ethernet, 10 Base-T	1991
Категорія 4	20 МГц	Token Ring 16 МБіт/с	1993
Категорія 5	100 МГц	100Base-TX (Fast Ethernet)	1995

		ATM 155	
Категорія 5E	100 МГц	100Base-TX (Fast Ethernet) 1000Base-T (Gigabit Ethernet)	1999
Категорія 6	200 МГц	Gigabit Ethernet 1000Base-TX	2002

Для того, щоб кабельна підсистема 5-й категорії, зібрана на базі 4-х парних неекранованих кручених парах (а саме UTP кабель застосовується в даних підсистемах), працювала надійно, необхідно дотримуватися певних правил:

- у межах однієї горизонтальної підсистеми використовувати кабель однієї марки того самого виробника;
- уся підсистема повинна містити вироби тільки 5-й категорії (включаючи патч-панелі, розетки та роз'єми);
- горизонтальні кабелі повинні мати довжину порядку 90 метрів (стандарт IEEE 802.3 забороняє застосування кабелю довжиною більш 90 м);
- сполучні кабелі (кабелі, що прокладаються від розетки до мережного адаптера комп'ютера) не повинні мати довжину більш 10 метрів;
- загальна довжина горизонтального і сполучного кабелів не повинна перевищувати 100 метрів;
- загальна кількість репітерів у горизонтальній проводці не повинна перевищувати чотирьох пристроїв.

При виборі кабелю беруться до уваги також наступні характеристики: смуга пропущення, відстань, фізична захищеність, електромагнітна перешкодозахищеність, вартість. Крім того, при виборі кабелю потрібно враховувати, яка кабельна система вже встановлена на підприємстві, а також які тенденції й перспективи існують на ринку в цей момент.

3.2.2 Вертикальні підсистеми

Кабель вертикальної (або магістральної) підсистеми, яка з'єднує поверхи будинку повинен передавати дані на більші відстані і з більшою швидкістю в порівнянні з кабелем горизонтальної підсистеми. У минулому основним видом кабелю вертикальних підсистем був коаксіальний кабель. Тепер для цієї мети все частіше використовується оптоволоконний кабель.

Треба відзначити, що керування мережею є найбільше зручним на топологіях, що підтримуються UTP-кабелем, а товстий коаксіальний кабель на наших територіях застосовується настільки рідко, що про можливість його застосування проектувальники починають забувати. Щодо цього цікавий

північноамериканський регіон, де обсяги продажів товстого коаксіального кабелю та трансіверів до нього досить великі по теперішній час. Найбільш підходяща область застосування UTP-кабелів – кабельні підсистеми робочої групи, горизонтальні підсистеми будинків і вертикальні підсистеми (при використанні STP-кабелю). Тонкий коаксіальний кабель доцільно використовувати для організації магістралей у монтажних шафах, робочих груп у приміщеннях із твердою прив'язкою робочих місць, низькошвидкісних вертикальних кабельних підсистем. Оптоволоконний кабель – найкраще рішення для організації швидкісного середовища передачі даних вертикальної підсистеми, магістралі між комутаційними вузлами і між будинками (адміністративна та базова підсистеми). Товстий коаксіальний кабель сьогодні знаходить застосування дуже рідко тільки в окремих випадках: для організації низькошвидкісних магістралей між сусідніми будинками (до 500 м). При цьому його застосування нерідке визначається тим, що кабель " уже є" або навіть "раніше прокладений для інших цілей".

До складу структурованих кабельних систем входять спеціальні короби різного перерізу для укладання кабелю, фурнітура кріплення, розетки (комп'ютерні, телефонні, електроживлення), монтажні шафи, кросові або патч-панелі, забиті на кінцях коаксіальні, UTP і волоконно-оптичні кабелі різної довжини. При цьому топологія кабельної системи збирається тільки на кросовій панелі, дозволяючи організовувати в межах однієї крос-панелі різних топологій локальних мереж без зміни фізичної конфігурації кабелів.

Адміністративну підсистему, як правило, не виділяють у вигляді самостійної структури. З одного боку, це правильно, але часто її бажане позначити перед Замовником як окрему структуру. Адміністративна підсистема кабельного монтажу – це функціональна підсистема. Її призначення зв'язувати підсистеми робочих груп і горизонтальні підсистеми в єдине ціле. Вона повинна забезпечувати можливість установлення резервних зв'язків, підключення додаткових робочих місць і інших підсистем. Нерідко в рамках адміністративної підсистеми потрібна підтримка автономної системи енергопостачання, голосового та відео-зв’язку. Одно з основних вимог до адміністративної підсистеми – гнучкість і можливість збільшення потужності.

Базові підсистеми (кампуси) служать для об'єднання вертикальних або адміністративних підсистем один з одним. У цьому випадку найбільш виправданим є застосування оптоволокна. Багато компаній використовують для організації базових підсистем устаткування, що підтримує FDDI стандарт –

волоконний розподілений інтерфейс даних, що має продуктивність 100 Мбіт/сек і вище. Останнім часом, із твердженням стандарту на АТМ, у світі усе ширше починає застосовуватися цей тип устаткування.

3.2.3 Вимоги до системи кабельних каналів

Кабельні канали повинні відповідати міжнародним кабельним стандартам, керівництвам про інсталяцію СКС і методам побудови телекомунікаційних розподільних систем. перерізи кабельних трас повинні бути обрані з обліком 30% запасу на розвиток і переконфігурацію кабельної системи виходячи з максимальної кількості робочих місць із урахуванням зв'язків із кросовою АТС.

Вбудовані телекомунікаційні роз’єми СКС і розетки системи електроживлення розташовані уздовж зовнішньої стіни нижче робочої поверхні столів.

Кабель прокладається в коробах по периметру приміщення. Інформаційні і силові розетки монтуються в пластикові монтажні рамки, які можуть бути встановлені в ці короби. У приміщеннях, де пред'являються підвищені вимоги до дизайну, можливі інші рішення. Коридором основний потік кабелів прокладається у металевому лотку.

Рисунок 3.5 – Короба для прокладки крученої пари

Для забезпечення підключення інформаційних портів СКС до телефонної системи будинку від кожного центру комутації до кросового залу АТС повинна бути прокладена необхідна кількість N-парної крученому пари мінімум 3-їй категорії виходячи з умови: кількість пара з розрахунку максимальної кількості робочих місць – N/2. У кросовому залі АТС встановлюється шафа із кросом типу

KRONE. Комутація між панелями телефонної системи і панелями горизонтальної СКС проводиться шнурами з розніманнями RJ45-RJ45.

3.3. Рекомендації щодо вибору активного обладнання

Активне мережне встаткування, повинне задовольняти вимогам стандарту IEEE 802.x на локальні обчислювальні мережі заданої в технічному завданні технології.

Вимоги до активного мережного встаткування [4]:

- розширюваність;
- можливість встановлення пріоритетів і контроль смуги пропущення різного мережного трафіка для забезпечення безперебійної роботи мультисервісних додатків;
- підтримка програмних систем централізованого адміністрування мережі.
- локалізацію трафіка структурних підрозділів (відділів, підрозділів), розташованих у будь-якій частині ЛВС;
- підтримка автономних серверів (серверів робочих груп) і периферійних пристроїв (принтерів, плоттерів тощо);
- підключення серверів безпосередньо до ядра мережі для забезпечення найвищої продуктивності;
- можливість розподілу навантаження між компонентами ЛВС;
- масштабованість системи;
- гнучке керування ЛВС;
- доступ до ресурсів інтернету і організацію зовнішніх підключень.

Передбачити по можливості 15-25 % запас мережних портів для підключення додаткового встаткування і користувачів.

Для розміщення устаткування центрів комутації будинків використовувати комутаційні та серверні шафи (rack), які дозволяють:

- розміщати відповідне устаткування з урахуванням резерву;
- обмежувати доступ до устаткування;
- обслуговувати устаткування, встановлене в конструктив, з доступом не менш ніж із двох сторін конструктиву, а також можливістю змінювати напрямок відкривання двері;
- встановлювати устаткування, що обслуговує магістралі ЛВС.

3.4. Розробка фізичної схеми

Перш за все розглянемо локальні мережі Gigabit Ethernet – мережі третього покоління локальних мереж, відповідні до стандарту IEEE 802.3z. Цей стандарт доповнює стандарти IEEE 802.3 і IEEE 802.3u для мереж Ethernet (10 Mbps) і, відповідно, FastEthernet (100 Mbps) можливістю роботи на швидкості 1000 Mbps.

Gigabit Ethernet використовуються у якості магістральних мереж для з'єднання мереж FastEthernet і Ethernet. У мережах Gigabit Ethernet у якості середовищ передачі даних можуть використовуватися:

- 2 багатомодові оптоволокна (62,5/125 мкм) для коротких хвиль (специфікація 1000Base-sx). Слід зазначити, що звичайно може використовуватися й оптоволокно 50/125 мкм, але воно не передбачене в стандартах для Gigabit Ethernet;
- 2 одномодові або багатомодові оптоволокна (62,5/125 мкм) для довгих хвиль (специфікація 1000Base-lx);
- 2 пари коаксіального екранованого кабелю Jumper на 150 Ом (2х75 Ом) (специфікація 1000Base-cx);
- 4 пари скручених проводів UTP категорії 5 (специфікація 1000Base-T).

Для того щоб локальна мережа Gigabit Ethernet працювала нормально, необхідне виконання певних вимог, установлених стандартом IEEE 802.3z. Вимоги залежать від режиму роботи мережі. Мережі Gigabit Ethernet, як і мережі FastEthernet і Ethernet, можуть працювати як у напівдуплексному, так і в дуплексному режимі. Обмеження при роботі мереж Gigabit Ethernet у дуплексному режимі описані нижче.

Для середовища передачі даних ці умови наступні:

- використання в кожному домені колізій не більш одного повторювача. Той самий повторювач може з'єднувати середовища типів 1000Base-SX, 1000Base- SX, 1000Base-CX і 1000Base-T;
- максимально припустима довжина сегмента середовища;
- максимально припустимий діаметр одного домена колізій.

Деякі характеристики й обмеження стандартів по фізичній конфігурації мереж FastEthernet представлено в табл. 3.2 та 3.3.

Таблиця 3.2 – Характеристика сегментів середовища для Gigabit Ethernet

Тип сегмента середовища	*Підключень на один сегмент*	*Максимальна довжина одного сегмента, м*
1000Base-T	2	100

1000Base-cx	2	25
1000Base-sx, 1000Base-lx	2	316

Таблиця 3.3 – Максимальний діаметр одного домена колізій, м

Модель мережі	*Тип сегмента середовища*				
	T	*CX*	*SX/LX*	*T і SX/LX*	*CX і SX/LX*
Без повторювача	100	25	316	–	–
Один повторювач	200	50	220	210	220

Малий діаметр (до 220 м, залежно від використовуваного середовища одного домена колізій для мереж Gigabit Ethernet не становить великої проблеми, тому що кілька таких фрагментів мережі можуть бути з'єднані за допомогою мостів (комутаторів) або/і маршрутизаторів, розширюючи, таким чином, область охвату мережі в цілому. Кінцевим устаткуванням даних (КУД) може бути будь-яке джерело кадрів у мережі, тобто будь-яка складова, працює як мінімум до рівня даних мережної моделі OSI, у тому числі: міст (комутатор), маршрутизатор, шлюз, станція. Повторювачі працюють на фізичному рівні моделі OSI ISO і не є КУД.

Очевидно, правильність конфігурації мереж GigabitEthernet може бути визначена і на основі обчислення часу подвійного оберту сигналу між найбільш вилученими двома станціями (PDV), максимально припустиме значення якого становить 4096 bt. У цьому випадку можна не перевіряти виконання вимоги щодо використання не більш одного повторювача або вимоги відносно максимально припустимого діаметра одного домена колізій мережі.

У роботі передбачається практична перевірка виконання вимог стандартів щодо фізичної конфігурації мереж Gigabit Ethernet. На відміну від стандартів для мереж Ethernet, дані Комітету IEEE 802.3 щодо затримки сигналу складовими мереж GigabitEthernet зазначені без диференціації сегментів на ліві, праві або проміжні. Максимально припустиме значення PDV рівно 4096 bt. Рекомендується передбачити резерв в 32-40 bt. Резерв, рекомендований IEEE, рівний 32 bt. Дані щодо затримки сигналу середовищем, мережними адаптерами КУД і повторювачами, установлені стандартом IEEE 802.3z для мереж Gigabit Ethernet, представлено в табл. 3.4 і 3.5 відповідно.

Таблиця 3.4 – Подвійний час поширення сигналу по середовищу

Тип сегмента	*Затримка середовищем на 1 m, bt*
UTP кат. 5	11-12

1000Base-CX	10
1000Base-LX, 1000Base-SX	10

Таблиця 3.5 – Подвійна затримка сигналу адаптерами і повторювачем

Тип адаптерів	*Подвійна затримка, bt*
Адаптери двох КУД	864
Один повторювач	976

З метою визначення значення PDV для заданої пари станцій мережі, обчислюється час поширення сигналу по кожному сегменту середовища, а також затримка сигналу, викликана встаткуванням між цими станціями. Потім отримані значення складаються.

Значення PDV, для заданого домена колізій мережі Gigabit Ethernet, дорівнює значенню PDV для найбільш віддалених двох станцій. У деяких випадках не є очевидним, які це дві станції; тоді порівнюються значення PDV для відповідної множини пар станцій і в якості значення PDV береться найбільше з них.

Мережі Gigabit Ethernet можуть бути з'єднані з мережами Fastethernet і Ethernet за допомогою мостів (комутаторів) як на рис. 3.6. Така сумісність спрощує перехід від технологій Ethernet і FastEthernet до Gigabit Ethernet, дозволяє використання мереж Gigabit Ethernet у якості магістральних мереж для з'єднання мереж Ethernet і FastEthernet тощо.

З'єднання мереж Gigabit Ethernet з мережами FastEthernet і Ethernet за допомогою комутаторів Gigabit Ethernet можливо через те, що порти останніх можуть працювати, при необхідності, як на швидкості в 1000 Mbps, так і на швидкості в 100 Mbps або 10 Mbps. Таким чином, гібридна мережа Gigabit Ethernet/Fastethernet/Ethernet розділяється комутаторами на окремі домени колізій Gigabit Ethernet, FastEthernet і Ethernet. Для передачі даних між портом комутатора Gigabit Ethernet і відповідною станцією мережі FastEthernet або Ethernet, спочатку між ними узгоджується режим роботи. У результаті вибирається відповідна швидкість роботи в 1000 Mbps, 100 Mbps або 10 Mbps. Існують і мережні адаптери в складі станцій, які можуть працювати зі швидкістю в 1000 Mbps, 100 Mbps або 10 Mbps. Відповідні станції можуть працювати як у мережах Gigabit Ethernet, так і в мережах FastEthernet або/і Ethernet, по необхідності.

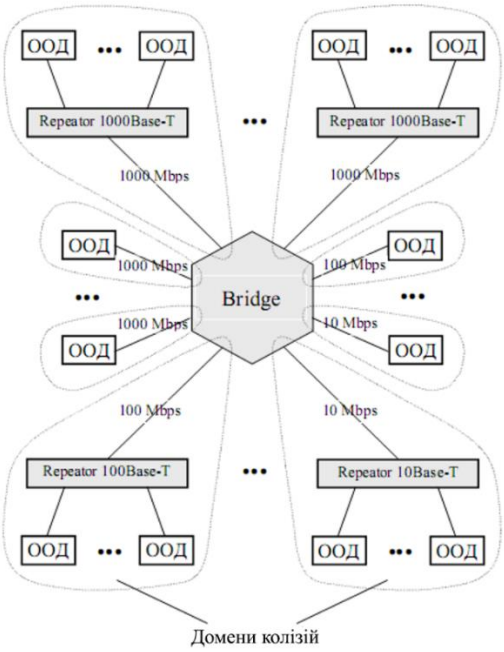


Рисунок 3.6 – З'єднання мостом доменів колізій зі швидкістю роботи в 1000, 100 і 10 Mbps.

Правильне фізичне конфігурування гібридних мереж Gigabit Ethernet/ FastEthernet/Ethernet полягає в дотриманні стандартів для кожного типу мереж окремо, як відносно сегментів середовища, так і відносно значення PDV та інших характеристик відповідно до стандартів. Таким чином, для перевірки правильності фізичної конфігурації гібридної мережі GigabitEthernet/FastEthernet/Ethernet, спочатку визначаються мережні фрагменти-домени колізій Gigabit Ethernet, FastEthernet і Ethernet; потім для кожного із цих фрагментів-доменів колізій окремо перевіряється виконання вимог відповідних стандартів.

При роботі в дуплексному режимі середовище є нерозділеним – кожен пристрій доступу до середовища використовує для передачі даних окремий канал і тому доменів колізій немає. Тому діаметр мережі не обмежений часом подвійного оберту сигналу між найбільш вилученими двома станціями мережі. Він обмежений лише максимально припустимими довжинами використовуваних сегментів середовища, виходячи з характеристик передачі сигналів [5].

Приклад фізичної схеми мережі наведений в додатку В.

3.5 Складання кошторису на кабелі та обладнання

У загальному кошторисі на кабелі та обладнання повинні бути враховані усі матеріали та активне/пасивне обладнання, що будуть використані при

побудові мережі. При цьому слід врахувати, що майже всі матеріали потребують запасу 10-15% від розрахункової кількості.

Приклад кошторису наведений у табл. 3.6.

Таблиця 3.6 – Кошторис на активне та пасивне обладнання

Тип	*Найменування*	*Одиниця виміру*	*Кількість*	*Ціна за одиницю*	*Вартість*
Пасивне	Чотирьох-парний кабель 1000BASE-T (CAT-5e)	бухта	12	715	8580
	Коннектор RJ-45	од.	500	0,6	300
	Оптоволоконний кабель 1000BASE-LX	м.	4110	41	168510
	Мережна розетка Hypernet MB-UTP1	од.	86	34	2924
	Короб 100x50 MK Premier NCT1050/D1	м.	430	267	114810
	Короб 16x16 MK Ega Mini (YT1/D1)	м.	100	33	3300
Активне	Маршрутизатор D-Link DSR-250	од.	1	3785	6140
	Комутатор D-link DGS-1210-52	од.	2	15000	30000
	Комутатор TP-Link TL-SG1048	од.	1	9315	9315
	Медіаконвертер TP-LINK MC220L	од.	2	621	1242
	Wi-Fi роутер TP-Link Archer C5	од.	1	2000	2000
	Wi-Fi роутер TP-Link Archer C7	од.	7	2800	19600
	Принтер Canon i-SENSYS MF237w	од.	8	6854	54832
	Робоча станція Lenovo V510z (10NH000VPB)	од.	70	17500	1225000
	Сервер HP ProLiant ML110 (794997-425) + 2 жорстких диски HP 6TB 7.2K 12G SAS LFF + 1 планка ОЗУ HP SmartMemory LRDIMM DDR4 2133MHz 32GB	од.	1	78033	78033
	NAS Qnap TS-228 + 2 жорстких диски WD Red WD60EFRX	од.	1	16402	16402
Усього					1738633

4. Програмне забезпечення та адміністрування мережі

4.1 Вибір мережевої операційної системи

Першим кроком із налаштування програмного оточення в локальній мережі є вибір операційної системи (ОС) – як для хостів, так й для серверу. І перш за все цей вибір повинен бути обумовлений вимогами цільового підприємства. Фактично, для ОС хостів існує лише три альтернативи – Windows, Linux та MacOS. І вибір між ними робиться з огляду на ПЗ, яке будуть використовувати працівники підприємства. Якщо їх рід діяльності вимагає певного ПЗ під певну платформу, то вже це є головним обмеженням та примушує вибирати цю певну платформу (та платити за неї). Якщо ж жорстких обмежень немає, то припустим є вибір безкоштовної альтернативи. Але тут треба керуватися здоровим глуздом та міркувати.

Наприклад, якщо проектується мережа ігрового інтернет-клубу, то найдешевшим рішення буде встановити на хости одну з багатьох версій Linux. Це забезпечить базову офісну функціональність через один з офісних пакетів та вихід до інтернету через численні браузери. Але якщо брати ігрову складову, то більшість сучасних ПК-ігор розроблено для платформи Windows, – і тому саме цю платформу доцільно обрати для клубу. Аналогічно й з випадками, коли робочий процес на підприємстві передбачає використання деякого специфічного програмного забезпечення –якщо воно вимагає конкретної ОС, то вибір очевидний. Звичайно, можна розглянути питання віртуалізації та запуск клієнтського софту у серверних контейнерах, але такий підхід вимагає більш складної ІТ-інфраструктури та виходить за рамки створення простої локальної мережі підприємства. Отже, при виборі ОС для хостів слід врахувати:

1) Основну предметну діяльність підприємства.
2) Потреби підприємства (або його окремих відділів) у спеціалізованих пакетах ПЗ.
3) Попередньо встановлене ПЗ, що поставляється вкупі із обладнанням.
4) Загальну вартість усіх копій ОС відповідно до розмірів підприємства.

Тепер можна перейти до вибори серверної ОС. І перше питання – а чи потрібний підприємству сервер взагалі? Питання виходу до інтернету для невеликого підприємства можна вирішити і без окремого проміжного серверу (див. пп.4.3). Якщо сервер все ж таки є необхідним (наприклад, для встановлення серверної частини деякого клієнтського ПЗ), то головні критерії вибору серверної ОС майже ідентичні критеріям вибору ОС для хосту (див. вище). Але

слід зазначити, що дуже важливо дотримуватися принципу «одна задача – один сервер». Тобто не слід купувати один дорогий потужний сервер і навішувати на нього абсолютно усі завдання – адміністрування, мережевий екран, обмін файлами, СКБД, спеціалізоване серверне ПЗ тощо. Бо у разі проблем із таким сервером будуть зупинені усі служби підприємства і більшість мережевої інфраструктури підприємства стане неробочою. Ця очевидна проблема централізації може бути вирішена шляхом встановлення не одного, а декількох серверів – хай менш потужних, але окремих.

Звичайно, принцип «одна задача – один сервер» на практиці є дуже затратним, але ніщо не заважає згрупувати основні функції між 2-3 серверами, і таким чином підвищити надійність інфраструктури. Причому на кожному сервері можуть бути встановлені різні ОС, кожна з яких є найбільш прийнятною для конкретних задач. Далі проведемо невеликий порівняльний аналіз основных сучасних серверних ОС (рис. 4.x).

Рисунок 4.1 – Основні серверні ОС

FreeBSD

Одна з найстаріших ОС з багатою історією. Але з кожним роком кількість користувачів цієї системою скорочується, хоча вона вважається однією з числа надійних і безпечних ОС. Є кілька причин падінь популярності даної ОС, головна з них - одна команда розробників і зовсім невелика кількість комерційного ПЗ для FreeBSD. Поточна версія системи успішно працює на безлічі процесорних архітектур і дає можливість для тонкої настройки ядра. До переваг FreeBSD потрібно віднести відмінну реалізацію роботи з пам'яттю, мережею і системою введення-виведення. Для установки програм необхідно використовувати порти (їх налічують близько 25000). На відміну від пакетів, вони мають відкритий вихідний код, який компілюється на ПК. Це не особливо зручно для звичайних користувачів, але має переваги для серверної ОС.

Windows Server

Найбільш поширена ОС для серверів підприємств. Комп'ютер, на якому встановлена така ОС, може виконувати ролі файлового сервера, сервера служби веб-додатків, сервера терміналів, поштового сервера, сервера віддаленого доступу, служби DNS (доменних імен), служби каталогів, сервера потоків мультимедіа тощо [6].

Windows Server є досить швидкою і надійною ОС. Надійність забезпечує платформа додатків, в яку вбудовані функції сервера додатків. Цю ОС досить просто розгорнути і проводити її адміністрування. Вона дає можливість управляти мережею за допомогою політик і автоматизації виконання будь-яких завдань.

Багато особливостей Windows Server надають можливість співробітникам організації працювати більш продуктивно. Файлові служби та служби друку дозволяють управляти файловими ресурсами. У той же час зберігається безпеку і доступ для користувачів. Служба каталогів (Active Directory, див. пп. 4.2) зберігає відомості про мережеві об'єкти і дозволяє адміністратору швидко знайти цю інформацію. Ця служба також спрощує роботу з проектування, розгортання та управління каталогами мережі.

До Windows Server 2012 на виділених серверах для управління доступом до файлів і папок використовувалася система Access Control List (ACL). Вона дозволяла давати доступ тільки на підставі облікових записів користувачів або членства користувача в групі. Щоб відкрити папку складався список груп або користувачів, які мають право доступу. Для того, щоб у користувача був доступ, він повинен бути включений в цей список або в групу, у якої є право доступу. В такій моделі присутні деякі недоліки:

1) Якщо є досить багато загальних ресурсів, то доведеться створити багато груп.
2) Не можна проконтролювати доступ з урахуванням будь-яких атрибутів користувача або характеристик пристрою, з якого здійснюється підключення, – досить членства користувача в певній групі.
3) Досить проблематично здійснити складні сценарії доступу – користувач може випадково викласти закриту інформацію в загальну папку, де кожен з членів групи може її прочитати.

Тому Windows Server 2012 з'явилася концепція Dynamic Access Control (DAC). Вона дозволяє управляти доступом до файлів і папок у всій мережі. DAC робить можливим управління доступом на підставі будь-якого атрибута або

критерію. За допомогою цієї концепції можна створювати правила доступу до даних, які проводять перевірку членства користувача в тих чи інших групах. Ці правила застосовні до будь-якого з серверів мережі в формі політик. Тим самим створюється загальна система безпеки.

Red Hat Enterprise Linux

Одна з найпопулярніших і затребуваних ОС. В основному система призначена для корпоративного використання, і відрізняється особливою надійністю і безпекою. Дану ОС використовують для розгортання важливих додатків на світових біржах, у фінансових установах, провідних телекомунікаційних компаніях, анімаційних студіях тощо. Основний недолік – ОС платна. Головна особливість – є комерційна підтримка дистрибутива. Періодичність виходу нових версій – 3 роки.

CentOS

Безкоштовний аналог Red Hat, який користується неабиякою популярністю. Кожна версія підтримується терміном на 10 років, релізи оновлюються з періодичністю в 6 місяців. Система вважається вільним і популярним аналогом RHEL. Відрізняється характерною стабільністю і може відмінно працювати на комп'ютерах з 64-бітної і 32-бітною архітектурою.

Число користувачів цієї ОС величезна, що дозволяє оперативно вирішувати всі виниклі проблеми і баги. Перевага – наявність безлічі форумів, де зможуть допомогти з питаннями про CentOS. До значних плюсів Centos можна також віднести дуже зручний і спритний менеджер пакетів yum, а мінусом вважають наявність не найостанніших версій супутнього програмного забезпечення в стандартних сховищах (репозиторіях) пакетів для Centos.

Debian

Є найбільш затребуваним дистрибутивом для серверного обладнання – ОС підтримує чималу кількість платформ, прекрасно справляється з функцією управління пакетами, має оперативну підтримку.

Дистрибутив Debian є одним з найстаріших і популярних дистрибутивів Linux. На ньому засновано чималу кількість інших дистрибутивів, в тому числі і Ubuntu. Основні причини популярності:

1) відкритий вихідний код і ширина вибору інструментів;
2) швидке і легке оновлення системи в кілька хвилин;

3) підтримка великої кількості процесорних архітектур;
4) Bug Tracking System з відправкою повідомлень на підтримку;
5) ефективна робота з пам'яттю в порівнянні з іншими ОС.
6) інтеграція пакетів;
7) легка установка і безкоштовна підтримка;
8) поліпшення безпеки ОС (наприклад, системи шифрування GPG);
9) стабільність роботи.

Слід зауважити, що багато (якщо не все) з цього переліку зараз можна віднести до будь-якого сучасного Linux-дистрибутива. Але саме Debian за роки існування зробив всі ці критерії обов'язковими вимогами до хорошого Linux-дистрибутива.

Ubuntu Server

Кодова база Ubuntu базується на Debian і не може існувати без неї. Спочатку вона планувалася як тимчасове відгалуження Debian, яке потім перетворилося в окрему операційну систему.

Ubuntu Server не володіє якоюсь особливою простотою і зручністю, в порівнянні з іншими серверними збірками. Особливості настільної версії, де упор йде на зручне графічне оточення, незастосовні до серверного варіанту. Серверна система має інші відмітні ознаки, і на сьогоднішній момент Ubuntu Server є не просто відгалуженням настільної гілки системи, а повноцінним серверним дистрибутивом рівня Enterprise. І підтверджуютmcz це такими ознаками [7]:

1) На базі Ubuntu Server будується і підтримується робота хмарної інфраструктури на основі технологій Openstack.
2) Компанія Canonical, розробник Ubuntu, розвиває і підтримує сумісність з сучасною системою оркестрації контейнерів Kubernetes, яку можна будувати на базі серверного дистрибутива. Так само приділяється пильна увага роботі контейнерів Docker, нові версії якої в першу чергу оптимізуються і тестуються під Ubuntu Server.
3) Йде активне впровадження Ubuntu в інтернет речей, для чого і була оголошена збільшена підтримка в 10 років для серверних версій – це актуально насамперед для інтернету речей.
4) Компанія Canonical забезпечує (за оплату) цілодобову технічну підтримку своєї системи і продуктів, заснованих на ній.

4.2 Стратегія адміністрування у мережі

Говорячи про стратегію адміністрування у мережі, перш за все слід зупинитися на принципах організації комп’ютерів в мережі. Розглянемо це питання стосовно ОС Windows, де такі принципи реалізуються за допомогою доменів, робочих і домашніх груп. Основна їх відмінність полягає в тому, як здійснюється управління комп'ютерами та іншими ресурсами.

Комп'ютери під керуванням Windows в мережі повинні бути частиною робочої групи або домену. Комп'ютери в домашній мережі також можуть бути частиною домашньої групи, але це не обов'язково. Комп'ютери в домашніх мережах зазвичай входять до складу робочих груп і, можливо, домашньої групи, а комп'ютери в мережах на робочих місцях – до складу доменів.

Особливості ***робочих груп***:

- всі комп'ютери є одноранговими вузлами мережі;
- жоден комп'ютер не може контролювати інший;
- на кожному комп'ютері знаходиться кілька облікових записів користувача;
- щоб увійти в систему будь-якого комп'ютера, що належить до робочої групи, необхідно мати на цьому комп'ютері обліковий запис;
- у складі робочої групи зазвичай налічується не більше двадцяти комп'ютерів;
- робоча група не захищена паролем;
- всі комп'ютери повинні перебувати в одній локальній мережі або підмережі.

Особливості ***домашньої групи***:

- комп'ютери в домашній мережі мають належати робочій групі, але вони також можуть складатися в домашній групі;
- за допомогою домашньої групи надавати доступ до документів і принтерів іншим користувачам набагато простіше;
- домашня група захищена паролем, але він вводиться тільки один раз при додаванні комп'ютера в домашню групу.

В ***домені***:

- один або кілька комп'ютерів є серверами;
- адміністратори мережі використовують сервери для контролю безпеки і дозволів для всіх комп'ютерів домену –

- це дозволяє легко змінювати налаштування, так як зміни автоматично виробляються для всіх комп'ютерів;
- користувачі домену повинні вказувати пароль або інші облікові дані під час входу до домену;
- якщо користувач має обліковий запис в домені, він може увійти в систему на будь-якому комп'ютері – для цього не потрібно мати обліковий запис на самому комп'ютері;
- права зміни параметрів комп'ютера можуть бути обмежені, так як адміністратори мережі хочуть бути впевнені в однаковості налаштувань комп'ютерів;
- в домені можуть бути тисячі комп'ютерів, при цьому вони можуть належати до різних локальних мереж.

Системні адміністратори використовують технологію Active Directory в Windows Server для зберігання та організації об'єктів в мережі в ієрархічну захищену логічну структуру, наприклад користувачів, комп'ютерів або інших фізичних ресурсів [8].

У Active Directory використовується наступна термінологія:

- ***сервер*** – комп'ютер, що виконує певні ролі в домені);
- ***контролер домену*** – сервер, який зберігає каталог та обслуговуючий запити користувачів до каталогу;
- ***домен*** – мінімальна структурна одиниця організації Active Directory, може складатися з користувачів, комп'ютерів, принтерів, інших загальних ресурсів;
- ***дерево доменів*** – ієрархічна система доменів, що має єдиний корінь – кореневої домен);
- ***ліс доменів*** – безліч дерев доменів, що знаходяться в різних формах довірчих відносин.

Ліс і домен складають основу логічної структури. Домени можуть бути структуровані в ліс, щоб забезпечити незалежність даних і сервісів (але не ізоляцію) і оптимізацію реплікації. Поділ логічних і фізичних структур поліпшує керованість системи і знижує адміністративні витрати, тому що на логічну структуру не впливають зміни в фізичному пристрої. Ліси, домени і організаційні одиниці (OU) складають основні елементи логічної структури Active Directory. Ліс визначає єдиний каталог і представляє кордон безпеки. Ліси містять домени (рис. 4.1).

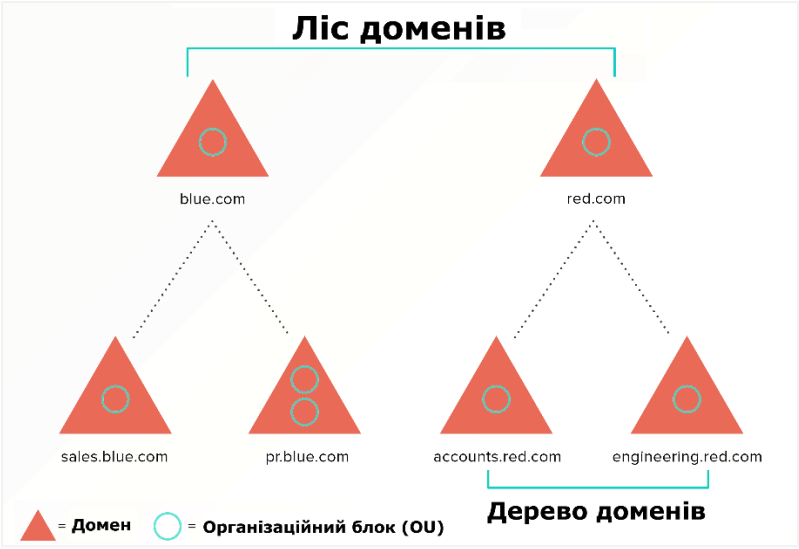


Рисунок 4.1 – Структурна організація Active Directory

Дані, що зберігаються в Active Directory, можуть надходити з різних джерел. З великою кількістю різних джерел даних і множиною різних типів даних Active Directory повинен використовувати деякий стандартизований механізм зберігання, щоб підтримувати цілісність інформації, що зберігається (рис. 4.2).

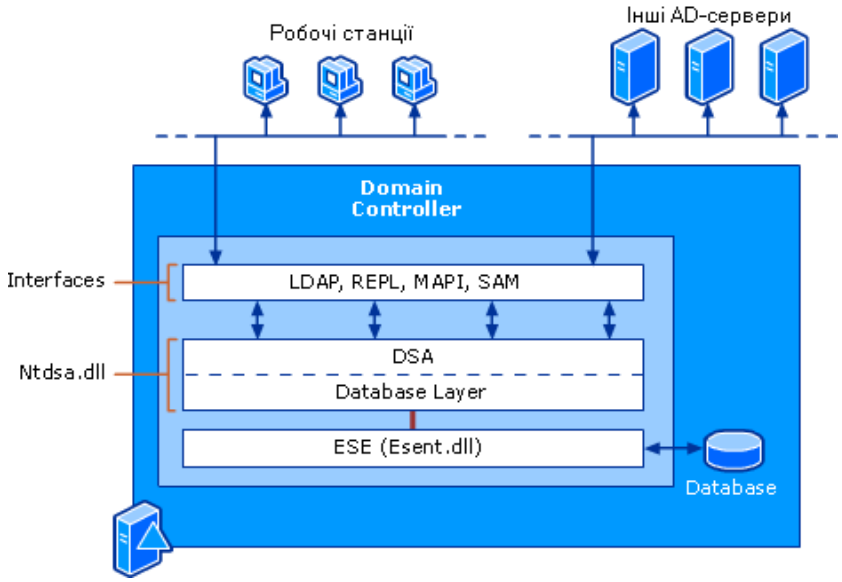


Рисунок 4.2 – Зберігання та доступ до даних на контролері домену

У Active Directory об'єкти використовують каталоги для зберігання інформації, всі об'єкти визначені в схемі. Визначення об'єктів містять інформацію, таку як тип даних і синтаксис, які каталог використовує, щоб гарантувати достовірність зберігання. Ніякі дані не можуть бути збережені в

каталозі, поки вони не визначені в схемі. Схема за замовчуванням містить всі визначення і опису об'єктів, які необхідні для коректної роботи Active Directory.

Сам каталог реалізується через фізичну структуру, що складається з бази даних, яка зберігається на всіх контролерах домену в лісі. Сховище Active Directory обробляє весь доступ до БД. Сховище даних складається з служб і фізичних файлів, які керують правами доступу, процесами читання і запису даних усередині бази даних на жорсткому диску кожного контролера (рис. 4.2).

Побудова структури домену повинна виконуватись відповідно до вимог підприємства, для якого проектується мережа. Важливо не перевантажити мережеву структуру надто дрібним підрозділом на окремі частини, бо в такому випадку адміністрування набуває зайвої складності. Домени потрібно використовувати лише там, де вони дійсно є необхідними.

4.3 Спільний доступ до зовнішніх мереж

Спільний доступ до інтернету в локальній мережі підприємства може бути організований за допомогою NAT/PAT або за допомогою проксі-сервера. Розглянемо обидва варіанти більш детально.

Технологія підміни мережевих адрес (Network Address Translation, NAT) передбачає передачу в зовнішнє середовище пакетів, IP-адреси яких відрізняються від діючих всередині мережі. Основними причинами використання NAT є дефіцит адрес у постачальника (за одним або кількома зовнішніми адресами може ховатися велика приватна мережа) і необхідність приховати структуру корпоративної мережі та інформацію про її трафіку.

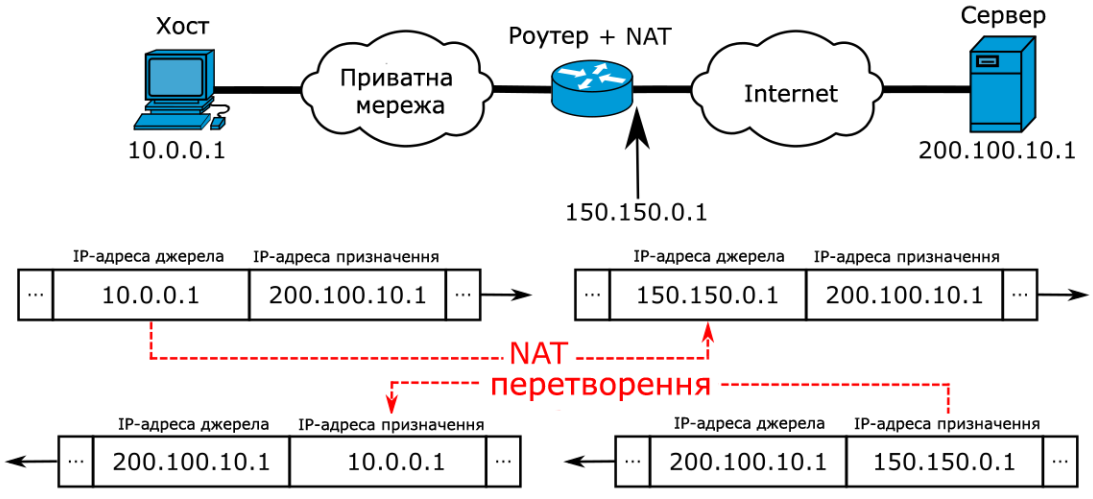
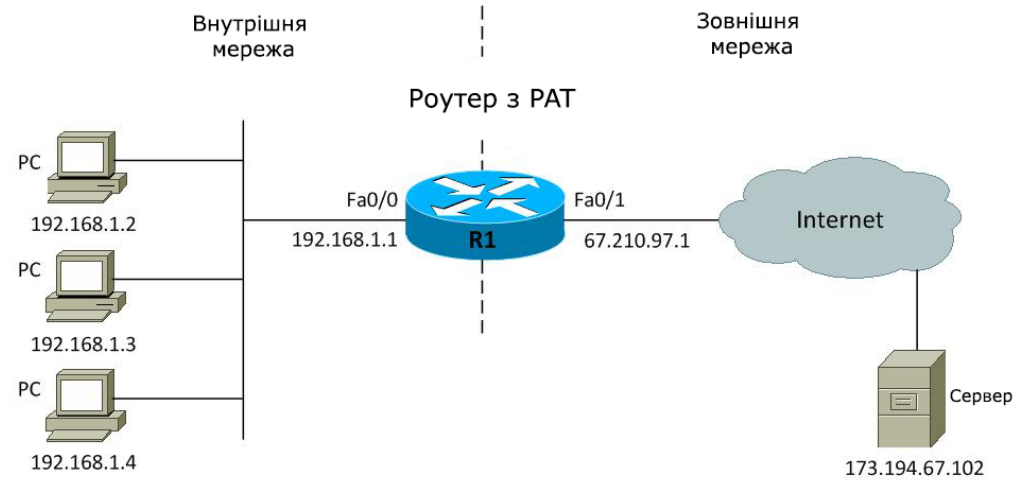


Рисунок 4.3 – Принцип роботи NAT

NAT-пристрій динамічно відображає набір приватних адрес на набір глобальних адрес, отриманих підприємством від постачальника послуг і привласнених зовнішньому інтерфейсу маршрутизатора підприємства (рис. 4.3).

Оголошення протоколів маршрутизації про зовнішні мережах «пропускаються» межовими маршрутизаторами у внутрішні мережі. Протилежне твердження є невірним – маршрутизатори зовнішніх мереж не отримують оголошень про внутрішні мережах, оголошення про них фільтруються при передачі на зовнішні інтерфейси.

При використанні базової трансляція мережевих адрес в кожен момент часу кількість внутрішніх вузлів, які отримують можливість взаємодіяти із зовнішньою мережею, обмежується кількістю адрес в глобальному наборі. При цьому приватні адреси деяких вузлів можуть відображатися на глобальні адреси статично (до вузлів можна звертатися ззовні, використовуючи закріплені глобальні адреси). Відповідність внутрішніх адрес зовнішнім задається таблицею, яку підтримує маршрутизатор або інший пристрій, на якому встановлено програмне забезпечення NAT.



Таблиця NAT-трансляції

Протокол	Внутрішній локальний IP: порт	Внутрішній глобальний IP: порт
ICMP	192.168.1.2 : 18	67.210.97.1 : 18
ICMP	192.168.1.3 : 19	67.210.97.1 : 19
ICMP	192.168.1.4 : 20	67.210.97.1 : 20

Рисунок 4.4 – Принцип роботи PAT

Окремим варіантом NAT є PAT (Port Address Translation), яка дозволяє всім вузлам внутрішньої мережі одночасно взаємодіяти із зовнішніми мережами, використовуючи єдиний зовнішній IP-адресу. Для ідентифікації відправника залучається додаткова інформація – при проходженні пакета з внутрішньої в зовнішню мережу кожній парі <приватна адреса; номер TCP-/UDP-порта

відправника> ставиться у відповідність пара <глобальний IP-адреса; призначений номер TCP-/UDP-порту>. Призначений номер порту обирається довільно, але повинен зберігатися принцип унікальності (рис. 4.4).

Ще одним способом організації виходу хостів внутрішньої мережі в зовнішню мережу (інтернет) є ***проксі-сервер*** – проміжний сервер, який фактично являє собою комплекс програм.

Спочатку клієнт підключається до проксі-сервера і запитує який-небудь ресурс, розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного серверу і отримує ресурс у нього, або повертає ресурс із власного кешу (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінені проксі-сервером в певних цілях. Варіанти розміщення проксі наведені на рис. 4.5.

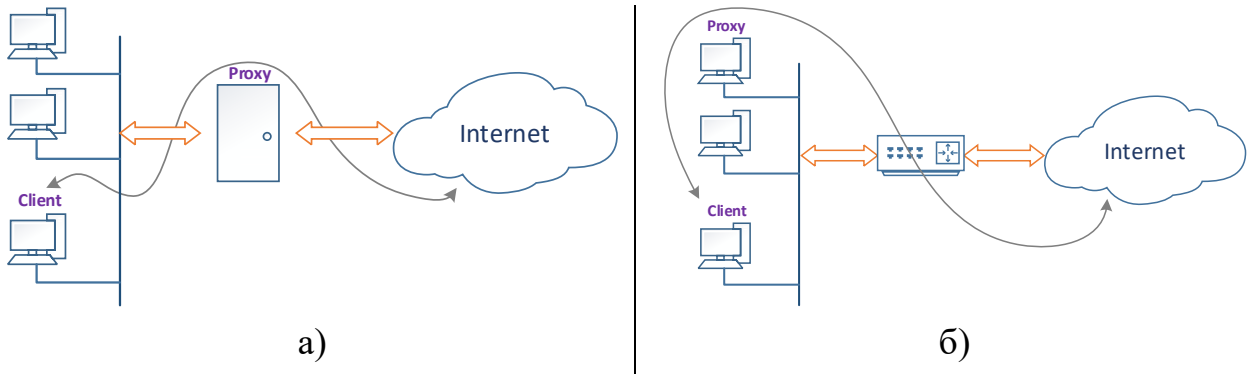


Рисунок 4.5 – Варіанти розміщення проксі: а) на сервері (мережевому екрані); б) на хості мережі

На сьогоднішній день проксі-сервери використовуються в основному для приховування реальної IP-адреси. Причин для цього може бути декілька. Найбільш популярні – необхідність відвідати сайт, доступ до якого заблокований для вашого IP, і необхідність анонімної відправки пошти. Додаткові переваги:

- захист мережі або локального комп'ютера від деяких видів мережевих атак і необхідність захисту конфіденційної інформації;
- обмеження доступу користувачів до деяких типів веб-ресурсів – використовується в компаніях, щоб запобігти нераціональному витрачанню робочого часу співробітниками;
- бажання підключити до інтернету кілька комп'ютерів при наявності однієї IP-адреси – налаштування можуть бути виконані таким чином,

що від зовнішніх хостів буде прихована інформація про локальні хости, бачити вони зможуть тільки посередника;

- потреба в економії споживаного трафіку – отримана з інтернету інформація буде передана користувачеві в компактному вигляді;
- необхідність зниження навантаження на інтернет-канал і забезпечення клієнтам оперативного доступу до інформації – для таких випадків виконується кешування файлів і їх подальше зберігання на проксі-сервері.

Розрізняють два основних види проксі:

1. *Прозорий* – схема зв'язку, що перенаправляє маршрутизатором частину трафіку (або весь) на проксі-сервер. Перевагою є можливість клієнта користуватися всіма перевагами проксі-сервера без виконання будь-яких налаштувань, але це ж є і недоліком, тому що позбавляє користувача вибору.
2. *Зворотний* – проксі-сервер, який, на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або кілька серверів, логічно розташованих у внутрішній мережі. Часто використовується для балансування мережного навантаження між декількома веб-серверами і підвищення їх безпеки, граючи при цьому роль брандмауера на прикладному рівні.

Найбільшу популярність проксі отримали в корпоративному сегменті – саме через них здійснюється вихід в онлайн-мережі з локальних мереж юридичних осіб. Причинами популярності в цьому випадку є:

- здійснюється повний контроль доступу, зручний облік трафіку, його фільтрація (у випадках інтеграції з антивірусами);
- можливість роботи з мінімальними правами на будь-якій ОС;
- відсутність виходу в інтернет за іншими протоколами значно підвищує безпеку обміну інформацією в корпоративній мережі.

Незважаючи на появу порівняно недорогих апаратних маршрутизаторів з функцією NAT, проксі-сервери продовжують переважати на підприємствах. В основному це пов'язано з тим, що маршрутизатори не в змозі забезпечити достатнього контролю над виходом до інтернету і фільтрації контенту.

Найбільш популярними сучасними програмними реалізаціями проксі є Shadowsocks (багатоплатформовий), 3proxy (багатоплатформовий), nginx (веб-сервер з режимом зворотного проксі). Актуальною тенденцією є також

винесення частини функціональності проксі за межі мережі за допомогою сторонніх сервісів з оплатою за передплатою.

4.4 Мережеві екрани та антивірусне програмне забезпечення

Комп'ютерна мережа від самого початку є системою, незахищеною і вразливою для зовнішніх атак. Щоб запобігти несанкціонованому доступу до апарата, який підключається до глобальної або приватної мережі, необхідно використовувати спеціальні засоби, звані Firewall (міжмережевий екран, брандмауер, шлюз безпеки) [9].

Існує кілька способів реалізацій міжмережевих екранів, основні з яких наведені на рис. 4.6.

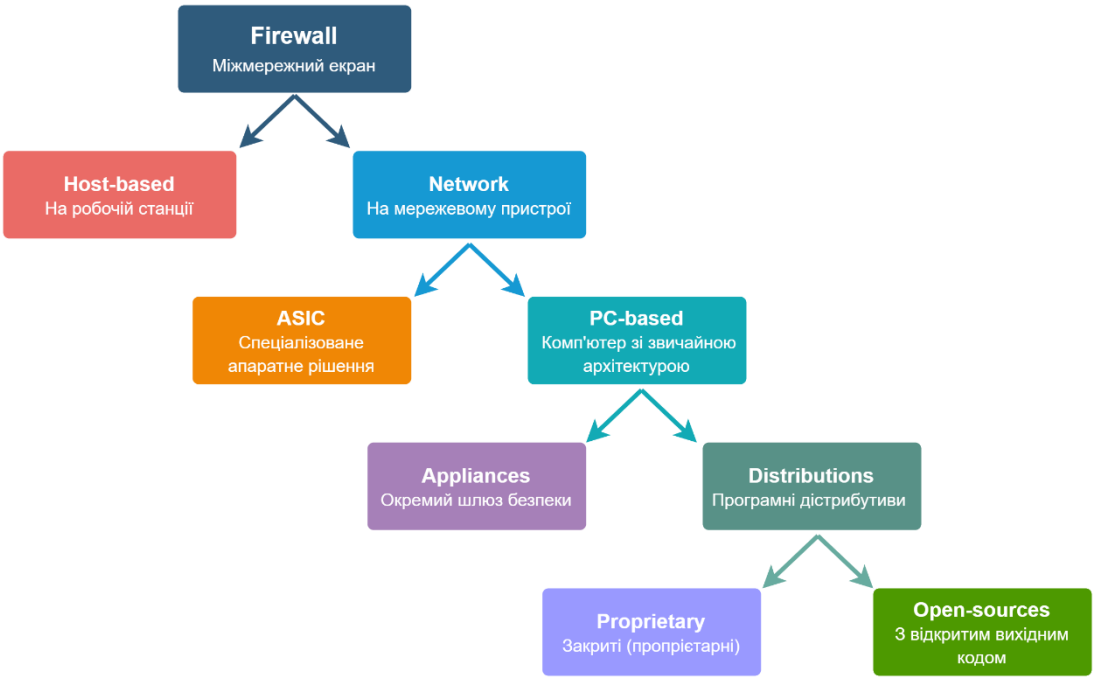


Рисунок 4.6 – Способи реалізації міжмережевих екранів (firewalls)

Host-based-екран встановлюється безпосередньо на клієнтську машину (поверх існуючої ОС) і захищає виключно одну цю машину. Це може бути корисно в домашніх умовах (особливо, якщо це всього один комп'ютер і він безпосередньо підключений до модему) або в мережевому оточенні, як додатковий засіб безпеки [10].

Network-екран захищає всю мережу і зазвичай служить шлюзом для цієї мережі. Мережа може складатися як з одного комп'ютера, так і з багатьох тисяч. Тип екрану вибирається залежно від мережевого середовища та потреб.

Network-екрани, в свою чергу, поділяються на два види – PC-based (засновані на комп'ютері із звичайною архітектурою) і ASIC-рішення. Під ASIC (application-specific integrated circuit) маються на увазі машини, в яких основна функціональність екрану реалізована на апаратному рівні. Як правило, це дуже дорогі системи, вартість яких часто доходить до декількох десятків і навіть сотень тисяч доларів. Використовуються зазвичай в ISP-подібних організаціях, яким потрібна дуже висока пропускна здатність.

Всі інші екрани є PC-based, які знову поділяються на дистрибутиви і коробкові рішення (appliances).

Переваги дистрибутивів:

1. *Дешевизна* – залежно від ситуації, в наявності вже може бути потрібне залізо, яке можна виділити під firewall.
2. *Універсальність* – можна купити сервер/комп'ютер, великий чи маленький на вибір, наприклад, за відносно дешевою ціною.
3. *Гнучкість* – в цей сервер можна додати кілька мережевих карток, або поставити ОС на RAID масив тощо.
4. *Мобільність* – якщо знадобиться, можна перенести або перевстановити ПО на інший сервер.
5. *Незалежність* – всі технічні характеристики сервера відомі і доступні для апгрейду незалежно від постачальника.

Переваги коробкових рішень:

1. Менше проблем при виборі обладнання, особливо при спробі осягнути неосяжне і прорахувати вперед зростання підприємства, обсяг трафіку тощо. Фахівці постачальника, як правило, можуть підказати який саме прилад з їх асортименту слід брати, і часто будуть праві.
2. Не все обладнання підтримується всіма збірками, часто софт жорстко обрізається для досягнення кращих показників швидкості. При установці ПЗ на новий сервер, можна потрапити в ситуацію, коли обладнання однозначно не підтримується дистрибутивом. Причому передбачити таку ситуацію заздалегідь досить важко.
3. Зазвичай такі рішення мають "правильну" форму, тобто маленькі акуратні коробки (рис. 4.7а) або 1U rackmounts під серверну стійку (рис. 4.7б).

а) б)

Рисунок 4.7 – Приклади коробочних рішень міжмережевих екранів Cisco

4. Як правило, вони вже підігнані під певні категорії використання, тобто CPU, RAM, HD будуть підходити під певні потреби, а за кількістю мережевих інтерфейсів вони будуть перевершувати стандартні 1U-сервера.
5. Підтримуються як appliance, тобто одна адреса підтримки і для обладнання, і для ПЗ, плюс жодних проблем з установкою ПЗ.

Дистрибутиви діляться на 2 види: з відкритим кодом і пропрієтарні.

Відкриті екрани жодним чином не поступаються за якістю своїм закритим товаришам. Навіть не будучи програмістом, можна вирішити багато проблем, бо на форумах є досить людей, які з радістю допоможуть, аж до того, що можуть навіть написати невеликі патчі. Також у відкритому вихідному коді можна завжди подивитися в код і спробувати зрозуміти, що і як працює. Це часто допомагає при вирішенні проблем.

З іншого боку, постачальник закритого ПЗ надає підтримку (за чималі гроші, звичайно) і спеціально навчені професіонали допоможуть вирішити будь-яку проблему. Звичайно, такий вид підтримки існує і в відкритому ПО, але там, як правило, люди намагаються впоратися самі.

Ще із сучасних тенденцій в розвитку екранів слід зазначити такі:

1. Уніфіковане управління погрозами *(***Unified Threat Management, UTM***)*. По суті, це той же PC-based firewall, тільки оброслий додатковою функціональністю. Сюди додають як стандартні функції екрану: IDS/IPS, VPN, load-balancing, routing, так і інші – content filtering, antivirus, anti-spam тощо. Зазвичай тільки невеликі організації з маленьким бюджетом користуються UTM. Фахівці настійно рекомендують все-таки розділяти і ставити хост з функціональністю UTM за екраном.
2. **IDS/IPS –** щось схоже на аналізатора трафіку, що працює на основі бази підписів і намагається виявити аномалії. IDS (intrusion detection system)

намагається їх знайти, в той час як IPS (intrusion prevention system) намагається їх ще й зупинити. Багато екрани сьогодні мають цю функціональність вбудованої або ж додають її як пакет.

3. IDS/IPS не ідеальні, бо не розуміють протоколів, тому для більш серйозного захисту використовується **Layer 7 firewall**. Як правило, мається на більшості екранів. Варто зауважити, що і IDS/IPS і Layer 7 firewall досить ненажерливі в плані CPU і RAM.
4. **Відхід від універсального сервера**, у якого в наявності і екран, і пошта, і FTP, і файлосховище, і ще купа речей. Незважаючи на неймовірну зручність такої багатої функціональності, користуватися ним вкрай не рекомендується, бо в плані безпеки - це просто одна велика діра.
5. **Надлишок функцій** –більшість екранів намагаються включити в себе всілякі доповнення та розширення, і при правильному маркетингу це звучить красиво. Тому завжди бажано зрозуміти – що потрібно, що пропонують і почитати докладніше про кожну функції, щоб не потрапляти на вудку і не платити за те, що ніколи не буде використано.

Серед найбільш популярних сучасних дистрибутивів необхідно відзначити pfSense, IPFire, ClearOS.

Окрім встановлення міжмережевого екрану для всієї мережи, ще одним стандартом корпоративної безпеки є використанні антивірусного ПЗ безпосередньо на клієнтських машинах. Якими б суворими не були вимоги безпеки, працівники все одно будуть користуватися USB-накопичувачами, завантажувати підозрілі файли з електронної пошти тощо. Отже, антивірусні засоби на кінцевому пристрої мережі є обов’язковими

Кількість і різноманіття вірусів постійно зростає, і для того, щоб швидко і ефективно їх виявити, антивірусне ПЗ повинне відповідати таким параметрам:

1) *Стабільність і надійність роботи* – цей параметр, без сумніву, є визначним; навіть найкращий антивірус виявиться абсолютно марним, якщо він не зможе нормально функціонувати на комп'ютері, та в результаті будь-якого збою в роботі програми процес сканування носіїв інформації не пройде до кінця; так, завжди є ймовірність того, що деяка кількість заражених файлів залишиться непоміченою;
2) *Навантаження на систему* – якщо фонове функціонування антивірусного ПЗ буд перевантажувати систему та заважати працювати, то такий антивірус просто будуть відключати; крім того, для мобільних

пристроїв, високе навантаження на систему призведе до швидкого розрядження батареї.

3) *Розміри вірусної бази програми* – з урахуванням постійної появи нових вірусів база даних повинна регулярно оновлюватися, адже у програмі, що не розпізнає нових вірусів, немає сенсу.
4) *Використання евристичних методів* – використання набору правил, які застосовуються для виявлення дій шкідливого ПЗ без необхідності визначення конкретної загрози, на відміну від класичного виявлення на основі сигнатур; перевагою цієї моделі є можливість виявлення не тільки варіантів існуючого шкідливого ПЗ, але й раніше невідомих вірусів.

Рисунок 4.8 – Результати незалежного тестування антивірусного ПЗ в лютому 2020 р. [11]

Докладний огляд антивірусного ПЗ та вибір конкретного рішення виходить за рамки курсового проекту. Треба лише знати, що незалежні організації (AV-TEST, Virus Bulletin тощо) проводять періодичні докладні тестування найпопулярніших антивирусів, які оприлюднюються на відповідних сайтах (рис. 48).

Отже при виборі антивірусного ПЗ для клієнтів локальної мережі, можна спиратися на результати таких тестувань та не забувати про питання ціни – при виборі платного антивірусу, загальна вартість необхідної кількості копій може досягати досить значних сум відносно загальної вартості всього програмного забезпечення мережі.

4.5 Організація зберігання даних та резервне копіювання

Задачу зберігання даних в локальній мережі можна вирішити декількома способами. На рис. 4.9 наведені три основні технології (DAS, NAS, SAN), які відрізняються складністю реалізації, надійністю результату та загальним масштабом цільової локальної мережі [12].

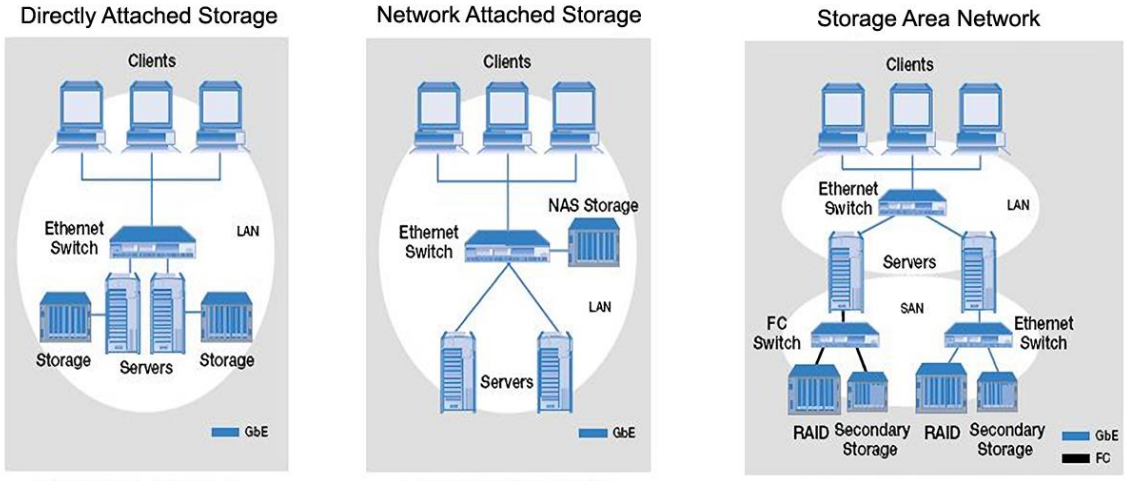


Рисунок 4.9 – Наочне порівняння DAS, NAS та SAN

DAS (Directly Attached Storage) – пристрої зберігання підключаються безпосередньо до серверу (чи робочих станцій). Фактично, реалізує прямі запити введення виведення (рис. 4.10). Приклад – вбудовані жорсткі диски серверу.

NAS (Network Attached Storage) – втілює окремий пристрій, що містить вбудовану логіку (повноцінну платформу із ОС) та масив жорстких дисків (рис. 4.11). Підключається безпосередньо до мережевого комутатора, підтримує декілька протоколів передачі даних (CIFS, NFS тощо) то налаштування

дискового масиву в форматі різних типів RAID. Сучасні NAS-пристрої є повноцінними серверами, орієнтованими перш за все на зберігання спільних даних, але підтримують багато додаткових функцій.

SAN (Storage Area Network) – передбачає розгортання окремої мережі для апаратно-програмного забезпечення систем зберігання даних. Монтується до серверів базової мережі за допомогою iSCSI або Fiber Channel (рис. 4.12). Протоколи дозволяють системі бачити увесь доступний простір як локальне сховище, тим самим дозволяючи більшості програм використовувати його належним чином.

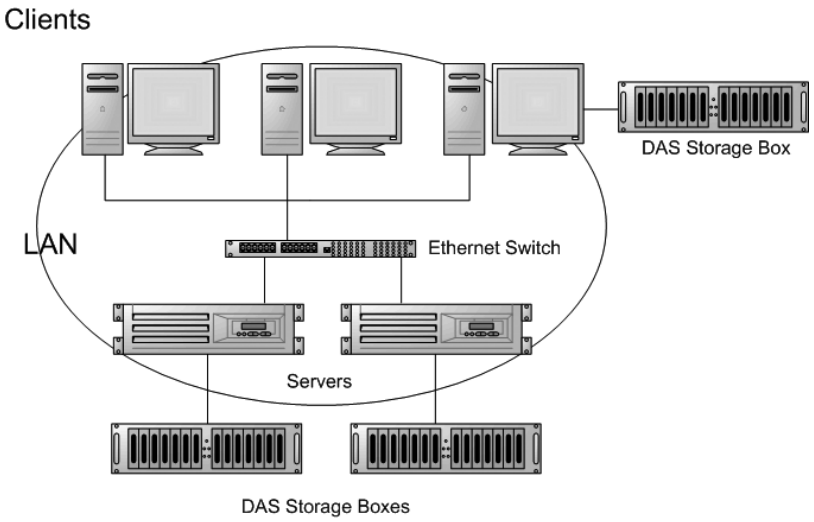


Рисунок 4.10 – Технологія DAS (Directly Attached Storage)

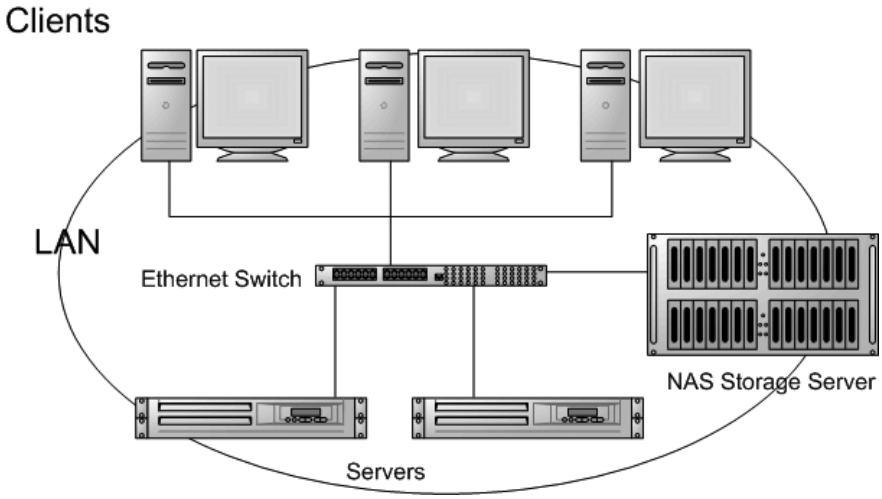


Рисунок 4.11 – Технологія NAS (Network Attached Storage)

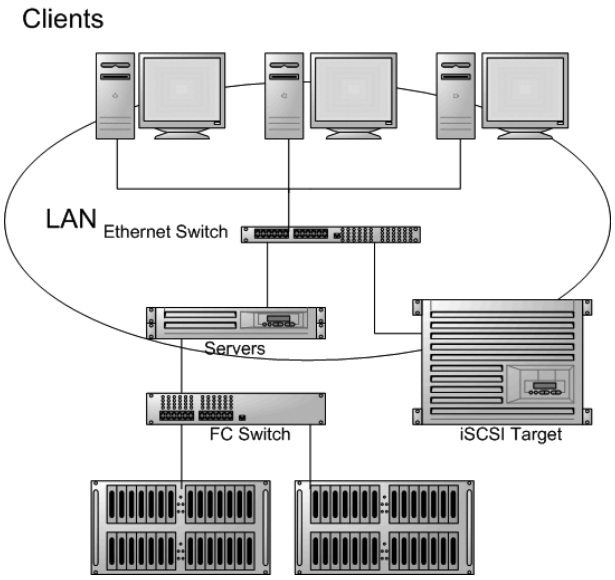


Рисунок 4.12 – Технологія SAN (Storage Area Network)

Усі ці технології зберігання передбачають різну логіку роботи із даними та файловою системою. Відмінності наочно наведені на рис. 4.13.

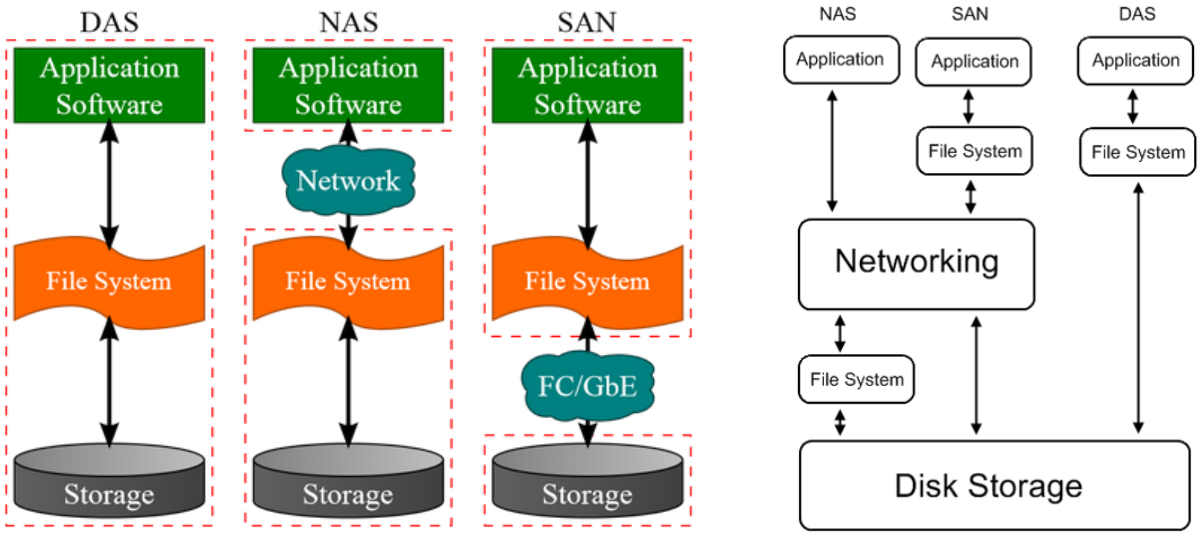


Рисунок 4.13 – Логіка роботи DAS, NAS та SAN із файловою системою

Технічні завдання до КП передбачають проектування малих та середніх за розміром локальних мереж та не мають космічного бюджету, то більш докладно зупинимося на двох перших технологіях.

Окремий дата сервер (DAS)

У разі вибору варіанту із сервером, то перш за все необхідно забезпечити універсальну доступність даних та їх надійне зберігання. І якщо проста

доступність зазвичай забезпечуються засобами мережевої ОС, то забезпечення надійності треба починати із апаратного рівня. Найчастіше за це відповідає технологія RAID (Redundant Array of Independent Disks) – віртуалізації даних, яка об'єднує кілька дисків в логічний елемент для надійності збереження інформації та підвищення продуктивності накопичувачів.

Існують сім базових рівнів RAID, які є стандартизованими (рис. 4.14-4.15). Кожен з чотирьох основних рівнів RAID використовує унікальний метод запису даних на диски, і тому всі рівні забезпечують різні переваги. Рівні RAID 1,3 і 5 забезпечують дублювання даних або зберігання бітів парності; і тому дозволяють відновити інформацію у разі збою одного з дисків. Розглянемо кожен з рівнів більш докладно.

RAID-0 (striping, чередування) – дисковий масив з двох або більше жорстких дисків без резервування. Інформація розбивається на блоки даних фіксованої довжини і записується на обидва / декілька дисків по черзі, тобто один блок на перший диск, а другий блок на другий диск відповідно. Перевага – швидкість зчитування файлів збільшується в *n* раз, де *n* – кількість дисків. При цьому така оптимальна продуктивність досягається тільки для великих запитів, коли фрагменти файлу знаходяться на кожному з дисків. Недолік – збільшується ймовірність втрати даних.

RAID 1 (mirroring, віддзеркалення) – масив з двох (або більше) дисків, які є повними копіями один одного. Переваги:

1) Забезпечує прийнятну швидкість запису і виграш по швидкості читання при розпаралелювання запитів.
2) Має високу надійність -–працює доти, поки функціонує хоча б один диск в масиві. При виході з ладу одного з дисків слід терміново вживати заходів та відновлювати надмірність.

Недолік – за ціною двох (і більше) жорстких дисків користувач фактично отримує обсяг лише одного.

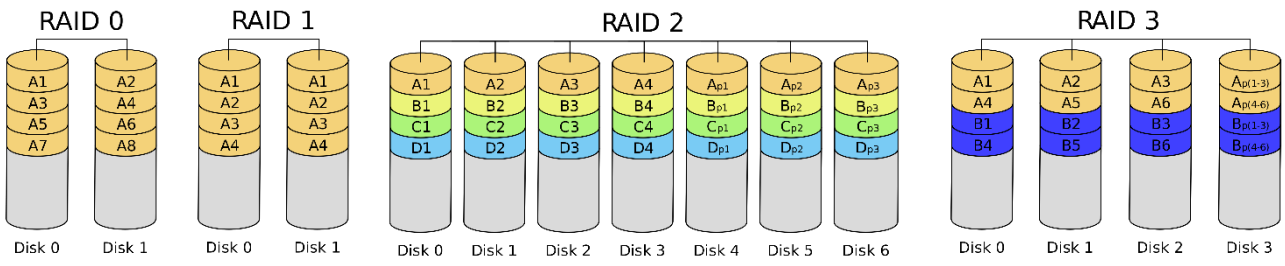


Рисунок 4.14 – Рівні RAID 0 – 3

RAID-2 – засновані на використанні коду Хеммінга. Диски діляться на дві групи: для даних і для кодів корекції помилок, причому якщо дані зберігаються на 2^n-n-1 дисках, то для зберігання кодів корекції необхідно n дисків. Сумарна кількість дисків при цьому буде дорівнювати 2^n-1. Дані розподіляються по дискам, призначеним для зберігання інформації, так само, як і в RAID 0, тобто вони розбиваються на невеликі блоки по числу дисків. Решта дисків зберігають коди корекції помилок, за якими в разі виходу будь-якого жорсткого диска з ладу можливі корекція або відновлення інформації. Перевагою є підвищення швидкості дискових операцій в порівнянні з продуктивністю одного диска та можливість відновлення даних. Недоліком є те, що мінімальна кількість дисків, при якому має сенс його використовувати – 7, тільки починаючи з цієї кількості для нього потрібно менше дисків, ніж для RAID 1 (4 диска з даними, 3 диска з кодами корекції помилок), в подальшому надмірність зменшується по експоненті.

RAID 3 – n дисків дані розбиваються на шматки розміром менше сектора (розбиваються на байти або блоки) і розподіляються по n-1 дискам. Ще один диск використовується для зберігання блоків парності. У RAID 2 для цієї мети застосовувався n-1 диск, але інформація на контрольних дисках призначався для корекції помилок «на льоту», в той же час більшість користувачів влаштовує просте відновлення інформації в разі її пошкодження, для чого вистачає даних, що вміщується на одному виділеному диску. Переваги – висока швидкість читання/запису даних та відносна відмовостійкість. Недоліки:

1) Підходить тільки для роботи з великими файлами (час доступу до окремого сектору, дорівнює максимальному з інтервалів доступу до секторів кожного з дисків).
2) Велике навантаження на контрольний диск, і, як наслідок, його надійність сильно падає в порівнянні з дисками, що зберігають дані.

Мінімальна кількість дисків для створення масиву дорівнює трьом.

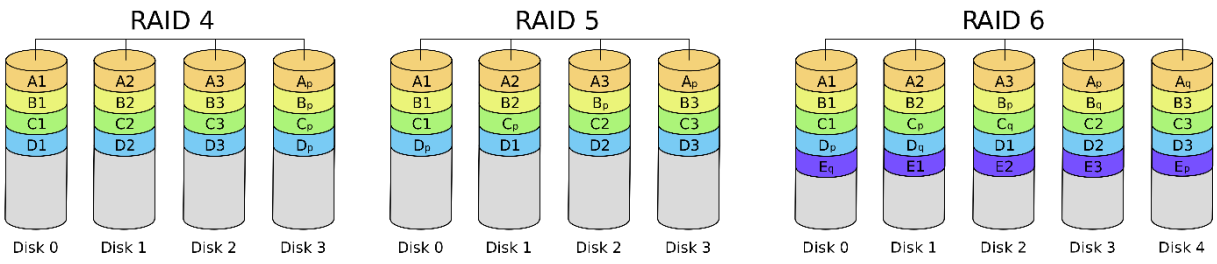


Рисунок 4.15 – Рівні RAID 4 – 6

RAID 4 – схожий на RAID 3, але відрізняється від нього тим, що дані розбиваються на блоки, а не на байти. Таким чином вдалося подолати проблему низької швидкості передачі даних невеликого обсягу. Запис же проводиться повільно через те, що парність для блоку генерується під час запису і записується на єдиний диск.

RAID 5 – виправляє недолік RAID 2-4: неможливість паралельних операцій запису, бо для зберігання інформації про парність використовується окремий диск. В RAID 5 блоки даних і контрольні суми циклічно записуються на всі диски масиву, немає асиметричності конфігурації дисків.

Під контрольними сумами мається на увазі результат операції XOR (виключаюче або). Операція має особливість, яка дає можливість замінити будь-який операнд результатом, і, застосувавши алгоритм xor, отримати в результаті якого бракує операнд.

Наприклад: *a xor b = c* (де *a, b, c* – три диска рейд-масиву). В разі якщо *a* відмовить, можна відновити його, поставивши на його місце *c* і провівши xor між *c* і *b*: *c xor b = a*. Це може бути застосовано незалежно від кількості операндів: *a xor b xor c xor d = e*. Якщо відмовляє *c*, тоді *e* встає на його місце і, провівши xor, в результаті отримуємо *c*: *a xor b xor e xor d = c*.

Для зберігання результату xor потрібно всього один диск, розмір якого дорівнює розміру будь-якого іншого диска в RAID. Мінімальна кількість необхідних дисків дорівнює трьом.

Переваги:

1) Економічність – обсяг дискового масиву розраховується за формулою (n-1) * hddsize, тобто «загубиться» всього 25% проти 50% RAID 10. При цьому зі збільшенням кількості дисків в масиві економія продовжує збільшуватися.
2) Забезпечує високу швидкість читання – виграш досягається за рахунок незалежних паралельних потоків даних з декількох дисків масиву.

Недоліки:

1) Продуктивність на операціях типу Random Write (записи в довільному порядку) падає на 10-25% від RAID 0, так як вимагає більшої кількості операцій з дисками (кожна операція запису замінюється на контролері RAID на чотири – дві операції читання і дві операції запису).
2) При виході з ладу одного диска надійність відразу знижується до рівня RAID 0 з відповідною кількістю дисків.

3) Для повернення масиву до нормальної роботи потрібен тривалий процес відновлення, пов'язаний з відчутною втратою продуктивності і підвищеним ризиком. В ході відновлення здійснюється тривале інтенсивне читання, яке може спровокувати вихід з ладу ще одного або декількох дисків масиву.
4) В процесі читання можуть виявлятися раніше не виявлені збої читання в масивах cold data, що перешкоджають відновленню. Якщо до повного відновлення масиву відбудеться вихід з ладу або виникне помилка читання хоча б на ще одному диску, то масив руйнується і дані на ньому відновленню звичайними методами не підлягають.

RAID 6 – схожий на RAID 5, але має більш високу ступінь надійності: два (або більше) диска даних і два диска контролю парності. Заснований на кодах Ріда-Соломона і забезпечує працездатність після одночасного виходу з ладу будь-яких двох дисків. Використання RAID 6 викликає приблизно 10-15% падіння продуктивності відносно RAID 5, що викликано великим обсягом роботи для контролера (більш складний алгоритм розрахунку контрольних сум), а також необхідністю читати і перезаписувати більше дискових блоків під час запису кожного блоку.

Існують також комбіновані варіанти RAID. Наприклад, RAID 1+0 та RAID 0+1, рис. 4.16. Усі вони є поєднаннями базових рівнів між собою.

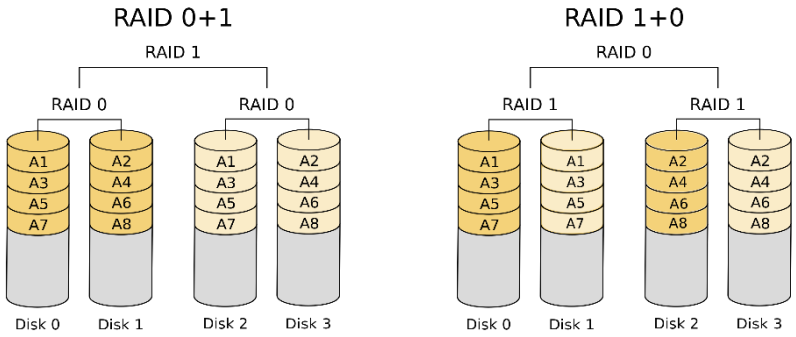


Рисунок 4.16 – Рівні RAID 0+1 та 1+0

З огляду на значне здешевлення жорстких дисків, масив рівня RAID 1 фактично є стандартом де-факто для сервері. А якщо у якості накопичувачів використати SSD-диски (та ще й об’єднати їх в RAID-масив!), то це значно підвищить і надійність, і швидкість дискової системи.

Окремий спеціалізований пристрій (NAS)

NAS (Network Attached Storage, мережевий накопичувач) є сукупністю носія інформації великого обсягу і спеціальної апаратної платформи, що дозволяє підключити цей носій до локальної мережі.

Сучасні NAS використовують в якості носія інформації жорсткі диски в силу їх порівняно великих (щодо інших технологій зберігання інформації) доступних ємностей при низькій вартості зберігання за одиницю об'єму. Все частіше зустрічаються рішення на основі SSD з набагато більше швидкістю і, відповідно, ціною. Але слід враховувати, що величезні швидкості SSD можуть обмежуватися фіксованою пропускною спроможністю мережі, і тоді весь потенціал швидкості SSD не буде розкритий.

Ключовою відмінністю NAS від звичайних файлових серверів на основі ПК є оптимізація апаратної платформи і вбудованої ОС під завдання мережевого зберігання даних і управління дисковими масивами.

Всі сучасні NAS мають спеціалізовану систему управління з наочним графічним користувацьким інтерфейсом, яка розміщена у внутрішній пам'яті платформи і в багатьох випадках незалежна від використовуваних дискових накопичувачів, що дає істотний приріст надійності всієї системи. Як і у випадку з повнорозмірними ПК-серверами, NAS мають можливість віддаленого адміністрування, але організований цей процес через веб-інтерфейс, що дозволяє зручно управляти мережевим накопичувачем з будь-якого сегменту локальної мережі, а також з інтернету за допомогою звичайних браузерів.

За рівнем керованості і контролю доступу сучасні NAS не поступаються традиційним файл-серверам. Вони можуть працювати в Windows-доменах, у багатьох з них реалізована підтримка групових шаблонних політик доступу і безпеки Windows Active Directory. Захищеність доступу до інформації, що зберігається, можливості шифрування даних і поділу прав використання на окремі папки та файли роблять мережеві накопичувачі зручним засобом зберігання даних в корпоративній мережі.

Сучасні NAS можуть мати різне виконання – окремі пристрої та елементи для серверних стойок і різну кількість накопичувачів – від 1 до 16+. На рис. 4.17 наведено декілька пристроїв із модельного ряду компанії Synology.

Звісно, усі NAS підтримують актуальні режими RAID, а деякі із виробників пропонують власні технології об’єднання дисків в масив. Наприклад, Synology Hybrid RAID (SHR), яка дозволяє збільшити корисний об’єм накопичувачів та

підтримує «гарячу» заміну дисків і розширення без переформатування усього масиву [13].

Рисунок 4.17 – Приклади форм-факторів NAS Synology

У якості накопичувачів для NAS краще обрати HDD із спеціалізованих лінійок, що є в арсеналі кожного виробника. Режим роботи NAS передбачає функціонування 24/7, тому й HDD повинні мати відповідну надійність, хай й за рахунок можливого зниження швидкості. Прикладом таких сімейств HDD є Western Digital Red/Red PRO, Hitachi (HGST) Deskstar NAS, Seagate IronWolf, Toshiba MG (рис. 4.18). Зазвичай такі HDD мають швидкість обертання шпинделя 5400 об./хв., але зустрічаються й швидкісні 7200 об./хв.

Рисунок 4.18 – Приклади HDD для NAS

NAS в 2020 році – це не тільки засоби зберігання, но і ціла система додаткових вбудованих в систему керування служб і сервісних додатків, що забезпечують безліч додаткових функцій, здатних задовольнити підприємства середніх розмірів. В мережевих накопичувачах на якісному рівні реалізовані такі функції, як серверний друк, сервер відеоспостереження, веб- та FTP-сервер, DLNA-сервер, багаточисленні сервіси резервного копіювання, синхронізація із хмарними сервісами та багато іншого. Провідними виробниками NAS є Synology, QNAP, ASUSTOR.

З програмної точки зору, сучасні NAS оснащені ОС на базі Linux, що робить їх майже повноцінними серверами із розвиненою підтримкою системи зберігання даних (рис. 4.19).

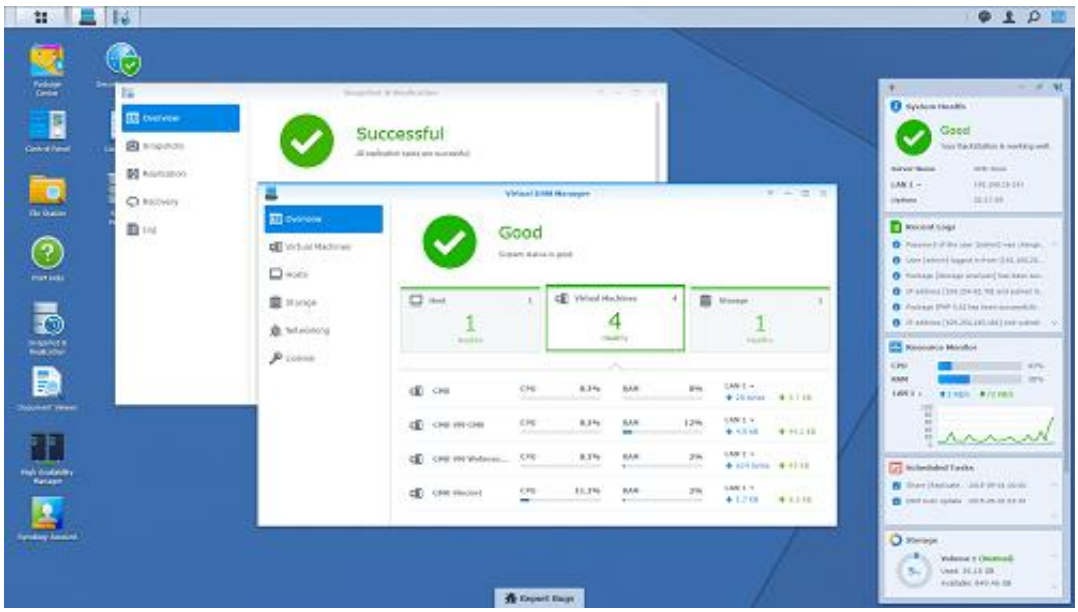


Рисунок 4.19 – ОС Synology DiskStation Manager

ОС від Synology має широкі можливості для розширення за рахунок підтримки пакетів (рис 4.20):

– офіційні пакети – власні розробки Synology;
– від суспільства (підписані) – розробляються сторонніми компаніями, підтримуються Synology, завантажуються з офіційного репозитарію;
– від суспільства (непідписані) – розробляються сторонніми компаніями, завантажуються вручну [14].

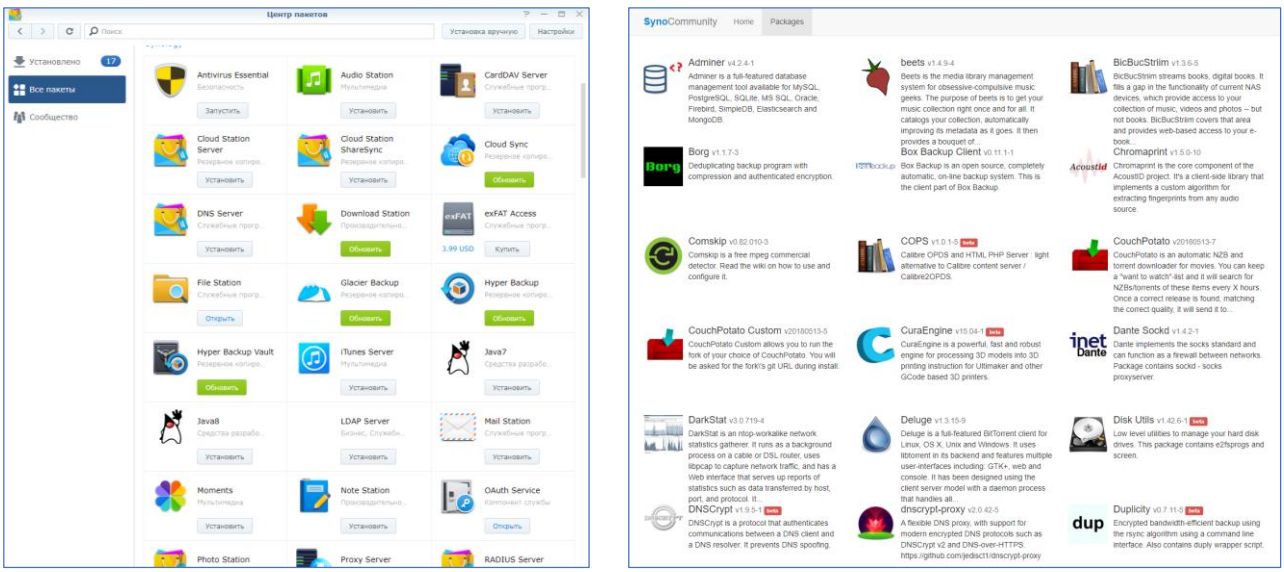


Рисунок 4.20 – Пакети в ОС Synology DiskStation Manager

Отже, в рамках завдання до КП для локальної мережі підприємства буде доцільно обрати NAS із кількістю дисків від 2 до 8, в залежності від розміру

підприємства та задач, що будуть покладені на NAS. Слід зазначити, що при необхідності зменшення бюджету, не слід економити власне на пристрої та купувати модель із меншою кількістю відсіків для дисків. Краще купити пристрій із великою кількістю відсіків, спочатку використати лише частину, а пізніше –збільшити кількість дисків і, відповідно, загальний розмір масиву.

4.6 Складання кошторису на програмне забезпечення

Після повного аналізу усього необхідного ПЗ та вибору конкретних рішень складається загальний кошторис на ПЗ. Приклад такого кошторису наведений в табл. 4.1. Слід зазначити, що до його складу також входить спеціалізоване ПЗ, що пов'язане із професійної діяльністю підприємства (наприклад, CAD-системи, видавничі комплекси, IDE для розробки ПЗ тощо).

Також очевидним є факт, що при виборі набору ПЗ слід всіляко намагатися мінімізувати загальний кошторис, але звичайно не на шкоду якості та безпеки локальної мережі. При цьому вибір певних технологій реалізації мережевих функцій може призвести до змін в кошторисі на обладнання (див. табл. 3.6) – наприклад, вибір сервера чи NAS для зберігання даних вимагає купівлі відповідних пристроїв.

Таблиця 4.1 – Кошторис на програмне забезпечення.

Найменування	*Кількість*	*Ціна за од. (грн)*	*Вартість (грн)*
Антивірус ESET Secure Business	71	1097	77 887
Операційна система Windows 10 Pro	70	125	8 750
Операційна система Windows Server 2016 Essentials	1	510	5 510
Офісний пакет Microsoft Office 2016 Professional Plus	18	187	3 366
Офісний пакет OpenOffice	52	0	0
СУБД Microsoft SQL Server 2016 Enterprise	1	50 736	50 736
СУБД MySQL	1	0	0
Середовище розробки ПЗ Microsoft Visual Studio 2017 Pro	4	13 264	53 056
Середовище розробки ПЗ Microsoft Visual Studio 2017 Community	30	0	0

Найменування	*Кількість*	*Ціна за од. (грн)*	*Вартість (грн)*
Середовище розробки ПЗ Jetbrains PyCharm Professional Edition	4	5174	20 696
Середовище розробки ПЗ Jetbrains PyCharm Community Edition	14	0	0
QNAP Qfinder	70	0	0
Усього			221 312

5. Моделювання мережі у середовищі Cisco Packet Tracer

5.1 Розробка та налаштування моделі мережі

Важливим етапом розбудови локальної мережі є моделювання, бо саме таким чином можна виявити критичні недоліки ще на етапі проектування, до прокладання кабельних мереж та монтування обладнання.

Існує декілька популярних програм для моделювання мережі – Cisco Packet Tracer (CPT), NetSim, GNS3. В КП запропоновано використати CPT – багатофункціональна програма моделювання мереж, яка дозволяє студентам експериментувати з поведінкою мережі і оцінювати можливі сценарії. Зокрема, будучи невід'ємною частиною комплексної програми навчання мережної академії, Packet Tracer полегшує викладання і вивчення складних технологічних принципів та надає можливість виконувати дії, які розвивають глибоке розуміння мережних технологій. Packet Tracer дозволяє студентам створювати мережі з практично необмеженою кількістю пристроїв, воно є безкоштовним для навчальних цілей [15].

На момент виконання КП студенти вже мають навички моделювання локальних мереж в середовищі CPT – при виконанні лабораторних робіт було докладно розглянуто окремі аспекти побудування мережі та налаштування мережевого обладнання. Модель мережі в CPT відповідає логічній моделі мережі (див. п. 2.2) з урахуванням вибору відповідного обладнання, що наявне в CPT. Крім того, деякі моменти можуть бути спрощені. Наприклад, якщо ТЗ передбачає підмережу з однотипних 40 хостів , то в моделі CPT її можна замінити одним хостом – очевидно, що логіка роботи при цьому не зміниться.

Отже, основні етапи побудування моделі мережі в CPT є такими:

1. Встановлення активного обладнання та хостів.
2. Зв’язування обладнання відповідним типом кабелю.
3. Налаштування ручної або автоматичної IP-адресації.
4. Налаштування віртуальних підмереж (VLAN).
5. Налаштування статичної або динамічної маршрутизації.
6. Створення списків доступу ACL.
7. Налаштування NAT або PAT.
8. Налаштування WiFi.

Окремі етапи можуть бути відсутні (відповідно до ТЗ). Приклад моделі мережі наведений на рис. 5.1.

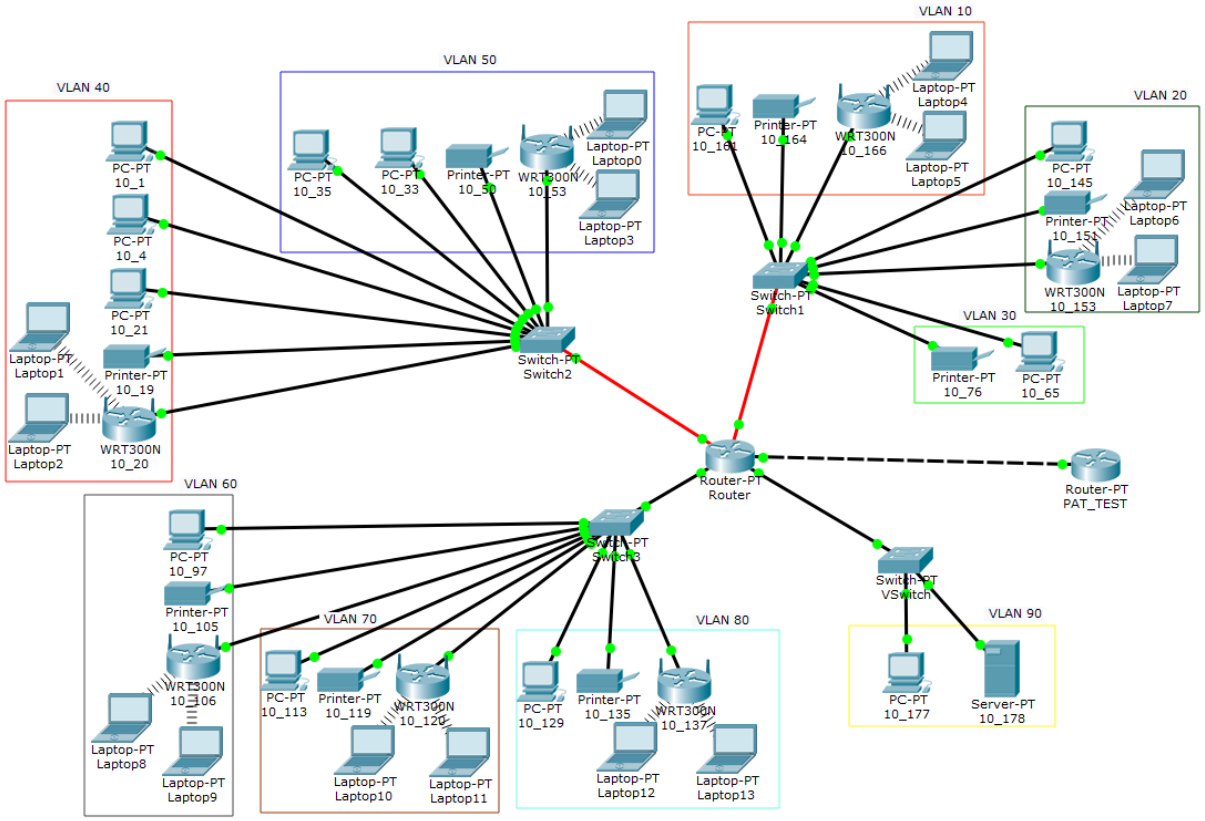


Рисунок 5.1 – Модель мережі в CPT

Розглянемо етапи побудови моделі більш докладно

Встановлення активного обладнання та хостів

При виборі обладнання треба прагнути до максимальної відповідності віртуального аналога реальному, переліченому в п. 3.5. Звичайно, CPT базується на лінійці обладнання від Cisco, але при моделюванні це не має визначної ролі.

Так, для моделювання роутерів доцільно обрати універсальну модель Router-PT, а для комутаторів – Switch-PT. Аналогічно у якості моделей робочої станції та мережевого принтеру використовуються PC-PT та Printer-PT, для моделювання мобільного пристрою – Laptop-PT (з модулем WPC300N), сервера – Server-PT. Також бажано при моделюванні використовувати пристрої лише з портами Gigabit Ethernet.

Зв’язування обладнання відповідним типом кабелю

В переважній кількості випадків в моделі використовується кручена пара (Copper Straight-through) та оптичне волокно (Fiber), але можливе використання послідовних портів (Serial DCE and DTE) для з’єднання обладнання між собою. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристрої. Синхронізація DTE виконується за вибором. Сторону DCE можна

визначити по маленькій іконці "годин" поруч з портом. При виборі типу з'єднання Serial DCE перший пристрій, до якого застосовується з'єднання, стає DCE-пристроєм, а друге – автоматично стане стороною DTE. Можливо і зворотне розташування сторін, якщо обраний тип з'єднання Serial DTE.

Налаштування ручної або автоматичної IP-адресації

Якщо за ТЗ задано ручне налаштування IP-адрес, то його можна виконати навіть засобами віконного інтерфейсу CPT (рис. 5.2)

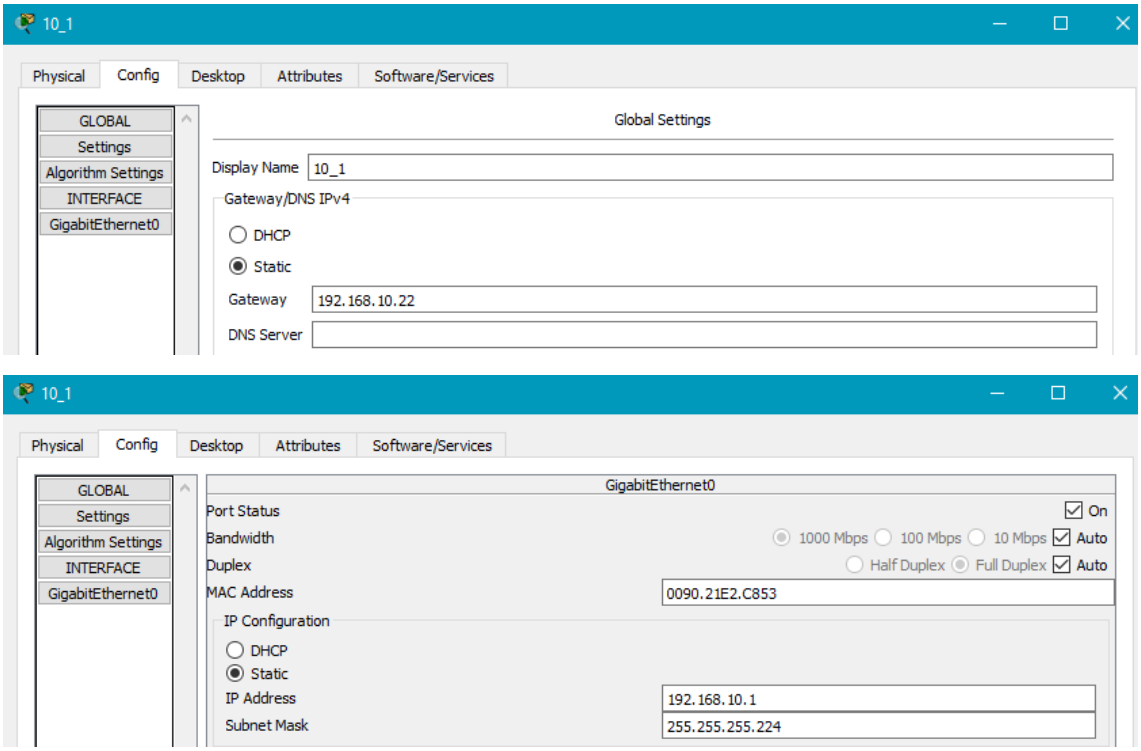


Рисунок 5.2. – Ручне налаштування IP-адреси

Якщо ж за ТЗ заданий автоматичний режим розподілу IP-адрес, то необхідно задіяти протокол DHCP. Налаштування DHCP на роутері виконується наступним чином:

```
R1(config)#interface FastEthernet0/0
R1(config-if)# ip address 10.1.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#ip dhcp pool “1stnetwork”
R1(dhcp-config)#network 10.1.10.0 255.255.255.0
R1(dhcp-config)#default-router 10.1.10.1
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.1.10.2 10.1.10.10
```

Після цього треба налаштувати та перевірити роботу DHCP на хостах та іншому обладнанні (рис. 5.3).

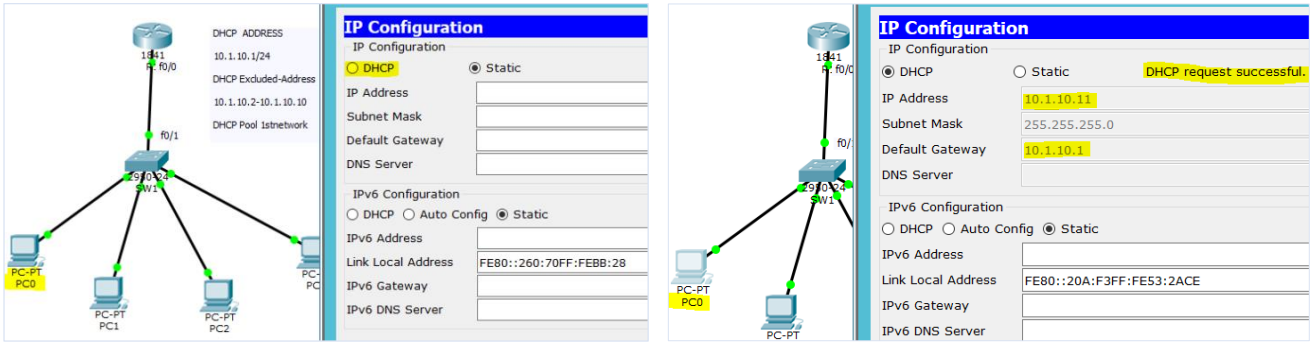


Рисунок 5.3. – Налаштування DHCP на хостах

Якщо організація мережі передбачає налаштування VLAN, то при розподілі IP-адрес для усіх портів пристроїв необхідно врахувати, що кожна локальна мережа має бути підключена до порту під-інтерфейсу, а не інтерфейсу, маршрутизатора (Layer 3 Subinterfaces). Приклад:

```
Router(config)#int gig4/0.40
Router(config-subif)#encapsulation dotlQ 40
Router(config-subif)#ip addr 192.168.10.22 2S5.255.255.224
Router(config-subif)#ex
Router(config)#int gig4/0.50
Router(config-subif)#Hencapsulation dotlQ 50
Router(config-subif)#ip addr 192.168.10.54 255.255.255.224
Router(config-subif)#ex
```

Налаштування віртуальних підмереж (VLAN)

Для налаштування VLAN на комутаторі необхідно створити VLAN з певними номерами і призначити їх інтерфейсам, до яких підключені комп'ютери відповідної мережі:

```
Switch(config)#vlan 10
Switch(config-vlan)#name 10
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name 20
Switch(config-vlan)#ex
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#int gig3/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config-if)#ex
```

Також на кожному комутаторі необхідно налаштувати магістральний режим віртуальної мережі:

```
Switch(config)#int gig0/1
Switch(config-if)#switchport mode trunk
```

Головне, що треба пам’ятати при створенні віртуальних мереж – вони не повинні повністю повторювати топологічні підмережі, що вже існують на схемі.

Налаштування статичної або динамічної маршрутизації

В разі статичної маршрутизації, необхідно на кожному з роутерів прописати усі маршрути, наявні в мережі. Це дуже довга та кропітка робота, тому – якщо не зазначено інше – краще використати один з протоколів маршрутизації (RIP, OSPF тощо). Оптимальним вибором буде RIPv2:

Включення RIPv2на виконується відповідною командою, що передбачає введення безпосередньо підключених до роутера мереж. Наприклад:

```
Router1(config)# router rip
Router1(config-router)# version 2
Router1(config-router)# network 172.16.10.0
Router1(config-router)# network 10.1.1.0

Router2(config)# router rip
Router2(config-router)# version 2
Router2(config-router)# network 10.1.1.0

Router4(config)# router rip
Router4(config-router)# version 2
Router4(config-router)# network 172.16.10.0
```

На кожному роутері за допомогою команди show running-config можна подивитися, як роутером були оброблені відповідні команди. Далі командою show ip protocols можна оцінити параметри протоколу:

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 6 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
Default version control: send version 1, receive any version
Interface         Send        Recv        Triggered RIP Key-chain
Serial2/0         1           2 1
FastEthernetO/O   1           2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.16.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway   Distance    Last Update
Distance:(default is 120)
```

Перегляд таблиці маршрутів:

```
Router2# sh ip route

  10.0.0.0/24 is subnetted, 1 subnets
C     10.1.1.0 is directly connected, FastEthernet0/0
R     172.16.0.   0/16 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0
```

З цього листінгу можна зрозуміти, що протокол побудував маршрут до мережі 172.16.10.0/24 до адреси 10.1.1.1. Це можна перевірити пінгом:

```
Router2# ping 172.16.10.1
Router2# ping 172.16.10.2
```

Командою *debug ip rip* можна переглянути як роутери обмінюються маршрутною інформацією. Наприклад, для Router1 кожні 30 секунд повторюються такі повідомлення:

```
Router1# debug ip rip

RIP: sending update to 255.255.255.255 via Serial0 (172.16.10.1)
  subnet 10.1.1.0, metric 1
RIP: sending update to 255.255.255.255 via Ethernet0 (10.1.1.1)
  subnet 172.16.10.0, metric 1
RIP: received update from 172.16.10.2 on Serial0
RIP: received update from 10.1.1.2 on Ethernet0
```

Створення списків доступу ACL

Якщо згідно з ТЗ необхідно заблокувати певні зв’язки або ізолювати окремі хости, то для цього необхідно використати налаштування списків доступу (Access Control List, ACL). Принципи використання ACL є досить простими. Наприклад, згідно із топологією на рис. 5.4 необхідно заборонити хосту 10.0.3.2 доступ в сегмент сервера (тільки цьому хосту, іншим доступ дозволено).

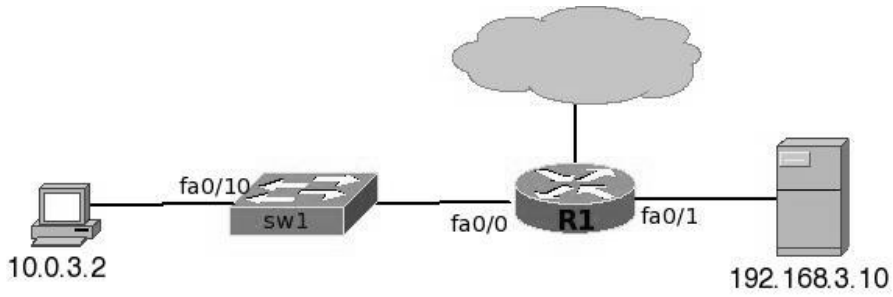


Рисунок 5.4 – Приклад для налаштування стандартного ACL

Створюємо стандартний нумерований ACL

```
R1(conf)# access-list 1 deny 10.0.3.2
R1(conf)# access-list 1 permit any
```

та застосовуємо його на інтерфейсі

```
R1(conf)# interface fa0/1
R1(conf-if)# ip access-group 1 out
```

Аналогічна задача може бути вирішена більш зручно за допомогою іменованих ACL:

```
R1(conf)# ip access-list standard Test_ACL
R1(config-std-nacl)# deny 10.0.3.2
R1(config-std-nacl)# permit any

R1(conf)# interface fa0/1
R1(conf-if)# ip access-group Test_ACL out
```

Зверніть увагу, що в кінці кожного ACL є невидимий допис *deny ip any any* – тому й маємо дописувати *permit any*. Щодо *deny ip any any*, то його часто дописують наочно, щоб за спрацюванням лічильників знати, що трафік був заблокований саме ACL.

Окрім стандартних ACL існують також розширені ACL, які дозволяють більш докладно обробляти трафік:

– для протоколів IP та ICMP вказувати відправника та/або отримувача:

```
router(conf)# access-list acl-number <permit|deny> <ip|icmp|ospf|eigrp...>
source source-wildcard destination destination-wildcard
```

– для протоколів TCP та UDP, вказувати порти відправника та/або отримувача:

```
router(conf)# access-list acl-number <deny|permit> <tcp|udp> source source-
wildcard [operator [port]] destination destination-wildcard [operator [port]]
[log]
```

Наприклад, для топології на рис. 5.5 необхідно створити розширений ACL із такими вимогами:

– заборонити хосту 10.0.3.2 доступ до серверу за RDP;
– заборонити хосту 10.0.3.1 доступ за HTTP;
– дозволити все усім іншим хостам із мережі 10.0.3.0;
– заборонити все іншим хостам.

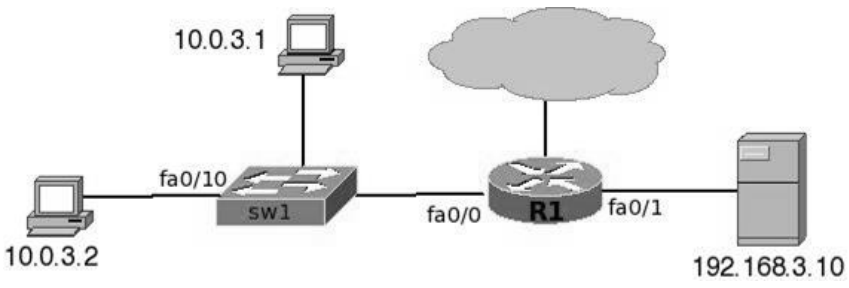


Рисунок 5.5 –Приклад для налаштування розширеного ACL

Відповідний нумерований ACL:

```
R1(conf)# access-list 100 deny tcp host 10.0.3.2 host 192.168.3.10 eq 3389
R1(conf)# access-list 100 deny tcp host 10.0.3.1 any eq 80
R1(conf)# access-list 100 permit ip 10.0.3.0 0.0.0.255 any
R1(conf)# access-list 100 deny ip any any

R1(conf)# interface fa0/0
R1(conf-if)# ip access-group 100 in
```

Розширений іменований ACL:

```
R1(conf)# ip access-list extended Test_ACL_extend
R1(config-ext-nacl)# deny tcp host 10.0.3.2 host 192.168.3.10 eq 3389
R1(config-ext-nacl)# deny tcp host 10.0.3.1 any eq 80
R1(config-ext-nacl)# permit ip 10.0.3.0 0.0.0.255 any
R1(config-ext-nacl)# deny ip any any

R1(conf)# interface fa0/0
R1(conf-if)# ip access-group Test_ACL_extend in
```

Налаштування NAT або PAT

Для підключення мережі до інтернету та приховування особливостей організації локальної мережі зовні може бути використаний один із видів NAT (Network Address Translation – статичний, динамічний або PAT.

NAT налаштовується на межовому роутері, що має безпосередній зв’язок із провайдером. Наприклад, для найпростішого NAT – статичного (тобто перетворення внутрішньої адреси в єдину зовнішню) – треба спочатку налаштувати адреси, що перетворюються:

```
Router1(config)#ip nat inside source static 10.10.1.2 175.10.1.1
```

а потім відмітити, який інтерфейс є внутрішнім, а який – зовнішнім:

```
Router1(config)#interface fa0/0
Router1(config-if)#ip nat inside
Router1(config-if)#interface s2/0
Router1(config-if#ip nat outside
```

Для перегляду таблиці перетворень адрес можна використати команду *show ip nat translations*:

```
Router1#show ip nat translations

Pro   Inside global     Inside local      Outside local     Outside global
      169.10.1.2        10.10.1.2         ---               ----
```

Налаштування динамічного NAT, тобто перетворення внутрішньої адреси в одну з пула зовнішніх адрес, є більш складним (рис. 5.6).

Перш за все, включаємо IP-маршрутизацію та відмічаємо внутрішні та зовнішні інтерфейси (fast ethernet 0/0 – внутрішній, serial interface s0/0 – зовнішній):

```
R1# configure terminal
R1(config)# ip routing
R1(config)# interface fastethernet0/0
```

```
R1(config-if)# ip nat inside
R1(config-if)# interface serial0/0
R1(config-if)# ip nat outside
R1(config-if)# exit
```

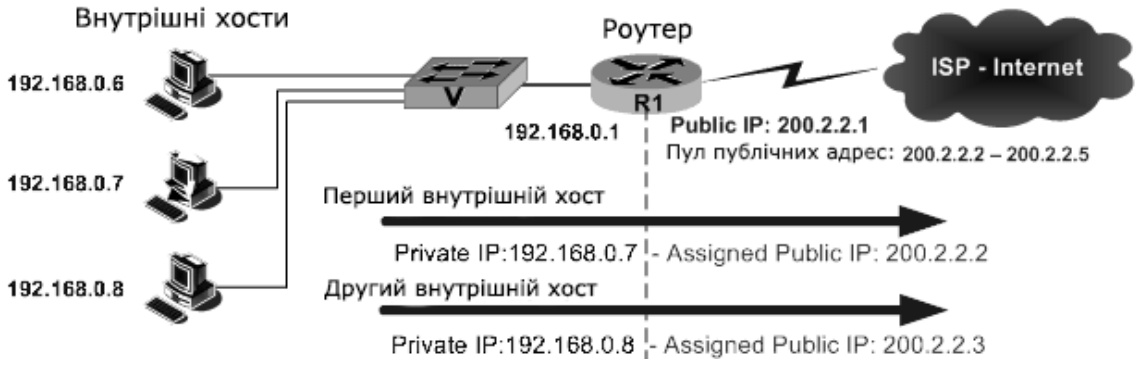


Рисунок 5.6 – Приклад налаштування динамічного NAT

Наступним кроком є створення пулу IP-адрес, які маршрутизатор буде надавати внутрішнім хостам, які намагаються підключитися до інтернету. Кожен раз, коли хост надсилає пакет, призначений для інтернету, маршрутизатор автоматично виділяє одну з загальнодоступних IP-адрес протягом тривалості сеансу. Коли сеанс закінчується (наступає таймаут) і публічна IP-адреса звільняється та становиться знову доступною для пулу Dynamic NAT. Визначимо пул адресів:

```
R1(config)# ip nat pool Public-IPS 200.2.2.2 200.2.2.5 prefix-length 29
```

Далі необхідно створити ACL, який буде включати локальні (приватні) хости або мережі, залежно від того, наскільки великою є внутрішня мережа. Цей ACL буде застосовано до пулу NAT під назвою «Public-IPS», і буде контролювати хости, яким буде призначена публічна IP-адреса для виходу в інтернет. ACL-список може бути стандартним або розширеним, в залежності від того, наскільки вибірково треба визначити хости, що мають виходити до інтернету. Попередньо прив’яжемо лист до вже визначеного пулу адрес:

```
R1(config)# ip nat inside source list 100 pool Public-IPS
R1(config)# access-list 100 remark [Control NAT Pool Service]
R1(config)# access-list 100 permit ip 192.168.0.0 0.0.0.255 any
```

Таким чином, перша команда з лістингу вказує маршрутизатору дозволити мережі 192.168.0.0/24 використовувати пул NAT і надати кожному хосту унікальну динамічну загальнодоступну IP-адресу. Перевіримо:

```
R1# show ip nat translations
Pro     Inside global     Inside local    Outside local      Outside global
---      200.2.2.2          192.168.0.6     ---                ---
---      200.2.2.3          192.168.0.8     ---                ---
```

Тобто, двом внутрішнім адресам (192.168.0.6 та 192.168.0.8) було надано відповідні зовнішні адреси. Ці перетворення із часом вичерпаються, якщо від внутрішніх хостів немає активності. Якщо ж потрібно примусово очистити їх, це можна легко зробити:

```
R1# clear ip nat translation *
```

Статистика служби Dynamic NAT надає інформацію щодо використання пулу Dynamic NAT та доступних загальнодоступних IP-адрес. Отримати статистику можна відповідною командою:

```
R1# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces:
Serial0/0
Inside interfaces:
FastEthernet0/0
Hits: 8968 Misses: 2
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 100 pool Public_IPS refcount 2
pool PUBLIC: netmask 255.255.255.0
start 200.2.2.2 end 200.2.2.5
type generic, total addresses 4, allocated 2 (50%), misses 0
```

PAT (який ще називають «перевантаженим NAT») передбачає перетворення внутрішньої пари «IP:порт» у відповідну зовнішню пару. Це дозволяє сховати локальну мережу за єдиною зовнішньою IP-адресою (рис. 5.7).

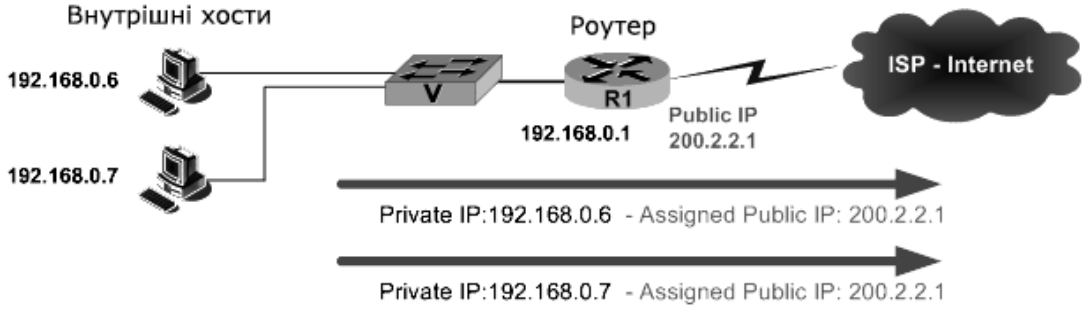


Рисунок 5.7 – Приклад налаштування PAT (перевантаженого NAT)

Налаштування PAT є подібним до динамічного NAT. Перш за все, необхідно відмітити зовнішні та внутрішні інтерфейси:

```
R1# configure terminal

R1(config)# interface fastethernet0/0
R1(config-if)# ip nat inside

R1(config-if)# interface serial0/0
R1(config-if)# ip nat outside
```

Далі необхідно створити ACL-список, що задає набір внутрішніх адрес, що потребують перетворення

```
R1(config)# access-list 100 remark == [Control NAT Service]==
R1(config)# access-list 100 permit ip 192.168.0.0 0.0.0.255 any
```

І прив’язати цей список до зовнішнього інтерфейсу роутера:

```
R1(config)# ip nat inside source list 100 interface serial 0/0 overload
```

Після деякого періоду мережевою активності можна перевіряти результати перетворення:

```
R1# show ip nat translations
Pro Inside global    Inside local       Outside local     Outside global
udp 200.2.2.1:53427  192.168.0.6:53427  74.200.84.4:53    74.200.84.4:53
udp 200.2.2.1:53427  192.168.0.6:53427  195.170.0.1:53    195.170.0.1:53
tcp 200.2.2.1:53638  192.168.0.6:53638  64.233.189.99:80  64.233.189.99:80
tcp 200.2.2.1:57585  192.168.0.7:57585  69.65.106.48:110  69.65.106.48:110
tcp 200.2.2.1:57586  192.168.0.7:57586  69.65.106.48:110  69.65.106.48:110
```

В цьому прикладі перші два перетворення спрямовані на 74.200.84.4 та 195.170.0.1, – це запити DNS від внутрішнього хоста 192.168.0.6. Третій запис представляється http-запитом на веб-сервер з IP-адресою 64.233.189.99. Дивлячись на четвертий та п’ятий записи перекладу, слід визначити їх як pop3-запити на зовнішній сервер, можливо, генерований клієнтом електронної пошти. Оскільки ці записи створюються динамічно, вони є тимчасовими і через деякий час будуть видалені з таблиці перекладу.

Треба також враховувати, що при використанні програм, які створюють багато з'єднань (наприклад, Utorrent, Limewire тощо), можна отримати значне зниження продуктивності роутера, оскільки він намагається вчасно обробити усі ці перетворення. Наявність тисячі підключень, що проходять через маршрутизатор, може поставити серйозне навантаження на процесор.

Очищення таблиці трансляції та перегляд статистики виконується аналогічно до вже наведених вище.

Налаштування WiFi

Для забезпечення бездротового з’єдання за технологією WiFi можна використати два підходи:

1) *Використати Access Point* – кінцеву точку доступу, що фактично є мостом між мережею і бездротовим пристроєм (БП). При підключенні нового пристрою, він фактично становиться частиною підмережі, до якою приєднана сама точка доступу.

2) *Використати Wireless-N Broadband Router* – фактично, звичайний роутер із модулем бездротового доступу. Такий роутер має значно більше налаштувань, бо фактично підіймає свою окрему мережу для підключених бездротових пристроїв.

Який саме спосіб обрати, залежить від масштабів мережі, бюджету тощо. Розглянемо другий варіант

Для підключення до мережі мобільних пристроїв необхідно призначити WAN-інтерфейсу маршрутизатора WRT300N IP-адресу, що належить даній підмережі, та задати у налаштуваннях адресу та маску підмережі для роздавання за DHCP адрес з вказаного діапазону.

Для налаштування бездротового маршрутизатору слід (рис. 5.8):

– обрати маршрутизатор;
– перейти до вкладки «GUI»;
– обрати тип з'єднання «Static IP» та ввести IP-адресу з даної підмережі, маску та адресу відповідного під-інтерфейсу маршрутизатора;
– в пункті «Network Setup» ввести адресу підмережі, маску та діапазон адрес для роздавання з використанням DHCP.

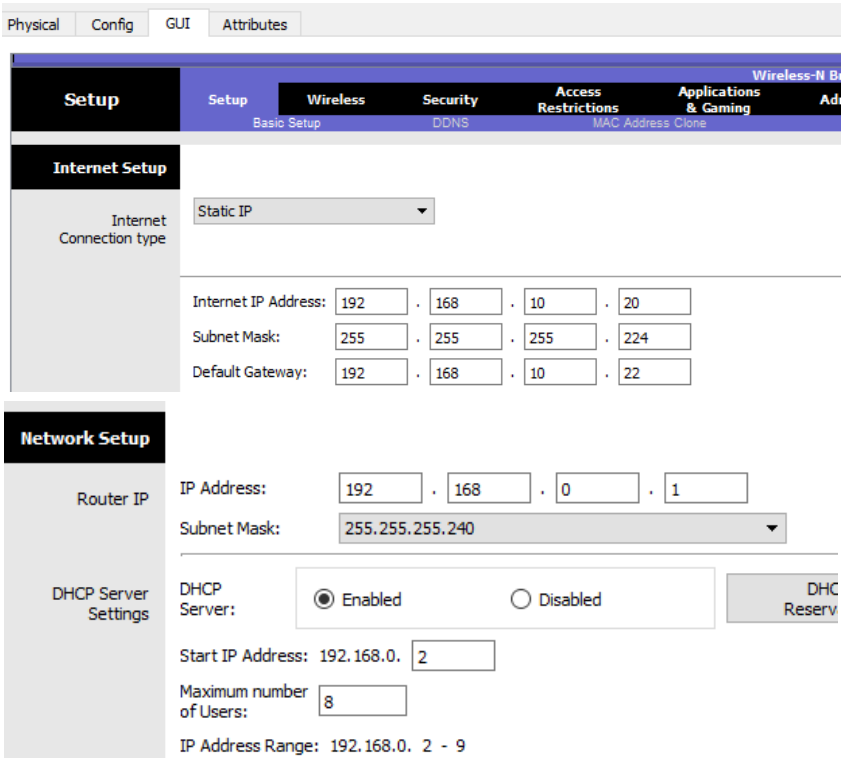


Рисунок 5.8 – Налаштування WRT300N

5.2 Перевірка працездатності моделі

Для перевірки працездатності мережі можна використати звичайний ping, як між хостами, так й в парах «інтерфейс-хост» (рис. 5.9). При цьому також широко застосовується режим симуляції (*simulation mode*) в CPT.

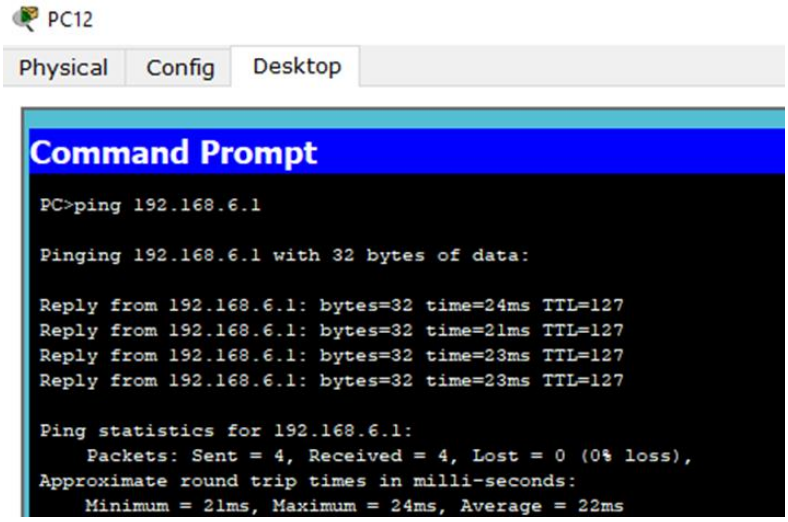


Рисунок 5.9 – Виконання ping

Усі інші тести повинні враховувати особливості кожної з специфічних функції мережі:

- маршрутизація за стандартними протоколами перевіряється за допомогою *show ip route*, *debug ip rip* та базовим *traceroute*;
- для перевірки налаштування VLAN треба перевірити доступність віртуальних мереж одна з іншої за допомогою ping або traceroute,
- для перевірки налаштування ACL-списків достатньо *ping*, *traceroute* та *show access-list*;
- для тестування NAT (PAT) до центрального роутера доцільно під’єднати ще один роутер, який буде імітувати роутер провайдера, пропігнувати його та переглянути таблиці трансляції.

5.3 Оцінка шляхів вдосконалення мережі

Будь яка мережа вже у момент проектування є недосконалою, бо сам розробник в процесі роботи знаходить «деякі вузьки» місця. Оперативне позбавлення від них часто є неможливим через декілька можливих причин – вони

можуть потребувати значної переробки проекту, виходити за рамки бюджету, передбачати використання недоступного на цей час обладнання.

Отже, в цьому пункті пояснювальної записки розробник повинен сформулювати декілька (4-5) конкретних та очевидних (або навіть необхідних, як з його точки зору) покращень, яких потребує мережа з огляду на можливості майбутнього збільшення кількості хостів, додавання нових функцій, підвищення рівня безпеки та загального вдосконалення користувацького досвіду користування мережею.

Для конкретизації майбутніх кроків та прискорення процесу, ці покращення мають бути класифіковані за категоріями:

1) Структурні – складні та вельми дорогі зміни, що вимагають зміни в топології мережі та модифікації логічної і фізичної схем локальної мережі, часто фактично аналогічні побудуванню нової мережі.
2) Апаратні – пов’язані із точковою заміною чи додаванням деякого обладнання без значного втручання в топологію. Такі зміни є відносно безболісним шляхом до покращення продуктивності мережі за помірні гроші.
3) Програмні – передбачають встановлення та налаштування певного ПЗ (на активному обладнанні, сервері чи хостах). Є найпростішим шляхом до вдосконалення безпеки та додавання нової функціональності.

Висновки

Запропоновані методичні вказівки описують процес проектування, моделювання та тестування локальної мережі підприємства. Кожен етап організації локальної мережі містить докладні рекомендації щодо вибору необхідного обладнання або програмного забезпечення.

Перший розділ методичних вказівок містить варіанти завдань та вимоги до змісти та оформлення усіх частин пояснювальної записки.

Другий розділ присвячений побудові логічної схеми мережі. Виконується загальний аналіз, аналіз потреб підприємства, вибір топології, розрахунок характеристик мережі та розподіл мережевих адрес.

Третій розділ описує планування структурованої кабельної системи мережі, вибір типу кабелю для підсистем, особливості вибору активного обладнання, процес розробки фізичної схеми та складання кошторису на кабелі і обладнання.

Четвертий розділ присвячений програмного забезпеченню. Спочатку обирається мережева операційна системи та визначається стратегія її адміністрування, потім організовується спільний доступ до зовнішніх мережі із захистом за допомогою мережевих екранів та антивірусного програмного забезпечення. Далі описано організацію зберігання даних та резервне копіювання, після чого розділ підсумовується складання кошторису на програмне забезпечення

П’ятий розділ містить відомості щодо моделювання розробленої мережі в середовищі Cisco Packet Tracer. Спочатку виконується розробка та налаштування моделі мережі, після чого проводиться перевірка працездатності та тестування моделі,за результатами яких надаються рекомендації щодо вдосконалення мережі.

Отже, підсумковим результатом курсового проекту є докладний опис усіх етапів проектування із обґрунтуванням вибору топології, обладнання та програмного забезпечення, та результати моделювання мережі у Cisco Packet Tracer.

Перелік посилань

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2013. – 960 с.
2. Мінухін В., Кавун С.В., Знахур С.В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж. Навчальний посібник. – Харків: Вид. ХНЕУ, 2008. – 210 с.
3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПб.: Питер, 2020. – 1008 с.: ил.
4. Римський Ю.С., Олексюк В.П., Балик А.В. Адміністрування комп'ютерних мереж і систем: Навч. пос. – Тернопіль: Навчальна книга – Богдан. 2010. – 196 с.
5. James Kurose, Keith Ross. Computer Networking: A Top-Down Approach. – Pearson, 2017. – 856 p.
6. Преимущества и недостатки OS Windows Server для выделенного Сервера [електронний ресурс]. – Режим доступу: https://unit-is.com/ru/support/articles/preimusshestva-i-nedostatki-os-windows-server-dlya-vyidelennogo-servera.
7. Ubuntu Server – обзор, сравнение, отзывы [електронний ресурс]. – Режим доступу: https://ubuntu-admin.ru/ubuntu-server-obzor.
8. Структура хранилища Active Directory [електронний ресурс]. – Режим доступу: https://1cloud.ru/help/windows/struktura-hranilischa-active-directory.
9. Функции и типы Firewall [електронний ресурс]. – Режим доступу: http://www.starlink.ru/articles/firewall/.
10. Firewalls — немного теории для или что надо знать перед покупкой [електронний ресурс]. – Режим доступу: https://habr.com/ru/post/130090/
11. The best Windows antivirus software for users [електронний ресурс]. – Режим доступу: https://www.av-test.org/en/antivirus/home-windows/windows-10/february-2020/
12. Storage technologies – DAS, NAS and SAN [електронний ресурс]. – Режим доступу: https://abdullrhmanfarram.wordpress.com/2013/04/08/storage-technologies-das-nas-and-san/

13. What is Synology Hybrid RAID (SHR) [електронний ресурс]. – Режим доступу: https://www.synology.com/en-global/knowledgebase/DSM/tutorial/Storage/What_is_Synology_Hybrid_RAID_SHR
14. Packages for Synology NAS [електронний ресурс]. – Режим доступу: https://synocommunity.com/
15. Basic of Cisco Packet Tracer [електронний ресурс]. – Режим доступу: https://www.cisco.com/c/uk_ua/training-events/networking-academy/courses/cisco-packet-tracer.html

Перелік рекомендованої літератури

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2013. – 960 с.
2. Peter L. Dordal. An Introduction to Computer Networks. Release 1.9.21. – Loyola University Chicago, 2020. – 896 p.
3. Joseph Migga Kizza. Guide to Computer Network Security – Springer, 2017. – 568 p.
4. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В. Комп'ютерні мережі: навч. посіб. – Л.: Магнолія-2006, 2013. – 256 с.
5. Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп’ютерні мережі : навчальний посібник – Вінниця: ВНТУ, 2013. – 371 с.
6. Організація комп’ютерних мереж: підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки» / КПІ ім. Ігоря Сікорського; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с
7. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПб.: Питер, 2020. – 1008 с.: ил.
8. Мінухін .В., Кавун С.В., Знахур С.В. Комп’ютерні мережі. Загальні принципи функціонування комп’ютерних мереж. Навчальний посібник. – Харків: Вид. ХНЕУ, 2008. – 210 с.
9. James Kurose, Keith Ross. Computer Networking: A Top-Down Approach. – Pearson, 2017. – 856 p.
10. Минаси М., Грин К., Бус К., Батлер Б. Windows Server 2012 R2. Полное руководство. Том 1. Установка и конфигурирование сервера, сети, DNS. – М.: Вильямс, 2014. – 960 с.

Додаток А – Шаблон технічного завдання

друкується на одному листі А4 з обох боків

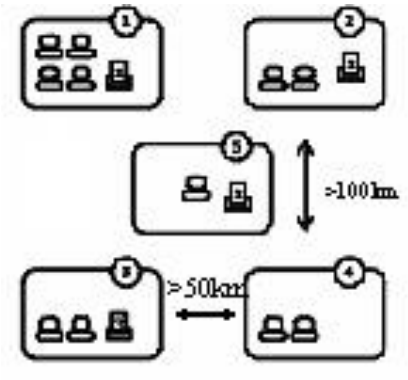
ЗАТВЕРДЖУЮ
Зав. кафедрою комп'ютерної інженерії
професор_____ В.А. Святний
«___» _____ 2019 р.

Технічне завдання

студенту групи _____ _____
(група) (ПІБ)

Термін здачі роботи 17 листопада 2019 р.

Варіант 3. Аналіз можливих рішень при об'єднання мережі магазинів.



Мережа магазинів 1 (3 поверхи), 2, 3, 4 (2 поверху), розташованих в різних містах (на великій відстані один від одного), і склад 5.

Необхідно визначити найбільш ефективне рішення по організації повноцінної взаємодії між усіма магазинами і складом:

- забезпечити динамічне оновлення даних про товари в кожному магазині;
- організувати можливість отримання статистичної інформації в центральному магазині 1 усіма повноважними користувачами мережі, а також введення інформації на складі.
- забезпечити можливість використання електронної пошти в усіх магазинах.

Параметри будівлі 1: 60 * 50 * 15 м.
Параметри будівель 2,3,4: 40 * 12 * 6 м.

- Топологія мережі – обґрунтувати;
- протокол канального рівню – 10Mb Ethernet/100Mb Ethernet/1Gb Ethernet/Token Ring;
- середовище передачі даних: коаксіальний кабель / кручена пара / оптоволокно;
- метод призначення IP-адрес – автоматично / вручну;
- служба шлюзу – Proxy / NAT стат/ NAT дин./ PAT;
- обов'язкова складова – VLAN / WI-FI.

Розділи пояснювальної записки, що підлягають розробці:

Титул
Технічне завдання
Реферат
Зміст
Вступ
1. *Логічна схема та характеристики мережі*
   1.1. Аналіз потреб підприємства і вибір топології

1.2. Розробка логічної схеми мережі
1.3. Розрахунок ефективного трафіку
1.4. Пропускна здатність та коефіцієнт використання мережі
1.5. Розподіл мережевих адрес

2. *Планування кабельної системи та вибір обладнання*
   2.1. Структурована кабельна система
   2.2. Вибір типу кабелю для підсистем
   2.3. Вибір активного обладнання
   2.4. Розробка фізичної схеми
   2.5. Складання кошторису на кабелі та обладнання
3. *Програмне забезпечення та адміністрування мережі*
   3.1. Вибір мережевої операційної системи
   3.2. Стратегія адміністрування у мережі
   3.3. Спільний доступ до зовнішніх мереж
   3.4. Мережеві екрани та антивірусне програмне забезпечення
   3.5. Організація зберігання даних та резервне копіювання
   3.6. Складання кошторису на програмне забезпечення
4. *Моделювання мережі у середовищі Cisco Packet Tracer*
   4.1. Розробка та налаштування моделі мережі
   4.2. Перевірка працездатності моделі
   4.3. Оцінка шляхів вдосконалення мережі

Висновок
Література
Додатки
Графічна частина

Графічна частина:

1. Логічна структура мережі (формат А3).
2. Фізична структура мережі (формат А3).

Графік виконання курсової роботи:

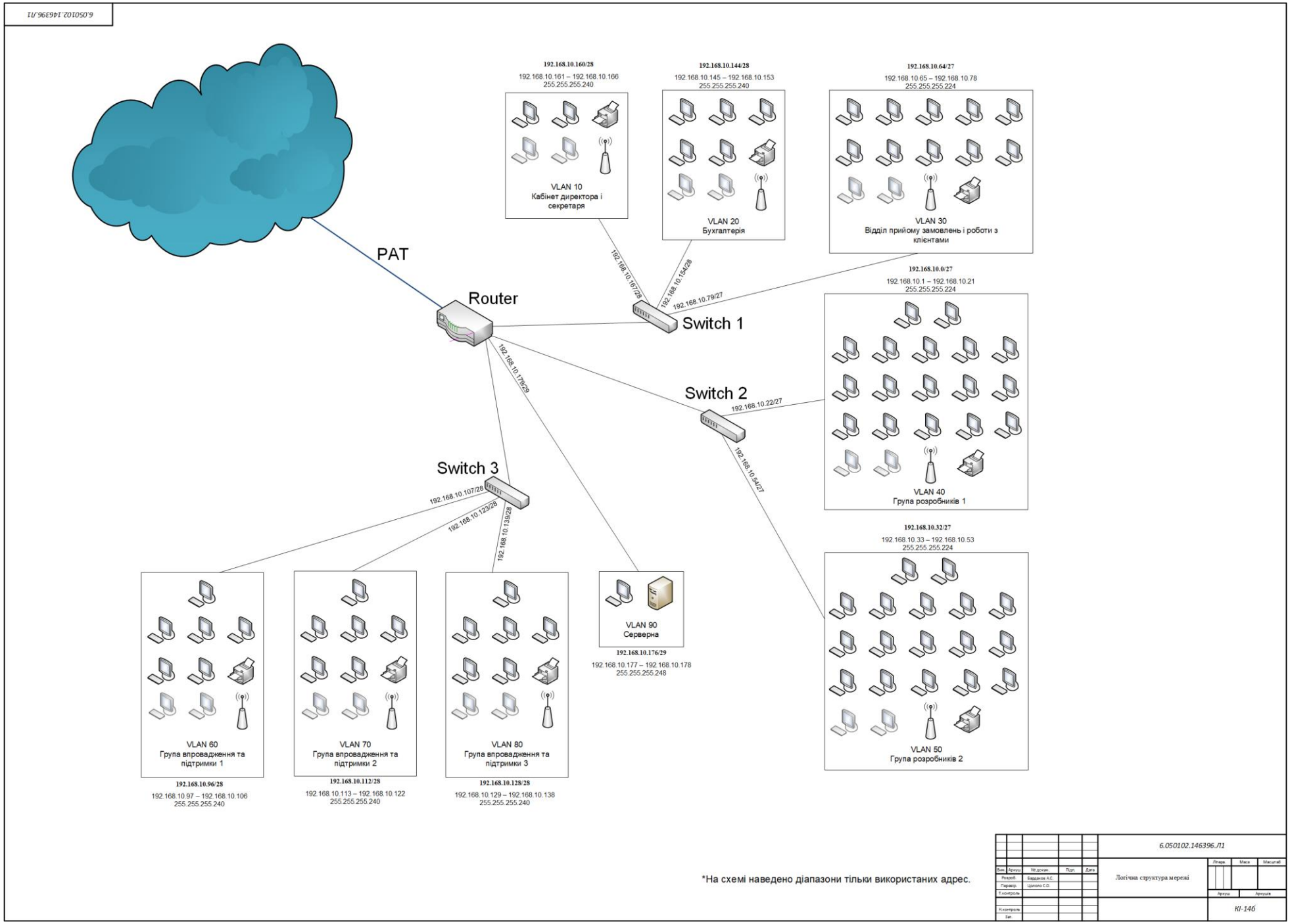
1 тиждень – складання та аналіз технічного завдання, з'ясування одержаної задачі,
2-3 тижні – планування трафіку та логічної структури мережі,
4-5 тижні – розробка СКМ підприємства, вибір активного обладнання,
6-7 тижні – вибір та обґрунтування стратегії її адміністрування і управління,
8-9 тижні – розробка моделі мережі,
10 тижні – експериментальні дослідження,
11 тижні – оформлення пояснювальної записки,
12 тиждень – захист курсової роботи.

Дата видання завдання 10 вересня 2019 р.

Завдання прийняв до виконання _____ І.І. Іваненко
(підпис студента)
Керівник роботи _____ С.О. Цололо
(підпис викладача)

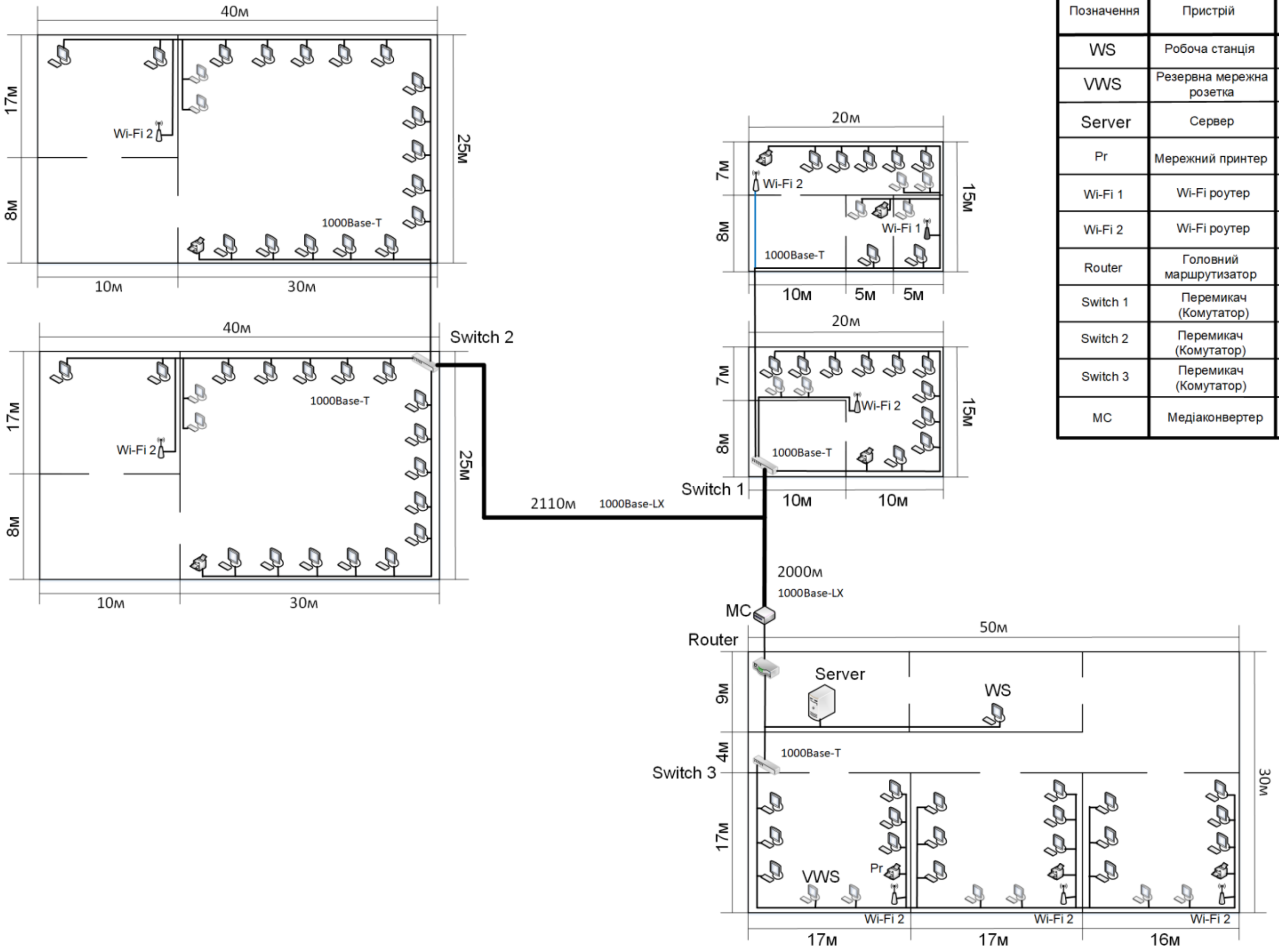
Додаток Б – Приклад логічної схеми мережі

друкується на листі А3



Додаток В – Приклад фізичної схеми мережі

[друкується на листі А3]



Умовні позначення			
Позначення	Пристрій	Модель пристрою	Кількість
WS	Робоча станція	Lenovo V510z (10NH000VPB)	70
VWS	Резервна мережна розетка	***	16
Server	Сервер	HP ProLiant ML110 (794997-425)	1
Pr	Мережний принтер	Canon i-SENSYS MF237w	8
Wi-Fi 1	Wi-Fi роутер	TP-Link Archer C5	1
Wi-Fi 2	Wi-Fi роутер	TP-Link Archer C7	7
Router	Головний маршрутизатор	D-Link DSR-250	1
Switch 1	Перемикач (Комутатор)	D-link DGS-1210-52	1
Switch 2	Перемикач (Комутатор)	D-link DGS-1210-52	1
Switch 3	Перемикач (Комутатор)	TP-Link TL-SG1048	1
MC	Медіаконвертер	TP-LINK MC220L	2

6.050102.146396.Ф1

Топологічна структура мережі

КІ-146

Додаток Г – Приклад налаштувань обладнання в CPT

Router:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
no ip cef
no ipv6 cef
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.10.107 255.255.255.240
 ip nat inside
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 192.168.10.123 255.255.255.240
 ip nat inside
interface GigabitEthernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.10.139 255.255.255.240
 ip nat inside
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet1/0.90
 encapsulation dot1Q 90
 ip address 192.168.10.179 255.255.255.248
 ip nat inside
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
 shutdown

interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet4/0
 no ip address
interface GigabitEthernet4/0.40
 encapsulation dot1Q 40
 ip address 192.168.10.22 255.255.255.224
 ip nat inside
interface GigabitEthernet4/0.50
 encapsulation dot1Q 50
 ip address 192.168.10.54 255.255.255.224
 ip nat inside
interface GigabitEthernet5/0
 ip address 192.168.10.254 255.255.255.240
 ip nat outside
 duplex auto
 speed auto
interface GigabitEthernet6/0
 no ip address
interface GigabitEthernet6/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.167 255.255.255.240
 ip nat inside
interface GigabitEthernet6/0.20
 encapsulation dot1Q 20
 ip address 192.168.10.154 255.255.255.240
 ip nat inside
interface GigabitEthernet6/0.30
 encapsulation dot1Q 30
 ip address 192.168.10.79 255.255.255.224
 ip nat inside
ip nat inside source list 1 interface
GigabitEthernet5/0 overload
ip classless
ip flow-export version 9
access-list 1 permit 192.168.10.0 0.0.0.255
line con 0
line aux 0
line vty 0 4
 login
end
```

Switch1:

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
interface GigabitEthernet0/1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport mode trunk
interface GigabitEthernet2/1
 switchport access vlan 10
 switchport mode access
interface GigabitEthernet3/1
 switchport access vlan 20
 switchport mode access
interface GigabitEthernet4/1
 switchport access vlan 30
 switchport mode access
interface GigabitEthernet5/1
 switchport access vlan 10
 switchport mode access
interface GigabitEthernet6/1
 switchport access vlan 20
 switchport mode access
interface GigabitEthernet7/1
 switchport access vlan 30
 switchport mode access
interface GigabitEthernet8/1
 switchport access vlan 10
 switchport mode access
interface GigabitEthernet9/1
 switchport access vlan 20
 switchport mode access
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

Switch2:

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
interface GigabitEthernet0/1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport access vlan 40
 switchport mode access
 speed 1000
interface GigabitEthernet2/1
 switchport access vlan 50
```

```
 switchport mode access
interface GigabitEthernet3/1
 switchport access vlan 40
 switchport mode access
interface GigabitEthernet4/1
 switchport access vlan 50
 switchport mode access
interface GigabitEthernet5/1
 switchport access vlan 40
 switchport mode access
interface GigabitEthernet6/1
 switchport access vlan 50
 switchport mode access
interface GigabitEthernet7/1
 switchport access vlan 40
 switchport mode access
interface GigabitEthernet8/1
 switchport access vlan 40
 switchport mode access
interface GigabitEthernet9/1
 switchport access vlan 50
 switchport mode access
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

Switch3:

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
interface GigabitEthernet0/1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport access vlan 60
 switchport mode access
interface GigabitEthernet2/1
 switchport access vlan 70
 switchport mode access
interface GigabitEthernet3/1
 switchport access vlan 80
 switchport mode access
interface GigabitEthernet4/1
 switchport access vlan 60
 switchport mode access
interface GigabitEthernet5/1
 switchport access vlan 70
 switchport mode access
interface GigabitEthernet6/1
 switchport access vlan 80
 switchport mode access
interface GigabitEthernet7/1
 switchport access vlan 60
 switchport mode access
interface GigabitEthernet8/1
 switchport access vlan 70
interface GigabitEthernet9/1
 switchport access vlan 80
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

VSwitch:

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
interface GigabitEthernet0/1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport access vlan 90
 switchport mode access
interface GigabitEthernet2/1
 switchport access vlan 90
 switchport mode access
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```