

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проєкту

Фаховий молодший бакалавр

(освітньо-професійний ступінь)

на тему: Налаштування керованих комутаторів другого рівня для роботи у
великих локальних мережах

Виконав студент IV курсу, групи ОК- 43
ОПП «Обслуговування комп'ютерних систем та мереж»

Спеціальності 123 Комп'ютерна інженерія

Деркач Дмитро Вікторович

(прізвище, ім'я по батькові)

Керівник

Мар'яна Селемонавічус

(підпис)

(ім'я прізвище)

Нормоконтролер

Любомира Кужій

(підпис)

(ім'я прізвище)

Рецензент

(підпис)

(ім'я прізвище)

Голова ЕК

Олег Гіщак

(підпис)

(ім'я прізвище)

Члени ЕК

Любомира Кужій

(підпис)

(ім'я прізвище)

Андрій Селемонавічус

(підпис)

(ім'я прізвище)

Дипломний проєкт захищений в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія *Комп'ютерних систем і мереж*
Освітньо-професійний ступінь *Фаховий молодший бакалавр*
Освітньо-професійна програма *Обслуговування комп'ютерних систем та мереж*
Спеціальність *123 Комп'ютерна інженерія*

ЗАТВЕРДЖУЮ

Завідувач відділення

«Комп'ютерних систем і мереж»

_____ Володимир СТАХІВ

« ____ » _____ 2025 року

**ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ СТУДЕНТУ**

Деркачу Дмитру Вікторовичу

(прізвище, ім'я та по батькові)

1. Тема проєкту Налаштування керованих комутаторів другого рівня для роботи у великих локальних мережах

керівник проєкту Селемонавічус Мар'яна Михайлівна

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом директора від «20» березня 2025 року № 20 - ст

2. Строк подання студентом проєкту «10» червня 2025 року

3. Вихідні дані до проєкту

- розглянути основи мережевої комутації;

- розглянути керовані комутатори фірми D-Link;

- налаштувати комутатор DES-3526 для роботи в мережі коледжу;

- для створення схем використати редактор Visio.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

4.1 Сучасні технології комутації

4.2 Віртуальні локальні мережі

4.3 Налаштування комутатору D-Link DES-3526 для сегментації трафіку в локальній мережі

4.4 Техніко-економічне обґрунтування

4.5 Охорона праці та безпека життєдіяльності

5. Перелік графічного матеріалу

5.1.	Схема мережі коледжу
5.2.	Створення VLAN
5.3.	Налаштування комутатора DES-3526
5.4.	Кошторис витрат на розробку проектного рішення

6 Консультанти розділів проекту

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		Завдання видав	Завдання отримав
Техніко-економічне обґрунтування	<i>Тетяна Підкуймуха</i>		
Охорона праці та безпека життєдіяльності	<i>Роман Томків</i>		

7. Дата видачі завдання «01»квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту	Термін виконання	Примітка
1	Огляд технологій комутації	25.03.2025	
2	Огляд керованих комутатори фірми D-Link	30.03.2025	
3	Опис віртуальних локальних мереж	15.04.2025	
4	Налаштування комутатору D-Link DES-3526	20.04.20	
5	Техніко-економічні показники	15.05.2025	
6	Техніка безпеки та охорона праці	20.05.2025	
7	Створення демонстраційних креслень	31.05.2025	

Студент

(підпис)

Керівник проекту

(підпис)

Дмитро Деркач

(ім'я, прізвище)

Мар'яна Селемонавічус

(ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка дипломного проекту: 72с., 31рис., 14табл., 10 джерел, 4 демонстраційних аркуші.

Об'єкт дослідження – Налаштування комутатору 2-го рівня

Мета роботи – створити інструкцію з налаштування комутатору 2-го рівня для сегментації локальної мережі коледжу.

Результати роботи дозволили налаштувати комутатор для сегментації локальної мережі коледжу для підвищення ефективності локальної мережі.

Галузь використання – інформаційні системи

КОМУТАТОРИ, МЕТОДИ КОМУТАЦІЇ, DLINK, VLAN, ВІРТУАЛЬНІ МЕРЕЖІ, СЕГМЕНТАЦІЯ ТРАФІКУ, АСИМЕТРИЧНІ VLAN, GVRP

ЗМІСТ

	ст.
ВСТУП	6
1 СУЧАСНІ ТЕХНОЛОГІЇ КОМУТАЦІЇ	7
1.1 Комутація першого рівня	9
1.2 Комутація другого рівня.....	10
1.3 Комутація третього рівня.....	14
1.4 Комутація четвертого рівня.....	23
2 ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ.....	26
2.1 Потреби використання VLAN	26
2.2 Тегування трафіка VLAN	27
2.3 Комутатор і Vlan'и	27
3 НАЛАШТУВАННЯ КОМУТАТОРУ D-LINK DES-3526 ДЛЯ СЕГМЕНТАЦІЇ ТРАФІКУ В ЛОКАЛЬНІЙ МЕРЕЖІ.....	40
3.1 Постановка задачі	40
3.2 Розв'язок задачі	40
3.3 Комутатор DES-3526. Характеристики	41
3.4 Налаштування комутатора DES-3526.....	43
4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ.....	52
4.1 Розрахунок витрат на розробку програмного продукту.....	52
4.2 Розрахунок витрат на налагодження та дослідну експлуатацію програмного продукту на ПК.....	56
5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ.....	58
5.1 Електробезпека	58
5.2 Техніка безпеки при роботі за комп'ютером.....	59
5.3 Пожежна безпека.....	61
5.4 Виробниче приміщення та робоче місце	63
ВИСНОВКИ.....	66
ПЕРЕЛІК ПОСИЛАНЬ.....	67
КОПІЇ ДЕМОНСТРАЦІЙНИХ АРКУШІВ	68
Лист 1. Схема мережі коледжу.....	69
Лист 2. Створення VLAN.....	70
Лист 3. Налаштування комутатора DES-3526.....	71
Лист 4. Кошторис витрати на розробку проектного рішення.....	72



ВСТУП

На сьогодні практично всі організації, що мають локальні мережі, зупинили свій вибір на мережах типу Ethernet. Даний вибір виправданий тим, що початок впровадження такої мережі сполучене з низькою вартістю й простотою реалізації, а розвиток - з гарною масштабованістю й економічністю.

Однорангові локальні мережі добре справляються зі своєю задачею в невеликих організаціях. Збільшення кількості працівників в організації веде до ускладнення комп'ютерної інфраструктури. При кількості комп'ютерів більше ніж 100 локальна мережа комп'ютерів під управлінням Microsoft Windows починає втрачати свою ефективність через активне використання цією операційною системою ширококомовних пакетів для виявлення структури мережі.

Один з стандартних методів для вирішення проблеми перевантаження мережі ширококомовними пакетами – використання технології віртуальних мереж VLAN. Цей метод полягає в сегментації локальної мережі на невеликі підмережі, які не можуть взаємодіяти між собою. Для того, щоб ці підмережі однак могли взаємодіяти з окремими мережевими ресурсами використовується технологія асиметричних VLAN.

Звичайне широко поширене мережеве обладнання з дешевого цінового діапазону не має можливості роботи з технологією VLAN. Для реалізації сегментації локальної мережі в цій роботі використовується мережевий комутатор 2-го рівня фірми Dlink, модель DES-3526.

Метою даної роботи є планування ефективної структури локальної мережі з сегментацією та розробка інструкції з налаштування мережевого комутатора DES-3526 для роботи в сегментованій локальній мережі.

1 СУЧАСНІ ТЕХНОЛОГІЇ КОМУТАЦІЇ

Подальший розвиток мереж ішов декількома шляхами:

- збільшення швидкості,
- впровадження сегментування на основі комутації,
- об'єднання мереж за допомогою маршрутизації.

Збільшення швидкості при колишній логічній топології - загальна шина, привело до незначного росту продуктивності у випадку великої кількості портів.

Більшу ефективність у роботі мережі принесло сегментування мереж з використанням технології комутації пакетів. Комутація найбільш діюча в наступних варіантах:

Варіант 1, іменованій зв'язком “багато з багатьма” – це однорангові мережі, коли одночасно існують потоки даних між парами робочих станцій. При цьому переважніше мати комутатор, у якого всі порти мають однакову швидкість (рис. 1.1).

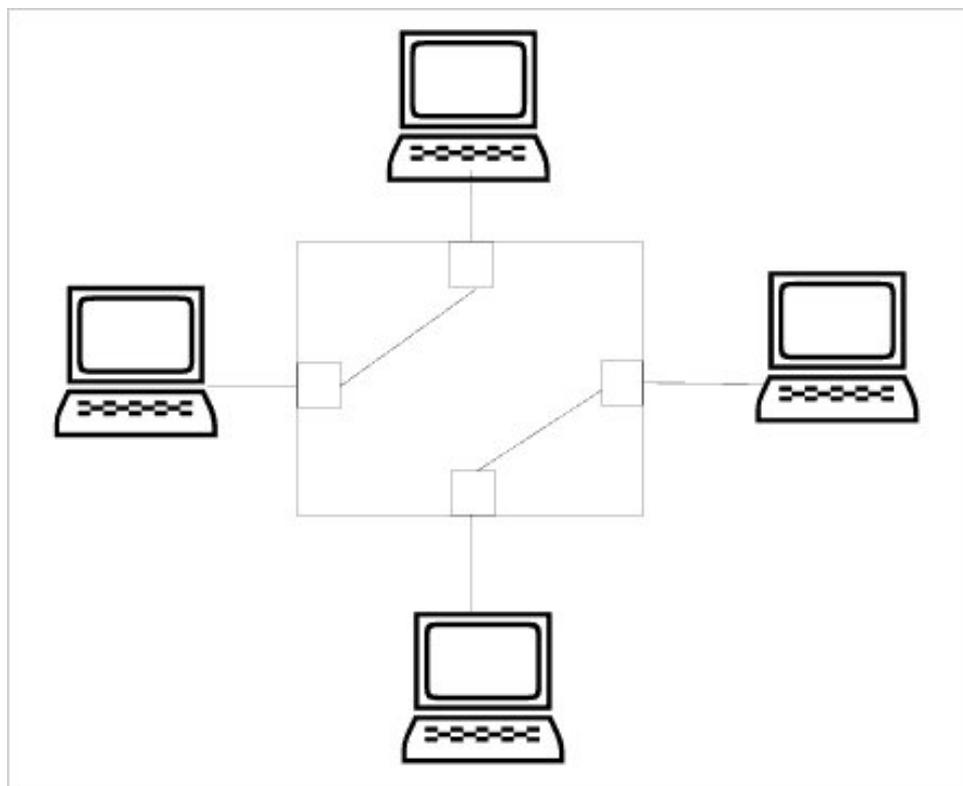


Рисунок 1.1 - Зв'язок «багато з багатьма»

- Варіант 2, іменованій зв'язком “один з багатьма” – це мережі клієнт-сервер, коли всі робочі станції працюють із файлами або базою даних сервера. У цьому випадку краще мати комутатор, у якого порти для підключення робочих станцій мають однакову невелику швидкість, а порт, до якого підключається сервер, має більшу швидкість (рис.1.2).

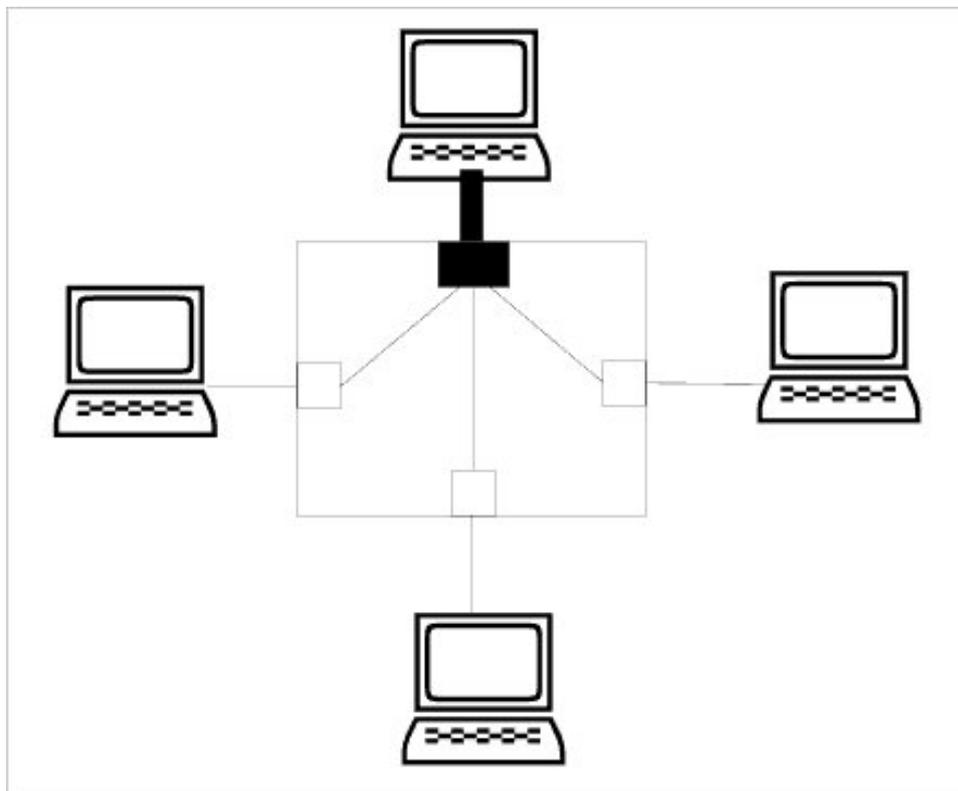


Рисунок 1.2 - Зв'язок «один з багатьма»

Коли компанії почали зв'язувати розрізнені системи один з одним, маршрутизація забезпечувала максимально можливу цілісність і надійність передачі трафіка з однієї мережі в іншу. Але з зростанням розміру й складності мережі, а також у зв'язку з все більш широким застосуванням комутаторів у локальних мережах, базові маршрутизатори (найчастіше вони одержували всі дані, що посилають комутаторами) стали із труднощами справлятися зі своїми задачами.

Проблеми із трафіком, пов'язані з маршрутизацією, проявляються найбільше гостро в середніх і великих компаніях, а також у діяльності операторів Internet, тому що вони змушені мати справу з більшими обсягами Ір-трафіка,

причому цей трафік повинен передаватися вчасно й ефективно. Але з зростанням розміру й складності мережі, а також у зв'язку з все більш широким застосуванням комутаторів у локальних мережах, базові маршрутизатори.

З підключенням настільних систем безпосередньо до комутаторів на 10/100 Мбіт/сек між ними й магістраллю виявляється усе менше проміжних пристроїв. Чим вище швидкість підключення настільних систем, тим більш швидкісною повинна бути магістраль. Крім того, на кожному рівні пристрої повинні справлятися із вхідним трафіком, інакше виникнення заторів не уникнути.

1.1 Комутація першого рівня

Термін “комутація першого рівня” у сучасній технічній літературі практично не описується. Для початку дамо визначення, з якими характеристиками має справу фізичний або перший рівень моделі OSI:

Фізичний рівень визначає електротехнічні, механічні, процедурні й функціональні характеристики активації, підтримки й дезактивації фізичного каналу між кінцевими системами. Специфікації фізичного рівня визначають такі характеристики, як рівні напруг, синхронізацію зміни напруг, швидкість передачі фізичної інформації, максимальні відстані передачі інформації, фізичні з'єднувачі й інші аналогічні характеристики. У мережах передачі даних дана технологія застосовується в повністю оптичних комутаторах

Зміст комутації на першому рівні моделі OSI означає фізичне (за назвою рівня) з'єднання. Із прикладів комутації першого рівня можна привести релейні комутатори деяких старих телефонних і селекторних систем. У більш нових телефонних системах комутація першого рівня застосовується разом з різними способами сигналізації викликів і посилення сигналів. У мережах передачі даних дана технологія застосовується в повністю оптичних комутаторах. Специфікації фізичного рівня визначають такі характеристики, як рівні напруг, синхронізацію зміни напруг, швидкість передачі фізичної інформації, максимальні відстані передачі інформації, фізичні з'єднувачі й інші аналогічні характеристики.

1.2 Комутація другого рівня

Розглядаючи властивості другого рівня моделі OSI і його класичне визначення, побачимо, що даному рівню належить основна частка комутуючих властивостей.

Визначення. Канальний рівень (формально називаний інформаційно-канальним рівнем) забезпечує надійний транзит даних через фізичний канал. Канальний рівень вирішує питання фізичної адресації (на противагу мережевої або логічної адресації), топології мережі, лінійної дисципліни (яким способом кінцевій системі використовувати мережевий канал), повідомлення про несправності, упорядкованої доставки блоків даних і керування потоком інформації.

Насправді, обумовлена канальним рівнем моделі OSI функціональність служить платформою для деяких із сьогоdnішніх найбільш ефективних технологій. Велике значення функціональності другого рівня підкреслює той факт, що виробники встаткування продовжують вкладати значні кошти в розробку пристроїв з такими функціями.

З технологічної точки зору, комутатор локальних мереж являє собою пристрій, основне призначення якого - максимальне прискорення передачі даних за рахунок паралельно існуючих потоків між вузлами мережі. У цьому - його головна відмінність від інших традиційних пристроїв локальних мереж - концентраторів (Hub), що надають усім потокам даних мережі всього один канал передачі даних.

Комутатор дозволяє передавати паралельно кілька потоків даних з максимально можливою для кожного потоку швидкістю. Ця швидкість обмежена фізичною специфікацією протоколу, яку також часто називають "швидкістю пропускання". Це можливо завдяки наявності в комутаторі великої кількості центрів обробки й просування кадрів і шин передачі даних.

Комутатори локальних мереж у своєму основному варіанті, що став класичним уже з початку 90-х років, працюють на другому рівні моделі OSI,

застосовуючи свою високопродуктивну паралельну архітектуру для просування кадрів каналних протоколів. Інакше кажучи, ними виконуються алгоритми роботи моста, описані в стандартах IEEE 802.1D і 802.1H. Також вони мають і багато інших додаткових функцій, частина яких увійшла в нову редакцію стандарту 802.1D-1998, а частина залишається поки не стандартизованою.

Комутатори ЛМ відрізняються більшою різноманітністю можливостей і, отже, цін - вартість 1 порту коливається в діапазоні від 50 до 1000 доларів. Однією із причин настільки великих різниць є те, що вони призначені для розв'язку різних класів завдань. Комутатори високого класу повинні забезпечувати високу продуктивність і щільність портів, а також підтримувати широкий спектр функцій керування. Прості й дешеві комутатори мають зазвичай невелике число портів і не здатні підтримувати функції керування. Однією з основних відмінностей є використовувана в комутаторі архітектура. Оскільки більшість сучасних комутаторів працюють на основі патентованих контролерів ASIC, устрій цих мікросхем і їх інтеграція з іншими модулями комутатора (включаючи буфери вводу-виводу) відіграє найважливішу роль. Контролери ASIC для комутаторів ЛМ діляться на 2 класу - більші ASIC, здатні обслуговувати безліч портів, що комутируються (один контролер на пристрій) і невеликі ASIC, що обслуговують по кілька портів і поєднувані в матриці комутації.

Існує 3 варіанта архітектури комутаторів:

1. переключення (cross-bar) з буферизацією на вході,
2. само маршрутизація (self-route) з поділюваною пам'яттю
3. високошвидкісна шина.

На рисунку 1.3 показана блок-схема комутатора з архітектурою, використовуваною для почергового з'єднання пар портів. У будь-який момент такий комутатор може забезпечити організацію тільки одного з'єднання (пари портів). При невисокому рівні трафіка не потрібне зберігання даних у пам'яті перед відправленням у порт призначення - такий варіант називається комутацією на лету cut-through. Однак, комутатори cross-bar вимагають буферизації на вході від кожного порту, оскільки у випадку використання єдиного можливого з'єднання

комутатор блокується (рисунок 1.4). Незважаючи на малу вартість і високу швидкість просування на ринок, комутатори класу cross-bar занадто примітивні для ефективною трансляції між низько швидкісними інтерфейсами Ethernet або token ring і високо швидкісними портами ATM і FDDI.

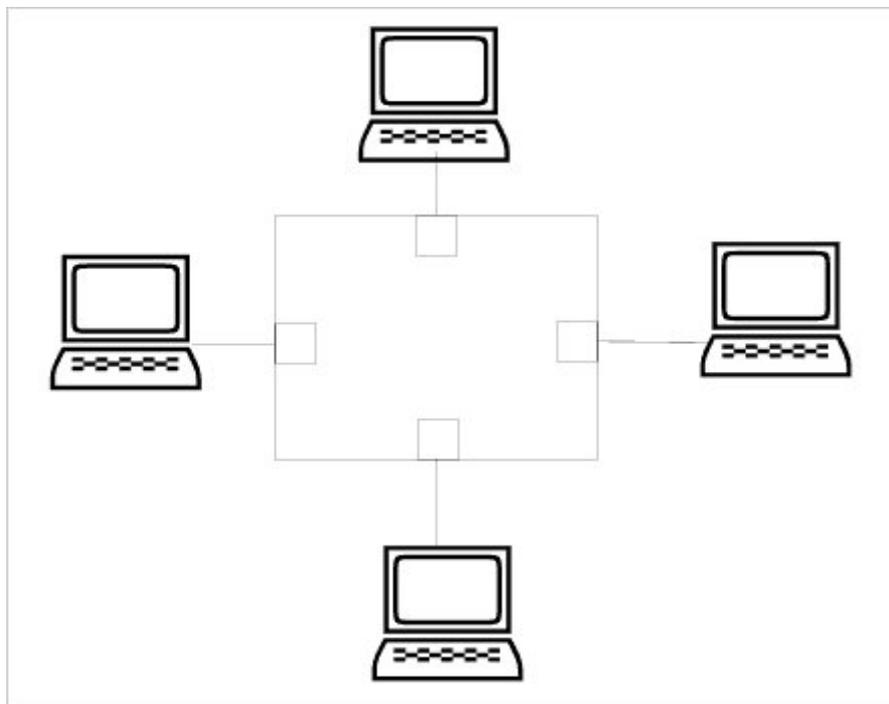


Рисунок 1.3 - Почергове з'єднання пар портів

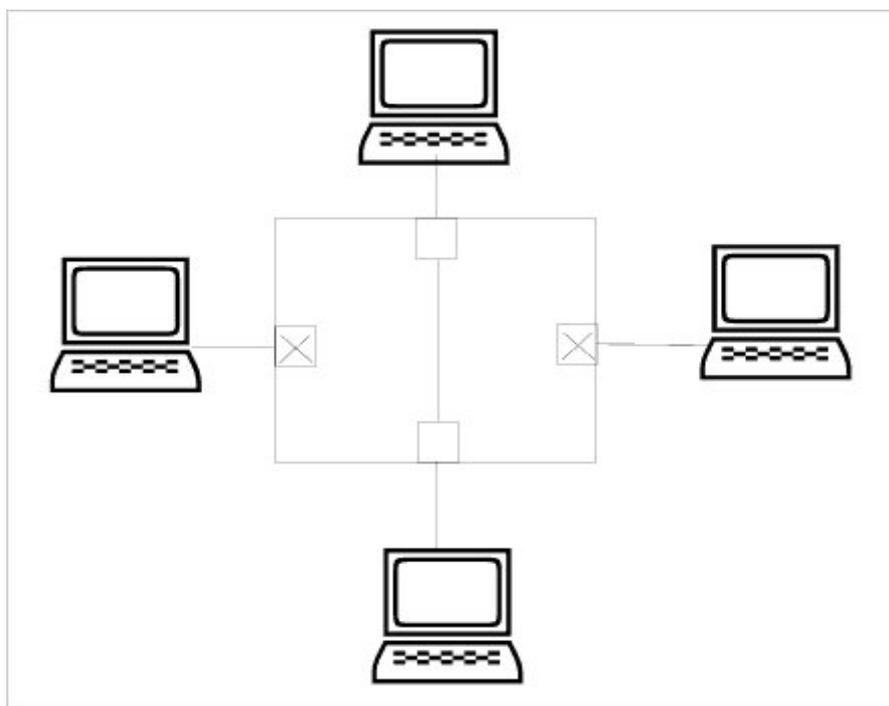


Рисунок 1.4 - Блокування комутатору типу cross-bar

Комутатори з поділюваною пам'яттю мають загальний вхідний буфер для всіх портів, використовуваний як внутрішня магістраль пристрою (backplane). Буферизація даних перед їх розсиланням (store-and-forward - зберегти й переслати) приводить до виникнення затримки. Однак, комутатори з поділюваною пам'яттю, як показано на рисунку 1.5 не вимагають організації спеціальної внутрішньої магістралі для передачі даних між портами, що забезпечує ним більш низьку ціну в порівнянні з комутаторами на базі високошвидкісної внутрішньої шини.

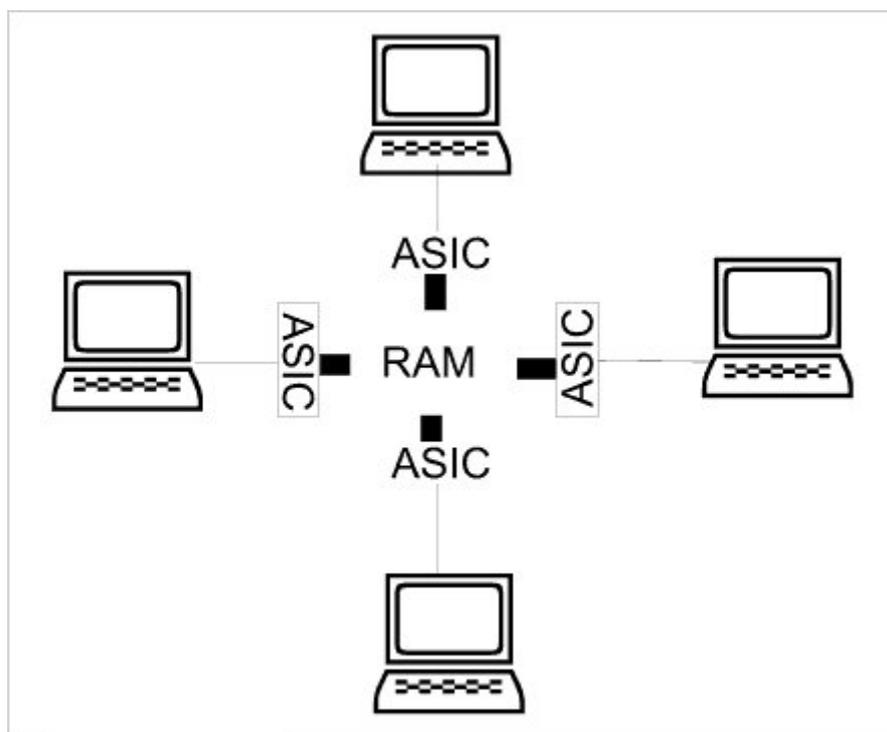


Рисунок 1.5 - Комутатори з поділюваною пам'яттю

3. На рисунку 1.6 показана блок-схема комутатора з високошвидкісною шиною, що зв'язує контролери ASIC. Після того, як дані перетворюються в прийнятний для передачі по шині формат, вони поміщаються на шину й далі передаються в порт призначення. Оскільки шина може забезпечувати одночасну (паралельну) передачу потоку даних від усіх портів, такі комутатори часто називають “неблокуємі” (non-blocking) - вони не створюють пробок на шляху передачі даних.

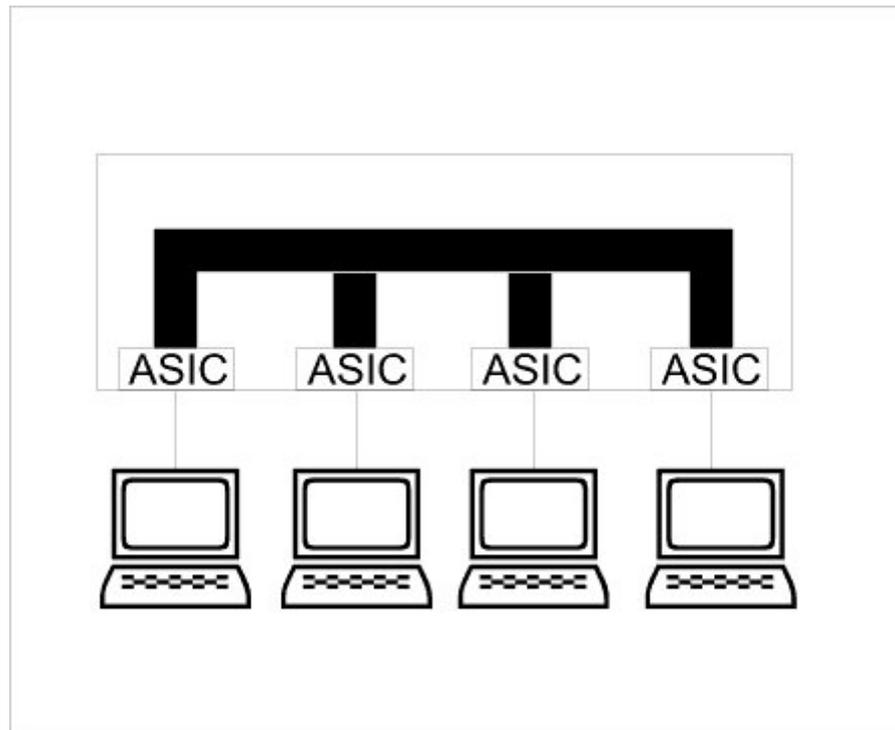


Рисунок 1.6 - Комутатор з високошвидкісною шиною

1.3 Комутація третього рівня

Застосування аналогічної паралельної архітектури для просування пакетів мережевих протоколів привело до появи комутаторів третього рівня моделі OSI. Це дозволило суттєво, в 10-100 раз підвищити швидкість маршрутизації в порівнянні із традиційними маршрутизаторами, у яких один центральний універсальний процесор виконує програмне забезпечення маршрутизації.

По визначенню Мережевий рівень (третій) - це комплексний рівень, який забезпечує можливість з'єднання й вибір маршруту між двома кінцевими системами, підключеними до різних "підмереж", які можуть перебувати в різних географічних пунктах. У цьому випадку "підмережа" це, по суті, незалежний мережевий кабель (іноді називаний сегментом).

Комутація на третьому рівні - це апаратна маршрутизація. Традиційні маршрутизатори реалізують свої функції за допомогою програмно-керованих процесорів, що будемо називати програмною маршрутизацією. Традиційні маршрутизатори звичайно просувають пакети зі швидкістю близько 500000

пакетів у секунду. Комутатори третього рівня сьогодні працюють зі швидкістю до 50 мільйонів пакетів у секунду. Можливо й подальше її підвищення, тому що кожен інтерфейсний модуль, як і в комутаторі другого рівня, оснащений власним процесором просування пакетів на основі ASIC. Так що нарощування кількості модулів веде до нарощування продуктивності маршрутизації. Використання високошвидкісної технології великих замовлених інтегральних схем (ASIC) є головною характеристикою, що відрізняє комутатори третього рівня від традиційних маршрутизаторів. Комутатори 3-го рівня діляться на дві категорії: пакетні (Packet-by-Packet Layer 3 Switches, PPL3) і наскрізні (Cut-Through Layer 3 Switches, CTL3). PPL3 - означає просто швидку маршрутизацію (рисунок 1.7). CTL3 – маршрутизацію першого пакета й комутацію всіх інших (рисунок 1.8).

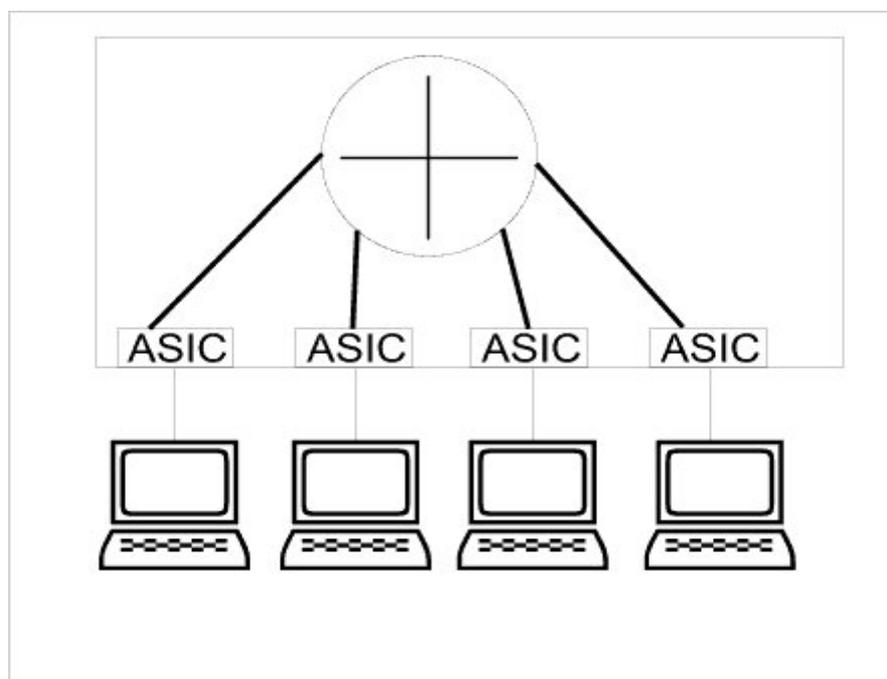


Рисунок 1.7 - Швидка маршрутизація

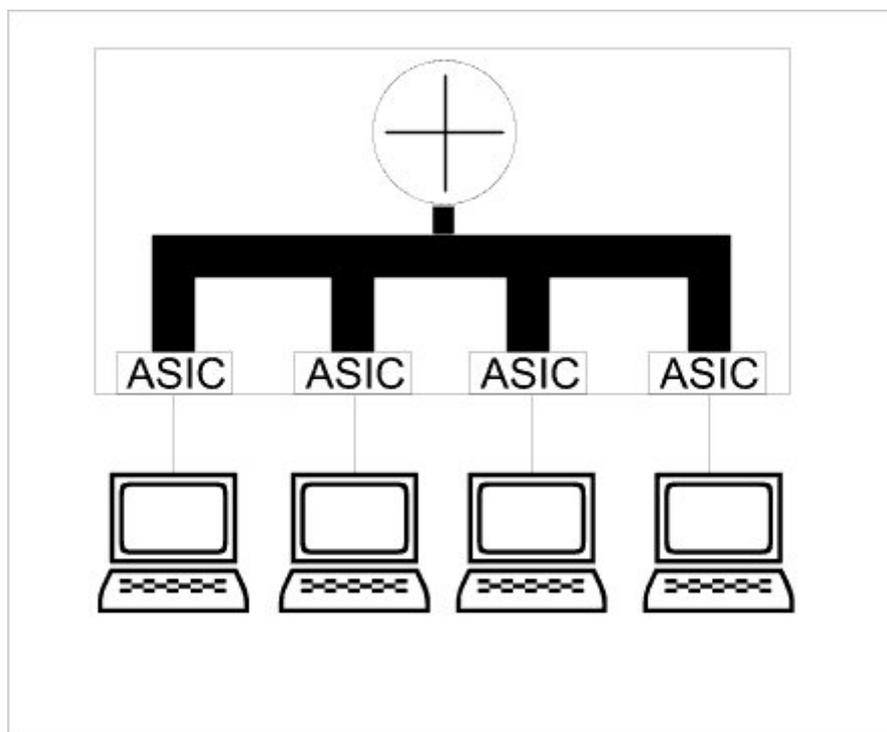


Рисунок 1.8 - Комутація першого пакета

У комутатора третього рівня, крім реалізації функцій маршрутизації в спеціалізованих інтегральних схемах, є кілька особливостей, що відрізняють їх від традиційних маршрутизаторів. Ці особливості відображають орієнтацію комутаторів 3-го рівня на роботу, в основному, у локальних мережах, а також наслідки сполучення в одному пристрої комутації на 2-м і 3-м рівнях:

- підтримка інтерфейсів і протоколів, застосовуваних у локальних мережах,
- усічені функції маршрутизації,
- обов'язкова підтримка механізму віртуальних мереж,
- тісна інтеграція функцій комутації й маршрутизації, наявність зручних для адміністратора операцій за завданням маршрутизації між віртуальними мережами.

Найбільша “комутаторна” версія високошвидкісної маршрутизації виглядає в такий спосіб (рисунок 1.9). Нехай комутатор третього рівня побудований так, що в ньому є інформація про відповідність мережеских адрес (наприклад, Ір-Адрес) адресам фізичного рівня (наприклад, Мас-Адресам) Усі ці Мас-Адреси

звичайним образом відображені в комутаційній таблиці, незалежно від того, чи належать вони даній мережі або іншим мережам.

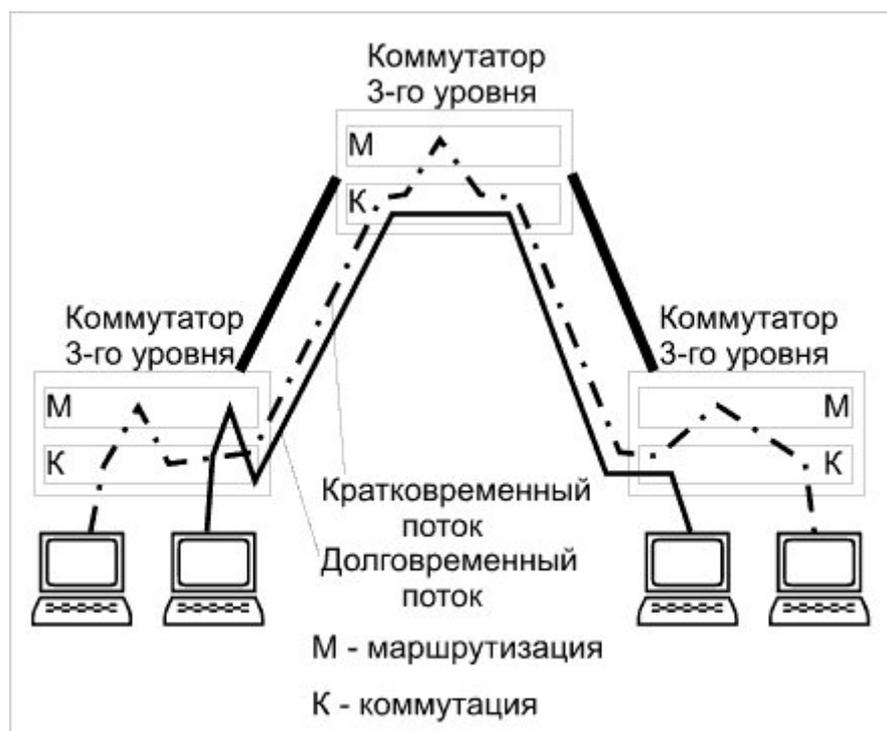


Рисунок 1.9 - Схема комутації при високошвидкісній маршрутизації

Перший комутатор, на який надходить пакет, частково виконує функції маршрутизатора, а саме, функції фільтрації, що забезпечують безпеку. Він вирішує, пропустити чи ні даний пакет в іншу мережу. Якщо пакет пропустити потрібно, то комутатор по Ір-адресі призначення визначає Мас-адресу вузла призначення й формує новий заголовок другого рівня зі знайденою Мас-адресою. Потім виконується звичайна процедура комутації по даному Мас-адресі з переглядом адресної таблиці комутатора. Усі наступні комутатори, побудовані по цьому ж принципу, обробляють даний кадр як звичайні комутатори другого рівня, не залучаючи функцій маршрутизації, що значно прискорює його обробку. Однак функції маршрутизації не є для них надлишковими, оскільки й на ці комутатори можуть надходити первинні пакети (безпосередньо від робочих станцій), для яких необхідно виконувати фільтрацію й підстановку Мас-адрес.

Цей опис носить схематичний характер і не розкриває способів розв'язку виникаючих при цьому численних проблем, наприклад, проблеми побудови таблиці відповідності Ір-адрес і Мас-адрес.

Прикладами комутаторів третього рівня, що працюють за цією схемою, є комутатори Smartswitch компанії Cabletron. Компанія Cabletron реалізувала в них свій протокол прискореної маршрутизації Securefast Virtual Network, SFVN.

Для організації безпосередньої взаємодії робочих станцій без проміжного маршрутизатора необхідно сконфігурувати кожен з них так, щоб вона вважала власний інтерфейс маршрутизатором за замовчуванням. При такій конфігурації станція намагається самостійно відправити будь-який пакет кінцевому вузлу, навіть якщо цей вузол перебуває в іншій мережі. Тому що в загальному випадку (рисунок 1.10) станції невідома Мас-адреса вузла призначення, то вона генерує відповідний Агр-Запит, який перехоплює комутатор, що підтримує протокол SFVN. У мережі передбачається наявність сервера SFVN Server, що є повноцінним маршрутизатором і підтримуючого загальну Агр-таблицю всіх вузлів Sfvn-Мережі. Сервер повертає комутатору Мас-адресу вузла призначення, а комутатор, у свою чергу, передає її вихідній станції. Одночасно сервер SFVN передає комутаторам мережі інструкції про дозвіл проходження пакета з Мас-адресою вузла призначення через границі віртуальних мереж. Потім вихідна станція передає пакет у кадрові, що містить Мас-адресу вузла призначення. Цей кадр проходить через комутатори, не викликаючи звертання до їхніх блоків маршрутизації. Відмінність протоколу SFVN компанії Cabletron від - описаної вище загальної схеми в тому, що для знаходження Мас-адреси по Ір-адресі в мережі використовується виділений сервер.

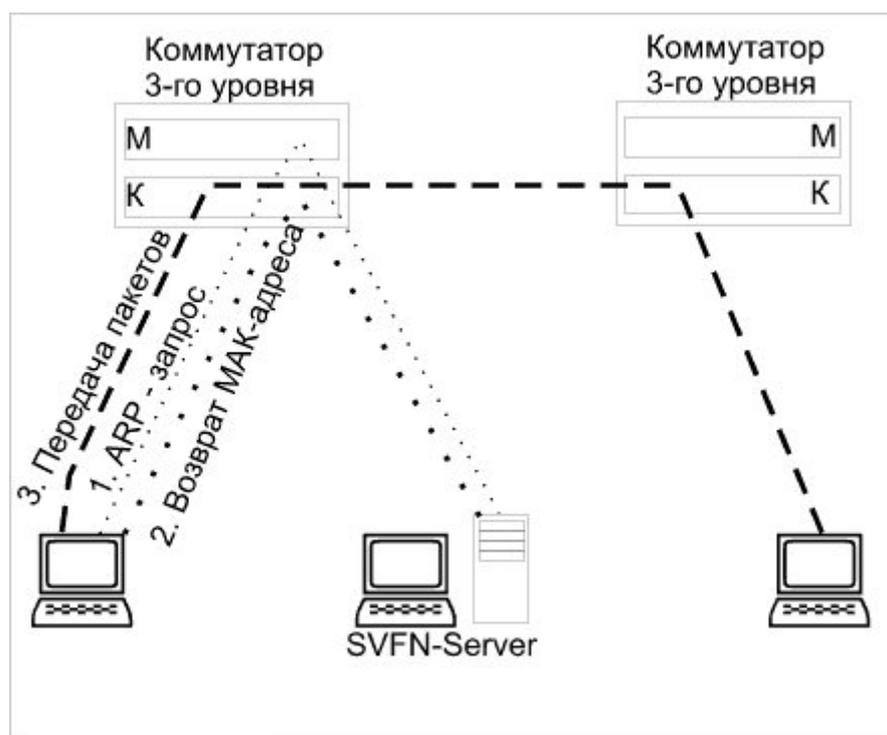


Рисунок 1.10 - SVFN-мережа

Протокол Fast IP компанії 3Com є ще одним прикладом реалізації підходу з відображенням Ір-адреси на Мас-адреси. У цьому протоколі основними діючими особами є мережеві адаптери (що не дивно, тому що компанія 3Com є визнаним лідером у виробництві мережевих адаптерів Ethernet) З одного боку, такий підхід вимагає зміни програмного забезпечення драйверів мережевих адаптерів, і це мінус, але зате не потрібно змінювати все інше мережеве встаткування.

При необхідності передати пакет вузлу призначення іншої мережі, вихідний вузол відповідно до технології Fast IP повинен передати запит по протоколу NHRP (Next Hop Routing Protocol) маршрутизатору мережі. Маршрутизатор переправляє цей запит вузлу призначення, як звичайний пакет Вузол призначення, який також підтримує Fast IP і NHRP, одержавши запит, відповідає кадром, що відсилаються вже не маршрутизатору, а безпосередньо вузлу-джерелу (по його Мас-адресі, що втримується в Nhrp-Запиті). Після цього обмін іде на каналному рівні на основі відомих Мас-адрес. Таким чином, знову маршрутизувався тільки перший пакет потоку (як на рисунку 1.9 короткочасний потік), а всі інші комутувалися (як на рисунку 1.9 довгочасний потік).

Ще один тип комутаторів третього рівня — це комутатори, що працюють із протоколами локальних мереж типу Ethernet і FDDI. Ці комутатори виконують функції маршрутизації не так, як класичні маршрутизатори. Вони маршрутизують не окремі пакети, а потоки пакетів.

Потік — це послідовність пакетів, що мають деякі загальні властивості. Щонайменше, у них повинні збігатися адреса відправника й адреса одержувача, і тоді їх можна відправляти по тому самому маршруту. Якщо класичний спосіб маршрутизації використовувати тільки для першого пакета потоку, а всі інші обробляти на підставі досвіду першого (або декількох перших) пакетів, то можна значно прискорити маршрутизацію всього потоку.

Розглянемо цей підхід на прикладі технології Netflow компанії Cisco, реалізованої в її маршрутизаторах і комутаторах. Для кожного пакета, що надходить на порт маршрутизатора, обчислюється хеш-функція від Ір-адреси джерела, призначення, портів UDP або TCP і поля TOS, що характеризує необхідне якість обслуговування. У всіх маршрутизаторах, що підтримують дану технологію, через які проходить даний пакет, у кеш-пам'яті портів запам'ятовується відповідність значення хеш-функції й адресної інформації, необхідної для швидкої передачі пакета наступному маршрутизатору. Таким чином, утворюється квазивіртуальний канал (рис. 1.11), який дозволяє швидко передавати по мережі маршрутизаторів усі наступні пакети цього потоку. При цьому прискорення досягається за рахунок спрощення процедури обробки пакета маршрутизатором - не проглядаються таблиці маршрутизації, не виконуються Арр-Запити.

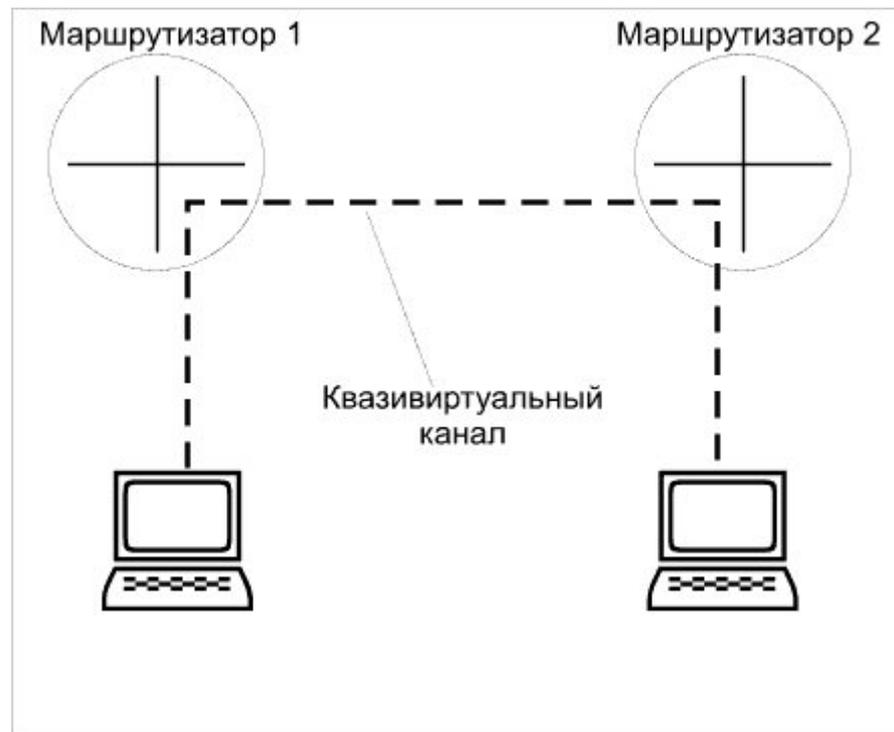


Рисунок 1.11 - Маршрутизація потоками пакетів

Цей прийом може використовуватися в маршрутизаторах, що взагалі не підтримують комутацію, а може бути перенесений у комутатори. У цьому випадку такі комутатори теж називають комутаторами третього рівня. Прикладів маршрутизаторів, що використовують даний підхід, є маршрутизатори Cisco 7500, а комутаторів третього рівня — комутатори Catalyst 5000 і 5500. Комутатори Catalyst виконують усічені функції описаної схеми, вони не можуть обробляти перші пакети потоків і створювати нові записи про хеш-функції і адресу інформацію потоків. Вони просто одержують дану інформацію від маршрутизаторів 7500 і обробляють пакети вже розпізнаних маршрутизаторами потоків.

Вище був розглянутий спосіб прискореної маршрутизації, заснований на концепції потоку. Його сутність полягає в створенні квазивіртуальних каналів у мережах, які не підтримують віртуальні канали у звичайному розумінні цього терміна, тобто мережах Ethernet, FDDI, Token Ring і т.п. Слід відрізнити цей спосіб від способу прискореної роботи маршрутизаторів у мережах віртуальних каналів, що підтримують технологію, — ATM, frame relay, X.25. У таких мережах

створення віртуального каналу є штатним режимом роботи мережевих пристроїв. Віртуальні канали створюються між двома кінцевими крапками, причому для потоків даних, що вимагають різної якості обслуговування (наприклад, для даних різних додатків) може створюватися окремий віртуальний канал. Хоча час створення віртуального каналу суттєво перевищує час маршрутизації одного пакета, вигравш досягається за рахунок наступної швидкої передачі потоку даних по віртуальному каналу. Але в таких мережах виникає інша проблема — неефективна передача коротких потоків, тобто потоків, що полягають із невеликої кількості пакетів (класичний приклад — пакети протоколу DNS).

Накладні витрати, пов'язані зі створенням віртуального каналу, що доводяться на один пакет, знижуються при передачі об'ємних потоків даних. Однак вони стають неприйнятно високими при передачі коротких потоків. Для того щоб ефективно передавати короткі потоки, пропонується наступний варіант, при передачі декількох перших пакетів виконується звичайна маршрутизація. Потім, після того як розпізнається стійкий потік, для нього будується віртуальний канал, і подальша передача даних відбувається з високою швидкістю по цьому віртуальному каналу. Таким чином, для коротких потоків віртуальний канал взагалі не створюється, що й підвищує ефективність передачі.

За такою схемою працює вже класичної технологія, що стала, IP Switching компанії Ipsilon. Для того щоб мережі комутаторів АТМ передавали б пакети коротких потоків без установаження віртуального каналу, компанія Ipsilon запропонувала вмонтувати в усі комутатори АТМ блоки Ір-маршрутизації (рисунок 1.12) звичайні таблиці, що будують, маршрутизації по звичайних протоколах RIP і OSPF.

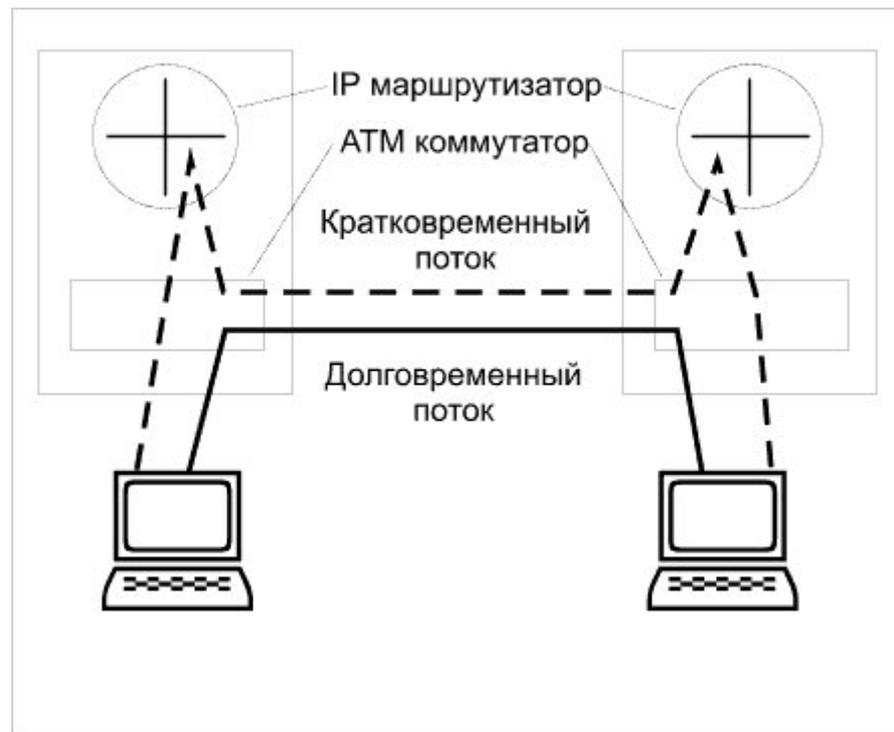


Рисунок 1.12 - Використання АТМ-маршрутизації

Компанія Cisco Systems висунула в якості альтернативи технології IP Switching свою власну технологію Tag Switching, але вона не стала стандартною. У цей час IETF працює над стандартним протоколом обміну мітками MPLS (*Multi-Protocol Label Switching*), який узагальнює пропозиція компаній Ipsilon і Cisco, а також вносить деякі нові деталі й механізми. Цей протокол орієнтований на підтримку якості обслуговування для віртуальних каналів, утворених мітками.

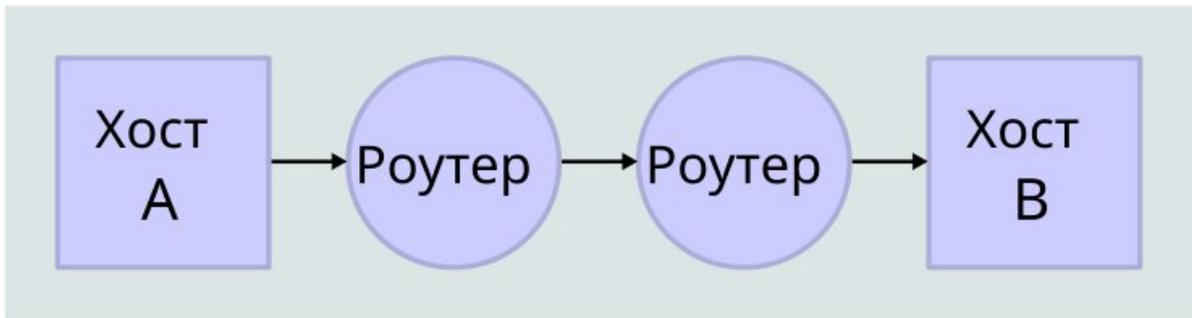
1.4 Комутація четвертого рівня

Властивості четвертого або транспортного рівня моделі OSI наступні: транспортний рівень забезпечує послуги із транспортування даних. Зокрема, турботою транспортного рівня є розв'язок таких питань, як виконання надійного транспортування даних через об'єднану мережу. Надаючи надійні послуги, транспортний рівень забезпечує механізми для установки, підтримки й упорядкованого завершення дії віртуальних каналів, систем виявлення й усунення

несправностей транспортування й керування інформаційним потоком (з метою запобігання переповнення даними з іншої системи).

Деякі виробники заявляють, що їх системи можуть працювати на другому, третьому й навіть четвертому рівнях. Однак розгляд опису стека TCP/IP (рисунок 1.13), а також структури пакетів IP і TCP (рисунок 1.14, 1.15), показує, що комутація четвертого рівня є фікцією, тому що всі стосовні до комутації функції здійснюються на рівні не вище третього. А саме, термін комутація четвертого рівня з погляду опису стека TCP/IP протиріч не має, за винятком того, що при комутації повинні вказуватися адреси комп'ютера (маршрутизатора) джерела й комп'ютера (маршрутизатора) одержувача. Пакети TCP мають поля локальний порт відправника й локальний порт одержувача, що несуть зміст точок входу в додаток (у програму), наприклад Telnet з одного боку, і точки входу (у даному контексті інкапсуляції) уривень IP. Крім того, у стеці TCP/IP саме рівень TCP займається формуванням пакетів з потоку даних, що йдуть від додатка. Пакети IP мають поля адреси комп'ютера (маршрутизатора) джерела й комп'ютера (маршрутизатора) одержувача й отже можуть поряд з MAC адресами використовуватися для комутації. Проте, назва прижилася, до того ж практика показує, що здатність системи аналізувати інформацію прикладного рівня може виявитися корисною — зокрема для керування трафіком. Таким чином, термін “залежний від додатка” більш точно відбиває функції так званих комутаторів четвертого рівня.

Топологія мереж



Потік даних

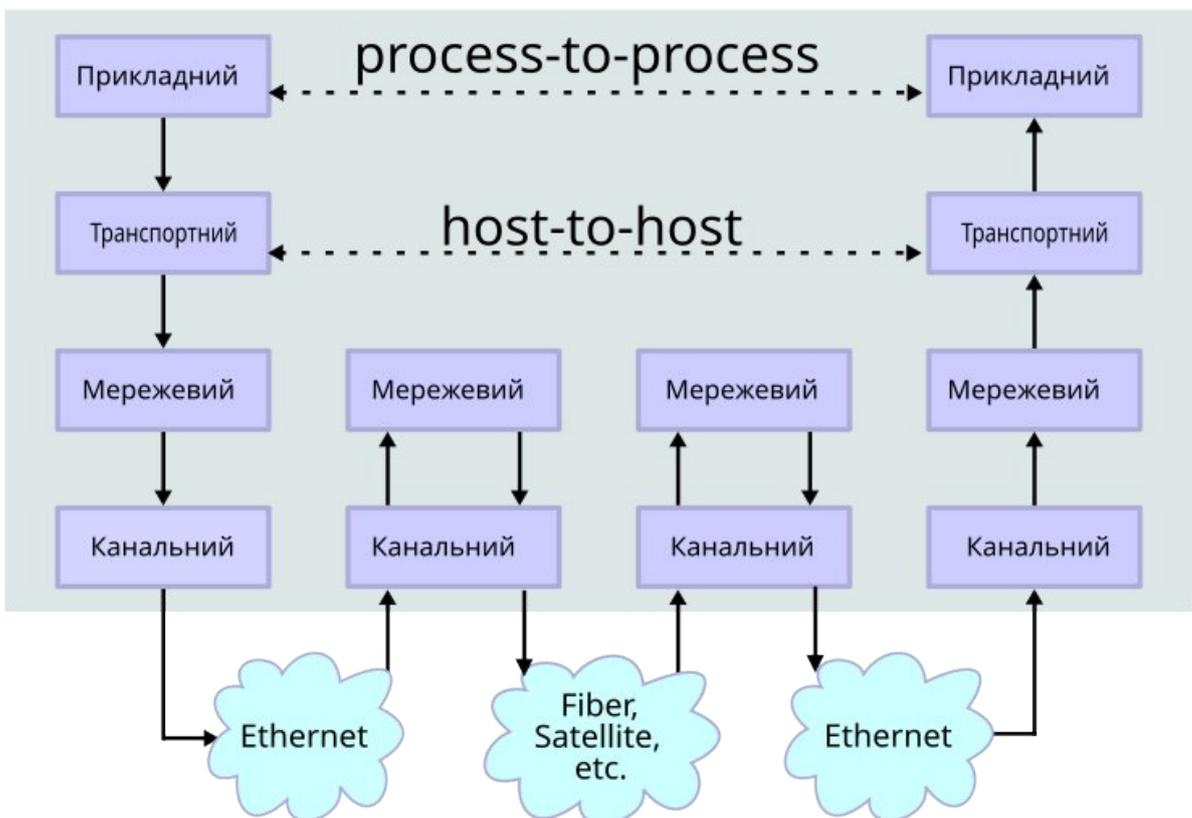


Рисунок 1.13 - Модель стеку TCP/IP

2 ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ

VLAN (Virtual Local Area Network) — група пристроїв, що мають можливість взаємодіяти між собою прямо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережевих комутаторів. І навпаки, пристрої, що перебувають у різних Vlan'ах, невидимі друг для друга на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому й більш високих рівнях.

У сучасних мережах VLAN — головний механізм для створення логічної топології мережі, що не залежить від її фізичної топології. VLAN'и використовуються для скорочення широкомовного трафіка в мережі. Мають велике значення з погляду безпеки, зокрема як засіб боротьби з Arp-Spoofing'ом.

2.1 Потреби використання VLAN

1. Гнучкий поділ пристроїв на групи

Як правило, одному VLAN відповідає одна підмережа. Пристрої, що перебувають у різних VLAN, будуть перебувати в різних підмережах. Але в той же час VLAN не прив'язаний до місця розташування пристроїв і тому пристрої, що перебувають на відстані друг від друга, однаково можуть бути в одному VLAN незалежно від місця розташування

2. Зменшення кількості широкомовного трафіка в мережі

Кожний VLAN — це окремий широкомовний домен. Наприклад, комутатор — це пристрій 2 рівня моделі OSI. Усі порти на комутаторі, де немає Vlan-ів, перебувають в одному широкомовному домені. Створення VLAN на комутаторі означає розбивку комутатора на кілька широкомовних доменів. Якщо той самий VLAN є на різних комутаторах, то порти різних комутаторів будуть утворювати один широкомовний домен.

3. Збільшення безпеки й керованості мережі

Коли мережа розбита на VLAN, спрощується завдання застосування політик і правил безпеки. З VLAN політики можна застосовувати до цілих підмереж, а не до окремого пристрою. Крім того, перехід з одного VLAN в інший припускає проходження через пристрій 3 рівня, на якому, як правило, застосовуються політики, що дозволяють або забороняють доступ з VLAN в VLAN.

2.2 Тегування трафіка VLAN

Комп'ютер при відправленні трафіка в мережу навіть не догадується, у якому Vlan'і він розміщений. Про це думає комутатор. Комутатор знає, що комп'ютер, який підключений до певного порту, перебуває у відповідному Vlan'і. Трафік, що приходить на порт певного Vlan'у, нічим особливим не відрізняється від трафіка іншого Vlan'у. Інакше кажучи, ніякої інформації про приналежність трафіка певному Vlan'у в ньому немає.

Однак, якщо через порт може прийти трафік різних Vlan'ів, комутатор повинен його якось розрізнити. Для цього кожний кадр (frame) трафіка повинен бути позначений якимось особливим образом. Позначка повинна говорити про те, якому Vlan'у трафік належить.

Найпоширеніший зараз спосіб ставити таку позначку описаний у відкритому стандарті IEEE 802.1Q. Існують пропріетарні протоколи, що вирішують схожі завдання, наприклад, протокол ISL від Cisco Systems, але їх популярність значно нижче (і знижується).

2.3 Комутатор і Vlan'и

Vlan'и можуть бути настроєні на комутаторах, маршрутизаторах, інших мережних пристроях і на хостах. Однак, для пояснення VLAN найкраще підійде комутатор.

Комутатор - пристрій 2го рівня й споконвічно всі порти комутатора перебувають, як правило, в VLAN 1 і, отже, в одному широкомовному сегменті.

Це значить, що якщо один з хостів, підключених до комутатора, відправить широкомовний фрейм, те всі інші хости підключені до нього також одержать його.

2.3.1 Принципи роботи комутатора

Для цього розділу комутатор обговорюється з налаштуваннями за замовчуванням, тобто, усі порти перебувають в VLAN 1.

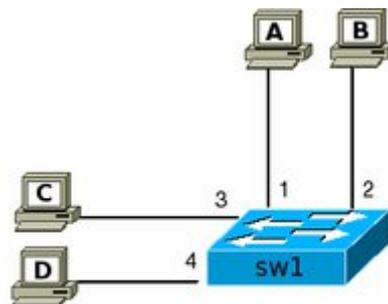


Рисунок 2.1 Схема мережі з комутатором

Для того щоб передавати фрейми, комутатор використовує таблицю комутації. Споконвічно, після включення комутатора таблиця порожня. Заповнює її комутатор автоматично, при одержанні фреймів від хостів. Коли комутатор одержує фрейм від хосту, він спочатку передає його у відповідності зі своїми правилами (описані нижче), а потім запам'ятовує Mac-адресу відправника у фреймі й ставить його у відповідність порту на якому він був отриманий.

Наприклад, для зображеної схеми, підсумкова таблиця комутації буде мати такий вид (після того як усі хости передавали якийсь трафік) (табл.2.1):

Таблиця 2.1 – Таблиця комутації для схеми на рис.2.1.

Порт комутатора	Mac-адреса хосту
1	A
2	B
3	C
4	D

Коли таблиця заповнена, комутатор знає на яких портах у нього перебувають які хости й передає фрейми на відповідні порти.

Unicast фрейм із Mac-адресою одержувача для якого в комутатора немає записи в таблиці комутації, називається unknown unicast.

2.3.2 Механізми передачі фреймів

Для того щоб передавати фрейми комутатор використовує три базові механізми:

- Flooding — фрейм отриманий на один з портів передається на інші порти комутатора. Комутатор виконує цю операцію у двох випадках:
 - при одержанні ширококомовного або multicast (якщо не настроєна підтримка multicast) фрейму,
 - при одержанні unknown unicast фрейму. Це дозволяє комутатору доставити фрейм хосту (за умови, що хост досяжний і існує), навіть коли він не знає де хост перебуває.
- Forwarding — передача фрейму отриманого на одному порті через інший порт відповідно до запису в таблиці комутації.
- Filtering— якщо комутатор одержує фрейм через певний порт і Mac-адреса одержувача доступна через цей же порт (це зазначене в таблиці комутації), то комутатор відкидає фрейм. Тобто, комутатор вважає, що в цьому випадку хост уже одержав цей фрейм і не дублює його.

На рис.2.2 зображений комутатор sw1 і повторювач (hub) до якого підключено два хости.

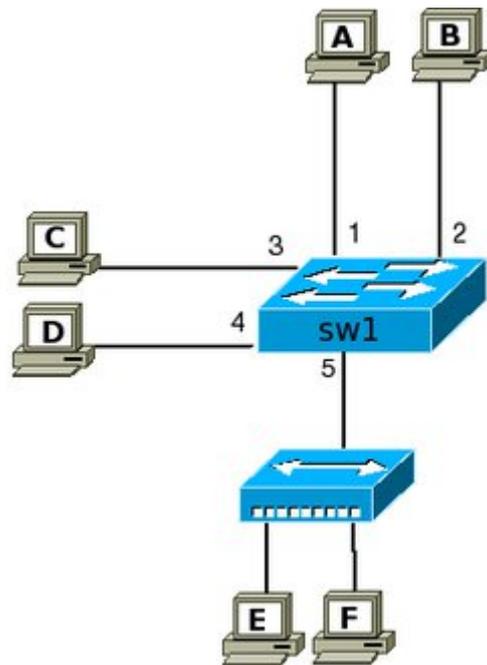


Рисунок 2.2 - Приклад мережі для демонстрації використання механізмів передачі фреймів

Спочатку до комутатора були підключено три хости А, В і С. Відповідно в комутатору така таблиця комутації (табл. 2.2.)

Таблиця 2.2 – Таблиця комутації з трьома хостами

Порт комутатора	Мас-адреса хосту
1	А
2	В
3	С

Коли хост А відправляє фрейм хосту В, комутатор використовує механізм forwarding, тому що йому відомо де перебувають обидва хости й хости перебувають на різних портах комутатора.

Далі до комутатора підключили хост D. Якщо хост А відправляє фрейм хосту D, то для комутатора це unknown unicast фрейм, тому що в таблиці комутації немає запису про Мас-адресу D. У відповідності зі своїми правилами комутатор виконує flooding і передає фрейм на всі порти, крім 1 (з якого фрейм був отриманий).

Після того як комутатор одержить фрейм від хосту D, він запам'ятає його адресу й створить відповідний запис у таблиці комутації.

До комутатора підключили повторювач із двома хостами й комутатор вивчив їхні адреси. Відповідна таблиця комутації (табл. 2.3.):

Таблиця 2.3 – Таблиця комутації з 6 хостами

Порт комутатора	Мас-адреса хосту
1	A
2	B
3	C
4	D
5	E
5	F

Якщо після цього хост E буде передавати фрейм хосту F, то комутатор одержить його, але не буде передавати далі. У цій ситуації комутатор використовує механізм filtering, тому що Мас-адреса одержувача доступна через той же порт, що й відправник.

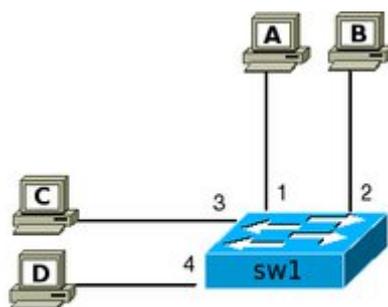


Рисунок 2.3 - Хости в одному VLAN на одному комутаторі

До комутатора підключено 4 хости. Для спрощення будемо вважати, що A, B, C і D це відповідні Мас-адреси хостів.

Відповідна таблиця комутації (табл.2.4.):

Таблиця 2.4 – Таблиця комутації з 4 хостами

Порт комутатора	Мас-адреса хосту
1	A
2	B
3	C
4	D

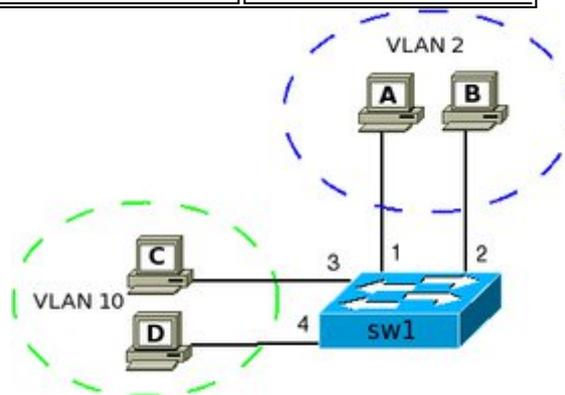


Рисунок 2.4 - Хости в різних VLAN на одному комутаторі

Звичайно, за замовчуванням усі порти комутатора вважаються нетегованими членами VLAN 1. У процесі настроювання або роботи комутатора вони можуть переміщатися в інші Vlan'и.

На комутаторі, який зображений на малюнку, настроєно два Vlan'и, усі порти настроєні як нетеговані (access-порти в термінології Cisco) у відповідних VLAN.

Після цього на комутаторі існують дві таблиці комутації (табл. 2.5.).

Для Vlan'у 2:

Таблиця 2.5 – Таблиця комутації з двома Vlan

Порт комутатора	Мас-адреса хосту
1	A
2	B

Для Vlan'у 10:

Порт комутатора	Мас-адреса хосту
3	C
4	D

Усі базові механізми комутатора залишаються точно такими ж як і до поділу на VLAN, але вони використовуються тільки в межах відповідного VLAN.

Наприклад, якщо хост із VLAN 10 відправляє ширококомовний фрейм, то він буде відправлений тільки на порти в цьому VLAN.

Виходить, що нетеговані порти це "звичайні" порти комутатора. Це просто можливість повідомити комутатор про те, якому VLAN-у належать порти. Потім комутатор використовує цю інформацію при передачі фреймів.

Як правило, реально в таблиці комутації в комутаторах вказується порт, Мас-адреса й VLAN. Тобто, для зазначеного прикладу таблиця комутації буде така (табл.2.6.):

Таблиця 2.6 – Таблиця комутації результуюча

Порт комутатора	VLAN	Мас-адреса хосту
1	2	A
2	2	B
3	10	C
4	10	D

Однак, далі для спрощення використовується запис таблиці комутації у вигляді відповідності між портами й Мас-Адресами.

2.3.3 Хости в різних VLAN на різних комутаторах

До використовуваного прикладу додається ще один комутатор.

Доданий другий комутатор і хости в VLAN 2

Для початку доданий комутатор sw2 і два хости E і F в VLAN 2. Якщо розглядати два комутатори окремо, то виходить, що на комутаторі sw1

залишилася колишня таблиця комутації, а на комутаторі sw2 таблиця така (поки що комутатори не з'єднані) (табл 2.7.):

Таблиця 2.7 – Таблиця комутації другого комутатора

Порт комутатора	Мас-адреса хосту
7	E
8	F

Тепер необхідно щоб хости A, B, E, F "побачили" один одного. Вони повинні перебувати в одному VLAN. Тобто, необхідно якимось образом указати комутатору, що ще на одному порті є хости у відповідному Vlan'і.

Для зазначеного прикладу досить додати на комутаторі sw1 порт 10 в VLAN 2, а на комутаторі sw2 порт 9 в VLAN 2. Приналежність до VLAN вказується настроюванням порту нетегованим в VLAN 2 (поки що). Після цього на комутаторах у таблицях комутації додадуться нові порти й відповідні Мас-адреси хостів. Тепер чотири хости на різних комутаторах перебувають в одному широкомовному сегменті.

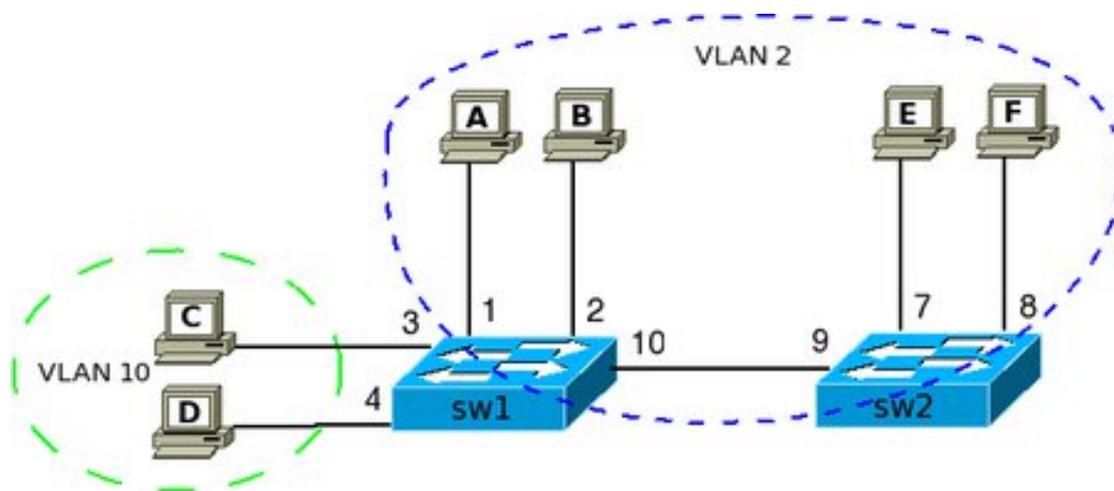


Рисунок 2.5 - Хости в різних VLAN на різних комутаторах

Таблиця комутації sw1 для VLAN'а 2 (табл. 2.8.):

Таблиця 2.8 – Таблиця комутації для VLAN'а 2

Порт комутатора	Мас-адреса хосту
1	A
2	B
10	E
10	F

Таблиця комутації sw2 для VLAN'у 2 (табл. 2.9):

Таблиця 2.9 – Таблиця комутації для sw2 для VLAN'у 2

Порт комутатора	Мас-адреса хосту
7	E
8	F
9	A
9	B

До другого комутатора додані хости в VLAN 10

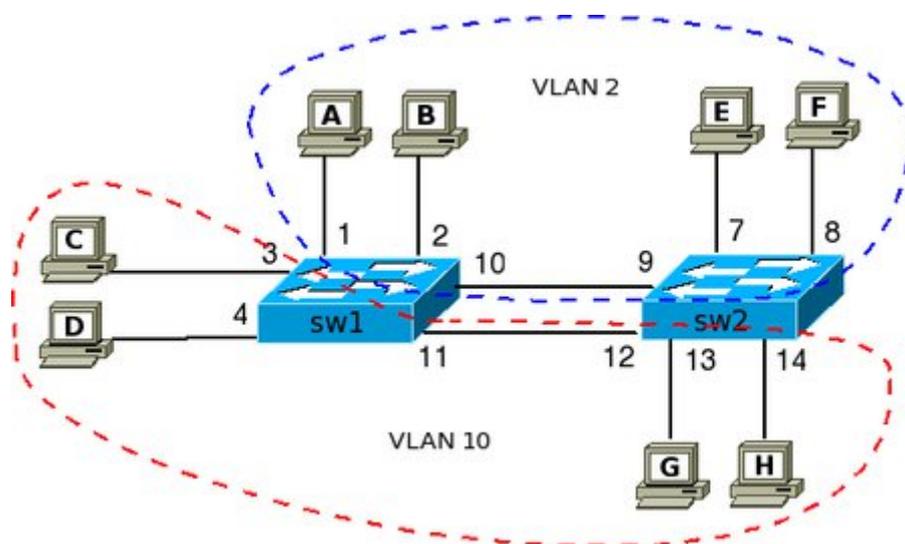


Рисунок 2.6 - Хости різних VLAN на різних комутаторах

До комутатора sw2 додано два хости G і H в VLAN 10.

Для того щоб хости C і D в Vlan'і 10 на комутаторі sw1, могли обмінюватися інформацією з хостами Vlan'у 10 на комутаторі sw2 доданий лінк між комутаторами. Логіка аналогічна додаванню хостів в VLAN 2.

Таблиця комутації sw1 для VLAN'а 10 (табл. 2.10):

Таблиця 2.10 – Таблиця комутації для sw1 для VLAN'а 10

Порт комутатора	Мас-адреса хосту
3	C
4	D
11	G
11	H

Таблиця комутації sw2 для VLAN'а 10 (табл. 2.11.):

Таблиця 2.11 – Таблиця комутації для sw2 для VLAN'а 10

Порт комутатора	Мас-адреса хосту
13	G
14	H
12	C
12	D

2.3.4 Створення тегового порту між комутаторами

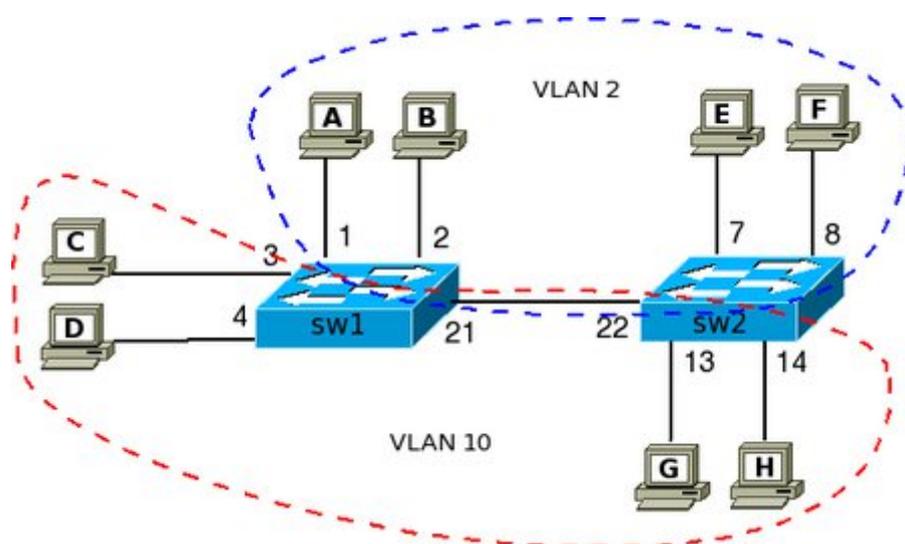


Рисунок 2.7 - Передумови створення тегового порту

Коли необхідно передати трафік одного-двох Vlan'ів між комутаторами, то схема, яка використовувалася вище виглядає нормально. Однак, коли кількість VLAN зростає, то схема явно стає дуже незручною, тому що для кожного VLAN треба буде додавати лінк між комутаторами для того щоб об'єднати хости в один ширококомовний сегмент.

Для розв'язку цієї проблеми використовуються теговані порти.

Тегований порт дозволяє комутатору передати трафік декількох Vlan'ів через один порт і зберегти при цьому інформацію про те, у межах якого саме Vlan'у передається фрейм.

На комутаторах sw1 і sw2 порти 21 і 22, відповідно, це теговані порти.

Для того щоб комутатори розуміли якому VLAN належить отриманий фрейм і використовували відповідну таблицю комутації для його обробки, виконується тегування фрейму.

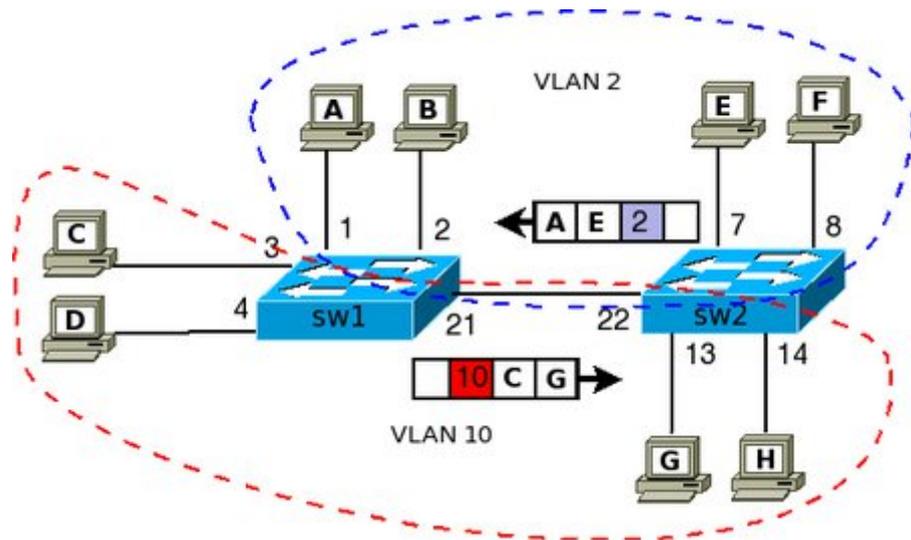


Рисунок 2.8 - Створення тегового порту

Наприклад, якщо хост Е передає фрейм хосту А, то комутатор sw2 перевіряє свою таблицю й бачить, що хост А доступний через порт 22. Так як порт настроений як тегований, то коли фрейм виходить із порту 22 у ньому проставляється тег, який вказує якому Vlan'і належить цей фрейм. У цьому випадку проставляється тег з Vlan'ом 2.

Комутатор sw1 одержує тегований фрейм через тегований порт 21. Для того щоб визначити на який порт його передавати далі sw1 використовує таблицю комутації для VLAN 2 (тому що цей VLAN був зазначений у тегу). На комутаторі sw1 порт 21 повинен бути настроєний як тегований для того щоб комутатор не відкидав теговані фрейми, а зчитував інформацію тегу. І відповідно щоб він також позначав фрейм тегом, коли буде передаватися трафік комутатору sw2.

Інші порти комутатора залишаються нетегованими. І для хостів операція тегування, яку виконують комутатори абсолютно прозора. Хости нічого не знають про теги й одержують звичайні фрейми.

Аналогічні дії виконуються, наприклад, при передачі фрейму від хосту С хосту G.

2.3.5 Приналежність VLAN

Порти комутатора, що підтримують Vlan'и, (з деякими допущеннями) можна розділити на дві множини:

1. Теговані порти (або транкові порти, *trunk-порти* в термінології Cisco).
2. Нетеговані порти (або порти доступу, *access-порти* в термінології Cisco);

Теговані порти потрібні для того, щоб через один порт була можливість передати кілька Vlan'ів і, відповідно, одержувати трафік декількох Vlan'ів на один порт. Інформація про приналежність трафіка Vlan'у, як було сказано вище, вказується в спеціальному тегу. Без тегу комутатор не зможе розрізнити трафік різних Vlan'ів.

Якщо порт нетегований у якомусь Vlan'і, то трафік цього VLAN передається без тегу. На Cisco нетегованим порт може бути тільки в одному VLAN, на деяких інших світчах (наприклад, Zyxel, D-Link і Planet) даного обмеження немає.

Якщо порт теговано для декількох VLAN'ів, то в цьому випадку весь нетегований трафік буде ухвалюватися спеціальним *рідним* VLAN'им (native VLAN). Із цим параметром (native, PVID, port VID) виникає найбільше плутанини.

Наприклад, світчі Planet для правильної роботи untagged порту вимагають помістити порт в VLAN, задати режим порту untagged, і прописати цей же номер VLAN в PVID цього порту. HP Procurve роблять навпаки, tagged порт починає працювати як tagged тільки якщо поставити його PVID в "None".

Якщо порт належить тільки одному VLAN як нетегований, то тегований трафік, що приходить через такий порт, повинен видалятися. На ділі ця поведінка звичайна настроюється.

Простіше всього це зрозуміти, якщо "забути" усю внутрішню структуру комутатора й відштовхуватися тільки від портів. Допустимо, є VLAN з номером 111, є два порти які належать до VLAN 111. Вони спілкуються тільки між собою, з untagged/ access-порту виходить нетегований трафік, з tagged/ trunk-порту виходить трафік тегований в VLAN 111. Усі необхідні перетворення прозора усередині себе робить комутатор.

Звичайно, за замовчуванням усі порти комутатора вважаються нетегованими членами VLAN 1. У процесі настроювання або роботи комутатора вони можуть переміщатися в інші Vlan'и.

Існують два підходи до призначення порту в певний VLAN:

1. *Статичне призначення* — коли приналежність порту VLAN'у задається адміністратором у процесі настроювання;
2. *Динамічне призначення* — коли приналежність порту VLAN'у визначається в ході роботи комутатора за допомогою процедур, описаних у спеціальних стандартах, таких, наприклад, як 802.1X. При використанні 802.1X для того щоб одержати доступ до порту комутатора, користувач проходить аутентифікацію на Radius-сервері. За результатами аутентифікації порт комутатора розміщується в тому або іншому Vlanі.

3 НАЛАШТУВАННЯ КОМУТАТОРУ D-LINK DES-3526 ДЛЯ СЕГМЕНТАЦІЇ ТРАФІКУ В ЛОКАЛЬНІЙ МЕРЕЖІ

3.1 Постановка задачі

В наявності є локальна мережа коледжу, орієнтовна кількість комп'ютерів – 100 одиниць. 99% комп'ютерів працюють під управлінням операційної системи WindowsXP.

Як відомо, комп'ютери під управлінням Microsoft Windows при роботі в мережі генерують ширококомовний трафік NetBIOS для отримання інформації про структуру мережі. При невеликій кількості комп'ютерів ширококомовний трафік не є помітним, але зростання кількості обладнання веде до збільшення об'єму ширококомовного трафіку і до підвищення навантаження на магістральне обладнання.

При виникненні затримок в роботі локальної мережі необхідно сегментувати трафік в мережі, щоб уникнути зайвого навантаження.

3.2 Розв'язок задачі

Для вирішення проблеми надлишкового трафіку в локальній мережі коледжу було закуплено 24-портовий мережевий комутатор 2-го рівня моделі DES-3526.

Використання комутаторів другого рівня в якості центральних (магістральних) дозволяє не тільки підвищити пропускну здатність центрального вузлу, але й ввести певний контроль (обмеження пропускну здатності для окремих сегментів, контроль підключення лише окремих комп'ютерів за допомогою контролю MAC-адресів, та багато інших функцій).

В даному випадку основна функція керування комутаторів 2-го рівня, яка нас цікавить – це сегментація трафіку за допомогою Vlan-ів.

3.3 Комутатор DES-3526. Характеристики

Комутатори серії 10/100 Мбіт/з D-Link DES-3500 є взаємно стекуємими комутаторами рівня доступу, що підтримують технологію Single IP Management (SIM, керування через єдину Ір-адресу). Ці комутатори, що мають 24 або 48 10/100BASE-TX портів і 2 комбо-порти 1000BASE-T/SFP Gigabit Ethernet у стандартному корпусі для установки в стійку, розроблені для гнучкого й безпечного мережевого підключення. Комутатори серії DES-3500 можуть легко поєднуватися в стек і налаштовуватися разом з будь-якими іншими комутаторами з підтримкою D-Link Single IP Management, включаючи комутатори 3-го рівня ядра мережі, для побудови частини багаторівневої мережі, структурованої з магістраллю й централізованими швидкодіючими серверами.

Економічний віртуальний стек - В загальному, комутатори серії DES-3500 формують стек мережі рівня підрозділу, надаючи порти 10/100 Мбіт/з і можливість організації гигабітного підключення до магістралі. Трафік, переданий між пристроями стеку, проходить через інтерфейси Gigabit Ethernet з підтримкою повного дуплекса й звичайні проводи мережі, дозволяючи уникнути використання дорогих і громіздких кабелів для стекування. Відмова від використання цих кабелів дозволяє усунути бар'єри, пов'язані з їхньою довжиною й обмеженнями методів стекування. У стек можуть бути об'єднані пристрої, розташовані в будь-якому місці мережі, виключаючи можливості появи будь-якої точки єдиної відмови (single point of failure).

Керування через єдину Ір-адресу (Single IP Management) - Комутатори серії DES-3500 спрощують і прискорюють задачу керування, тому що множина комутаторів можуть налаштовуватися, контролюватися й обслуговуватися через унікальну Ір-адресу з будь-якої робочої станції, що має Web-Браузер. Стек управляється як єдиний об'єкт, і всі пристрої стека визначаються по єдиній Ір-адресі. За допомогою вбудованого Web-Менеджера, можна одержати інформацію, представлену у вигляді дерева (Tree View) про члени стека й топології мережі із вказівкою місця розташування пристроїв стека й зв'язків між

ними. Таке просте й досить ефективне Web-керування виключає необхідність встановлення дорогого ПО для Snmp-керування.

Розширення до 32 пристроїв у стеці - В стек можна легко об'єднати до 32-х комутаторів, незалежно від моделі. Віртуальний стік підтримує будь-які моделі комутаторів із вбудованим Single IP Management. Це означає, що стік може бути розширений комутаторами, включаючи комутатори 3-го рівня для ядра мережі, комутатори на основі шасі або будь-які інші комутатори.

Розширені функції безпеки - Серія DES-3500 забезпечує розширений набір функцій безпеки для керування підключенням і доступом користувачів. Цей набір включає Access Control Lists (ACL) на основі Mac-адрес, портів комутатора, IP адрес і/або номерів портів TCP/UDP, аутентифікацію користувачів 802.1x і контроль Mac-Адрес. Крім цього, DES-3500 забезпечує централізоване керування адміністративним доступом через TACACS+ і RADIUS. Разом з контролем над мережевими додатками, ці функції безпеки забезпечують не тільки авторизований доступ користувачів, але й запобігають поширенню шкідливого трафіка по мережі.

Розширена продуктивність і доступність - Для підвищення продуктивності й безпеки мережі комутатори серії DES-3500 забезпечує розширену підтримку VLAN, включаючи GARP/GVRP, 802.1Q і асиметричні VLAN. Керування смугою пропускання дозволяє встановити ліміт трафіка для кожного порту, що дає можливість управляти обсягом трафіка на границі мережі. Комутатор підтримує установку резервного джерела живлення. Інші характеристики включають підтримку 802.3ad Link Aggregation, 802.1d Spanning Tree, 802.1w Rapid Spanning Tree і 802.1s Multiple Spanning Tree для підвищення надійності й доступності віртуального стека.

Багаторівнева якість обслуговування (Qos) - Серія DES-3500 має широкий набір багаторівневих (L2, L3, L4) Qos/Cos функцій, для гарантії того, що критично важливі мережеві сервіси, подібні Voip, ERP, Intranet або відеоконференції будуть обслуговуватися з належним пріоритетом. Підтримуються 4 черги пріоритетів для

802.1p/TOS/Diffserv із класифікацією на основі Mac-адрес джерела й приймачу, Ip-адрес джерела або приймачу й/або номерів портів TCP/UDP.

3.4 Налаштування комутатору DES-3526

Комутатор DES-3526 має консоль управління за допомогою веб-інтерфейсу. По замовчуванню IP-адреса комутатору – 192.168.1.1. Веб-інтерфейс працює по стандартному HTTP-порту – 80.

При заході на веб-інтерфейс користувач в першу чергу отримує запит авторизації – логін та пароль користувача. Після вводу адміністраторського паролю користувач перенаправляється на інтерфейс системи (рис. 3.1).

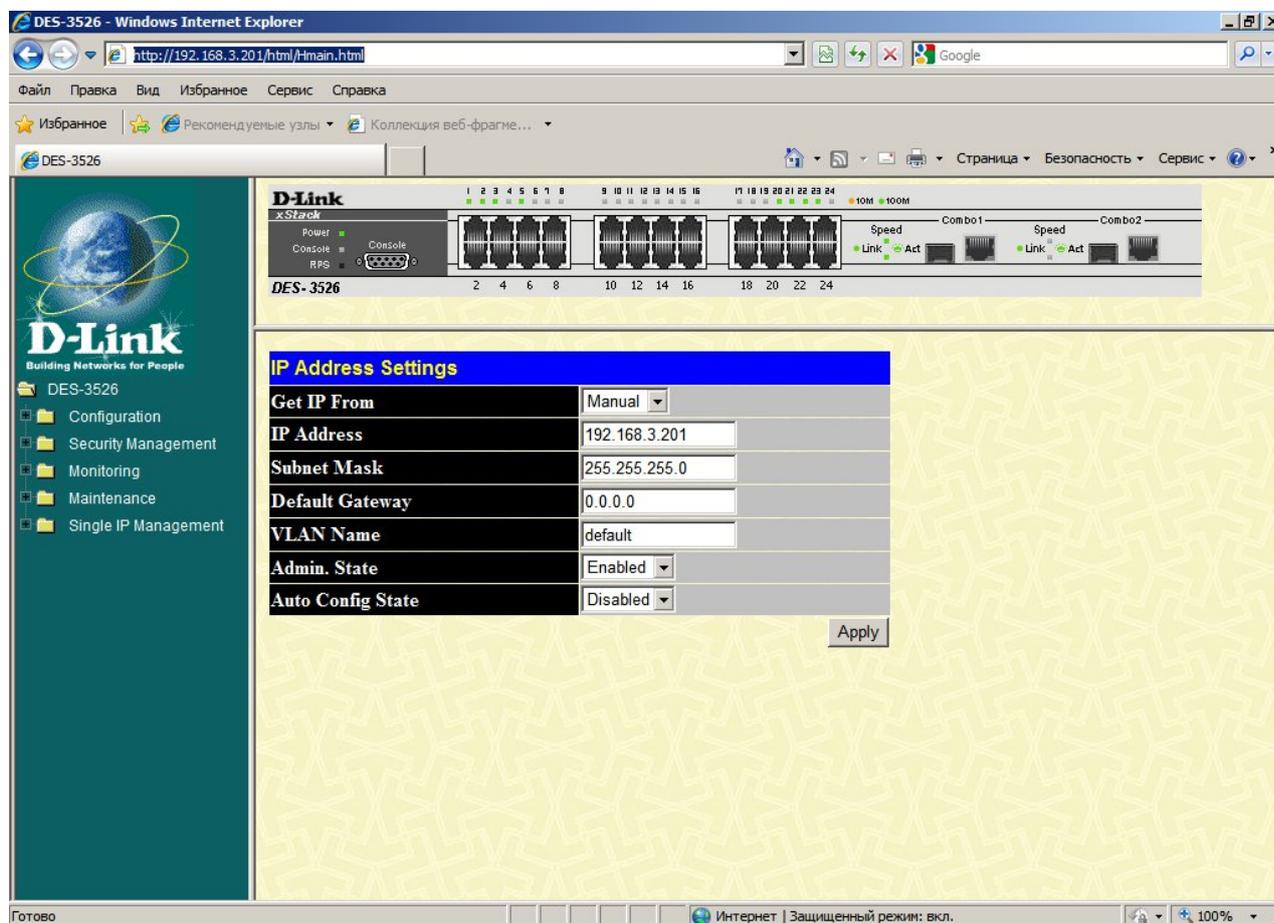


Рисунок 3.1 - Вхід в веб-інтерфейс

Ліва частина інтерфейсу – дерево опцій керування. Верхня частина – панель статусу, там відображено поточний стан комутатору, які порти під'єднані в даний момент.

Першим екраном по замовчуванню іде налаштування IP-адреси комутатору в локальній мережі.

З початку розглянемо пункти меню, які дають загальну інформацію про стан комутатору.

1. PortConfiguration – показує поточний стан портів, та дозволяє включити-відключити деякі порти або налаштувати їх швидкість, якщо значення по замовчуванню (автоматичне розпізнавання) вас не влаштовує (рис. 3.2.).

The screenshot shows the D-Link DES-3526 web interface. The top part displays the physical ports (1-24) and their status (Link, Speed). Below this is the 'Port Configuration' section with a table of settings for Port 1. The main part of the interface is 'The Port Information Table'.

From	To	State	Speed/Duplex	FlowCtrl	Learn	Trap	Apply
Port 1	Port 1	Disabled	Auto	Disabled	Disabled	Disabled	Apply

Port	State	Speed/Duplex	Connection	FlowCtrl	Learn	Trap
1	Enabled	Auto	100M/Full/None	Disabled	Enabled	Enabled
2	Enabled	Auto	100M/Full/None	Disabled	Enabled	Enabled
3	Enabled	Auto	100M/Full/None	Disabled	Enabled	Enabled
4	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
5	Enabled	Auto	100M/Full/None	Disabled	Enabled	Enabled
6	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
7	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
8	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
9	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
10	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
11	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
12	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
13	Enabled	Auto	Link Down	Disabled	Enabled	Enabled

Рисунок 3.2 - Port configuration

В даному режимі показується перелік портів, чи включені вони, чи ні, та поточний стан (швидкість та режим дуплексу).

Розділ “Port description” дозволяє зберігати опис портів на комутаторі.

В нашому випадку мережа має наступну структуру (рис.3.3).

The screenshot shows the web interface of a D-Link DES-3526 switch. The left sidebar contains a navigation menu with various configuration options. The main content area displays the 'Port Description Table' configuration page. At the top of this page, there are dropdown menus for 'Port 1' and 'Port 1', and an 'Apply' button. Below this is a table with two columns: 'Port' and 'Description'.

Port	Description
1	Lab 320
2	Lab 321
3	Lab 318
4	Lab 309
5	Library
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	Kadry+Director+Afganesyan
22	Denne
23	Andrew
24	Wi-Fi
25	Server
26	

Рисунок3.3 - Port Description

Розділ “Port description” дозволяє зберігати опис портів на комутаторі.

В нашому випадку мережа має наступну структуру (рис. 3.4.):

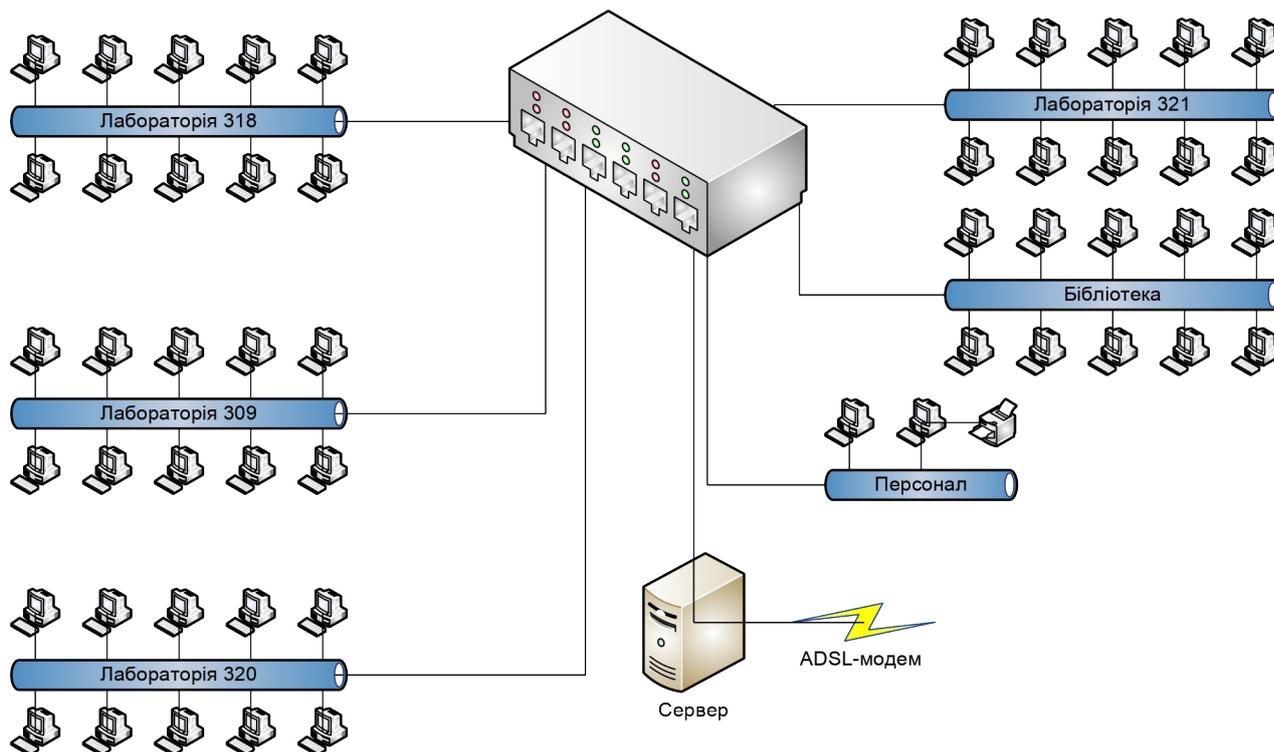


Рисунок 3.4 - Схема мережі

Сегментація трафіку має відбуватися наступним чином:

1. Всі сегменти мережі мають мати доступ до серверного комп'ютеру та викладацьких комп'ютерів.
2. Навчальні лабораторії мають мати доступ лише до загального сегменту. Надходження трафіку між навчальними лабораторіями має бути заблоковане.
3. Доступ до сегменту мережі з комп'ютерами керівництва має бути можливий лише з викладацьких комп'ютерів.

Таким чином, ми можемо виділити наступні окремі сегменти мережі:

1. Загальний сегмент (серверний комп'ютер-шлюз, викладацькі комп'ютери).
2. Лабораторія 318.
3. Лабораторія 320.
4. Лабораторія 321.
5. Лабораторія 309.

6. Бібліотека.
7. Комп'ютери керівництва.

Зазвичай сегментація мережі за допомогою керованих комутаторів відбувається з використанням технології віртуальних мереж (VLAN). В нашому випадку задача трохи ускладнюється тим, що перший (загальний) сегмент мережі має бути доступний з усіх інших сегментів. Для розв'язку такої задачі в обладнанні Dlink використовується технологія асиметричних віртуальних мереж (AsymmetricVLAN). За допомогою цієї технології ми зможемо зробити сегменти мережі, що пересікаються між собою.

По замовчуванню технологія AsymmetricVLAN в комутаторах DES-3526 відключена. Включити її можна на закладці AdvancedSettings, як зображено на рис. 3.5.

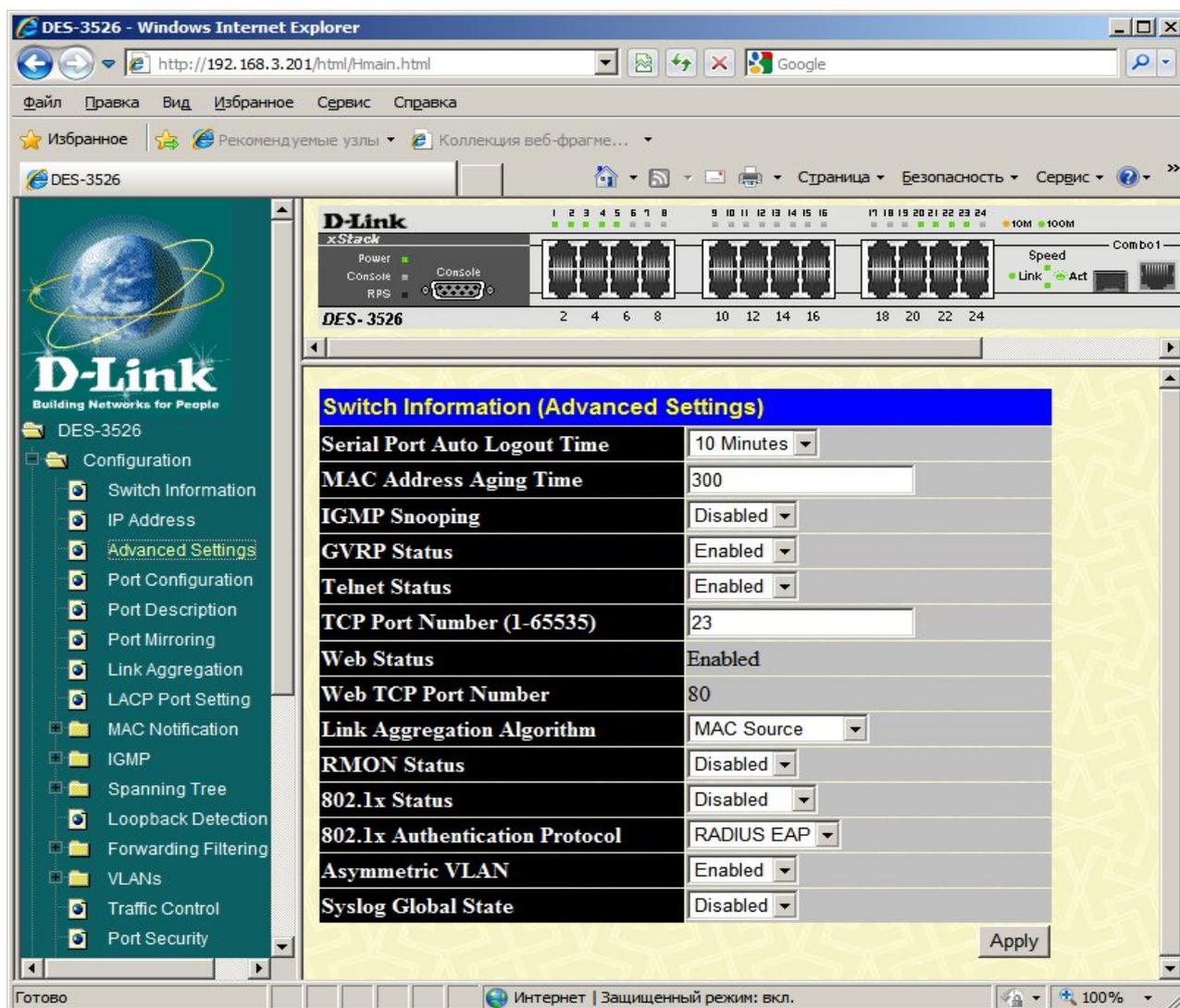


Рисунок 3.5 - Advanced Settings

Крім саме опції *Assymmetric VLAN*, нам знадобиться включити опцію *GVRP Status* (розглянемо трохи пізніше). Після цих налаштувань, ми можемо приступити безпосередньо до налаштування VLAN-ів. Відбувається це налаштування на закладці *StaticVLANentry* в піддереві *VLANs*.

По замовчуванню в системі є лише один VLAN – *default* з ідентифікатором 1. Без додаткових налаштувань вважається, що весь трафік належить до цього VLAN-у. Для додавання нового сегменту мережі натискаємо кнопку *AddNew 802.1QVLAN*.

Створимо другий сегмент нашої мережі – лабораторія 318. Як ми бачимо з таблиці описів портів, ця лабораторія є під'єднана до порту номер 3. Отже, для включення в цей VLAN ставимо помітку *Egress* щодо порту номер 3, та знімаємо тегування цього порту. Ті самі дії виконуємо стосовно загального сегменту - портів серверу та викладацьких комп'ютерів – порти 23,24 та 25. Не забуваємо ввести ім'я сегменту та ідентифікатор VLAN-у (рис.3.6.).

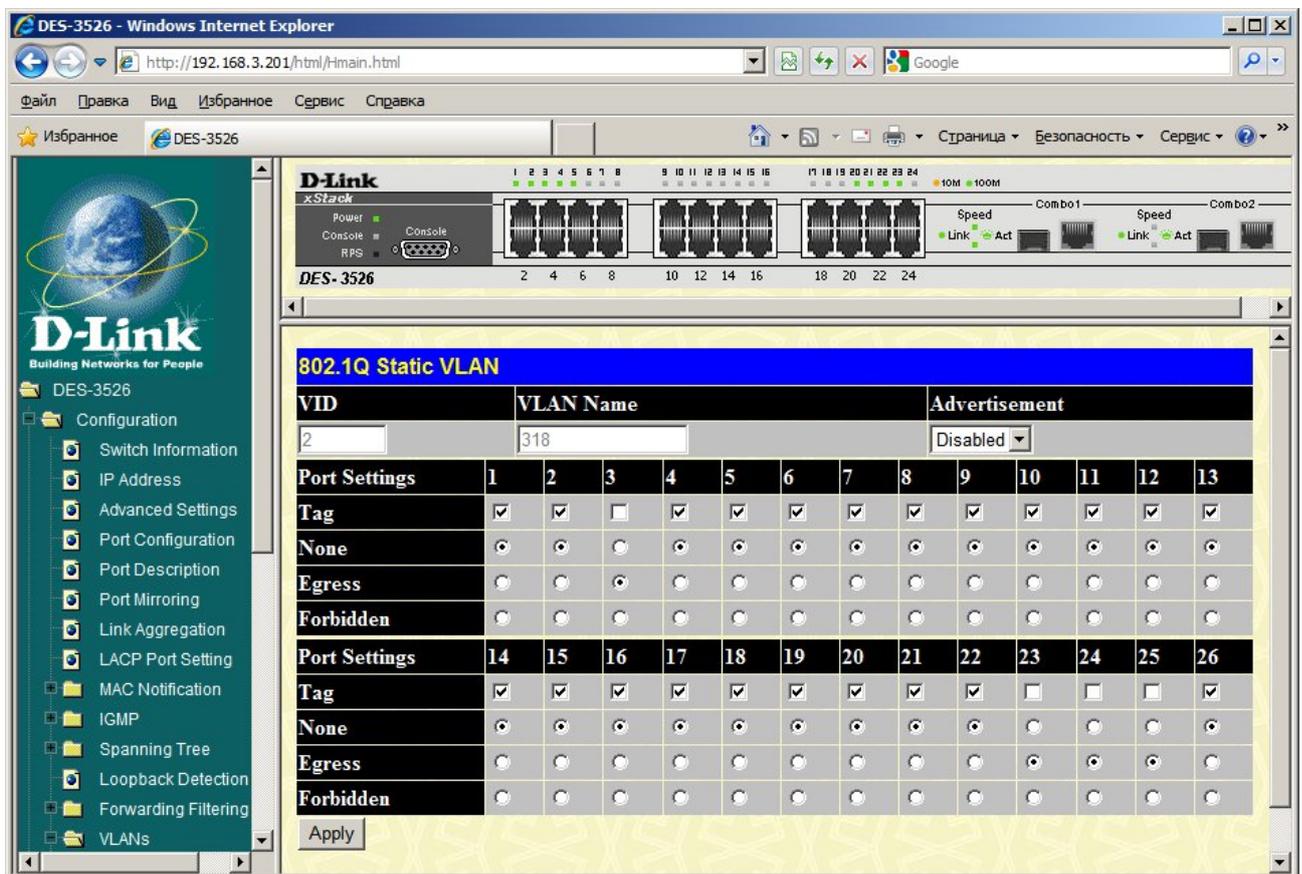


Рисунок 3.6 - Створення VLAN-у

Ті самі дії проробляємо для всіх наступних сегментів мережі (рис.3.7.):

VLAN 3 – Лабораторія 320. Порти 1, 23, 24, 25.

VLAN 4 – Лабораторія 321. Порти 2, 23, 24, 25.

VLAN 5 – Лабораторія 309. Порти 4, 23, 24, 25.

VLAN 6 – Бібліотека. Порти 5, 23, 24, 25.

VLAN 7 – Комп'ютери керівництва. Порти 20, 21, 22, 23, 24, 25.

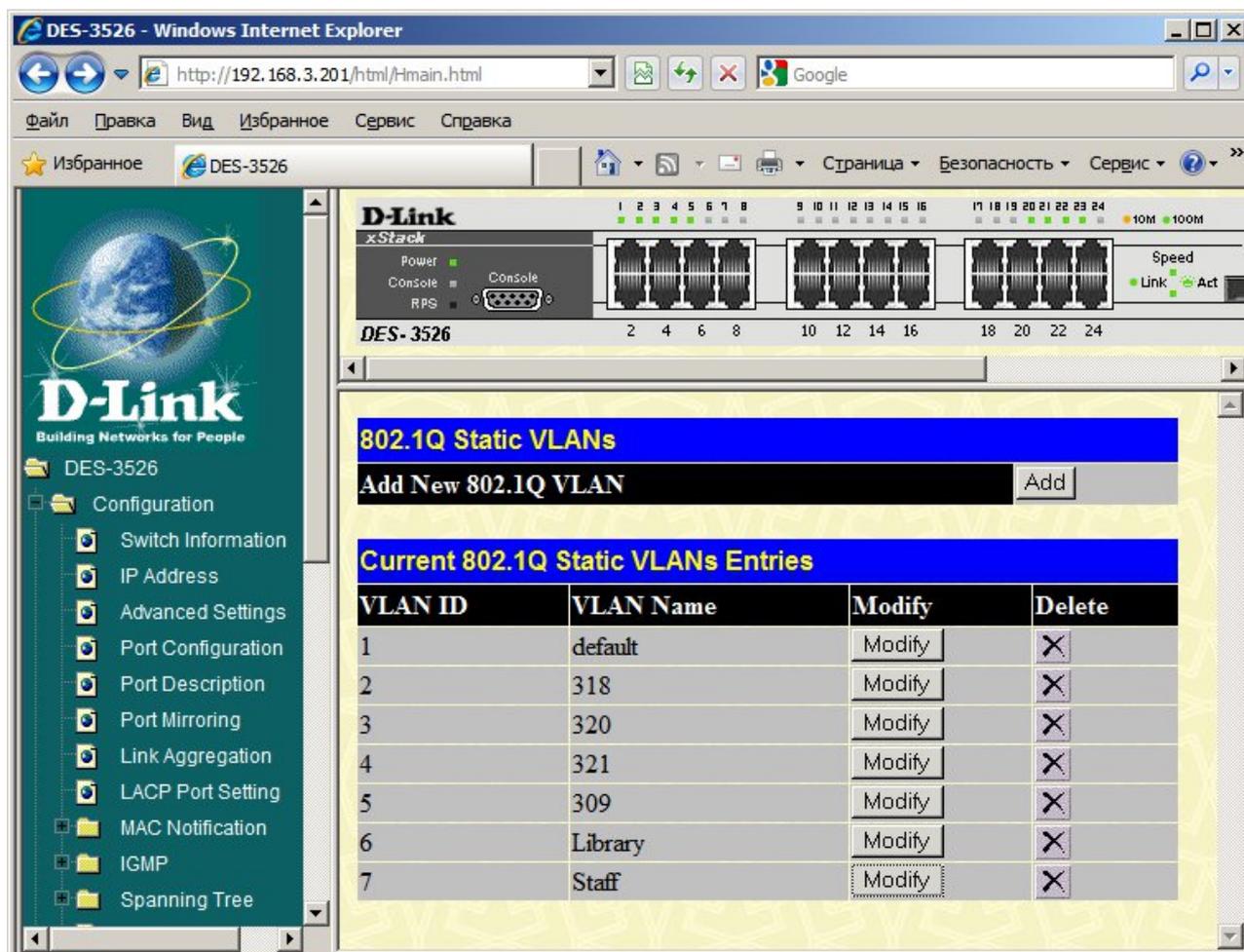


Рисунок 3.7 - Перелік VLAN-ів

Отже, всі порти було налаштовано для відношення до конкретного VLAN-у. Наступна частина проблеми полягає в тому, що трафік, що поступає до вказаних портів, має мати помітку відповідного VLAN-у. Функція маркування VLAN-ів доступна або в керованих комутаторах, маршрутизаторах, або дорогих

мережевих адаптерах. Інтегровані мережеві адаптери, які, звичайно, поширені на території коледжу, цієї функції не підтримують.

Отже, маркування має взяти на себе цей самий комутатор. Для цього використовується розділ *GVRPSettings* в тому самому підрозділі *VLANs* (рис.3.8.).

Надаємо портам значення VLAN-ів, до яких вони мають належати:

VLAN 1 – порти 23,24,25.

VLAN 2 – порт 3.

VLAN 3 – порт 1.

VLAN 4 – порт 2.

VLAN 5 – порт 4.

VLAN 6 – порт 5.

VLAN 7 – порти 20, 21, 22.

Опції GVRP та IngressChecking мають бути відключені для тих портів.

DES-3526 - Windows Internet Explorer
 http://192.168.3.201/html/hmain.html

Файл Правка Вид Избранное Сервис Справка

Избранное DES-3526

D-Link
 xStack
 Power Console RPS
 DES-3526
 2 4 6 8 10 12 14 16 18 20 22 24

802.1Q Port Settings

From	To	PVID	GVRP	Ingress	Acceptable Frame Type	Apply
Port 1	Port 1	1	Disabled	Disabled	Admit All	Apply

802.1Q Port Table

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	3	Disabled	Disabled	All Frames
2	4	Disabled	Disabled	All Frames
3	2	Disabled	Disabled	All Frames
4	5	Disabled	Disabled	All Frames
5	6	Disabled	Disabled	All Frames
6	1	Enabled	Disabled	All Frames
7	1	Enabled	Disabled	All Frames
8	1	Enabled	Disabled	All Frames
9	1	Enabled	Disabled	All Frames
10	1	Enabled	Disabled	All Frames
11	1	Enabled	Disabled	All Frames
12	1	Enabled	Disabled	All Frames
13	1	Enabled	Disabled	All Frames
14	1	Enabled	Disabled	All Frames
15	1	Enabled	Disabled	All Frames
16	1	Enabled	Disabled	All Frames
17	1	Enabled	Disabled	All Frames
18	1	Enabled	Disabled	All Frames
19	1	Enabled	Disabled	All Frames
20	7	Disabled	Disabled	All Frames
21	7	Disabled	Disabled	All Frames
22	7	Disabled	Disabled	All Frames
23	1	Disabled	Disabled	All Frames
24	1	Disabled	Disabled	All Frames
25	1	Disabled	Disabled	All Frames
26	1	Disabled	Enabled	All Frames

Configuration
 Switch Information
 IP Address
 Advanced Settings
 Port Configuration
 Port Description
 Port Mirroring
 Link Aggregation
 LACP Port Setting
 MAC Notification
 IGMP
 Spanning Tree
 Loopback Detection
 Forwarding Filtering
 VLANs
 Static VLAN Entry
 GVRP Setting
 Traffic Control
 Port Security
 QoS
 System Severity Setti
 System Log Server
 SNMP Settings
 Access Profile Table
 CPU Interface Filterin
 IP-MAC Binding
 Limited IP Multicast F
 Layer 3 IP Networkin
 Security Management
 Monitoring
 Maintenance

Рисунок 3.8 - Налаштування GVRP

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок витрат на розробку програмного продукту

Витрати на розробку та впровадження програмного продукту (К) включають:

$$K=K1+K2,$$

де К1 – витрати на розробку програмного продукту, грн.

К2 – витрати на налагодження та досліду експлуатацію програмного продукту на ПК, грн.

Витрати на розробку програмного продукту включають:

- витрати на оплату праці розробників (Воп);
- нарахування на зарплату (Нз);
- витрати на куповані вироби (Вк);
- накладні витрати (Нв);
- інші витрати (Він).

Для розробки програмного продукту потрібні 4 спеціалісти-розробники, а саме:

- керівник проекту (Кп);
- консультант з економічної частини (Ке);
- консультант з охорони праці (Коп);
- студент-дипломник (Сд).

Згідно з штатним розписом ВСП «Фаховий коледж інформаційних технологій «НУ ЛП», одна година навантажень становить для:

- керівник проекту (Кп) – 118,13 грн;
- консультант з економічної частини (Ке) - 118,13 грн;
- консультант з охорони праці (Коп) - 103,48 грн;
- студент-дипломник (Сд) - 8,73 грн.

Денна оплата студента дипломника визначається:

$$\text{Стипендія} / 173,$$

де 173 - місячний фонд робочого часу, год.

$$1510,00 / 173 = 8,73 \text{ грн/год}$$

Розрахунок витрат на оплату праці всіх спеціалістів проекту визначається за формулою:

$$\text{Воп} = \sum P_i * t_i * Z_{pi},$$

де P_i – чисельність розробників проекту i -спеціальності, роб.;

t_i – час, витрачений за розробку проекту розробником i -спеціальності, год.;

Z_{pi} – погодинна заробітна плата розробника i -спеціальності, грн..

Таким чином, витрати на оплату праці розробників складають:

$$Z_{kp} = 1 * 14 * 118,13 = 1\,653,82 \text{ грн}$$

$$Z_{ke} = 1 * 1 * 118,13 = 118,13 \text{ грн}$$

$$Z_{kop} = 1 * 1 * 103,48 = 103,48 \text{ грн}$$

$$Z_{cd} = 1 * 180 * 8,73 = 1\,571,4 \text{ грн}$$

Сумарні витрати на оплату праці:

$$\begin{aligned} \text{Воп} &= (1 * 4 * 118,13) + (1 * 1 * 118,13) + (1 * 1 * 103,48) + (1 * 180 * 8,73) = \\ &= 1\,653,82 + 118,13 + 103,48 + 1\,571,4 = 3\,446,83 \text{ грн} \end{aligned}$$

Розрахунок витрат на оплату праці розробників наведено у таблиці 4.1.

Таблиця 4.1 – Розрахунок витрат на оплату праці

Спеціальність розробника	Кількість розробників, роб.	Час роботи, год.	Погодинна заробітна плата розробника, грн.	Витрати на оплату праці, грн.
Керівник проекту	1	14	118,13	1 653,82
Консультант з економічної частини	1	1	118,13	118,13
Консультант з охорони праці	1	1	103,48	103,48
Студент-дипломник	1	180	8,73	1 571,4
Всього	4	-	-	3 446,83

Нарахування на зарплату визначаються за формулою:

$$Нз = (Воп - Зсд) * 22,0 / 100,$$

де Воп – витрати на оплату праці, тис.грн.

22 – норматив нарахувань на зарплату, %

$$Нз = (3\,446,83 - 1\,571,4) * 22,0 / 100 = 412,59 \text{ грн}$$

Витрати на куповані вироби визначаються за їх фактичними цінами з врахуванням найменування, номенклатури та необхідної кількості в проекті. Транспортно-заготівельні витрати становлять 10% від суми витрат на куповані вироби.

У таблиці 4.2 наведено розрахунок витрат на куповані вироби

Таблиця 4.2 – Розрахунок витрат на куповані вироби.

Найменування купованих виробів	Одиниця виміру	Кількість, шт.	Ціна за одиницю, грн.	Сума витрат, грн.
Папір А4 New Future Laser 80 г/м2	Пачка	1	250	250
Роздрук пояснювальної записки	Аркуш	80	3	240
Папка для дипломного проекту	-	1	230	230
Разом	-	-	-	520
Транспортно-заготівельні витрати (10%)	-	-	-	52
Всього	-	-	-	572

Витрати на куповані вироби становлять:

$$Вк = 250 + 240 + 230 + 52 = 572 \text{ грн}$$

Накладні витрати становлять 30% від витрат на оплату праці:

$$Нв = 3\,446,83 * 30 / 100 = 1\,034,05 \text{ грн}$$

Інші витрати обчислюються по їх питомій вазі у структурі собівартості (10%) :

$$Він = (Воп + Нз + Нв + Вк) * 10 / 90$$

$$Він = (3\,446,83 + 412,59 + 1\,034,05 + 572) * 10 / 90 = 607,27 \text{ грн}$$

Витрати на розробку програмного продукту визначаються за формулою:

$$K1 = \text{Воп} + \text{Нз} + \text{Нв} + \text{Вк} + \text{Він},$$

$$K1 = 3\,446,83 + 412,59 + 1\,034,05 + 572 + 607,27 = 6\,072,74 \text{ грн}$$

4.2 Розрахунок витрат на налагодження та дослідну експлуатацію програмного продукту на ПК

Програма була розроблена на протязі 30 днів із розрахунком 6 годин на день (t 180 год.).

Потужність комп'ютерної техніки (P) включає ПК який споживає 1,2 кВт/год. Вартість однієї машино-години роботи визначається за формулою:

$$S_{m.r.} = P * T_{\phi},$$

де P – потужність комп'ютерної техніки, кВт;

T ϕ - вартість 1 кВт-год електроенергії, грн. (T ϕ = 7,50).

$$S_{m.r.} = 1,2 * 7,50 = 9 \text{ грн/год}$$

Витрати на налагодження та дослідну експлуатацію програмного продукту на ПК визначаються за формулою:

$$K2 = S_{m.r.} * t,$$

де S $_{m.r.}$ – вартість однієї машино-години роботи, грн \ год.

t – машинний час, витрачений на налагодження та дослідну експлуатацію програмного продукту, год.

$$K2 = 9 * 180 = 1\,620 \text{ грн}$$

Таким чином, витрати на розробку та впровадження програмного продукту становлять:

$$K = 6\,072,74 + 1\,620 = 7\,752,74 \text{ грн}$$

У таблиці 4.3 наведено кошторис витрат на розробку та впровадження програмного продукту.

Таблиця 4.3 Кошторис витрат на розробку та впровадження програмного

Найменування елементів витрат	Сума витрат, грн.
Витрати на оплату праці	3 446,83
Нарахування на зарплату	412,59
Витрати на куповані вироби	572
Накладні витрати	1 034,05
Інші витрати	607,27
Витрати на налагодження та дослідну експлуатацію	1 620
Всього:	7 752,74

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

Охорона праці – це надзвичайно важлива система, яка складається з різноманітних правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та лікувально-профілактичних заходів та засобів. Вона має на меті збереження життя, здоров'я та працездатності людини у процесі трудової діяльності. У цьому контексті, важливими об'єктами охорони праці є людина в процесі праці, середовище виробництва та організації праці на ньому.

На підприємствах вкрай важливо створювати безпечні умови праці, адже це не тільки зберігає здоров'я та життя працівників, але й сприяє ефективнішому виробництву. Відповідно, слід дотримуватися вимог, викладених у нормативних документах. Це значно знизить наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відеодисплейними терміналами.

5.1 Електробезпека

Для забезпечення безпечної та ефективної експлуатації ЕОМ та ВДТ необхідно дотримуватись певних принципів та правил. Перш за все, регулярні щомісячні діагностичні огляди та чистка пристроїв допоможуть уникнути накопичення пилу, які можуть спричинити утворення електростатичного струму та пробою. Під час оглядів також необхідно оцінювати стан радіокомпонентів та замінювати їх на компоненти аналогічних номіналів за необхідності, щоб забезпечити найвищу продуктивність пристроїв. Крім того, монтаж електропроводів, кабелів та ЕОМ, а також їх ремонт та обслуговування має проводитись за допомогою діелектричних засобів та при повному відімкненні від загальної мережі для усунення можливості утворення струмів короткого замикання або струмів перенавантаження.

Електропроводи та кабелі, а також ЕОМ з ВДТ і ПП мають відповідати виконанням та ступеню захисту класу зони за НПАОП 40.1-1.32-01. Для забезпечення безпеки працівників, які працюють з ЕОМ та персональними комп'ютерами, необхідно дотримуватись вимог електробезпеки, встановлених нормативними документами, зокрема: «Правила улаштування електроустановок» (ПУЕ) та «Правилах охорони праці під час експлуатації електронно-обчислюваних машин» (НПАОП 0.00-1.28-10.). Також важливо враховувати, що лінія електромережі для живлення ЕОМ з ВДТ має бути виконана як окрема групова трипровідна мережа з фазового, нульового та захисного провідника. Усі провідники мають відповідати вимогам НПАОП 40.1-1.32-01. Нульовий захисний провідник має бути прокладений від стійки групового розподільного щита. ЕОМ з ВДТ має під'єднуватись до електромережі лише за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У приміщенні, де одночасно експлуатується або обслуговується більше ніж п'ять персональних ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Неприпустимим є підключення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ до звичайної двопровідної електромережі, в тому числі — з використанням перехідних пристроїв. Загалом, дотримання цих принципів та правил забезпечить безпечну та ефективну роботу ЕОМ та ВДТ.

5.2 Техніка безпеки при роботі за комп'ютером

Під час роботи на комп'ютері можуть діяти шкідливі фактори, які можуть вплинути на здоров'я користувача. Інформаційна безпека та електробезпека забезпечуються за допомогою ряду профілактичних заходів. Один з найважливіших аспектів є саме електробезпека. Для усунення ризику ураження струмом необхідно розміщувати обладнання та кабелі відповідно до вимог безпеки. Це може бути досягнуто за допомогою захисного заземлення,

використання безпечних розеток та електропроводки, розрахованих на потужність системи, а також ізоляції всіх проводів.

Для забезпечення ефективності та продуктивності роботи комп'ютера важливо регулярно чистити внутрішні частини від пилу, користуватися окремими вогнетривкими столами для комп'ютерів та іншого устаткування. Щоб запобігти іскрінню, необхідно рідше вставляти та виймати вилки з розеток.

Освітлення на робочому місці повинно відповідати характеру зорової роботи, який визначається трьома параметрами: об'єктом розрізнення, фоном та контрастом об'єкта і фону. Потрібно забезпечити рівномірне розподілення яскравості на моніторі та навколишньому просторі, відсутність різких тіней, відблисків та стабільну освітленість під час роботи. Вибирати оптимальну спрямованість світлового потоку та необхідний склад світла. Для забезпечення здоров'я користувача можна використовувати спеціальні світильники та підсвічування, які забезпечують оптимальні умови для зорової роботи. КПО > 1,5%.

Правила безпеки при роботі за комп'ютером:

- Увімкніть кондиціонер у приміщенні, щоб уникнути перегрівання пристроїв та забезпечити комфортну температуру для користувача.

- Переконайтесь у стабільному розташуванні обладнання на столі. Не забудьте, що нестабільна підставка для монітора може призвести до його падіння та пошкодження. Відкрийте монітор так, щоб було зручно спостерігати екран – прямо (не збоку) і трохи зверху вниз, з нахилом екрана, його нижній край ближче до користувача.

- Перевірте загальний стан обладнання, справність електропроводки, кабелів, вилок, розеток та заземлення захисного екрана. Якщо щось несправне, виправте це перед роботою.

- Налаштуйте освітлення робочого місця. Краще мати якісне та достатнє освітлення, щоб зменшити навантаження на очі та запобігти їх перевтомленню.

-Регулюйте та фіксуйте висоту крісла та зручний нахил спинки для користувача. Важливо, щоб користувач почував себе комфортно та міг працювати тривалий час без відчуття дискомфорту.

-Під'єднайте необхідне обладнання до системного блоку. Кабелі, що з'єднують системний блок з іншими пристроями, слід вставляти та виймати при вимкненому комп'ютері, щоб уникнути пошкодження пристроїв та пошкодження даних.

- Увімкніть комп'ютерне обладнання послідовно: монітор, системний блок, принтер (якщо потрібно друкувати). Це дозволить уникнути перезавантаження системи та забезпечити її стабільну роботу.

-Налаштуйте яскравість монітора та контрастність. Не робіть зображення надто яскравим, щоб не перевтомлювати очі. Також важливо відпочивати та робити паузи під час тривалої роботи за комп'ютером, щоб не перенапружувати очі та запобігти втомі.

5.3 Пожежна безпека

Пожежна безпека об'єкта – це важливий стан об'єкта, про який регламентом визначено імовірність виникнення та розвитку пожежі та впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей. Цей стан регулюється нормативними актами, зокрема ДБН В.1.1-7-2002 "Пожежна безпека об'єктів будівництва", ДСТУ 2272:2006 "Пожежна безпека. Терміни та визначення основних понять", НАПБ А.01.001-2004 "Правила пожежної безпеки в Україні".

Важливою складовою пожежної безпеки є належне ознайомлення всіх працівників з правилами пожежної безпеки, проходження протипожежних інструктажів та перевірки знань з питань пожежної безпеки. Зокрема, автоматична пожежна сигналізація повинна завжди бути у ввімкненому, черговому стані.

Приміщення для роботи повинно відповідати нормам, зазначеним у НАПБ А.01.001.-2004 про будівлі та приміщення для ЕОМ. Зокрема, підлога та стіни в такому приміщенні повинні входити в групу горючості Г1. Заборонено зберігати легкозаймисті та горючі речовини в будь-яких кількостях в приміщенні з ЕОМ. Важливо не залишати ЕОМ без нагляду під час роботи та вимикати їх від глобальної електромережі по закінченню роботи з ними. На робочому місці має бути встановлений легкий доступ до двох газових вогнегасників як засобів первинної пожежної безпеки. Меблі та обладнання повинні розміщуватися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (завширшки не менше 1 м). Евакуаційні шляхи та виходи необхідно постійно утримувати вільними, нічим не захарашувати. Документи, папір та інші горючі матеріали слід зберігати на відстані не менше 1 м від електрощитів і електрокабелів; 0,5 м від електросвітильників; 0,6 м від сповіщувачів пожежної сигналізації та 0,15 м від приладів центрального водяного опалення. Засоби протипожежного захисту слід утримувати у справному стані. Відстань від найбільш віддаленого місця до вогнегасника не повинна бути більшою за 20 м.

Приміщення, у яких розміщені ПЕОМ, слід оснащувати переносними вуглекислотними вогнегасниками з розрахунку один вогнегасник ВВК-2 або один ВВПА-400 на три ПЕОМ, але не менше ніж один вогнегасник зазначених типів на приміщення.

Крім того, рекомендується забезпечити додатковий простір для працівників, який забезпечить їм додаткові можливості для руху та роботи з ПЕОМ, а також забезпечити доступ до відповідних джерел електроживлення. З метою забезпечення повної пожежної безпеки рекомендується проводити щорічні перевірки на відповідність пожежним нормам та стандартам. Для гасіння пожеж класу В (горючі рідини) та класу Е (електроустановки, що знаходяться під напругою) вуглекислотні вогнегасники (ВВК) ефективно застосовуються. Їх механізм дії полягає в тому, що вони працюють шляхом витіснення кисню з зони горіння та охолодження матеріалів, що горять. Вогнегасники ВВК не залишають слідів після використання, що робить їх ідеальними для гасіння пожеж в

електронному обладнанні та на об'єктах з цінними матеріалами. Вуглекислотний вогнегасник ВВК-2 наведено на рисунку 5.1



Рисунок 5.1 – Вогнегасник вуглекислотний ВВК-2.

5.4 Виробниче приміщення та робоче місце

Згідно з вимогами ДСанПіН 3.3.2.007-98, приміщення, в яких планується робота з ВДТ, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Якщо ви плануєте працювати з відомчими документами та матеріалами на комп'ютері, то вам необхідно взяти до уваги правила розташування робочого місця, які забезпечать вам максимальний комфорт та безпеку під час роботи.

Розміщення робочих місць з ВДТ у підвальних приміщеннях та на цокольних поверхах заборонено. Якщо ваше робоче місце знаходиться в приміщенні, то зверніть увагу на доступність основних умов, необхідних для продуктивної роботи. На одного працівника площа робочого місця має становити не менше ніж $6,0 \text{ м}^2$, а об'єм – не менше ніж $20,0 \text{ м}^3$.

У залежності від того, яку роботу ви виконуєте, має бути враховано чинні санітарні норми освітлення, температури, відносної вологості повітря, сили та ступеня вібрації, звукового шуму, вогнестійкості, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря.

Щоб забезпечити високий рівень комфорту та безпеки під час роботи з комп'ютером, на кожную кімнату, де працюють співробітники, повинні бути наявні елементи природного та штучного освітлення відповідно до ДБН В.2.5-28-2006. Для досягнення максимального рівня безпечності та охорони праці при роботі з комп'ютером виробничі приміщення необхідно обладнати аптечками першої медичної допомоги, системами автоматичної пожежної сигналізації й вогнегасниками. На вікнах повинні бути встановлені сонцезахисні плівки.

При розташуванні елементів робочого місця користувача ПК необхідно враховувати робочу позу користувача, простір для розміщення користувача, можливість огляду елементів робочого місця, можливість ведення записів, розміщення документації та матеріалів, якими користуватиметься працівник. Робочі місця з ПК мають бути розташовані від стіни з вікнами на відстані не менше ніж 1,5 м, від інших стін – на відстані не менше ніж 1 м. Недопустиме таке розташування ПК, при якому працівник повернутий обличчям або спиною до вікон кімнати або до задньої частини ПК, у яку вмонтовані вентилятори. Загальні рекомендації до робочої пози та робочого місця наведені на рисунку 5.2

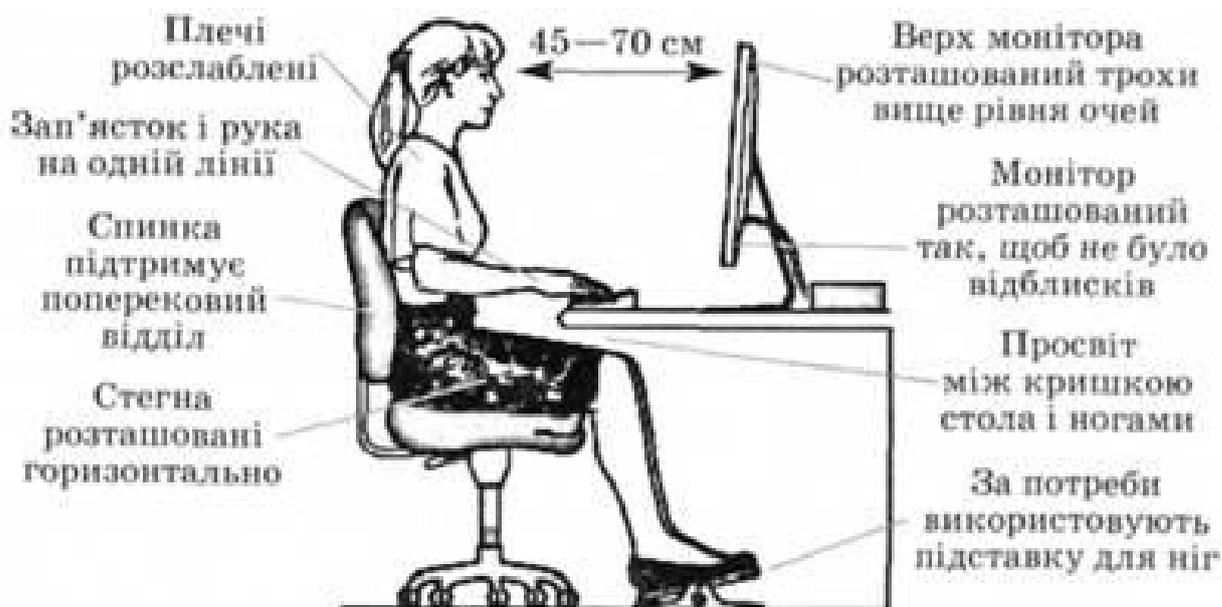


Рисунок 5.2 – Рекомендації до робочої пози та робочого місця

5.5 Висновки до розділу з охорони праці та безпеки життєдіяльності

Дипломний проєкт був виконаний з дотриманням усіх зазначених нижче стандартів та норм, що гарантували мою безпеку під час роботи:

-Електробезпека. Під час використання комп'ютера, були виконані всі вимоги електробезпеки, вказані в технічній документації виробника;

-Техніка безпеки при роботі за комп'ютером. Всі вимоги щодо безпеки користувача під час роботи за комп'ютером, такі як правильне розташування апаратури, ергономіка робочого місця, перерви в роботі та забезпечення зорового комфорту, були дотримані належним чином;

-Пожежна безпека. Умови зберігання та експлуатації, що забезпечують пожежну безпеку, згідно з технічною документацією виробників комп'ютерів, були виконані протягом усієї роботи;

-Виробниче приміщення та робоче місце. Робота над дипломним проєктом відбувалась в приміщенні з робочим місцем, яке відповідало всім стандартам та ергономічним нормам.

ВИСНОВКИ

Дипломний проєкт виконаний згідно завдання і представлений у вигляді пояснювальної записки на листах та графічною частиною на 4аркушах.

Під час проєктування було досліджено можливості налаштування керованих комутаторів.

В роботі наведено теоретичні відомості з питань мережевої комутації, розглянуті рівні комутації. Також розглянута в деталях технологія VLAN, яку використовується для сегментації трафіку в середині локальної мережі.

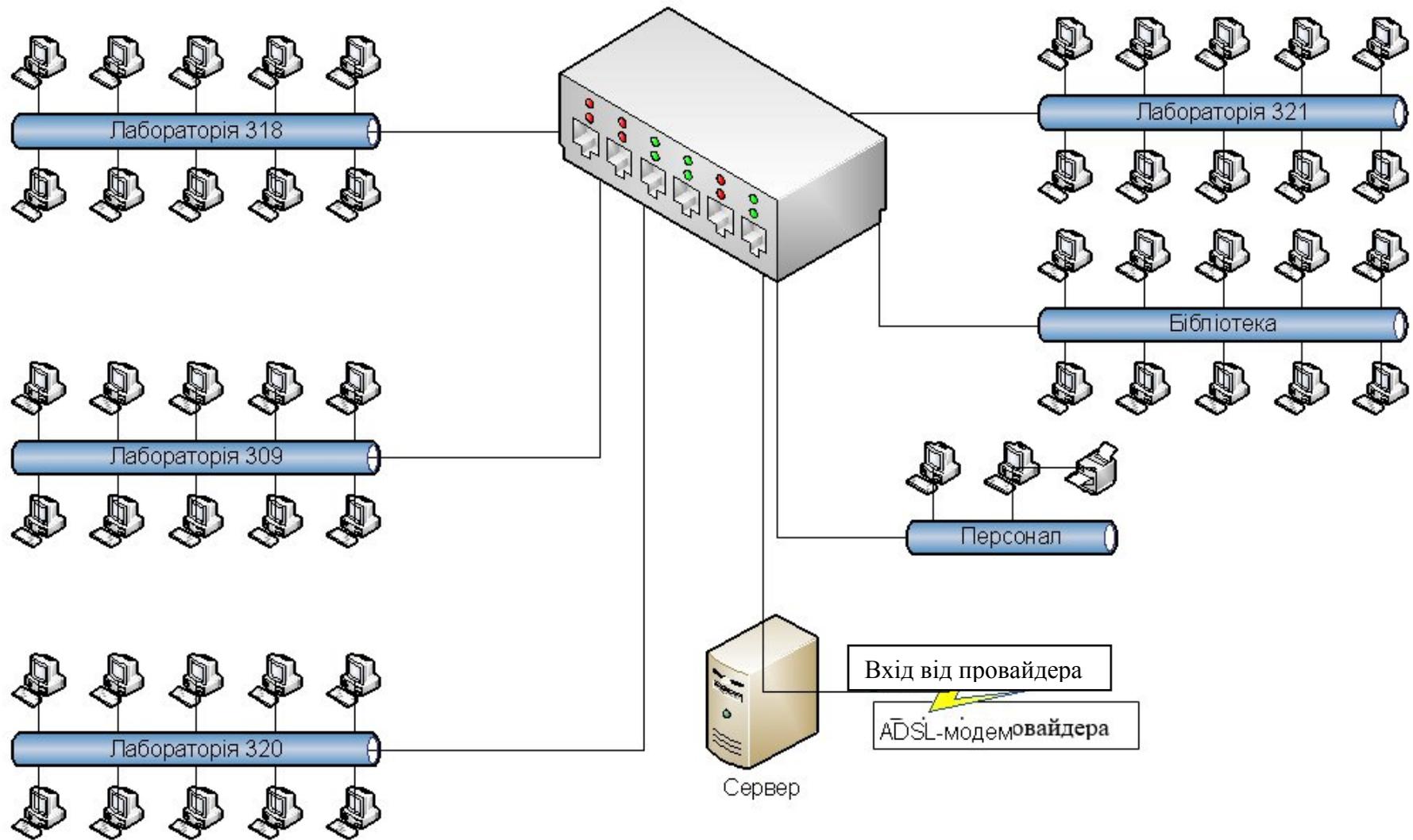
В процесі було налаштовано керований комутатор 2-го рівня DES-3526 для сегментації трафіку в середині локальної мережі коледжу, та розроблено детальну інструкцію з налаштування.

Розроблена інструкція має практичне застосування для коледжу і може бути використана в якості навчального матеріалу для студентів коледжу.

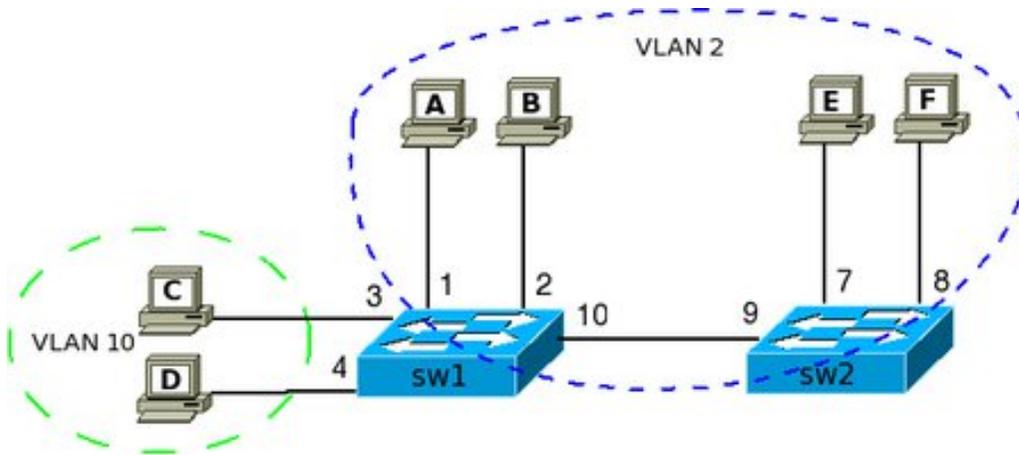
ПЕРЕЛІК ПОСИЛАНЬ

1. часні технолошві комутації (рівні комутації) -
<http://www.hub.ru/archives/4232>
2. Дэвид Хьюкаби, Стив Мак-Квери Руководство Cisco по конфигурированию коммутаторов Catalyst = Cisco Field Manual: Catalyst Switch Configuration. — М.: «Вильямс», 2004. — С. 560. — ISBN 5-8459-0700-4
3. Брайан Хилл Глава 9. Основные сведения о коммутаторах // Полный справочник по Cisco = Cisco: The Complete Reference. — М.: «Вильямс». — С. 1088. — ISBN 0-07-219280-1
4. Эндрю Таненбаум, 2003, «Computer Networks», Pearson Education International, New Jersey.
5. Сергей Пахомов, Возможности современных коммутаторов по организации виртуальных сетей,
<http://www.xnets.ru/plugins/content/content.php?content.92>
6. Евгений Патий, Технологии коммутации в сетях хранения данных,
<http://www.citforum.ru/nets/storage/commutation/>
7. Брайан Хилл Глава 9. Основные сведения о коммутаторах // Полный справочник по Cisco = Cisco: The Complete Reference. — М.: «Вильямс». — С. 1088. — ISBN 0-07-219280-1
8. Эндрю Таненбаум, 2003, «Computer Networks», Pearson Education International, New Jersey.
9. Сергей Пахомов, Возможности современных коммутаторов по организации виртуальных сетей,
<http://www.xnets.ru/plugins/content/content.php?content.92>
10. Евгений Патий, Технологии коммутации в сетях хранения данных,
<http://www.citforum.ru/nets/storage/commutation/>

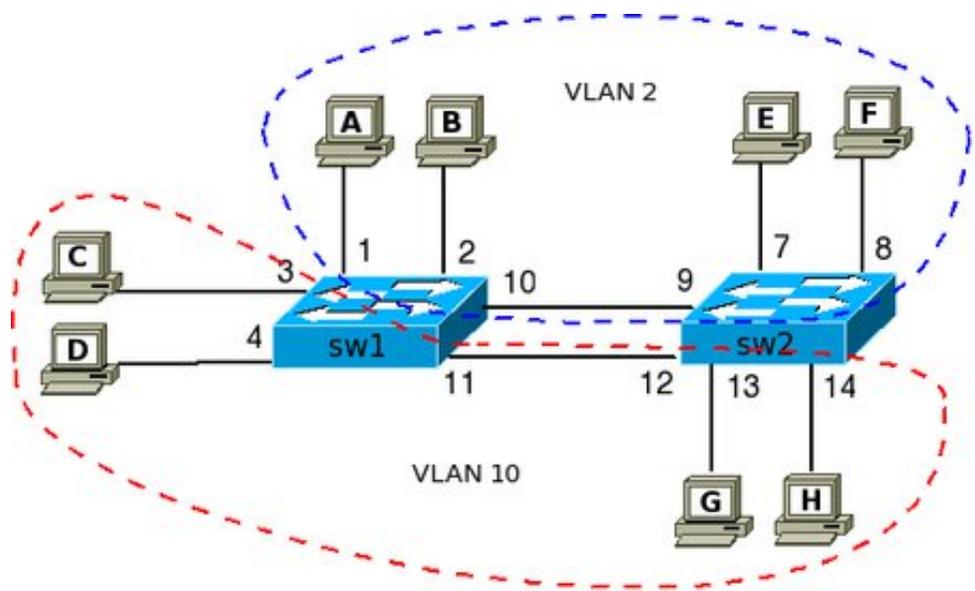
КОПІ ДЕМОНСТРАЦІЙНИХ АРКУШІВ



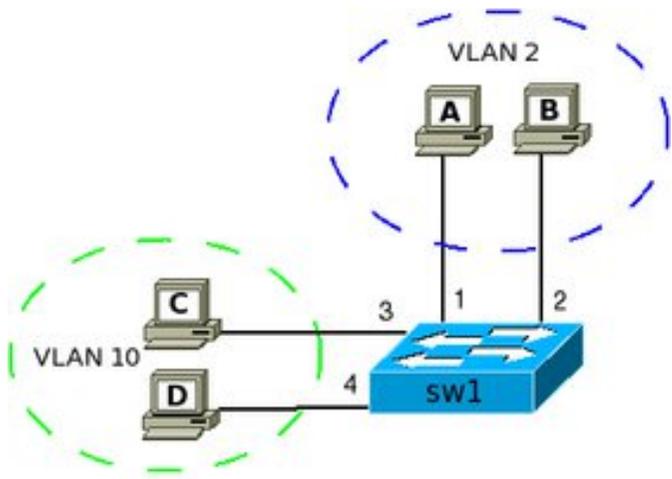
					Налаштування керованих комутаторів II-го рівня для роботи у великих локальних мережах.		
					Літера	Маса	Маштаб
<i>Зм.</i>	<i>Аркуш</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	Схема мережі коледжу		
<i>Розроб.</i>		Деркач Д.Б.					
<i>Керівник</i>		Селемонавіус М.М.					
<i>Реценз.</i>							
<i>Н. контр.</i>		Кужій Л.І.			<i>Аркуш</i>	<i>Аркушів</i>	
<i>Затверд.</i>							



Хости в різних VLAN на різних комутаторах

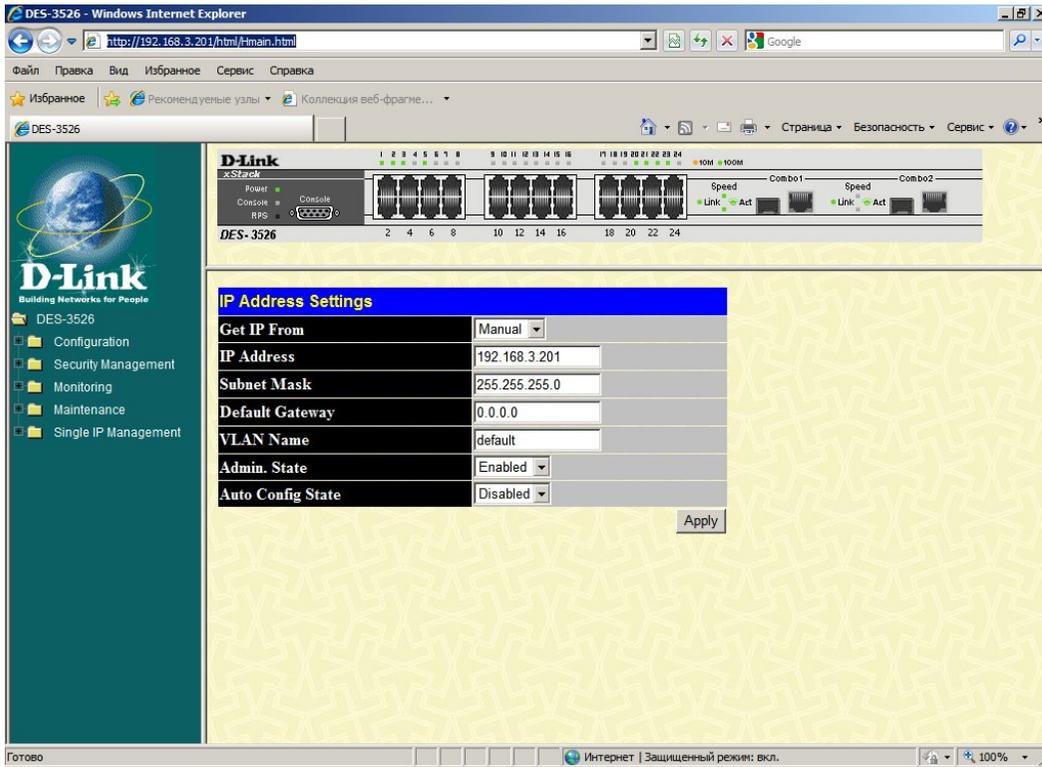


Хости різних VLAN на різних комутаторах

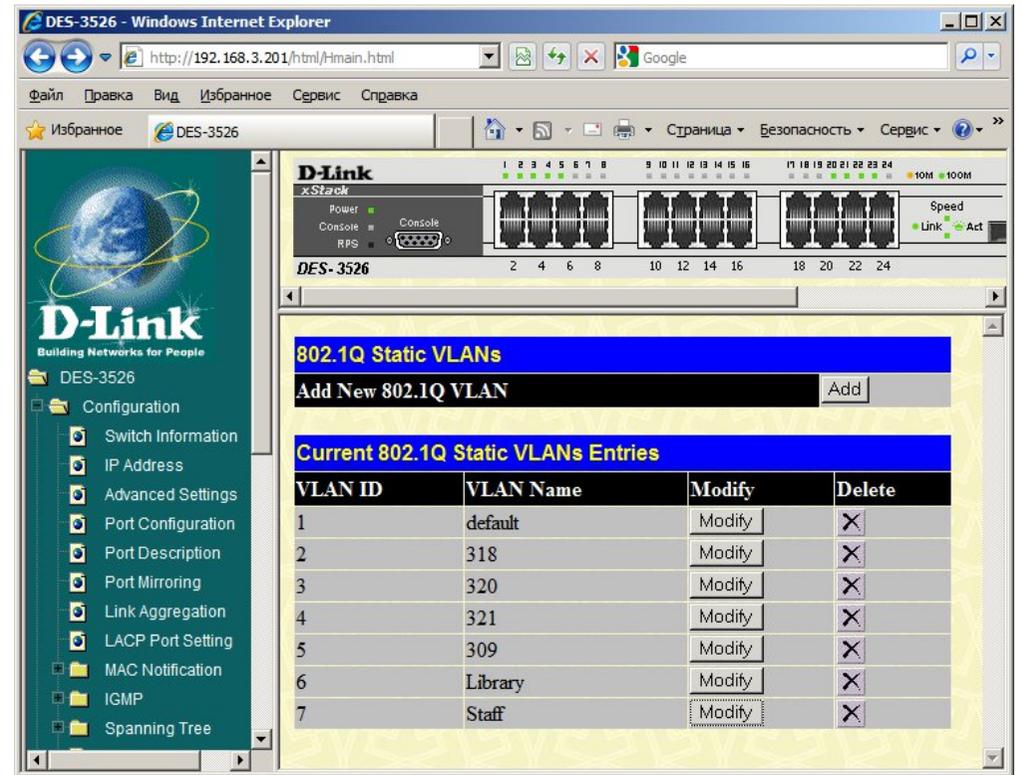


Хости в різних VLAN на одному комутаторі

					Налаштування керованих комутаторів другого рівня для роботи у великих локальних мережах			
						<i>Літера</i>	<i>Маса</i>	<i>Маштаб</i>
<i>Зм.</i>	<i>Аркуш</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	Створення VLAN			
<i>Розроб.</i>		Держак Д.Б.						
<i>Керівник</i>		Селемонавікус М.М.						
<i>Реценз.</i>								
<i>Н. контр.</i>		Кужій Л.І.			<i>Аркуш</i>		<i>Аркушів</i>	
<i>Затверд.</i>								



Вхід в веб-інтерфейс комутатора DES-3526



Перелік VLAN-ів

					Налаштування керованих комутаторів другого рівня для роботи у великих локальних мережах			
<i>Зм.</i>	<i>Аркуш</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	Налаштування комутатора DES-3526	<i>Літера</i>	<i>Маса</i>	<i>Маштаб</i>
<i>Розроб.</i>		Деркач Д.В.						
<i>Керівник</i>		Селемонавікус М.М.						
<i>Реценз.</i>						<i>Аркуш</i>	<i>Аркушів</i>	
<i>Н. контр.</i>		Кужій Л.І.						
<i>Затверд.</i>								

