Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему **Розробка проєкту комп'ютерної мережі підприємства з системою захисту передачі інформації**

Виконав: студент 6 курсу, групи 601дТТ
спеціальності 172 «Телекомунікації та
(шифр і назва напряму підготовки, спеціальності)
радіотехніка

Сталинський Р.М.
(прізвище та ініціали)
Керівник Жученко О.С.
(прізвище та ініціали)
Рецензент Штомпель М.А
(прізвище та ініціали)

Полтава – 2023 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій
_____О.В. Шефер
"04" 09 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Сталинському Роману Миколайовичу

1. Тема проекту (роботи) **«Розробка проєкту комп'ютерної мережі підприємства з системою захисту передачі інформації»**
керівник проекту (роботи) Жученко Олександр Сергійович , к.т.н., доцент
затверджена наказом вищого навчального закладу від "04" 09 2023 року № 986-ф

2. Строк подання студентом проекту (роботи) 13.12.2023 р.

3. Вихідні дані до проекту (роботи) Будівля підприємства, вимоги замовника, технічна документація.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Аналіз принципів побудови комутованих комп'ютерних мереж. Організація комп'ютерної мережі підприємства. Розподіл IP - адрес комп'ютерної мережі підприємства. Розрахунок інтенсивності потоків пакетів з мовою відео та даними. Впровадження фаерволу в мережу підприємства.

5. Перелік графічного матеріалу:
1) Локальна мережа кімнати A;
2) Локальна мережа кімнати B;
3) Локальна мережа кімнати C;

4) Локальна мережа кімнати D;
5) Локальна мережа кімнати E;
6) Таблиця ip-адрес;
7) Висновки по роботі.

6. Дата видачі завдання 02.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка (плакати)
1	Опис роботи сучасних мереж	11.10.23		15%	
2	Аналіз протоколів для роботи локальних мереж	18.10.23	I	30%	
3	Розрахунок необхідної техніки для підприємства	25.10.23		40%	
4	Розробка схеми розташування техніки	14.11.23		50 %	Пл. 3-7
5	Присвоєння IP-адрес	21.11.23	II	60%	Пл. 8
6	Розрахунок інтенсивності пакетів даних	28.11.23		70%	Пл. 9
7	Аналіз фаєрволів та впровадження їх	06.12.23		90%	
8	Оформлення магістерської роботи	13.12.23	III	100%	

Магістрант _____ Сталинський Р.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Жученко О.С.
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Завдяки розвитку технологій та впровадженню комп’ютерних систем, сучасні підприємства можуть використовувати електронний документообіг. Це дозволяє швидко та зручно обмінюватися даними між відділами підприємства, зменшує час доставки документів до мінімуму, покращує надійність інформації та забезпечує її безпеку. Електронний документообіг дозволяє автоматизувати процес обробки документів, відстежувати їхній потік, контролювати строки виконання завдань та організувати спільну роботу над проектами. Це збільшує ефективність роботи, сприяє легкості координації та спілкування між співробітниками. Окрім цього, електронний документообіг забезпечує звітність та аналітику даних. Завдяки цьому, керівництво підприємства може отримати швидкий доступ до необхідної інформації, зрозуміти поточний стан справ та приймати обґрунтовані рішення.

Такі зміни дозволяють підприємству значно підвищити ефективність своєї роботи. Централізоване управління дозволяє зібрати всю необхідну інформацію в одному місці і швидко аналізувати її, що сприяє прийняттю кращих управлінських рішень. Збір і обробка даних також дає можливість виявляти тренди і патерни, що допомагає управлінцям прогнозувати та адаптувати свою діяльність відповідно до них. Електронний документообіг забезпечує швидку та безпечну передачу і зберігання документів. Це дозволяє працівникам швидко отримувати доступ до необхідної інформації, зменшує ризик втрати або пошкодження документів, а також покращує процес співпраці та комунікації між різними підрозділами підприємства.

Застосування сучасних засобів зв'язку, таких як електронна пошта, IP-телефонія, миттєві повідомлення та відеоконференції, спрощує комунікацію і сприяє швидкому розповсюдженню інформації. Це дозволяє підприємству оперативно реагувати на зміни в ринкових умовах або внутрішніх процесах, тим самим підвищуючи свою конкурентоспроможність.

У сучасному бізнес-середовищі централізоване управління, збір і обробка даних, а також електронний документообіг є невід'ємною частиною успішної підприємницької діяльності. Вони допомагають підприємству бути більш ефективним, оперативним і безпечним, що, у свою чергу, дозволяє досягти конкурентних переваг на ринку.

Ethernet є найпоширенішою технологією для локальних мереж (LAN) через свої численні переваги. Вона використовується в бізнес-інфраструктурах, урядових організаціях, освітніх установах та домашніх мережах. Однією з головних переваг Ethernet є його низька вартість. Це робить його доступним для використання в будь-якому масштабі - від невеликих бізнесів до великих корпорацій. Використання Ethernet також досить просте, що робить його популярним у некваліфікованих користувачів. Мережі можна легко настроїти та розширити без спеціальних знань або дорогоцінного обладнання. Ethernet також пропонує велику кількість різноманітного обладнання, яке може бути використане для побудови і керування мережами. Це означає, що користувачі можуть вибирати обладнання, яке найкраще відповідає їх конкретним потребам і бюджету. Швидкість обміну даними в Ethernet також дуже висока, варіюючись від 10 до 1000 Мбіт/с. Це робить його ідеальним для передачі великого обсягу даних і забезпечує ефективне використання мережі.

Щодо протоколу обміну даними, Ethernet використовує стек протоколів, який надає всі необхідні функції для організації зв’язку, контролю прав доступу, маршрутизації та передачі сигналу по мережі. Цей стек дозволяє об'єднувати мережі, побудовані за різними технологіями, що забезпечує гнучкість і сумісність. Узагалі, Ethernet є найбільш ефективним і популярним вибором для локальних мереж через свої переваги вартості, простоти, швидкості та варіантів обладнання. Він постійно розвивається та вдосконалюється, щоб задовольнити зростаючі потреби мережевої інфраструктури.

Таким чином тема роботи є актуальною, яка передбачає в ході свого виконання розв’язування задач дослідницького та/або інноваційного характеру.

У ході підготовки та виконання роботи автором була використана інформація, у тому числі текст, формули, рисунки, схеми, алгоритми, методики проведення аналізу, досліджень, визначення певних характеристик, параметрів та вихідних даних, розрахунків тощо, що міститься у джерелах [1 – 23], наведених у списку використаних джерел, а також інформація, отримана в результаті консультування з керівником роботи, науковими, науково-педагогічними працівниками та іншими особами, яка є неопублікованими авторськими напрацюваннями, дозволеними для використання автору цієї роботи виключно при виконанні тільки цієї роботи.

РОЗДІЛ 1

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ КОМУТОВАНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Типова мережа може мати різну топологію, але одна з найпоширеніших є зіркова топологія. У цій топології кожен комп'ютер підключений до центрального вузла, такого як комутатор або концентратор.

Комутатор є розподільником даних і дозволяє підключати кілька комп'ютерів до одного порту, що забезпечує економію місця і спрощує управління мережею. Комутатор також забезпечує можливість комунікації між комп'ютерами в мережі шляхом використання MAC-адрес.

Маршрутизатор також є важливим компонентом мережі. Він використовується для пересилання пакетів даних між різними мережами. Маршрутизатори визначають найкоротший шлях для пересилки пакетів та забезпечують безпеку передачі даних.

Управління мережею проводиться за допомогою спеціального програмного забезпечення, яке дозволяє налаштувати параметри мережі, такі як швидкість передачі даних, адресація і безпека. Типова мережа також може мати додаткові компоненти, такі як файрволи, проксі-сервери або сервери зберігання даних.

Така мережева структура забезпечує високу пропускну здатність і низьку затримку при передачі даних. Крім того, комутатори дозволяють керувати трафіком мережі, встановлюючи пріоритети і розподіляючи пропускну здатність між різними користувачами або пристроями. Це робить мережу більш ефективною і забезпечує якісне обслуговування для всіх користувачів. Це дозволяє комутаторам просто передавати дані з одного пристрою на інший, без необхідності розуміти або маніпулювати змістом цих даних. Таким чином, комутатори є швидкими і ефективними пристроями для передачі даних на мережі. Вони забезпечують кращу пропускну здатність та

менші затримки порівняно з маршрутизаторами, які працюють на більш високих рівнях моделі OSI і вимагають детального аналізу заголовків пакетів.

Комутація 2-го рівня - це форма комутації даних в комп'ютерних мережах, яка відбувається на рівні каналу зв'язку. Вона здійснюється апаратно за допомогою комутаторів - мережевих пристроїв, які пересилають пакети даних між різними пристроями в мережі. Одна з основних причин використання комутації 2-го рівня - це сегментація мережі. Розподіл великої мережі на логічні сегменти дозволяє зменшити кількість пристроїв у фізичному сегменті. Це полегшує керування мережею та збільшує її продуктивність, оскільки обсяг переданих даних в окремих сегментах зменшується. Ще одна причина використання комутації 2-го рівня - це об'єднання робочих груп. Комутатори дозволяють підключати різні пристрої до одного комутатора, створюючи таким чином робочу групу. Це полегшує обмін даними між пристроями в групі та забезпечує швидкий доступ до ресурсів мережі.

Комутація 2-го рівня має високу продуктивність, оскільки пакет даних не зазнає змін під час комутації. Це дозволяє забезпечити швидке перемикання даних між пристроями у мережі. Висока продуктивність комутаторів сприяє ефективній роботі мережі та полегшує її адміністрування. Узагалі, комутація 2-го рівня використовується для ефективної організації та керування комп'ютерними мережами. Вона дозволяє забезпечити швидку та безперебійну передачу даних між пристроями, дозволяє розділити мережу на логічні сегменти, а також об'єднати робочі групи.

Таким чином, якщо на мережі постійно відбувається розсилка широкомовних кадрів, це може завантажити комутатори 2-го рівня і знизити продуктивність мережі. Додатково, широкомовні кадри можуть бути небезпечними з точки зору безпеки, оскільки якщо один комутатор невірно налаштований, він може передавати широкомовні кадри в усьому сегменті мережі, що може призвести до перевантаження мережі або витоку конфіденційної інформації.

1.1 Алгоритм роботи протоколу Spanning Tree Protocol (IEEE 802.1d)

Протокол Spanning Tree Protocol (STP) використовується для підвищення відмовостійкості Ethernet мережі шляхом усунення петель. Петлі в мережі можуть призвести до мультикастових бурьанів або неправильного приведення до одного мережевого комутатора, що спричиняє мережну недоступність.

STP працює шляхом визначення одного комутатора в мережі як кореневого комутатора, який визначає шляхи до всіх інших комутаторів. Цей кореневий комутатор вибирається на основі значень пріоритету комутатора і однозначного ідентифікатора комутатора. Потім STP вибирає найкоротший шлях до всіх інших комутаторів, щоб уникнути петель в мережі.

Якщо якийсь комутатор або посилка в мережі вийде з ладу, STP автоматично буде пересилати трафік через альтернативний шлях, який був попередньо підготовлений. Це дозволяє мережі зберігати зв'язність і надійність, навіть при випадкових відмовах.

Протокол STP є частиною сімейства протоколів Ethernet і є стандартом IEEE 802.1D. Існують також вдосконалені версії STP, такі як Rapid Spanning Tree Protocol (RSTP) і Multiple Spanning Tree Protocol (MSTP), які пропонують поліпшену продуктивність і масштабованість.

Поширення широкомовних повідомлень в мережах з петлями представляє серйозну проблему. Припустимо, що перший кадр, що надійшов від вузла 1, є широкомовною. Тоді всі комутатори пересилатимуть кадри нескінченно (рисунок 1.1), використовуючи всю доступну смугу пропускання мережі і блокуючи передачу інших кадрів у всіх сегментах.

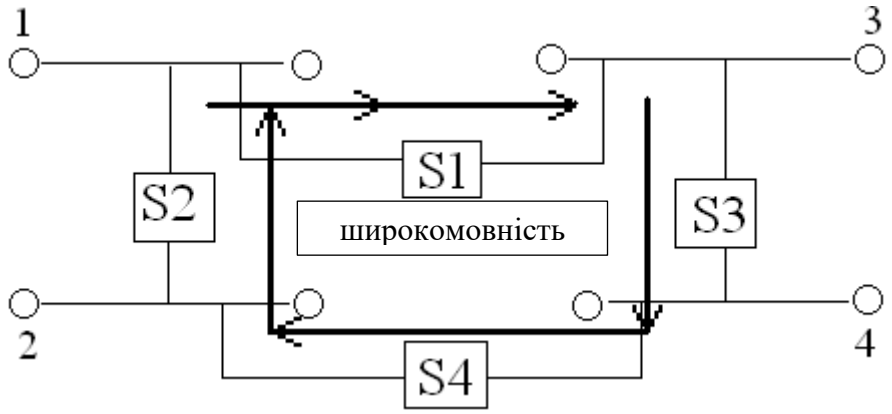

Рисунок 1.1 - Мостові петлі в середовищі прозорих мостових з'єднань

Ще одна проблема називається "broadcast storm". Вона виникає, коли комутатор отримує багато копій одного кадру, а таблиця комутації не може визначити правильного порту для переадресації кожної копії. Це може призвести до перевантаження комутатора і втрати даних. Крім того, постійне оновлення таблиці комутації забирає ресурси комутатора, що може призвести до його перевантаження і зниження продуктивності мережі.

Один зі способів вирішення цієї проблеми - використання протоколів, які запобігають широкомовному шторму, таких як Spanning Tree Protocol (STP) або Rapid Spanning Tree Protocol (RSTP). Ці протоколи дозволяють блокувати деякі порти на комутаторах, щоб уникнути формування замкнутих петель у мережі і забезпечити правильну передачу даних.

Крім того, можна застосовувати інші техніки, такі як використання VLAN (Virtual Local Area Network) або Quality of Service (QoS), для виділення каналу для певних типів трафіку та обмеження його потоку, щоб знизити ймовірність широкомовної повені.

В цілому, правильне налаштування і управління комутаторами, використання відповідних протоколів і технік можуть допомогти зменшити вплив широкомовної повені на роботу мережі.

Протокол STP розроблений для уникнення петель і забезпечення безперебійної комутації кадрів. Він дозволяє комутаторам в мережі обмінюватися інформацією про своїх сусідів і порти та автоматично визначає найоптимальніший шлях для передачі кадрів в мережі.

Алгоритм STA використовує два типи повідомлень - BPDU (Bridge Protocol Data Unit), яке використовується для обміну інформацією між комутаторами, і TCN (Topology Change Notification), яке використовується для сповіщення про зміну топології мережі.

Кожен комутатор в мережі обирає один з портів як кореневий порт (Root Port), який має найкоротший шлях до кореневого комутатора. Також кожен комутатор визначає своїх сусідів і порти, які ведуть до тих сусідів. За допомогою BPDU повідомлень, комутатори обмінюються інформацією про своїх сусідів і порти. STA алгоритм перебирає всі можливі конфігурації мережі і вибирає ту, яка не має петель і має найкоротший шлях до кореневого комутатора. Окрім того, протокол виявляє зміну топології мережі і виконує перерахунок шляхів для уникнення петель.

Протокол STP є надійним і ефективним рішенням для уникнення петель в об'єднаній мережі і забезпечення надійної комутації кадрів. Він дозволяє мережі працювати безперебійно навіть у складних топологіях з багатьма з'єднаннями та перехрестями. Комутатори, що підтримують протокол STP, автоматично створюють деревоподібну конфігурацію зв'язків без петель в комп'ютерній мережі. Така конфігурація називається покриваючим деревом - Spanning Tree. Конфігурація покриваючого дерева будується комутаторами автоматично з використанням обміну службовими пакетами.

1.2 Віртуальні локальні мережі VLAN

VLAN - це метод логічного розділення мережі на окремі віртуальні мережі на рівні комутатора. Кожна VLAN може мати свою власну політику доступу та настройки безпеки. Комутатори у мережі використовують тегування пакетів, щоб ідентифікувати, до якої VLAN належить пакет. Таким

чином, широкомовний трафік не поширюється між різними VLAN, що дозволяє ефективно контролювати трафік і запобігти насиченню смуги пропускання.

Організація VLAN може бути проведена на основі фізичних портів комутаторів (Port-based VLAN), або на основі ідентифікаторів мережевих протоколів (Protocol-based VLAN). У першому випадку, кожен порт комутатора призначається до певної VLAN, а у другому випадку, VLAN визначається на основі ідентифікаторів протоколів, що містяться в заголовках пакетів.

VLAN може бути використана для трьох основних цілей.

1. Сегментація мережі - дозволяє розділити фізичну мережу на кілька логічних сегментів, забезпечуючи ізоляцію та безпеку мережевого трафіку між сегментами.

2. Забезпечення безпеки - VLAN можуть бути використані для контролю доступу до ресурсів мережі, розділяючи користувачів на окремі VLAN та налаштовуючи політики безпеки для кожної VLAN.

3. Оптимізація трафіку - розділення мережі на VLAN дозволяє керувати широкомовним трафіком, знижуючи його поширення та покращуючи продуктивність мережі.

Використання VLAN дозволяє гнучко налаштовувати мережу і забезпечувати безпеку даних. Віртуальні мережі дозволяють обмежувати доступ до ресурсів мережі лише визначеній групі користувачів, забезпечуючи контроль над рівнем доступу до даних. Крім того, VLAN дозволяють злити кілька фізичних локальних мереж в одну віртуальну, що спрощує управління і обслуговування мережі. Використання VLAN також допомагає зменшити навантаження на смугу пропускання. Завдяки ізоляції трафіку між віртуальними мережами, передача даних обмежується лише до необхідних вузлів мережі, що дозволяє ефективно використовувати доступну смугу пропускання без розсіювання трафіку на непотрібні вузли. Це забезпечує покращення продуктивності мережі і забезпечує швидкості передачі даних.

У загальному, використання VLAN дозволяє досягти кращого керування трафіком, підвищити безпеку мережі і покращити її продуктивність. Віртуальні мережі допомагають ізолювати трафік і обмежувати доступ до ресурсів мережі, що забезпечує контроль і безпеку даних. Вони також сприяють ефективному використанню смуги пропускання та поліпшенню продуктивності мережі. При використанні VLAN на базі портів, кожен порт призначається у певну VLAN, незалежно від того, який користувач або комп'ютер підключений до цього порту. Це означає, що всі користувачі, підключені до цього порту, будуть членами однієї VLAN (рисунок 1.2). Конфігурація портів статична і може бути змінена тільки вручну.

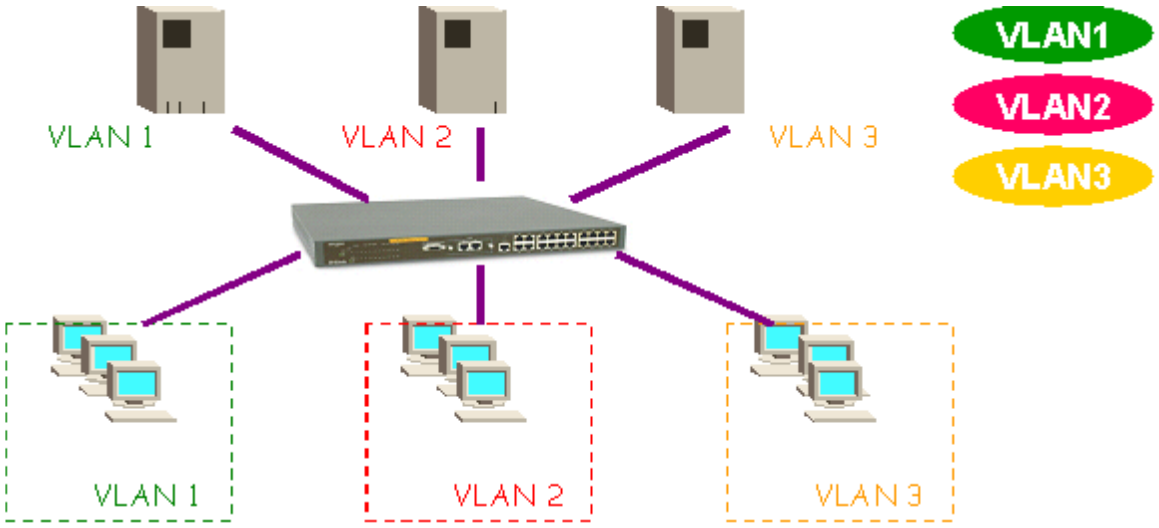

Рисунок 1.2 - VLAN на базі портів.

Розглянемо основні характеристики VLAN на базі портів.

1. Застосовуються в межах одного комутатора. Якщо необхідно організувати кілька робочих груп у межах невеликої мережі на основі одного комутатора, наприклад, необхідно рознести технічний відділ та відділ продажів, то рішення VLAN на базі портів оптимально підходить для даної задачі.

2. Простота налаштування. Створення віртуальних мереж на основі групування портів не вимагає від адміністратора великого обсягу ручної

роботи – досить кожному порту, який в одній VLAN, привласнити один і той же ідентифікатор VLAN (VLAN ID).

3. Можливість зміни логічної топології мережі без фізичного переміщення станцій - досить усього лише змінити настройки порту, з одного VLAN (наприклад, VLAN технічного відділу) на іншу (VLAN відділу продажів) і робоча станція відразу ж отримує можливість спільно використовувати ресурси з членами в новій VLAN. Таким чином, VLAN забезпечують гнучкість при переміщеннях, зміни та нарощуванні мережі.

4. Кожен порт може входити тільки в один VLAN. Тому для об'єднання віртуальних підмереж - як усередині одного комутатора, так і між двома комутаторами, потрібно використовувати мережевий рівень. Один з портів кожного VLAN підключається до інтерфейсу маршрутизатора, який створює таблицю маршрутизації для пересилання пакетів з однієї підмережі в іншу (IP адреси підмереж повинні бути різними).

Недоліком такого рішення є те, що один порт кожного VLAN необхідно підключати до маршрутизатора, при цьому порти і кабелі використовуються дуже неефективно.

Наступний спосіб, який використовується для утворення віртуальних мереж, заснований на груповані MAC-адрес. При існуванні в мережі великої кількості вузлів цей спосіб вимагає виконання великої кількості ручних операцій від адміністратора. Однак він виявляється більш гнучким при побудові віртуальних мереж на основі декількох комутаторів, ніж спосіб угруповання портів. Групування MAC-адрес в мережу на кожному комутаторі позбавляє від необхідності їх зв'язку декількома портами, однак, вимагає виконання великої кількості ручних операцій з маркування MAC-адрес на кожному комутаторі мережі (рисунок 1.3).

Широкомовні домени на базі MAC-адрес, дозволяють фізично переміщати станцію (підключати до будь-якого порту комутатора), дозволяючи залишатися їй в одному і тому ж широкомовному домені без будь-яких змін у налаштуваннях конфігурації.

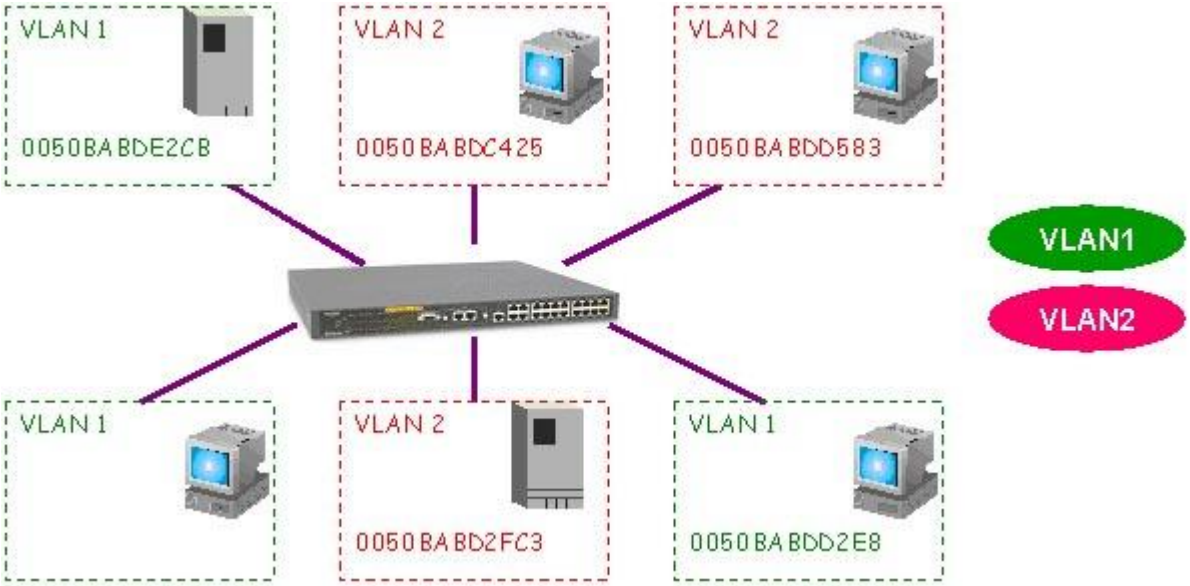

Рисунок 1.3 - VLAN на базі MAC-адресів

VLAN на базі міток - стандарт 802.1q. Цей підхід заснований на стандарті 802.1q і полягає в додаванні тегу до кадру Ethernet. Тег містить інформацію про приналежність кадру до певної VLAN. Коли кадр надсилається на комутатор, він перевіряє тег, щоб визначити, до якої VLAN належить кадр, і відповідно розподіляє його у потрібну віртуальну мережу.

Цей підхід дозволяє більш гнучке керування віртуальними LANами, оскільки кадри можуть бути пересилані між комутаторами без необхідності переналаштування адресних таблиць. Крім того, з використанням тегів можна легко розподіляти трафік між комутаторами у мульти-VLAN середовищі.

Проте, використання тегів може призвести до додаткової навантаження на комутатори, оскільки їм потрібно аналізувати і обробляти додаткову інформацію. Крім того, теги можуть призвести до збільшення розміру кадрів, що може викликати проблеми зі сумісністю з деякими пристроями.

Однак, в цілому підхід VLAN на базі міток є потужним інструментом для організації та управління віртуальними мережами у великих мережах. Він дозволяє розподіляти трафік ізолювати різні групи користувачів і покращує безпеку і продуктивність мережі. Стандарт IEEE 802.1q визначає зміни в

структурі кадру Ethernet, що дозволяють передавати інформацію про VLAN по мережі (рисунок 1.4).

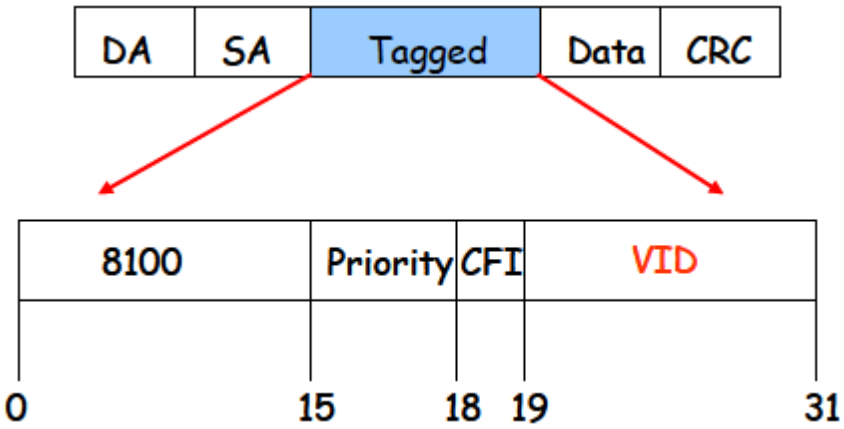

Рисунок 1.4 - Маркірований кадр Ethernet

З точки зору зручності і гнучкості налаштувань, VLAN на основі міток є кращим рішенням. Основні переваги цього рішення.

Основні переваги VLAN на основі міток включають таке.

1. Зручність налаштування. Використання міток для розділення мережі на віртуальні сегменти дозволяє адміністраторам з легкістю налаштовувати та керувати розподілом ресурсів мережі.

2. Гнучкість: VLAN на основі міток дозволяє гнучко налаштовувати та об'єднувати різні фізичні порти в одних віртуальних сегментах мережі. Це дозволяє забезпечувати розумне розподілення трафіку та оптимізувати використання ресурсів мережі.

3. Незалежність від фізичної інфраструктури. Використання міток дозволяє створювати віртуальні сегменти мережі, незалежні від фізичного розташування мережевого обладнання. Це дає можливість гнучкого розподілу ресурсів та зменшення часу та зусиль, необхідних для перетягування фізичного обладнання.

4. Безпека. VLAN на основі міток дозволяє обмежувати доступ між віртуальними сегментами мережі, що забезпечує підвищений рівень безпеки.

Адміністратори можуть налаштовувати права доступу для різних груп користувачів та обмежувати їх доступ до певних ресурсів мережі.

5. Швидкодія: Використання міток для віртуалізації мережі зменшує потребу у фізичних комутаторах та знижує затримку передачі даних. Це дозволяє покращити швидкодію мережі та забезпечити повну використання доступних ресурсів.

Усі ці переваги роблять VLAN на основі міток більш зручним та гнучким рішенням порівняно з іншими методами розподілу мережевих ресурсів.

РОЗДІЛ 2

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

2.1 Аналіз існуючого обладнання

Однією з особливостей мережі, є те, що частина обладнання вже є у наявності. Це з одного боку полегшує розрахунок параметрів мережі через вже відомі характеристики апаратури, з іншого − при розробці треба враховувати вже існуюче обладнання, що накладає деякі обмеження. Серед існуючого обладнання можна виділити голосовий шлюз, цифрові комутатори (IP АТС), VoIP WiFi шлюзи та IP телефони, основні характеристики яких наведено нижче.

Голосовий шлюз Dynamix DW – 2 FXS/2 FXO SIP має наступні характеристики:

- automatically Dial Path Selection (IP or PSTN) - автоматичне визначення напрямку з'єднання;

- PSTN Line switch to telephone set when power is failure - автоматичне вивільнення лінії при вимкненні живлення;

- PPPoE support подтримка протоколів PPPoE;

- можливість роботи в мережі з NAT;

- можливість працювати в одній мережі з DNS сервером;

- можливість працювати без SIP проксі сервера;

- можливість оновлення програм через TFTP чи FTP;

- можливість дистанційного конфігурування та презавантаження;

- підтримка протоколу DHCP;

- шлюзом підтримуютсья наступні аудіокодеки: G.711 a/μ law, G.723.1 (6.3kbps), G.729, G.729A;

- режим подавлення відлуння (эха) за стандартами G.168/165;

- динамічний буфер для подавлення джитера.

Також шлюз має 2 порти для підключення до нього до двох абонентських закінчень ТМЗК.

Цифровий комутатор Dynamix IP PBX-100 має наступні основні характеристики:

- підтримка протоколу SIP;
- підтримка наступних аудіокодеків:

  G.711(A-Law& //-Law) ;

  G.729;

  G723 Pass-Thru;

  GSM;

- можливість керування через Web браузер;
- оновлення ПЗ через HTTP;
- експорт та імпорт конфігурації;
- мережеві інтерфейси 1 WAN 1 LAN;
- підтримка до 100 користувачів;
- підтримка до 13 одночасних викликів.

VoIP WiFi шлюз Dynamix DW 3512 має наступні основні характеристики:

Інтерфейси:

Ethernet (RJ-45, 10/100 base-T):

- 1-WAN порт для підключення до маршрутизатора чи комутатора;
- 4-LAN порти для підключення комп'ютерів чи інших приладів;
- 3 телефонні порти (RJ-11) , в тому числі:
- 2-FXS для підключення аналогових телефонів (POTS).

Маршрутизація (IP шлюз):

-підтримка IPv4 (RFC 791);

- підтримка MAC адрес (IEEE 802.3);
- підтримка TCP/UDP (RFC 793/768);
- підтримка RTP/RTCP (RFC 1889/1890);
- підтримка ICMP (RFC 792);
- підтримка ARP (RFC 826);
- підтримка статичних IP (WAN);

- підтримка DHCP Client (RFC 2131);
- підтримка DHCP Server (RFC 2131);
- підтримка PPPoE Client (RFC 2516);
- підтримка DNS Client;
- підтримка Dynamic DNS;
- підтримка NAT/NAPT (RFC 1631);
-підтримка Firewall:
- IP фільтрації;
- фільтрації за портами;
- фільтрації за MAC адресами;
- фільтрації за URL адресами;
- перенаправлення портів;
- запобігання DoS: атаки на відмову у обслуговуванні;
- підтримка Quality of Service;
- 802.1Q VLAN Tag;
- DiffServ (RFC 2475).

Беспровідні мережі (Wireless LAN):

- сумісність зі стандартом IEEE 802.11 b/g;
- смуга частот: 2.4GHz (B) / 2.4GHz (G) / 2.4GHz (B+G) ;
- швидкості: 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M;
- шифрування і аутентифікація 802.1x:
- WEP (64/128bits), WPA/WPA1-TKIP/AES, Mixed WPA WPA2;
- WPA Authentication: PSK:Pre-Shared Key (Personal) / Radius (Enterprise);
- контроль доступу за MAC адресами;

IPтелефонія (VoIP):

- підтримка SIPv2 (RFC 3261);

мовні кодеки:

- G.711 (a-Law/u-Law): 64 bits (PCM);

- G.723.1: 6.3k/5.3k bits;

- G.726: G.726: 16/24/32/40K bits (ADPCM);

- G.729A: 8k bits (CS-SCELP);

- G.729B: VAD та CNG згідно до G.729;

- VAD (Визначення пауз), CNG (генерація комфортного шуму у паузах)^

- подавлення луни сумісне зі стандартом G.168/165;

- динамічний буфер пакетів;

- підтримка Caller ID.

Безпека:

- 802.1x безпровідна аутентифікація і шифрування;

- вбудований Firewall;

- захист від Denial of Service;

- MD5 для SIP аутентифікації (RFC 2069 / 2617);

Dynamix IP Phone PoE має такі основні характеристики:

- два повнодуплексні 10/100Mb Ethernet порти (RJ-45);

- підтримка статичних IP / DHCP / PPPoE.

Voice:

- заходження та генерація DTMF;

- компенсація відлуння;

- підтримка кодеків G.711a/u-Law, G.729;

- спеціальний буфер для контролю затримки (джитера);

- DTMF згідно з RFC2833.

Використовуючи наведену вище інформацію нам необхідно визначитись з аудіо кодеками, які будуть використовуватися у мережі (таблиця 2.1).

Таблиця 2.1 - Кодеки, що підтримуються обладнанням

Кодеки	Dynamix DW-2 FXS/2 FXO FXSO Gateway (SIP)	Dynamix IP PBX-100	VoIP WiFi шлюз Dynamix DW 3512	Dynamix IP Phone PoE
G.711 a/μ law	+	+	+	+
G723 Pass-Thru		+		
G.723.1 (5.3kbps)			+	
G.723.1 (6.3kbps)	+		+	
G.726			+	
G.729	+	+		+
G.729A	+		+	
G.729B			+	
GSM		+		

Як ми бачимо з таблиці єдиним кодеком, який підтримується усім існуючим на даний момент обладнанням є G.711, тому у подальших розрахунках треба орієнтуватися саме на нього.

2.2 Розробка схеми комп'ютерної мережі підприємства

Для організації мережі використовувалося таке обладнання як безпровідний маршрутизатор Dynamix з функціями шлюза та ip –телефонії, далі по тексту маршрутизатор.

Керований комутатор з 8 портами D – link та підтримкою STP,VLAN, QoS, далі по тексту комутатор.

Однією функцією яка можлива, але поки ще не задіяна це – VLAN.

Нею можливо організувати роботу комп’ютерів працівників підприємства та зробити так щоб доступ до них був обмежений своєю віртуальною мережею. Працівники в свою чергу будуть мати свою віртуальну мережу та мати доступ тільки до обмеженої кількості комп’ютерів.

Кімната А (рисунок 2.1) має 5 комп’ютерів з доступом до мережі підприємства та інтернет через комутатор, який з'єднаний з кореневим комутатором підприємства, який знаходиться в кімнаті D. Вихід в інтернет організований через безпровідний маршрутизатор який знаходиться в кімнаті В.

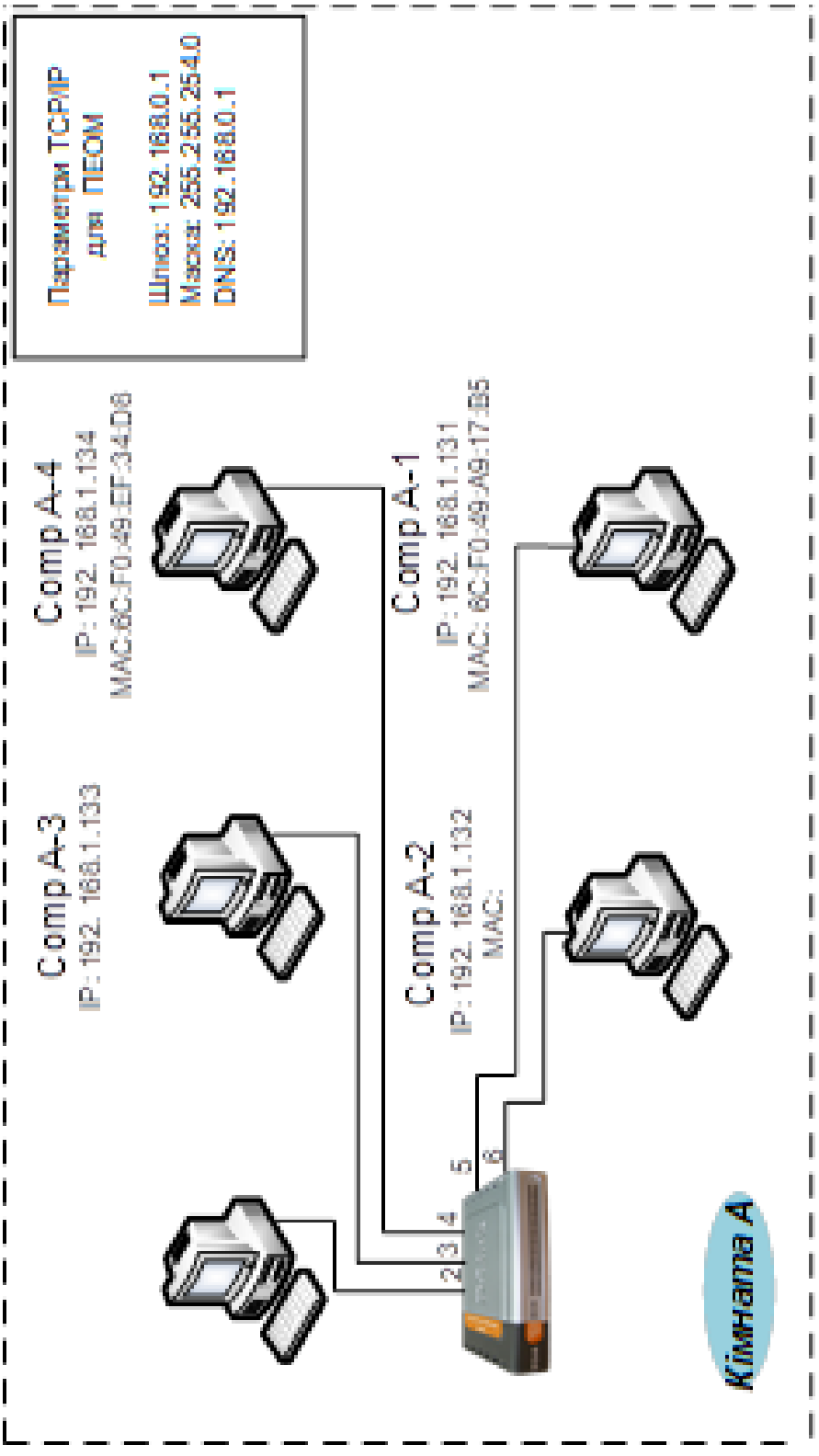

Рисунок 2.1 - Локальна мережа (кімната А)

Кімната В (рисунок 2.2) має 8 комп'ютерів з доступом до мережі підприємства та інтернет через комутатор, який з'єднаний з кореневим комутатором підприємства, який знаходиться в кімнаті D. Вихід в інтернет організований через безпровідний маршрутизатор, який з'єднаний з зовнішньою мережею.

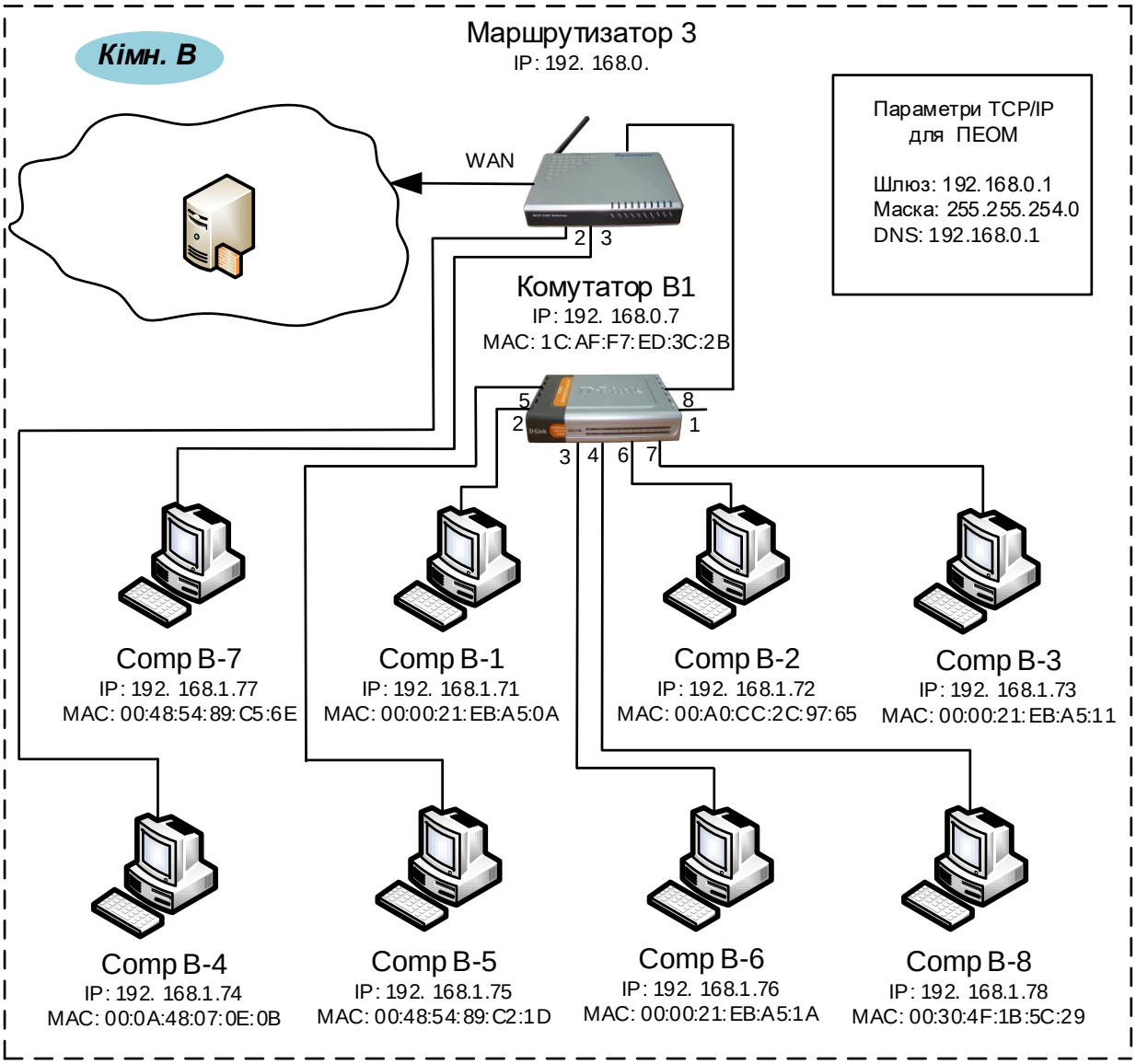

Рисунок 2.2 - Локальна мережа (кімната В)

Кімната C (рисунок 2.3) має 9 комп'ютерів з доступом до мережі підприємства та інтернет через 2 комутатори. Вихід в інтернет організований через безпровідний маршрутизатор, який знаходиться в кімнаті D.

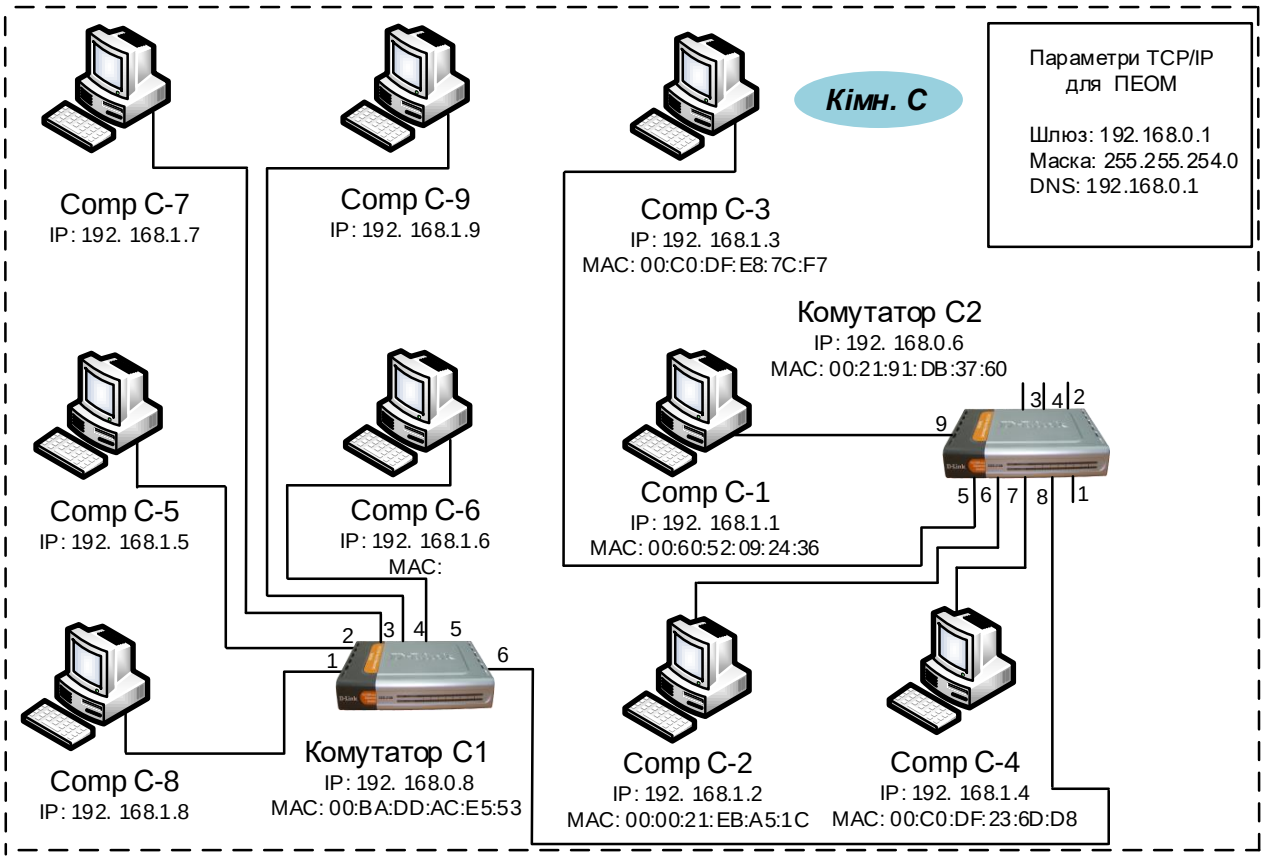

Рисунок 2.3 - Локальна мережа (кімната C)

Кімната D (рисунок 2.4) має 9 комп'ютерів з доступом до мережі підприємства та інтернет через 3 комутатори, які з четвертим комутатором утворюють кільце STP. Вихід в інтернет організований через безпровідний маршрутизатор.

Кімната E (рисунок 2.5) має 3 комп'ютери з доступом до мережі підприємства та інтернет через комутатор. Вихід в Інтернет організований через безпровідний маршрутизатор.

Схеми кімнат F, G показані на рисунках 2.6, 2.7.

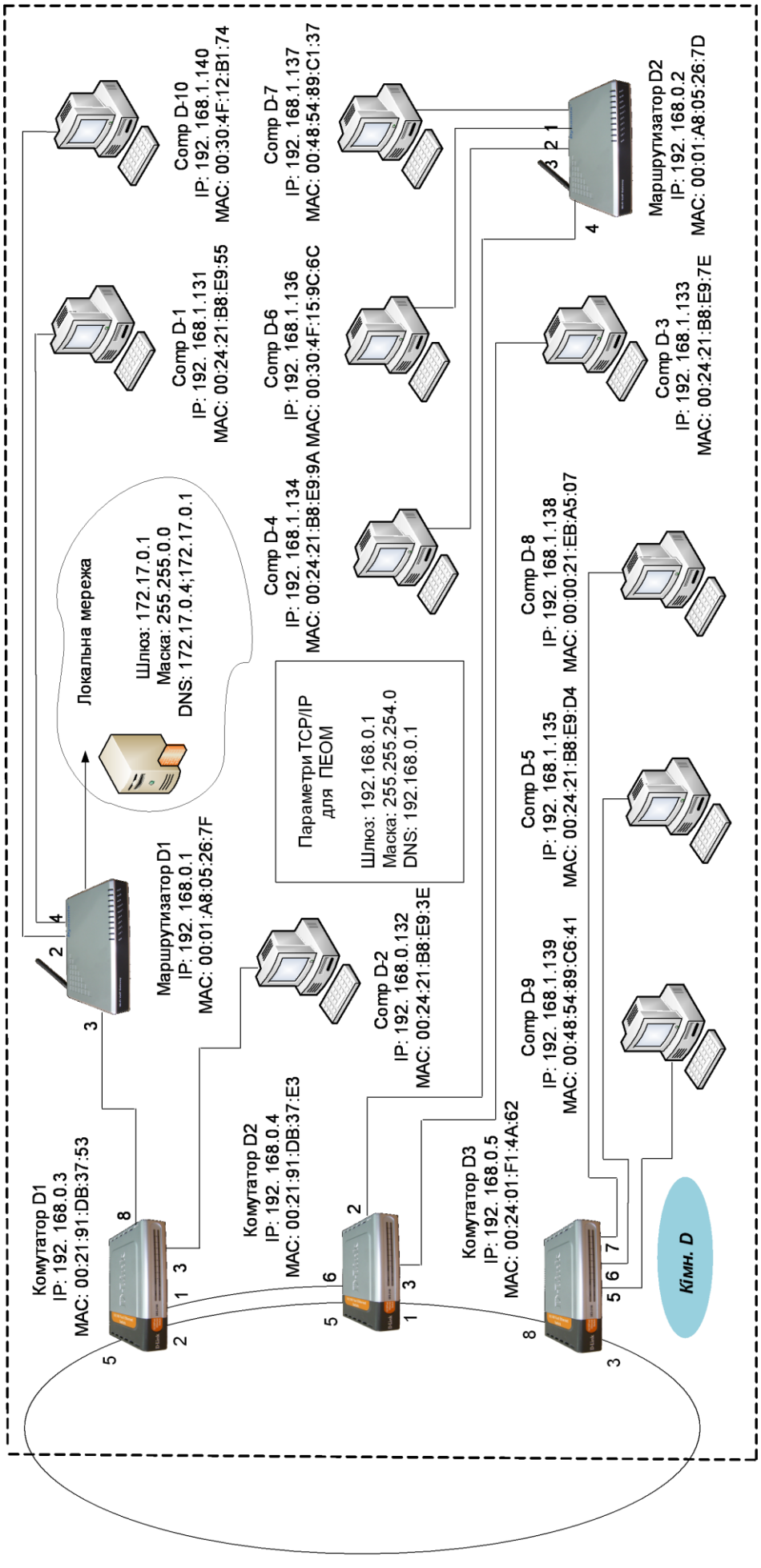

Рисунок 2.4 - Локальна мережа (кімната D)

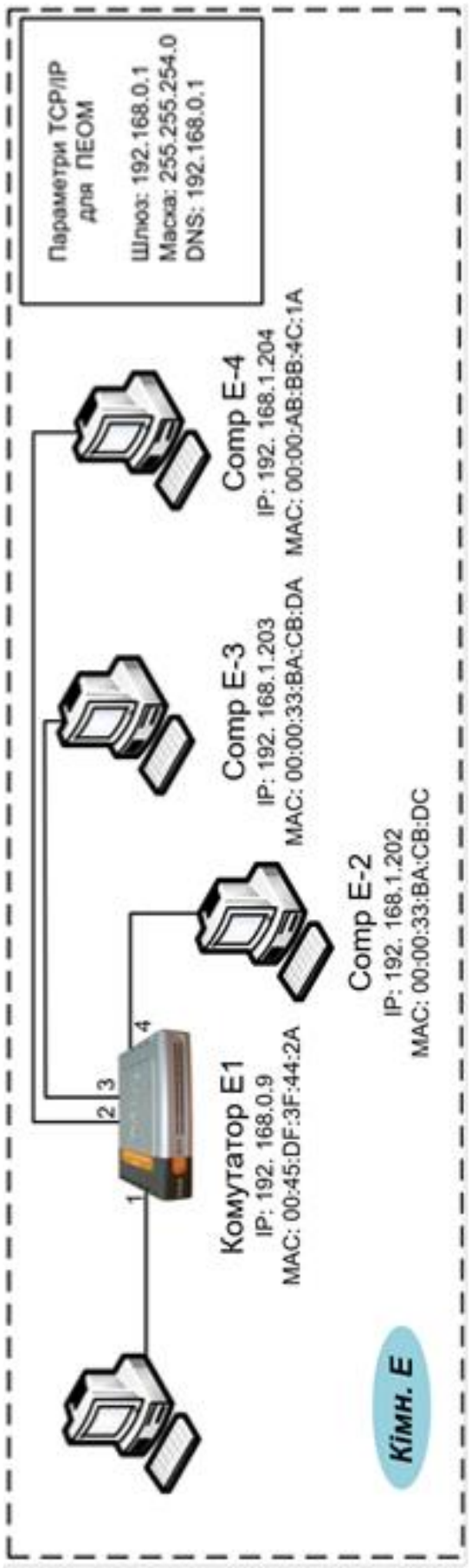

Рисунок 2.5 - Локальна мережа (кімната Е)

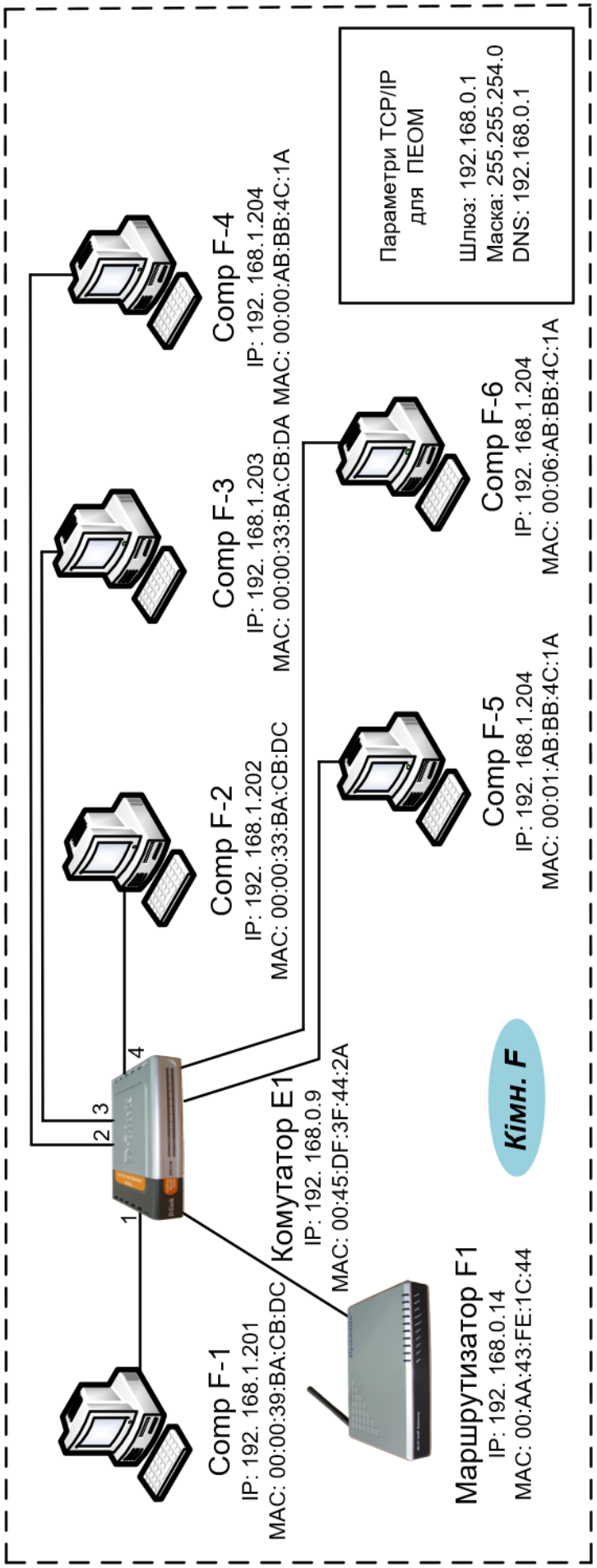

Рисунок 2.6 - Локальна мережа (кімната F)

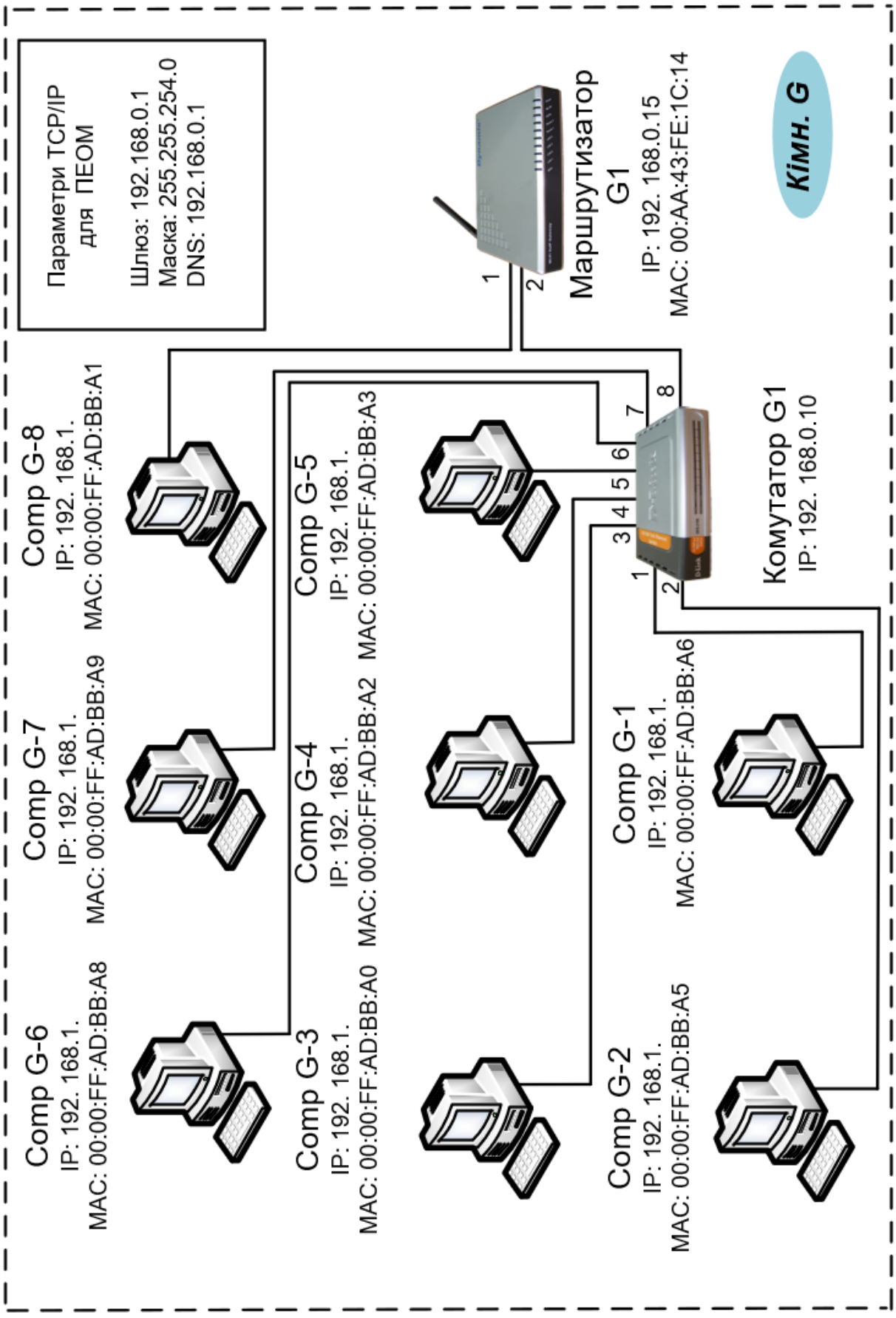

Рисунок 2.7 - Локальна мережа (кімната G)

РОЗДІЛ 3

РОЗПОДІЛ IP - АДРЕС КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Виконаємо розбиття мережі на підмережі за допомогою Free Advanced Subnet Calculator (рисунок 3.1)

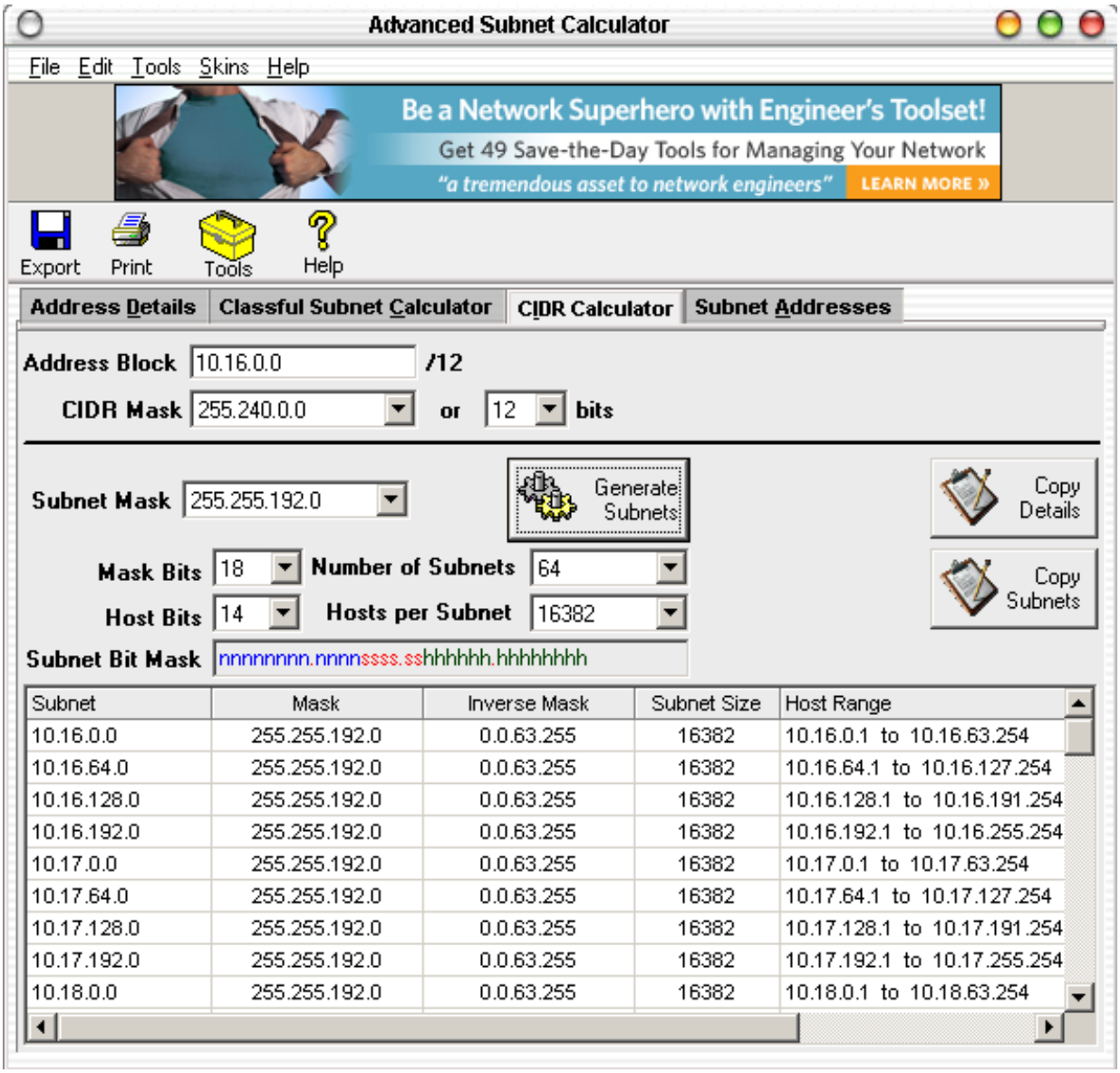

Рисунок 3.1 – Інтерфейс програми Free Advanced Subnet Calculator

Таблиця 3.1 – Розподіл IP - адрес локальної мережі

IP адреса	маска	Пристрій
192.168.0.1	255.255.254.0	Маршрут. D1
192.168.0.2	255.255.254.0	Маршрут. D2
192.168.0.3	255.255.254.0	комутатор
192.168.0.4	255.255.254.0	комутатор
192.168.0.5	255.255.254.0	комутатор
192.168.0.6	255.255.254.0	комутатор
192.168.0.7	255.255.254.0	комутатор
192.168.0.8	255.255.254.0	комутатор
192.168.0.9	255.255.254.0	VoIP Dynamix DW 2 FXS/2 FXO/S
192.168.0.10	255.255.254.0	IP ATC Dynamix IP ePBX
192.168.0.11	255.255.254.0	IP-Phone Dynamix
192.168.0.12	255.255.254.0	IP-Phone Dynamix
192.168.0.13	255.255.254.0	Маршрут. B1
192.168.0.14	255.255.254.0	Маршрут. F1
192.168.0.16	255.255.254.0	комутатор
192.168.0.17	255.255.254.0	комутатор
192.168.0.18	255.255.254.0	комутатор
192.168.0.40	255.255.254.0	DHCP DW B1
192.168.0.41	255.255.254.0	DHCP DW B1
192.168.0.42	255.255.254.0	DHCP DW B1
192.168.0.43	255.255.254.0	DHCP DW B1
192.168.0.44	255.255.254.0	DHCP DW B1
192.168.0.45	255.255.254.0	DHCP DW B1
192.168.0.46	255.255.254.0	DHCP DW B1
192.168.0.47	255.255.254.0	DHCP DW B1
192.168.0.48	255.255.254.0	DHCP DW B1

Продовження таблиці 3.1

IP адреса	маска	Пристрій
192.168.0.49	255.255.254.0	DHCP DW B1
192.168.0.50	255.255.254.0	DHCP DW B1
192.168.0.51	255.255.254.0	DHCP DW B1
192.168.0.52	255.255.254.0	DHCP DW B1
192.168.0.53	255.255.254.0	DHCP DW B1
192.168.0.54	255.255.254.0	DHCP DW B1
192.168.0.55	255.255.254.0	DHCP DW B1
192.168.0.56	255.255.254.0	DHCP DW B1
192.168.0.57	255.255.254.0	DHCP DW B1
192.168.0.58	255.255.254.0	DHCP DW B1
192.168.0.59	255.255.254.0	DHCP DW B1
192.168.0.60	255.255.254.0	DHCP DW F1
192.168.0.61	255.255.254.0	DHCP DW F1
192.168.0.62	255.255.254.0	DHCP DW F1
192.168.0.63	255.255.254.0	DHCP DW F1
192.168.0.64	255.255.254.0	DHCP DW F1
192.168.0.65	255.255.254.0	DHCP DW F1
192.168.0.66	255.255.254.0	DHCP DW F1
192.168.0.67	255.255.254.0	DHCP DW F1
192.168.0.68	255.255.254.0	DHCP DW F1
192.168.0.69	255.255.254.0	DHCP DW F1
192.168.0.70	255.255.254.0	DHCP DW F1
192.168.0.71	255.255.254.0	DHCP DW F1
192.168.0.72	255.255.254.0	DHCP DW F1
192.168.0.73	255.255.254.0	DHCP DW F1
192.168.0.74	255.255.254.0	DHCP DW F1

Продовження таблиці 3.1

IP адреса	маска	Пристрій
192.168.0.75	255.255.254.0	DHCP DW F1
192.168.0.76	255.255.254.0	DHCP DW F1
192.168.0.77	255.255.254.0	DHCP DW F1
192.168.0.78	255.255.254.0	DHCP DW F1
192.168.0.79	255.255.254.0	DHCP DW F1
192.168.0.80	255.255.254.0	DHCP DW D1
192.168.0.81	255.255.254.0	DHCP DW D1
192.168.0.82	255.255.254.0	DHCP DW D1
192.168.0.83	255.255.254.0	DHCP DW D1
192.168.0.84	255.255.254.0	DHCP DW D1
192.168.0.85	255.255.254.0	DHCP DW D1
192.168.0.86	255.255.254.0	DHCP DW D1
192.168.0.87	255.255.254.0	DHCP DW D1
192.168.0.88	255.255.254.0	DHCP DW D1
192.168.0.89	255.255.254.0	DHCP DW D1
192.168.0.90	255.255.254.0	DHCP DW D1
192.168.0.91	255.255.254.0	DHCP DW D1
192.168.0.92	255.255.254.0	DHCP DW D1
192.168.0.93	255.255.254.0	DHCP DW D1
192.168.0.94	255.255.254.0	DHCP DW D1
192.168.0.95	255.255.254.0	DHCP DW D1
192.168.0.96	255.255.254.0	DHCP DW D1
192.168.0.97	255.255.254.0	DHCP DW D1
192.168.0.98	255.255.254.0	DHCP DW D1
192.168.0.99	255.255.254.0	DHCP DW D1
192.168.0.100	255.255.254.0	DHCP DW D1

Продовження таблиці 3.1

IP адреса	маска	Пристрій
192.168.0.101	255.255.254.0	DHCP DW D1
192.168.0.102	255.255.254.0	DHCP DW D1
192.168.0.103	255.255.254.0	DHCP DW D1
192.168.0.104	255.255.254.0	DHCP DW D1
192.168.0.105	255.255.254.0	DHCP DW D1
192.168.0.106	255.255.254.0	DHCP DW D1
192.168.0.107	255.255.254.0	DHCP DW D1
192.168.0.108	255.255.254.0	DHCP DW D1
192.168.0.109	255.255.254.0	DHCP DW D1
192.168.0.110	255.255.254.0	DHCP DW D2
192.168.0.111	255.255.254.0	DHCP DW D2
192.168.0.112	255.255.254.0	DHCP DW D2
192.168.0.113	255.255.254.0	DHCP DW D2
192.168.0.114	255.255.254.0	DHCP DW D2
192.168.0.115	255.255.254.0	DHCP DW D2
192.168.0.116	255.255.254.0	DHCP DW D2
192.168.0.117	255.255.254.0	DHCP DW D2
192.168.0.118	255.255.254.0	DHCP DW D2
192.168.0.119	255.255.254.0	DHCP DW D2
192.168.0.120	255.255.254.0	DHCP DW D2
192.168.0.121	255.255.254.0	DHCP DW D2
192.168.0.122	255.255.254.0	DHCP DW D2
192.168.0.123	255.255.254.0	DHCP DW D2
192.168.0.124	255.255.254.0	DHCP DW D2
192.168.0.125	255.255.254.0	DHCP DW D2
192.168.0.126	255.255.254.0	DHCP DW D2

Продовження таблиці 3.1

IP адреса	маска	Пристрій
192.168.0.131	255.255.254.0	Comp D-1
192.168.0.132	255.255.254.0	Comp D -2
192.168.0.133	255.255.254.0	Comp D -3
192.168.0.134	255.255.254.0	Comp D -4
192.168.0.135	255.255.254.0	Comp D -5
192.168.0.136	255.255.254.0	Comp D 4-6
192.168.0.137	255.255.254.0	Comp D 4-7
192.168.0.138	255.255.254.0	Comp D -8
192.168.0.139	255.255.254.0	Comp D -9
192.168.0.140	255.255.254.0	Comp D -10
192.168.1.1	255.255.254.0	CompC-1
192.168.1.2	255.255.254.0	CompC-2
192.168.1.3	255.255.254.0	CompC-3
192.168.1.4	255.255.254.0	CompC-4
192.168.1.5	255.255.254.0	CompC-5
192.168.1.6	255.255.254.0	CompC-6
192.168.1.7	255.255.254.0	CompC-7
192.168.1.8	255.255.254.0	CompC-8
192.168.1.9	255.255.254.0	CompC-9
192.168.1.71	255.255.254.0	CompB-1
192.168.1.72	255.255.254.0	CompB-2
192.168.1.73	255.255.254.0	CompB-3
192.168.1.74	255.255.254.0	CompB-4
192.168.1.75	255.255.254.0	CompB-5
192.168.1.76	255.255.254.0	CompB-6
192.168.1.77	255.255.254.0	CompB-7

Продовження таблиці 3.1

IP адреса	маска	Пристрій
192.168.1.78	255.255.254.0	CompB-8
192.168.1.131	255.255.254.0	CompA-1
192.168.1.132	255.255.254.0	CompA-2
192.168.1.133	255.255.254.0	CompA-3
192.168.1.134	255.255.254.0	CompA-4
192.168.1.135	255.255.254.0	CompA-5
192.168.1.201	255.255.254.0	CompE-1
192.168.1.202	255.255.254.0	CompE-2
192.168.1.203	255.255.254.0	CompE-3
192.168.1.204	255.255.254.0	CompE-4
192.168.1.221	255.255.254.0	CompF-1
192.168.1.222	255.255.254.0	CompF-2
192.168.1.223	255.255.254.0	CompF-3
192.168.1.224	255.255.254.0	CompF-4
192.168.1.225	255.255.254.0	CompF-5
192.168.1.226	255.255.254.0	CompF-6
192.168.1.227	255.255.254.0	CompF-7
192.168.1.228	255.255.254.0	CompF-8

Так виконавши розбиття на підмережі IP – мережі підприємства ми зробили зручним пошук комп’ютерів та присвоїли кожному абоненту свою унікальну IP – адресу тим самим попередивши дублювання адрес.

РОЗДІЛ 4

РОЗРАХУНОК ІНТЕНСИВНОСТІ ПОТОКІВ ПАКЕТІВ З МОВОЮ ВІДЕО ТА ДАНИМИ

Так як для розрахунку використовується мережа підприємства на ній є велика кількість потоків інформації таких як, телефонія, обмін даними, доступ в Інтернет, відеоконференції та інші. Виберемо найбільш критичні до затримок (мову та відео), а інші будуть даними.

Комутатор може працювати у двох режимах: неоднорідний потік пакетів, або з відносними пріоритетами.

На рисунку 4.1 зображено схему затримки пакетів.

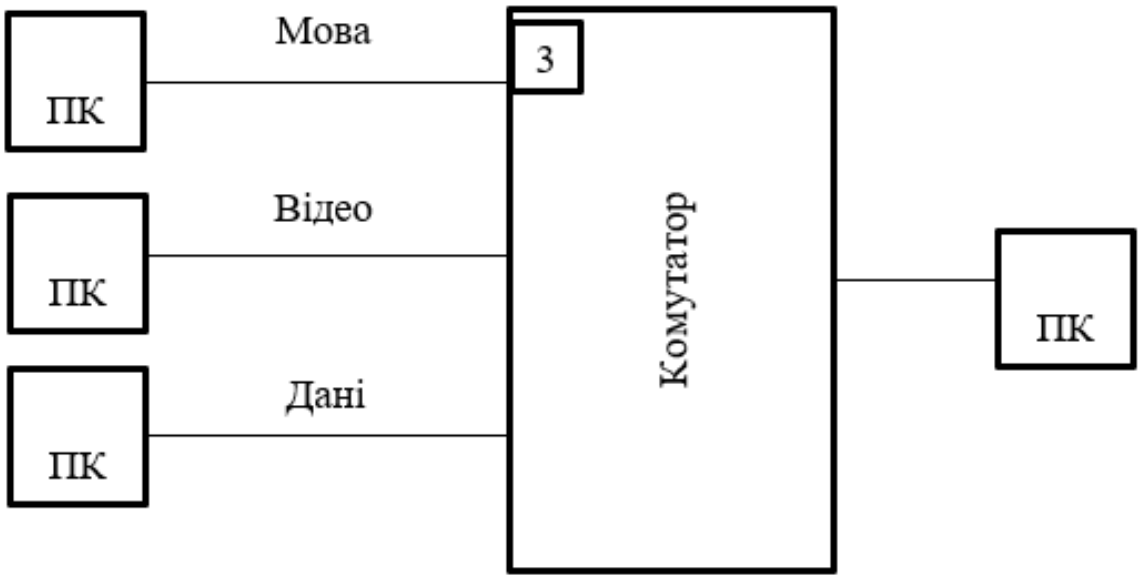

Рисунок 4.1 – Схема вимірювання затримки пакетів

Задамо 3 потоки аудіо, відео та данні (таблиця 4.1).

Таблиця 4.1 – Вихідні данні

Потік	Мова	Відео	Данні
Середня довжина потоку, біт.	60	600	1000
Інтенсивність потоку, пакетів\с.	50	800	1000
Коефіцієнт варіації потоку	0	1	1

$$R_{\text{транспорт}} = 1 \cdot 10^8 = 100 \text{ Мбіт\с.}$$

4.1 Розрахунок затримки в комутаторі при неоднорідному потоку пакетів

Середній час очікування є однаковим для всіх класів пакетів і визначається за наступною формулою:

$$\overline{T}_{\text{очік.обсл.}k} = \overline{T}_{\text{очік.обсл.}} = \frac{\sum_{i=1}^{H} \lambda_i \overline{T}^2_{\text{обсл.}i}(1 + C^2_{v\,i})}{2(1-R)}, \; k = 1, ..., H, \tag{4.1}$$

де $R = \sum_{i=1}^{H} \rho_i = \sum_{i=1}^{H} \lambda_i \overline{T}_{\text{обсл.}i}$ - сумарна загрузка системи, $\overline{T}_{\text{обсл.}i} = 1/\mu_i$, μ_i - інтенсивність потоку пакетів класу i.

Середнє значення часу перебування пакету класу k в системі:

$$\overline{T}_{\text{переб.в сист.}k} = \overline{T}_{\text{очік.обсл.}} + \overline{T}_{\text{обсл.}k}. \tag{4.2}$$

Середня кількість пакетів в черзі для пакетів класу k:

$$\overline{N}_{\text{черг.}k} = \lambda_k \overline{T}_{\text{очік.обсл.}} \tag{4.3}$$

Визначимо швидкість передачі:

$$R_{\text{перед.пот.мова}} = L_{\text{пак.пот.}x} \cdot \lambda_{\text{пот.}x}; \tag{4.4}$$

$$R_{\text{перед.пот.мова}} = L_{\text{пак.пот.мова}} \cdot \lambda_{\text{пот.мова}};$$

$$R_{\text{перед.пот.відео}} = L_{\text{паке.пот.відео}} \cdot \lambda_{\text{пот.відео}};$$

$$R_{\text{перед.пот.данні}} = L_{\text{пак.пот.данні}} \cdot \lambda_{\text{пот.данні}}.$$

Визначимо математичне очікування часу між пакетами:

$$T_{\text{між.пак.пот.}x} = \frac{1}{\lambda_{\text{пот.}x}}; \tag{4.5}$$

$$T_{\text{між.пак.пот.мова}} = \frac{1}{\lambda_{\text{пот.мова}}};$$

$$T_{\text{між.пак.пот.відео}} = \frac{1}{\lambda_{\text{пот.відео}}};$$

$$T_{\text{між.пак.пот.данні}} = \frac{1}{\lambda_{\text{пот.данні}}}.$$

Визначимо середній час обслуговування пакета:

$$T_{\text{обсл.пот.}x} = \frac{L_{\text{пак.пот.}x}}{R_{\text{транспорт}}}; \tag{4.6}$$

$$T_{\text{обсл.пот.мова}} = \frac{L_{\text{пак.пот.мова}}}{R_{\text{транспорт}}};$$

$$T_{\text{обсл.пот.відео}} = \frac{L_{\text{пак.пот.відео}}}{R_{\text{транспорт}}};$$

$$T_{\text{обсл.пот.данні}} = \frac{L_{\text{пак.пот.данні}}}{R_{\text{транспорт}}}.$$

Визначимо інтенсивність обслуговування потоку пакетів:

$$\mu_{\text{пот.}x} = \frac{1}{T_{\text{обсл.пот.}x}}; \tag{4.7}$$

$$\mu_{\text{пот.мова}} = \frac{1}{T_{\text{обсл.пот.мова}}};$$

$$\mu_{\text{пот.відео}} = \frac{1}{T_{\text{обсл.пот.відео}}};$$

$$\mu_{\text{пот.данні}} = \frac{1}{T_{\text{обсл.пот.данні}}}.$$

Визначимо коефіцієнт використання:

$$\rho_{\text{пот.}x} = \frac{\lambda_{\text{пот.}x}}{\mu_{\text{пот.}x}}; \tag{4.8}$$

$$\rho_{\text{пот.мова}} = \frac{\lambda_{\text{пот.мова}}}{\mu_{\text{пот.мова}}};$$

$$\rho_{\text{пот.відео}} = \frac{\lambda_{\text{пот.відео}}}{\mu_{\text{пот.відео}}};$$

$$\rho_{\text{пот.данні}} = \frac{\lambda_{\text{пот.данні}}}{\mu_{\text{пот.данні}}};$$

$$\rho\Sigma = \rho_{\text{пот.мова}} + \rho_{\text{пот.відео}} + \rho_{\text{пот.данні}}. \quad (4.9)$$

Визначимо середній час очікування обслуговування в черзі:

$$T_{\text{очік.обсл.пот.мови\_відео\_данних}} = \frac{\rho_{\text{пот.мова}} \cdot T_{\text{обсл.пот.мова}}[1 + (C_{v\ \text{пот.мова}})^2] + \rho_{\text{пот.відео}} \cdot T_{\text{обсл.пот.відео}}\left[1 + \left(C_{v\ \text{пот.відео}}\right)^2\right] + \rho_{\text{пот.данні}} \cdot T_{\text{обсл.пот.данні}}\left[1 + \left(C_{v\ \text{пот.данні}}\right)^2\right]}{2(1 - \rho\Sigma)}; \quad (4.10)$$

Визначимо середній час перебування в системі:

$$T_{\text{переб.в сист.пот.мова}} = T_{\text{очік.обсл.пот.мови\_відео\_данних}} + T_{\text{обсл.пот.мова}};$$

$$T_{\text{переб.в сист.пот.відео}} = T_{\text{очік.обсл.пот.мови\_відео\_данних}} + T_{\text{обсл.пот.відео}};$$

$$T_{\text{переб.в сист.пот.данні}} = T_{\text{очік.обсл.пот.мови\_відео\_данних}} + T_{\text{обсл.пот.данні}}.$$

Визначимо середню кількість пакетів в черзі:

$$N_{\text{черга пот.мова}} = \lambda_{\text{пот.мова}} \cdot T_{\text{очік.обсл.пот.мови\_відео\_данних}};$$

$$N_{\text{черга пот.відео}} = \lambda_{\text{пот.відео}} \cdot T_{\text{очік.обсл.пот.мови\_відео\_данних}};$$

$$N_{\text{черга пот.данні}} = \lambda_{\text{пот.данні}} \cdot T_{\text{очік.обсл.пот.мови\_відео\_данних}}.$$

1. Визначимо середню кількість пакетів в системі:

$$N_{\text{сист.пот.}x} = N_{\text{черга пот.}x} + \rho_{\text{пот.}x}; \quad (4.11)$$

$$N_{\text{сист.пот.мова}} = N_{\text{черга пот.мова}} + \rho_{\text{пот.мова}};$$

$$N_{\text{сист.пот.відео}} = N_{\text{черга пот.відео}} + \rho_{\text{пот.відео}};$$

$$N_{\text{сист.пот.данні}} = N_{\text{черга пот.данні}} + \rho_{\text{пот.данні}};$$

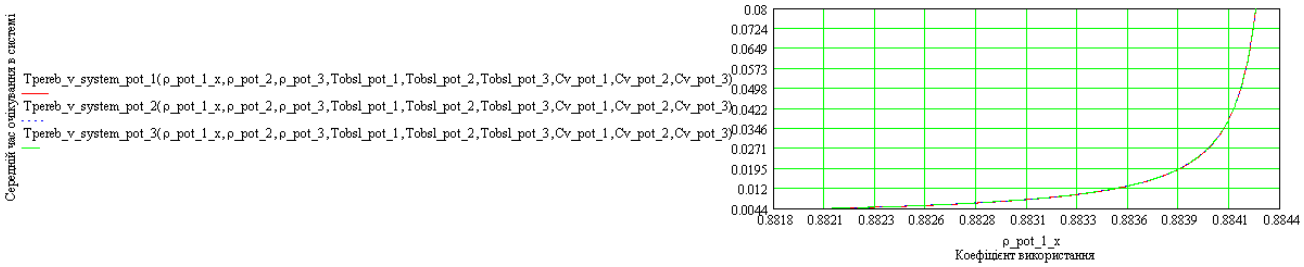

Рисунок 4.2 - Залежність середнього часу перебування в системі від коефіцієнту використання

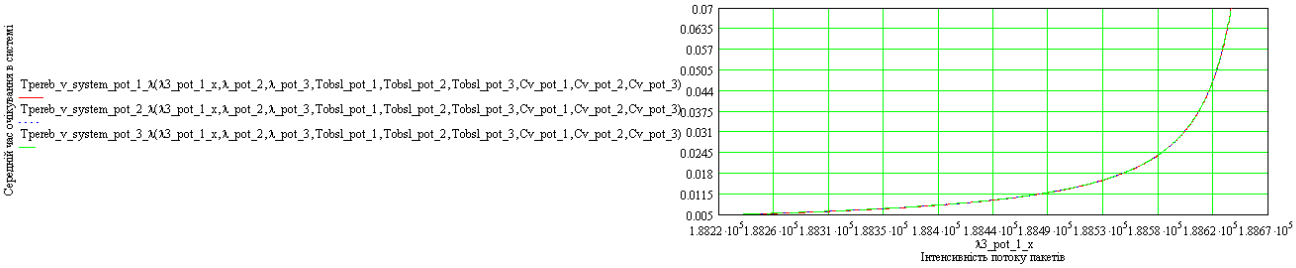

Рисунок 4.3 - Залежність середнього часу перебування в системі від інтенсивності потоку пакетів

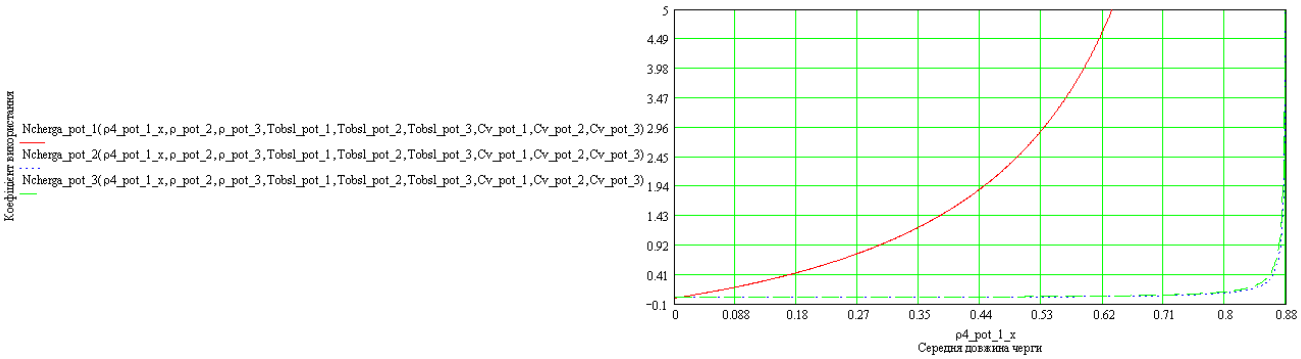

Рисунок 4.4 - Залежність середньої довжини черги від коефіцієнту використання

4.2 Розрахунок затримки в комутаторі при використанні відносних пріоритетів

Для дисципліни обслуговування з відносними пріоритетами середній час очікування заявок класу k визначається за наступною формулою:

$$\overline{T}_{\text{очік.обсл.}k} = \frac{\sum_{i=1}^{H} \lambda_i \overline{T}^2_{\text{обсл.}i}(1+C^2_{v\,i})}{2(1-R_{k-1})(1-R_k)},\ k=1,...,H, \tag{4.12}$$

де $R_{k-1} = \sum_{i=1}^{k-1} \rho_i = \sum_{i=1}^{k-1} \lambda_i \overline{T}_{\text{обсл.}i}$, $R_k = \sum_{i=1}^{k} \rho_i = \sum_{i=1}^{k} \lambda_i \overline{T}_{\text{обсл.}i}$ - загальне завантаження системи, створюване потоками пакетів з пріоритетом $k-1$ и k відповідно.

Середнє значення часу перебування пакету класу k в системі:

$$\overline{T}_{\text{переб.в сист.}k} = \overline{T}_{\text{очік.обсл.}k} + \overline{T}_{\text{обсл.}k}. \tag{4.13}$$

Середня кількість пакетів в черзі для пакетів класу k:

$$\overline{N}_{\text{черг.}k} = \lambda_k \overline{T}_{\text{очік.обсл.}k}. \tag{4.14}$$

Визначимо швидкість передачі:

$$R_{\text{перед.пот.мова}} = L_{\text{пак.пот.}x} \cdot \lambda_{\text{пот.}x}; \tag{4.15}$$

$$R_{\text{перед.пот.мова}} = L_{\text{пак.пот.мова}} \cdot \lambda_{\text{пот.мова}};$$

$$R_{\text{перед.пот.відео}} = L_{\text{паке.пот.відео}} \cdot \lambda_{\text{пот.відео}};$$

$$R_{\text{перед.пот.данні}} = L_{\text{пак.пот.данні}} \cdot \lambda_{\text{пот.данні}}.$$

Визначимо математичне очікування часу між пакетами:

$$T_{\text{між.пак.пот.}x} = \frac{1}{\lambda_{\text{пот.}x}}; \tag{4.16}$$

$$T_{\text{між.пак.пот.мова}} = \frac{1}{\lambda_{\text{пот.мова}}};$$

$$T_{\text{між.пак.пот.відео}} = \frac{1}{\lambda_{\text{пот.відео}}};$$

$$T_{\text{між.пак.пот.данні}} = \frac{1}{\lambda_{\text{пот.данні}}}.$$

Визначимо середній час обслуговування пакета:

$$T_{\text{обсл.пот.}x} = \frac{L_{\text{пак.пот.}x}}{R_{\text{транспорт}}}; \quad (4.17)$$

$$T_{\text{обсл.пот.мова}} = \frac{L_{\text{пак.пот.мова}}}{R_{\text{транспорт}}};$$

$$T_{\text{обсл.пот.відео}} = \frac{L_{\text{пак.пот.відео}}}{R_{\text{транспорт}}};$$

$$T_{\text{обсл.пот.данні}} = \frac{L_{\text{пак.пот.данні}}}{R_{\text{транспорт}}}.$$

Визначимо інтенсивність обслуговування потоку пакетів:

$$\mu_{\text{пот.}x} = \frac{1}{T_{\text{обсл.пот.}x}}; \quad (4.18)$$

$$\mu_{\text{пот.мова}} = \frac{1}{T_{\text{обсл.пот.мова}}};$$

$$\mu_{\text{пот.відео}} = \frac{1}{T_{\text{обсл.пот.відео}}};$$

$$\mu_{\text{пот.данні}} = \frac{1}{T_{\text{обсл.пот.данні}}}.$$

Визначимо коефіцієнт використання:

$$\rho_{\text{пот.}x} = \frac{\lambda_{\text{пот.}\boldsymbol{x}}}{\mu_{\text{пот.}x}}; \quad (4.19)$$

$$\rho_{\text{пот.мова}} = \frac{\lambda_{\text{пот.мова}}}{\mu_{\text{пот.мова}}};$$

$$\rho_{\text{пот.відео}} = \frac{\lambda_{\text{пот.відео}}}{\mu_{\text{пот.відео}}};$$

$$\rho_{\text{пот.данні}} = \frac{\lambda_{\text{пот.данні}}}{\mu_{\text{пот.данні}}};$$

$$\rho\Sigma = \rho_{\text{пот.мова}} + \rho_{\text{пот.відео}} + \rho_{\text{пот.данні}}. \quad (4.20)$$

Визначимо середній час очікування обслуговування в черзі:

$$T_{\text{очік.обсл.пот.мови}} = \frac{\rho_{\text{пот.мова}} \cdot T_{\text{обсл.пот.мова}}[1 + (C_{v\ \text{пот.мова}})^2] + \rho_{\text{пот.відео}} \cdot}{2(1-0)(1-\rho_{\text{пот.мова}})}$$

$$\frac{\cdot\ T_{\text{обсл.пот.відео}}\left[1 + \left(C_{v\ \text{пот.відео}}\right)^2\right] + \rho_{\text{пот.данні}} \cdot T_{\text{обсл.пот.данні}}\left[1 + \left(C_{v\ \text{пот.данні}}\right)^2\right]}{2(1-0)(1-\rho_{\text{пот.мова}})};$$

$$T_{\text{очік.обсл.пот.відео}} = \frac{\rho_{\text{пот.мова}} \cdot T_{\text{обсл.пот.мова}}[1 + (C_{v\ \text{пот.мова}})^2] + \rho_{\text{пот.відео}} \cdot}{2(1-\rho_{\text{пот.мова}})\left(1-\rho_{\text{пот.відео}}\right)}$$

$$\frac{\cdot\ T_{\text{обсл.пот.відео}}\left[1 + \left(C_{v\ \text{пот.відео}}\right)^2\right] + \rho_{\text{пот.данні}} \cdot T_{\text{обсл.пот.данні}}\left[1 + \left(C_{v\ \text{пот.данні}}\right)^2\right]}{2(1-\rho_{\text{пот.мова}})\left(1-\rho_{\text{пот.відео}}\right)};$$

$$T_{\text{очік.обсл.пот.данні}} = \frac{\rho_{\text{пот.мова}} \cdot T_{\text{обсл.пот.мова}}[1 + (C_{v\ \text{пот.мова}})^2] + \rho_{\text{пот.відео}} \cdot}{2(1-0)\left(1-\rho_{\text{пот.данні}}\right)}$$

$$\frac{\cdot\ T_{\text{обсл.пот.відео}}\left[1 + \left(C_{v\ \text{пот.відео}}\right)^2\right] + \rho_{\text{пот.данні}} \cdot T_{\text{обсл.пот.данні}}\left[1 + \left(C_{v\ \text{пот.данні}}\right)^2\right]}{2\left[1-\left(\rho_{\text{пот.мова}} + \rho_{\text{пот.відео}}\right)\right]\left(1-\rho_{\text{пот.данні}}\right)};$$

Визначимо середній час перебування в системі:

$$T_{\text{переб.в сист.пот.}x} = T_{\text{очік.обсл.пот.}x} + T_{\text{обсл.пот.}x}; \quad (4.21)$$

$$T_{\text{переб.в сист.пот.мова}} = T_{\text{очік.обсл.пот.мови}} + T_{\text{обсл.пот.мова}};$$

$$T_{\text{переб.в сист.пот.відео}} = T_{\text{очік.обсл.пот.відео}} + T_{\text{обсл.пот.відео}};$$

$$T_{\text{переб.в сист.пот.данні}} = T_{\text{очік.обсл.пот.данних}} + T_{\text{обсл.пот.данні}};$$

Визначимо середню кількість пакетів в черзі:

$$N_{\text{черга пот.}x} = \lambda_{\text{пот.}\boldsymbol{x}} \cdot T_{\text{очік.обсл.пот.}x}; \quad (4.22)$$

$$N_{\text{черга пот.мова}} = \lambda_{\text{пот.мова}} \cdot T_{\text{очік.обсл.пот.мови}};$$

$$N_{\text{черга пот.відео}} = \lambda_{\text{пот.відео}} \cdot T_{\text{очік.обсл.пот.відео}};$$

$$N_{\text{черга пот.данні}} = \lambda_{\text{пот.данні}} \cdot T_{\text{очік.обсл.пот.данних}}.$$

Визначимо середню кількість пакетів в системі:

$$N_{\text{сист.пот.}x} = N_{\text{черга пот.}x} + \rho_{\text{пот.}x}; \quad (4.23)$$

$$N_{\text{сист.пот.мова}} = N_{\text{черга пот.мова}} + \rho_{\text{пот.мова}};$$

$$N_{\text{сист.пот.відео}} = N_{\text{черга пот.відео}} + \rho_{\text{пот.відео}};$$

$$N_{\text{сист.пот.данні}} = N_{\text{черга пот.данні}} + \rho_{\text{пот.данні}};$$

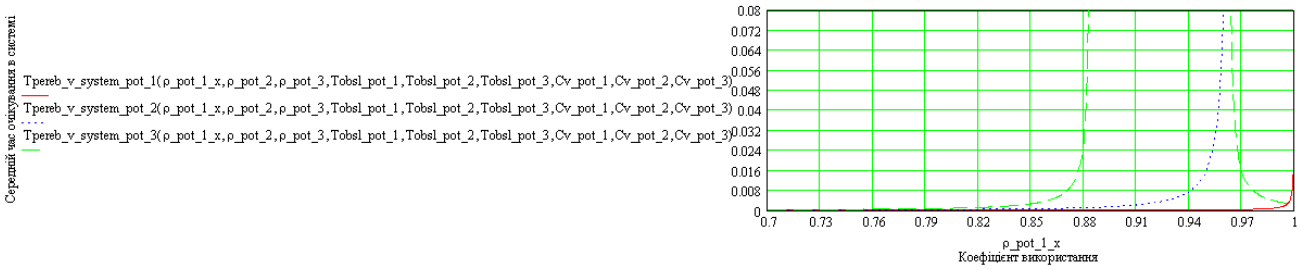

Рисунок 4.5 - Залежність середнього часу перебування в системі від коефіцієнту використання

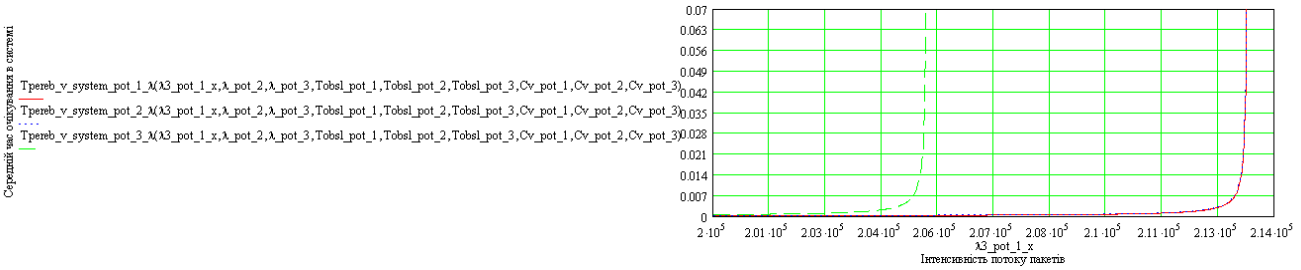

Рисунок 4.6 - Залежність середнього часу перебування в системі від інтенсивності потоку пакетів

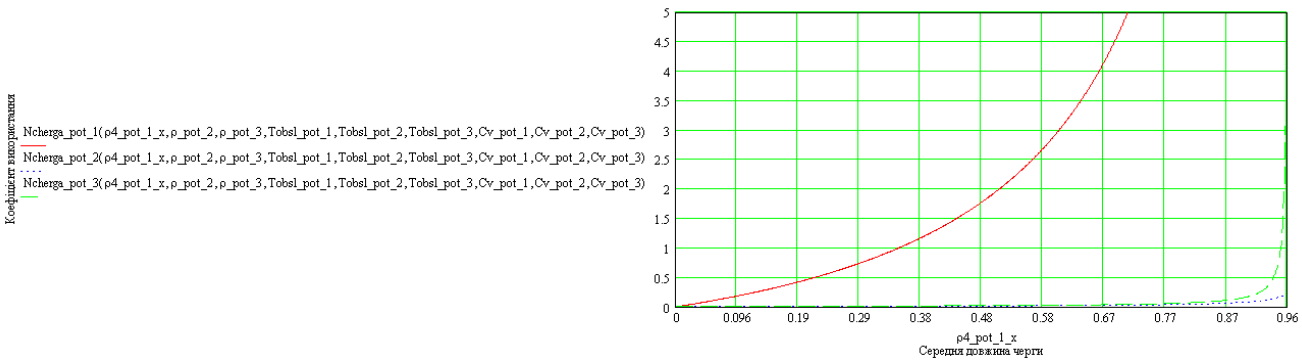

Рисунок 4.7 - Залежність середньої довжини черги від коефіцієнту використання

Використання відносних пріоритетів дає перевагу перед безпріоритетною дисципліною обслуговування в наданні мовних послуг для користувачів.

РОЗДІЛ 5

ВПРОВАДЖЕННЯ ФАЕРВОЛУ НОВОГО ПОКОЛІННЯ NGFW В МЕРЕЖУ ПІДПРИЄМСТВА

CheckPoint - це провідний постачальник NGFW рішень, який відзначається широким спектром функціональності. Вони пропонують рішення для захисту від атак з використанням інноваційних технологій, таких як машинне навчання та штучний інтелект. Checkpoint також володіє масштабуванням та ефективною продуктивністю, що робить його популярним серед великих корпорацій.

FortiNet також пропонує високоякісні NGFW рішення, які володіють потужністю і надійністю. Вони відомі своїми мультитенантними функціями, що дозволяють керувати безпекою мережі в режимі реального часу. FortiNet також має широкий спектр інтегрованих захисних служб, таких як захист від вторгнень, антивірусні програми та захист електронної пошти.

PaloAlto має репутацію міцного постачальника NGFW рішень, що пропонує широкий спектр функцій для захисту мережі. Вони володіють передовими технологіями, такими як deep packet inspection, що дозволяє виявляти та блокувати небезпечний трафік. PaloAlto також славиться своїми інтелектуальними алгоритмами, які здатні прогнозувати та попереджати про нові загрози.

З урахуванням всіх цих факторів, включаючи широкий спектр функціональності, продуктивності та надійності, CheckPoint було вибрано як провідний постачальник NGFW.

Одним з варіантів використання NGFW є його використання як основного засобу мережевого захисту в корпоративній мережі. Застосовуючи NGFW як пристрій периметру, всі вхідні та вихідні з'єднання будуть проходити через нього, що дозволить контролювати трафік, використовувати правила фільтрації та інші функціональні можливості пристрою. Інший варіант використання NGFW - це використання його як вузла внутрішньої

мережі. Таке розташування пристрою дозволяє контролювати і аналізувати трафік в мережі, що дозволяє виявити та запобігти внутрішнім загрозам. Наступний варіант використання NGFW - це комбіноване використання з іншими засобами захисту мережі. Наприклад, можна використовувати NGFW разом з системою виявлення вторгнень (IDS) для забезпечення комплексного захисту мережі.

Крім того, NGFW може використовуватися як засіб контролю доступу до ресурсів мережі. Це можливо завдяки можливості встановлення докладних правил фаєрволу та фільтрації трафіку.

Загалом, вибір варіанту використання NGFW залежить від потреб і вимог конкретної мережі. Слід враховувати особливості мережевої інфраструктури, розмір мережі, види трафіку та ризики, що виникають.

Пропонується такий варіант.

1. Віртуальна машина Check Point R81.10, яка виконує роль NGFW. Ця машина відповідає за аналіз мережевого трафіку, виявлення і захист від загроз, таких як віруси, шкідливі програми, атаки по переповненню буфера, DDoS атаки, тощо. Вона також включає механізми контролю доступу, такі як правила брандмауера, інспекція SSL-трафіку, VPN-з'єднання, IPSec, тощо.

2. Фізичний пристрій мережевого периметру, який включає маршрутизатори, комутатори, брандмауери. Цей пристрій забезпечує мережеву інфраструктуру, розподіляє трафік між різними мережевими сегментами, і контролює доступ до різних ресурсів мережі.

3. Сервери і додаткові пристрої у мережі, які мають доступ до Інтернету через NGFW. Ці пристрої можуть бути серверами файлів, поштовими серверами, відеоконференційними системами, тощо. Вони також можуть включати брандмауери та інші пристрої з додатковою функціональністю.

4. Центр управління і моніторингу. У центрі управління адміністратори налаштовують політики безпеки, контролюють інциденти, аналізують звіти про перевірку безпеки, і профілюють мережевий трафік. Цей центр також включає різноманітні інструменти для моніторингу.

Ця система забезпечить комплексний захист мережі шляхом поєднання мережевих ідентифікаційних технологій з функціями брандмауера та IPS/IDS. Вона забезпечить аналіз, фільтрацію, і захист від різноманітних загроз в реальному часі, забезпечуючи високу безпеку та надійність мережевого периметру.

ВИСНОВКИ

1. Проведено аналіз принципів побудови комутованих комп’ютерних мереж.

2. Розглянуто основні принципи роботи протоколу Spanning Tree Protocol (IEEE 802.1d).

3. Висвітлені основні принципи організації віртуальних локальних мережі VLAN.

4. Проведено аналіз існуючого обладнання.

5. Розроблено схеми мереж кожної кімнати підприємства, як складові загальної схеми комп’ютерної мережі підприємства.

6. Проведено розподіл IP - адрес комп’ютерної мережі підприємства.

7. Розраховано інтенсивності потоків пакетів з мовою, відео та даними.

8. Надані пропозиції з впровадження в мережу підприємства фаєрволу нового покоління NGFW.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні вказівки до практичних занять з дисципліни «Інтегральні цифрові мережі зв'язку» / Жученко О.С., Лисечко В.П. − Донецьк: ДонІЗТ, 2011.– 44 с.

2. Методичні вказівки до курсового, дипломного проектування та практичних занять з дисципліни «Телекомунікаційні та інформаційні мережі» на тему «Проектування регіональної територіально-розподіленої телекомунікаційної мережі» / Приходько С.І., Жученко О.С., Лисечко В.П., Безверха Г.С. − Харків: УкрДАЗТ, 2012. – 172 с.

3. Методичні вказівки до практичних занять з дисциплін «Телекомунікаційні та інформаційні мережі», «Інтегральні цифрові мережі зв'язку» (розподіл IP адрес) / Приходько С.І., Жученко О.С., Трубчанінова К.А., Єременко С.С. − Харків: УкрДАЗТ, 2012. – 42 с.

4. Методичні вказівки до практичних занять та самостійної роботи з дисциплін «Системи комутації в електрозв'язку», «Автоматичний телефонний зв'язок» з тем «Основи теорії розподілу інформації», «Цифрова комутація» / Приходько С.І., Жученко О.С., Волков О.С., Штомпель М.А. − Харків: УкрДАЗТ, 2013. – 110 с.

5. Методичні вказівки до курсового, дипломного проектування та практичних занять з дисциплін «Системи передачі даних», «Передача даних у цифрових мережах» / Трубчанінова К.А., Жученко О.С. − Харків: УкрДАЗТ, 2014. – 50 с.

6. Методичні вказівки до практичних занять з дисципліни «Багатоканальні системи передачі інформації» та «Системи передачі в електрозв'язку» / Трубчанінова К.А., Жученко О.С. − Харків: УкрДАЗТ, 2016. – 50 с.

7. Методичні вказівки до самостійної роботи, практичних занять та контрольних заходів на тему «Імітаційне моделювання сегментів мереж на основі технології Ethernet та протоколу IP» з дисциплін «Телекомунікаційні та інформаційні мережі», «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Інтегральні цифрові мережі зв'язку» / Приходько С. І., Жученко О.С., Штомпель М.А., Індик С. В. − Харків: УкрДУЗТ, 2017. – 34 с.

8. Протокол STP: навчальний посібник / Панченко С. В., Приходько С. І., Жученко О.С., Штомпель М.А. − Харків: УкрДУЗТ, 2017. – 72 с.

9. Динамічна маршрутизація в IP-мережах. Протокол OSPF: навчальний посібник / Панченко С. В., Приходько С. І., Жученко О.С., Штомпель М.А. − Харків: УкрДУЗТ, 2017. – 209 с.

10. Протокол IP. Статична маршрутизація в IP-мережах навчальний посібник / Панченко С. В., Приходько С. І., Жученко О.С., Штомпель М.А. − Харків: УкрДУЗТ, 2017. – 136 с.

11. Методичні вказівки до лабораторних, практичних занять і самостійної роботи на тему «Віртуальні локальні мережі VLAN» з дисциплін «Телекомунікаційні та інформаційні мережі», «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Мережеві технології», «Інтегральні цифрові мережі зв'язку» / Приходько С. І., Жученко О.С., Штомпель М.А., Сколота С. В. − Харків: УкрДУЗТ, 2018. – 41 с.

12. Методичні вказівки до лабораторних, практичних занять і самостійної роботи на тему «Комутатор третього рівня» з дисциплін «Телекомунікаційні та інформаційні мережі», «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Мережеві технології», «Інтегральні цифрові мережі зв'язку» / Приходько С.І., Жученко О.С., Штомпель М.А., Свергунова Ю.О. − Харків: УкрДУЗТ, 2018. – 33 с.

13. Технологія Ethernet : лабораторний практикум / М.О. Білова, С. П. Євсеєв, О.С. Жученко, І.С. Іванченко, О.В. Шматко. – Харків: НТУ «ХПІ», 2019. – 194 с.

14. Демида Б.А. Основи адміністрування LAN у середовищі MS Windows : навч. посіб. / Б.А. Демида, К.М. Обельовська, В.С. Яковина. − Львів: Видавництво Львівської політехніки, 2013. — 488 с.

15. Заміховська, О.Л. Комп'ютерні мережі та телекомунікації : навч. посіб. / О.Л. Заміховська. - Івано-Франківськ : ІФНТУНГ, 2013. - 177 с.

16. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас, С.І. Шматков / За редакцією Ю. І. Лосева. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 248 с.

17. Мультисервісні мережі / В.І. Басов, Г.І. Загарій, С.І. Приходько, Ю.М. Терещенко, А.А. Чікін., за заг. ред. Ю.М.Терещенка. − ЧП «Новое слово», 2009. – 198 с.

18. Телекомунікаційні системи та мережі : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. – 384 с.

19. Телекомунікаційні та інформаційні мережі: підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.

20. Телекомунікаційні та інформаційні мережі. Типові завдання : методичні вказівки до практичних занять і самостійної роботи з дисциплін «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Комп'ютерні мережі» / Індик С.В., Лисечко В. П., Жученко О.С. − Методичні вказівки до практичних занять, самостійної роботи та контрольних заходів на тему «Розрахунок характеристик волоконно-оптичних напрямних систем телекомунікацій» з дисциплін «Напрямні системи телекомунікацій», «Напрямні системи електричного та оптичного зв'язку», «Основи теорії напрямних систем», «Кабельні лінії та системи», «Лінії зв'язку та автоматики» / Штомпель М.А., Жученко О.С., Індик С.В. − Харків: УкрДУЗТ, 2019. – 38 с.

21. Телекомунікаційні та інформаційні мережі. Типові завдання: методичні вказівки до практичних занять і самостійної роботи з дисциплін «Телекомунікаційні та інформаційні мережі на залізничному транспорті», «Комп'ютерні мережі». Частина 1 / укладачі : С. В. Індик, О. С. Жученко, В. П. Лисечко ; кафедра транспортного зв'язку. - Харків : УкрДУЗТ, 2022. - 44 с.

22. NGFW – у чому переваги файрволів наступного покоління? – Режим доступу до ресурсу: https://ko.com.ua/ngfw.

23. Check Point R81.10 – Режим доступу до ресурсу: https://supportcenter.us.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=115155

ДОДАТОК А

IMPLEMENTATION OF A NEW GENERATION FIREWALL NGFW IN THE ENTERPRISE NETWORK

CheckPoint is a leading provider of NGFW solutions, noted for a wide range of functionality. They offer solutions to protect against attacks using innovative technologies such as machine learning and artificial intelligence. Checkpoint also has scalability and efficient performance, making it popular among large corporations.

FortiNet also offers high-quality NGFW solutions that have power and reliability. They are known for their multi-tenant features that allow real-time network security management. FortiNet also has a wide range of integrated security services, such as intrusion prevention, anti-virus programs and email protection.

PaloAlto has a reputation as a solid NGFW solution provider that offers a wide range of features for network security. They have advanced technologies such as deep packet inspection, which allows detecting and blocking dangerous traffic. PaloAlto is also famous for its intelligent algorithms that are able to predict and warn about new threats.

With all these factors in mind, including a wide range of functionality, performance and reliability, CheckPoint has been selected as a leading NGFW provider.

One of the uses of NGFW is to use it as the primary means of network security in a corporate network. By implementing an NGFW as a perimeter device, all inbound and outbound connections will pass through it, allowing for traffic control, filtering rules, and other device functionality. Another use case for an NGFW is to use it as an internal network node. This arrangement of the device allows monitoring and analysis of network traffic, which allows detection and prevention of internal threats. The next use case for NGFW is combined use with other network security tools. For example, you can use an NGFW in conjunction with an intrusion detection system (IDS) to provide comprehensive network protection.

In addition, NGFW can be used as a means of controlling access to network resources. This is possible thanks to the ability to set detailed firewall rules and traffic filtering.

In general, the choice of NGFW usage depends on the needs and requirements of the particular network. The specifics of the network infrastructure, network size, traffic types and emerging risks should be taken into account.

This option is offered.

1. Check Point R81.10 virtual machine acting as NGFW. This machine is responsible for analyzing network traffic, detecting and protecting against threats such as viruses, malware, buffer overflow attacks, DDoS attacks, etc. It also includes access control mechanisms such as firewall rules, SSL traffic inspection, VPN connections, IPSec, etc.

2. The physical device of the network perimeter, which includes routers, switches, firewalls. This device provides network infrastructure, distributes traffic between different network segments, and controls access to different network resources.

3. Servers and additional devices in the network that have access to the Internet through NGFW. These devices can be file servers, mail servers, video conferencing systems, etc. They may also include firewalls and other devices with additional functionality.

4. Management and monitoring center. In the management center, administrators configure security policies, monitor incidents, analyze security audit reports, and profile network traffic. This hub also includes a variety of monitoring and logging tools.

This system will provide comprehensive network protection by combining network identity technologies with firewall and IPS/IDS functions. It will provide analysis, filtering, and protection against various threats in real time, ensuring high security and reliability of the network perimeter.

ДОДАТОК Б

ПУБЛІКАЦІЇ ТА АПРОБАЦІЇ

УДК 621.313.26
О.С. Жученко, *к.т.н., доцент,*
Р.М. Сталинський, *магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

РОЗРОБКА ПРОЄКТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З СИСТЕМОЮ ЗАХИСТУ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Комунікація є смисловим аспектом соціальної взаємодії, однією із найбільших загальних характеристик будь-якої діяльності. Комунікацію можна визначити як форму зв'язку, як один із проявів обміну інформацією між живими істотами, у процесі їх безпосереднього спілкування або за допомогою технічних засобів. Дослідження показують, що працівники, зайняті в проектній діяльності, 50-80% усього часу витрачають на комунікації. Це здається дуже багато, але стає зрозумілим, якщо врахувати, що працівник займається цим постійно, щоб реалізувати свої ролі у міжособистих відносинах, інформаційному обміні та процесах прийняття рішень. Саме тому, важливо правильно організувати обмін інформації на підприємстві, найпростішим і надійнішим способом реалізації цього завдання є організація комп'ютерної мережі на підприємстві.

Найбільш значною перевагою яка забезпечило комп'ютерним мережам їх поширеність є можливість віртуальної роботи з інформацією. При цьому сама інформація може зберігатися в одній або різних точках мережі, а доступ до неї може здійснюватися з будь-якого робочого місця співробітника. Також, позитивними аспектами використання комп'ютерної мережі на підприємстві є можливість спільного використання апаратних та програмних ресурсів, що суттєво зменшує витрати на забезпечення процесу виробництва.

Важливим аспектом взаємодії всередині комп'ютерної мережі є забезпечення інформаційної безпеки. Основні проблеми захисту інформації при роботі в комп'ютерних мережах можна умовно поділити на три типи: перехоплення, модифікація інформації та підміна авторства. Рішення проблем захисту електронної інформації базується на використанні наступних методів захисту інформації, таких як: технічний, інженерний, організаційний та криптографічний методи.

Розглядаючи питання створення та експлуатації комп'ютерних мереж слід мати на увазі наступні визначення та поняття:

• реальна система (real system) – сукупність одної або кількох ЕОМ, програмного забезпечення, периферійного обладнання, терміналів та персоналу, яка повністю автономна й отримує та передає дані;

• реальна остаточна система (real end system) – реальна система, яка виконує в мережі функції станції даних, тобто є джерелом або приймачем даних;

• відкрита система (open system) – система, яка побудована і функціонує з дотриманням вимог міжнародних стандартів;

• комунікаційна система (communication system) – реальна відкрита система, яка забезпечує обмін даними між абонентськими системами у відкритій інформаційній системі;

• абонентська система (user system) – реальна відкрита система, яка є постачальником або споживачем ресурсів мережі, забезпечує доступ до них користувачів і керує взаємозв'язком відкритих систем;

• прикладний процес (application process) – процес у реальній остаточній системі, який обробляє дані для визначених потреб користувачів;

• середовище передавання даних (transmission medium) – сукупність ліній передавання даних та, можливо, іншого обладнання, яке забезпечує передавання даних між абонентськими системами;

• середовище зв'язку відкритих систем (open system interchange environment) – сукупність функцій, які дають можливість реальним відкритим системам обмінюватись даними відповідно до міжнародних стандартів.

ЛІТЕРАТУРА:

1. *Комп'ютерні мережі [Електронний ресурс]. – Режим доступу: MirZnanii.com/a/120994/kompyutern-merezh*

2. *Основні характеристики сучасних комп'ютерних мереж [Електронний ресурс]. – Режим доступу: informatika.udpu.edu.ua/?page_id=2797*

3. *Організація локальної обчислювальної мережі агентства нерухомості [Електронний ресурс]. – Режим доступу: MirZnanii.com/a/120889/organzatsya-lokalno-obchisl...gentstva-nerukhomost*

DESING OF A CORPORATE COMPUTER NETWORK WITH INFORMATION PROTECTION SYSTEM

***O. Zhuchenko**, Ph.D., Associate professor,*
***R. Stalynskyi**, Master's Student*
National University «Yuri Kondratyuk Poltava Polytechnic»

ДОДАТОК В

СЛАЙДИ