ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему Метод максимізації пропускної здатності мережі заданої топології

ДРМТР 2020017.00.00

Виконав: студент 2 курсу, група ТРм-19-2 _____ О.О. Польнов
підпис Ініціали, прізвище

Керівник: к-т техн. наук, доц. _____ К.Л. Горященко
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ С.К. Підченко
підпис Ініціали, прізвище

10 12 2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань 17 – *Електроніка та телекомунікації*
Спеціальність 172 – *Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою ТМІТ
С.К. Підченко
«*03*» *вересня* 2020р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Польнов Олексій Олегович

1 Тема роботи: *Метод максимізації пропускної здатності мережі заданої топології*
керівник роботи Горященко К.Л, к.т.н, доцент.
Затверджено наказом по університету від «1» вересня 2020р. № 118
2 Строк подання студентом роботи на кафедру: 05.12.2020р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи – дослідження сучасних програмних засобів моделювання телекомунікаційних мереж при сталому розміщенні вузлів в просторі та можливості визначення варіантів підключення між собою на прикладі бездротових мереж
Об'єкт дослідження – засоби моделювання телекомунікаційних мереж
Предмет дослідження – методи моделювання передачі інформації в мережах при взаємодії з бездротовими пристроями стандарту ZigBee
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
1 Постановка проблематики проектування структури мережі; 2 Загальні принципи формування мережевої інфраструктури; 3 Моделі вузлів мережевих пристроїв; 4 Проектування та моделювання роботи обчислювальних мереж

Завдання отримав
Науковий керівник

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз літературних		
	джерел	5.09. 20-14.09. 20	*виконано*
2	Написання 1 розділу	5.09. 20-14.09. 20	*виконано*
3	Визначення проблеми		
	дослідження	5.09. 20-14.09. 20	*виконано*
4	Написання 2 розділу	5.09. 20-14.09. 20	*виконано*
5	Розробка моделі	5.09. 20-14.09. 20	*виконано*
6	Написання 3 розділу	5.09. 20-14.09. 20	*виконано*
7	Теоретичне та практичне	.	
	моделювання	1.11.20-14.11.20	*виконано*
8	Написання 4 розділу	1.11.20-14.11.20	*виконано*
9	Оформлення роботи	20.11.20-30.11.20	*виконано*
10	Оформлення презентації	03.12.20	

Студент _____ Попилов О.О.
Підпис Ініціали, прізвище

Керівник роботи _____ _____
Підпис Ініціали, прізвище

ЗМІСТ

Перелік умовних скорочень

VLAN (Virtual Local Area Network) - віртуальна локальна мережа.

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного налаштування вузла.

EIGRP (Enhanced Interior Gateway Routing Protocol) - протокол динамічної маршрутизації.

NAT (Network Address Translation) — перетворення мережевих.

STP (Spanning Tree Protocol) - протокол остовного дерева.

VPN (Virtual Private Network) -виртуальная приватна мережа.

IPsec (скорочення від IP Security) - набір протоколів для забезпечення захисту даних.

GRE (Generic Routing Encapsulation) - загальна інкапсуляція маршрутів.

ВСТУП

В епоху до комерційного використання мереж, запити та пріоритети щодо побудови мереж були зовсім іншими. Мережа будувалась з обмеженою кількістю вузлів. Учасники мережі були також визначені, як і їх можливості.

Розвиток систем телекомунікацій, поява послуг з передачі відео, аудіо призвело до появи мережі нового покоління – NGN-мережі. Одночасно з цим, обсяги мережі, її учасники стрімко зросли. Сучасна мережа представляє собою динамічно формовану мережу.

Мережа Internet існує з 1969 року. В її основі лежить набір протоколів передачі даних TCP / IP. В якості основного протоколу рівня мережі використовується протокол IP, який спочатку планувався для передачі пакетів в мережах, що застосовувались для поєднання локальних мереж. Тому протокол IP був застосований до мереж зі складною топологією. Всі дані, що передаються в мережі поділяються на пакети фіксованої довжини. До кожної такої частини додається заголовок, що містить адресу одержувача, відправника та іншу службову інформацію. Такий IP - пакет є одиницею, з якої працюють маршрутизатори (router) - пристрої мережі, що відповідають за транспортування даних.

Зв’язок роботи з науковими програмами, **планами**, **темами.**

Магістерська робота виконана відповідно до поточних та перспективних планів наукової роботи Хмельницького національного університету, кафедри телекомунікацій, медійних та інтелектуальних технологій за тематикою створення нових підходів щодо передачі інформації в телекомунікаційних системах із застосуванням інтелектуальних систем та технологій.

Мета роботи – дослідження сучасних програмних засобів моделювання телекомунікаційних мереж при сталому розміщенні вузлів в просторі та можливості визначення варіантів підключення між собою на прикладі бездротових мереж.

Для досягнення поставленої мети в роботі необхідно вирішити **наступні завдання**:

1. 1. Виконати аналіз проблематики створення телекомунікаційної мережі різної складності. А особливо проаналізувати взаємодію телекомунікаційних мереж, що складаються зі стаціонарних елементів та мобільних пристроїв.

2. Проаналізувати існуючі принципи створення топології мережі. Для цього розглянути програмне забезпечення з емуляції роботи мережевого устаткування.

3. Провести дослідження роботи мережі у віртуальному середовищі програми емулятора мережі з використанням моделі бездротового пристрою для визначення конфігурацій з найкращими параметрами роботи.

Об'єкт дослідження – засоби моделювання телекомунікаційних мереж.

Предмет дослідження – методи моделювання передачі інформації в мережах при взаємодії з бездротовими пристроями стандарту ZigBee.

Науково-практична новизна роботи. Розглянуто існуючі безкоштовні та умовно-безкоштовні програмні засоби, що дозволяють виконувати задачі моделювання схеми, зв’язків та визначення фізичних параметрів телекомунікаційних мереж.

Публікації. На основі матеріалів магістерської роботи опублікована стаття у фаховому виданні ХНУ.

Структура та об'єм магістерської роботи

Робота складається з 4-х розділів, загальним обсягом 90 сторінок. В роботі використано 18 посилань на літературні джерела.

В роботі 41 рисунок та 4 таблиць.

РОЗДІЛ 1 ПОСТАНОВКА ПРОБЛЕМАТИКИ ПРОЕКТУВАННЯ СТРУКТУРИ МЕРЕЖІ

1.1 Задача проектування мережі

У наш час мільйони людей використовують Internet в повсякденному житті і це число постійно зростає. Сучасні технології дозволяють використовувати мережі зв'язку не тільки для звичайного перегляду web-сторінок і відправки електронних листів, але і для передачі голосу і відео. Трафік пакетних даних досяг таких обсягів, що для телекомунікаційних компаній будь-якого типу він став помітним джерелом доходів, тому мережі IP експлуатуються все активніше. З метою збільшення прибутку оператори намагаються підвищити ефективність використання мережі, а значить, методи оптимізації мереж IP набувають все більшої значущості. Максимальний комерційний ефект від мережі IP не може бути отриманий без раціонального використання всіх мережевих ресурсів - в першу чергу маршрутизаторів і каналів зв'язку. Функціонування пакетної мережі можна вважати ефективним тільки тоді, коли кожен ресурс завантажений, але водночас не перевантажений.

Кілька років тому послуги телебачення і телефону надавалися користувачам по різних мережах доступу. В кінці 90-х - початку 2000 року в телекомунікації почався новий етап розвитку індустрії, а саме конвергенція трафіку. Тепер по одним і тим же мереж доступу користувачі можуть отримувати послуги і телебачення, телефонії, доступу в Internet та ін. види сервісів. Однак методи маршрутизації, які застосовувалися для трафіку єдиного типу сервісу, стали неефективними для трафіку пакетів різних сервісів.

У зв'язку з цим виникла потреба створення систем маршрутизації, які при побудові шляху враховували б не тільки технічні характеристики обладнання і каналів, а й його вартість.

1.2 Історія розвитку IP мереж

До середини 1990-х років мережею Internet користувалися в основному науково-освітнє співтовариство і урядові структури в США.

Різке зростання Internet стався після створення World Wide Web (WWW) в 1990 році. Число хостів, підключених до мережі Internet зростає експоненційно, а зараз до хостів відносяться не тільки персональні комп'ютери, а також автономні процесорні системи. Хостом в мережі Internet називаються комп'ютер, що працюють з програмним забезпеченням, що підтримує протоколи TCP / IP і надають користувачам які-небудь мережні послуги.

Разом з числом користувачів Internet удосконалювалося та мережеве обладнання - маршрутизатори і лінії зв'язку. Пріоритетними завданнями були збільшення ширини пропускання каналів зв'язку і зменшення загасання сигналу на одиницю довжини каналу. В наші дні волоконно-оптичні лінії зв'язку мають найкращими характеристиками.

Також з вдосконаленням ресурсної складової Internet, розширювався і спектр послуг, пропонованих телекомунікаційними компаніями. З'явилися такі ресурсомісткі сервіси, як IP телефонія, відеоконференція і ін. Всі вони використовують протокол IP для передачі даних, але кожна послуга має свій ряд вимог до обробки IP пакетів.

Незмінним залишався і залишається протокол передачі даних, завданням якого є надійна передача даних в мережах з різною топологією. Від технології IP насамперед очікували, що вона дозволить створювати мережі довільно великого розміру, інтегрувати різні мережеві технології і надасть набір різноманітних сервісів.

1.3 Проблеми надання послуг необхідної якості

Для якісного надання будь-якої послуги оператори зв'язку повинні мати ресурсну базу (маршрутизатори, канали зв'язку та інше обладнання),

технічні характеристики які задовольняють всім вимогам цієї послуги. При цьому різні типи сервісів мають різні вимоги до технічних характеристик мережі зв’язку. Так, для простої передачі даних (пересилання електронної пошти або файлів) критична тільки ширина пропускання каналів зв’язку, тоді як для IP-телефонії найбільшим пріоритетом є мінімальний час затримки обробки IP пакетів на шляху проходження до адресата.

На різних ділянках мережі може перебувати різне обладнання зі своїм набором характеристик. Для деякого сервісу не всі пристрої мережі можуть задовольняти вимогам до ресурсів. Тому такі пристрої не повинні входити в маршрут прямування IP пакетів цього сервісу. Таким чином, не всі послуги можуть надаватися по деяких дільницях мережі.

У даній роботі вирішується завдання побудови збалансовано завантаженої мережі зв’язку. Для цього буде розроблений метод вибору шляхів проходження IP трафіку різних сервісів через мережу. Метод буде враховувати як вимоги сервісу до ресурсів мережі і завантаженість мережевого обладнання, так і вартість проходження трафіку по маршруту.

Подібного роду завдання виникають при підключенні нової послуги, при прийнятті рішення про розширення мережі, про її модернізації.

1.4 Стандарт IEEE 802.15.4 для безпровідних пристроїв

Стандарт 802.15.4 призначений для організації двох нижніх рівнів еталонної моделі OSI у безпровідній сенсорній мережі - фізичний (PHY) і канальний (підрівень MAC). Ці шари пропонують послуги вищим шарам (рис. 1.1). Інтерфейси між шарами служать для визначення логічних зв'язків. Фізичний рівень надає дві послуги: фізичне обслуговування даних і фізичне обслуговування управління. Завдання рівня - активація/дезактивація радіоприймача, вибір каналу, визначення рівня енергії (energy detection), передача і отримання пакетів через фізичне середовище. MAC рівень надає наступні послуги: обслуговування даних і обслуговування управління на канальному рівні. Завдання рівня - сигнальне управління, доступ до каналу,

управління GTS, затвердження пакетів, підтвердження доставки пакетів, з'єднання (асоціація) і роз'єднання (дизасоціація) з пристроями, крім того забезпечення механізму безпеки.

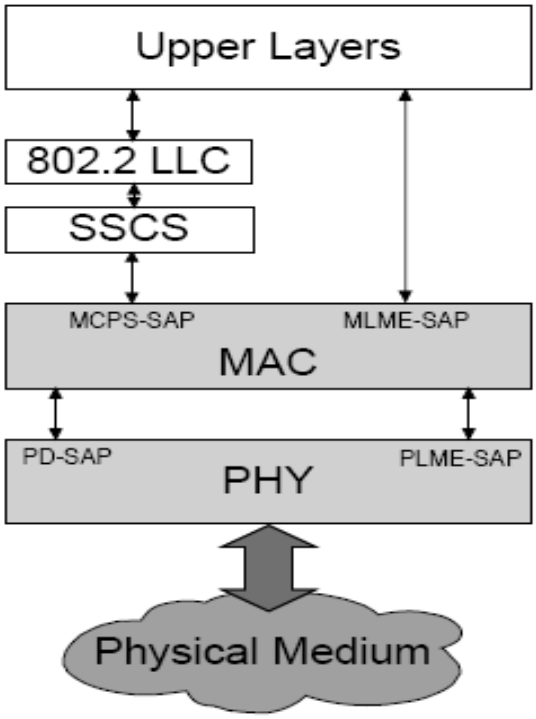


Рисунок 1.1 – Архітектура рівнів

Стандарт визначає протокол і взаємозв'язок пристроїв в наступних трьох радіодіапазонах, що не ліцензуються :

- 868,0 – 868,6 Мгц (Європа, один канал);
- 902 – 928 Мгц (Північна Америка, всього 10 каналів, крок центральних частот - 2 Мгц, сама нижня з них - 906 Мгц);
- 2450 Мгц (решта світу, всього 16 каналів, крок центральних частот - 5 Мгц, сама нижня з них - 2405 Мгц).

Мережа стандарту IEEE 802.15.4 містить два типи пристроїв — так звані напівфункціональні (FFD) і пристрої з зменшеною функціональністю (RFD). Їх основна відмінність: FFD можуть встановлювати з'єднання з будь-якими пристроями, RFD — тільки з FFD. У кожній підмережі (PAN) має бути пристрій — координатор PAN. Його функції може виконувати тільки FFD.

Мережа, що складається з одного FFD і декількох RFD, утворює топологію типу «зірка». Якщо в мережі FFD декілька, топологія може бути складнішою типу однорангової мережі (мережі рівноправних пристроїв, peer — to — peer) «кожен з кожним» (рис. 1.2) або об'єднання декількох зіркоподібних кластерів.

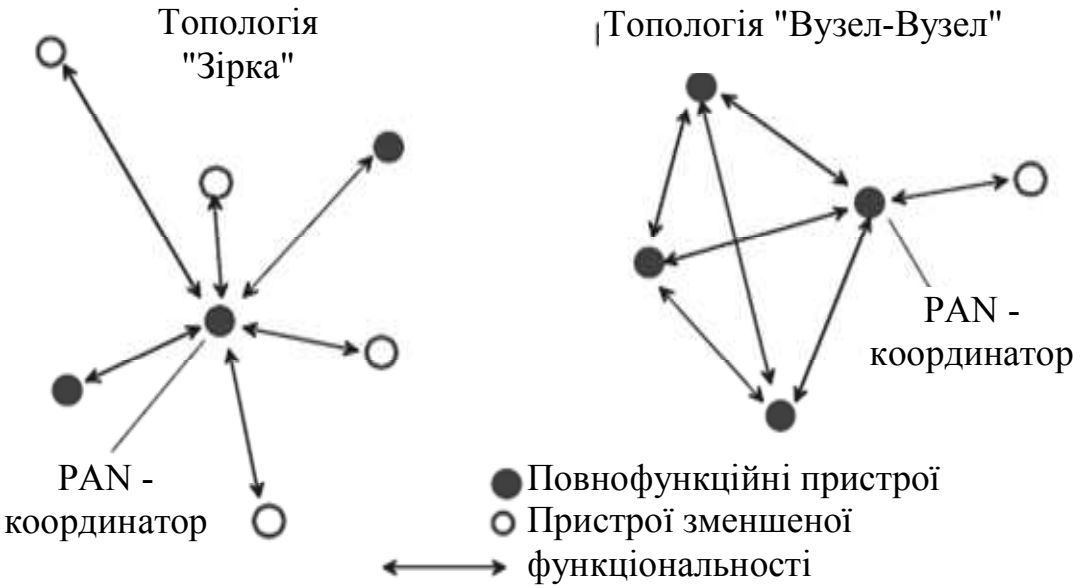


Рисунок 1.2 – Топологія мережі

Але у будь-якому випадку одне з FFD виконує функцію координатора мережі. Каж-будинку облаштуванню мережі привласнюється 64-розрядна адреса. Відмітимо, що стандарт передбачає взаємодію пристроїв не толь-ко у рамках однієї PAN, по і між різними сусідніми PAN (для чого і потрібна розвинена система адресації). Для спрощення об-мена усередині мережі координатор PAN може присвоїти пристроям коротші 16-разрядньте адреси. В цьому випадку для міжмережевої взаємодії використовуються 16-розрядні ідентифікатори мереж, що також призначаються координатором.

Швидкості передачі даних в каналах при цьому складають від 20 Кбит/з (у діапазоні 868 Мгц) до 250 Кбит/з (2450 Мгц).

У радіоканалі використаний метод широкосмугової передачі з розширенням спектру прямою послідовністю (DSSS) і паралельною (PSSS).

Уся використовувана «широка» смуга частот ділиться на деяке число підканалів. Кожен переданий біт інформації перетворюється, по заздалегідь зафіксованому алгоритму, в послідовність з n біт, і ці n біт передаються одночасно і паралельно, використовуючи усе n підканалів.

У кожен переданий інформаційний біт (логічний 0 або 1) вбудовується послідовність так званих чіпів. Чіпові послідовності, що вбудовуються в інформаційні біти, називають шумоподобными кодами (PN-послідовності), що підкреслює ту обставину, що результуючий сигнал стає шумоподібним і його важко відрізнити від природного шуму. Завдяки цьому можна використати одну і ту ж ділянку радіоспектру двічі — звичайними вузькосмуговими пристроями і «поверхних» — широкосмуговими.

Усі облаштування стандарту можна класифікувати по функціональності і за призначенням. По функціональності можна виділити два типи пристроїв : повнофункціональні (FFD) і напівфункціональні (RFD). Повнофункціональний пристрій може з'єднуватися з будь-яким пристроєм в мережі, а напівфункціональні - тільки з FFD. За призначенням існують три різні типи облаштувань ZigBee.

Координатор ZigBee (ZC) — найбільш відповідальний пристрій, формує шляхи дерева мережі і може зв'язуватися з іншими мережами. У кожній мережі є один координатор ZigBee. Він управляє мережею — призначає PAN ID мережі, роздає короткі адреси, вибирає частоту.

Маршрутизатор ZigBee (ZR) — може виступати проміжним маршрутизатором, передаючи дані з інших пристроїв. Він також може запускати функцію додатка.

Кінцеве облаштування ZigBee (ZED) — його функції дозволяють йому передавати інформацією до координатора, або маршрутизатора. Він не збирає дані. Завдяки цьому, більшу частину часу перебуває в сплячому стані, що дозволяє економити енергію. ZED вимагає мінімум пам'яті.

Виділяють наступні топології мережі :

- зірка;

- точка-точка (мережа рівноправних вузлів).

У топології «зірка» обмін даними відбувається між центральним головним контролером, званим PAN-координатором і іншими веденими пристроями. Він є первинним пристроєм в мережі і тому може живитися від стаціонарного джерела.

У топології «рівноправних вузлів» також є PAN-координатор, проте будь-який пристрій, на відміну від топології «зірка», може зв'язатися з іншим, поки вони знаходяться в межах один одного. Таким чином «рівноправні вузли» можуть утворювати складніші мережеві утворення, наприклад, петлю або кластерне дерево (рис. 1.3). В цьому випадку RFD пристрою з'єднуються з деревовидною кластерною схемою як листовий пристрій у кінці гілки.

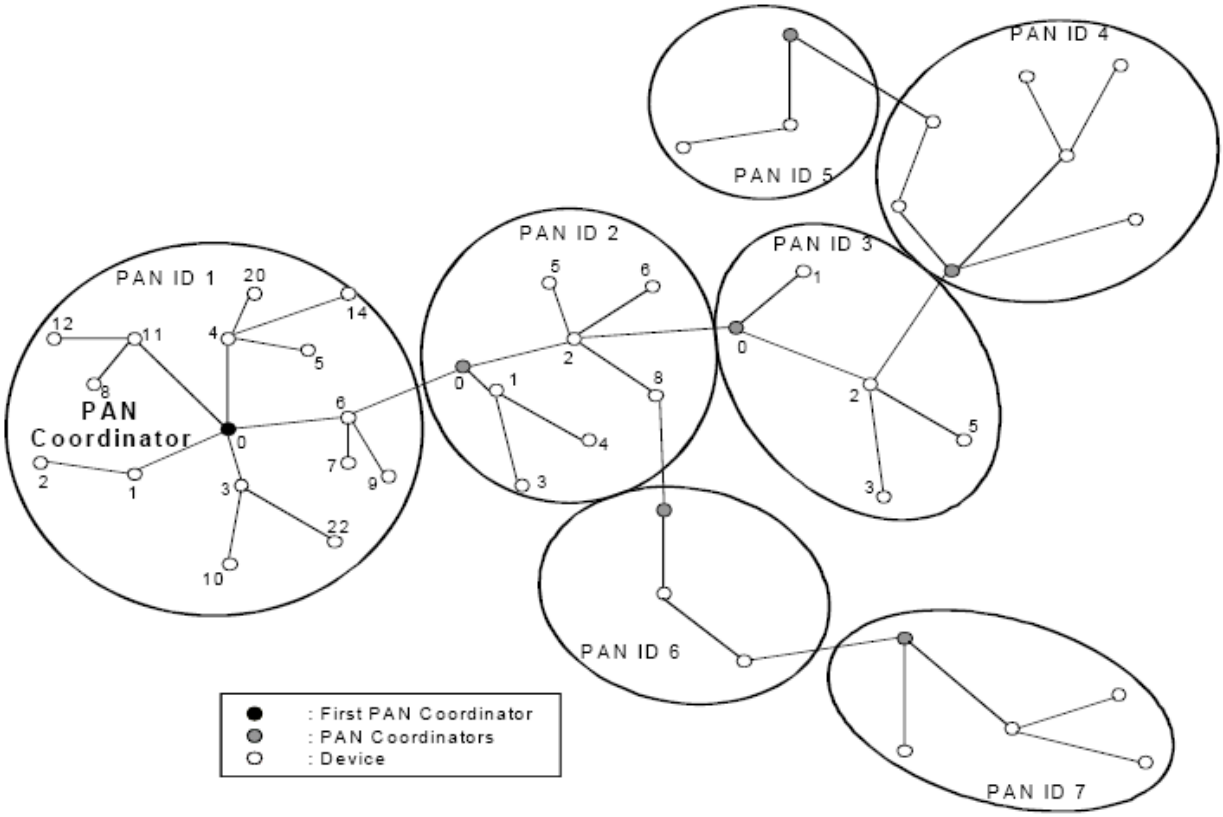


Рисунок 1.3 – Кластерна топологія [8]

Усі пристрої повинні підтримувати унікальні 64-розрядні адреси. Ці адреси використовуються для адресації в межах цієї мережі. Щоб зменшити трафік мережі передбачено використання 16-розрядних адрес, що призначаються координатором мережі.

У стандарті також визначено опціональне використання суперструктури (superframe). Вона визначається координатором і зв'язується маяками (beacon). Ці маяки передаються в першому слоті кожної суперструктури. Існує її два види - з активним і неактивним періодами. У течії неактивного періоду координатор може перейти в малопотужний режим. Якщо використати суперструктуру не обов'язково, то координатор перестане посилати маяки.

Маяки служать для синхронізації пристроїв з PAN-координатором під час з'єднання. Будь-який пристрій, бажаючий зв'язатися в течії CAP (період доступу), конкурує з іншими пристроями, використовуючи CSMA - CA механізм. Усі транзакції завершуються до наступного маяка. Для додатків, що вимагають низький рівень очікування або вимагають пропускну спроможність для специфічних даних, координатор виділяє спеціальні суперструктури - гарантовані тимчасові слоти (GTS). GTS формується у вільний період (CFP), який завжди з'являється у кінці активної суперструктури, після CAP.

Згаданий механізм CSMA - CA працює за принципом прослуховування частот впродовж певного часу і виявлення вільної частоти для передачі даних. Якщо канал зайнятий, то вузол «відстороняється» і чекає певна кількість часу, перш ніж знову зробити спробу відправки пакету. Уникнення колізій використовується для того, щоб поліпшити продуктивність CSMA, віддавши мережу єдиному передавальному пристрою.

Ця функція покладається на «стислий сигнал» в CSMA/CA. Поліпшення продуктивності досягається за рахунок зниження вірогідності колізій і повторних спроб передачі. Але очікування «стислого сигналу»

створює додаткові затримки, тому інші методики дозволяють досягти кращих результатів.

Модель пересилки даних містить в собі три види транзакцій. Перший вид - передача даних координаторові, другий - передача від координатора, третій вид - передача між рівними пристроями. У топології типу «зірка» застосовується тільки перші два види транзакцій, оскільки дані йдуть між координатором і пристроєм. У топології «рівноправних вузлів» можливі усі три види транзакцій.

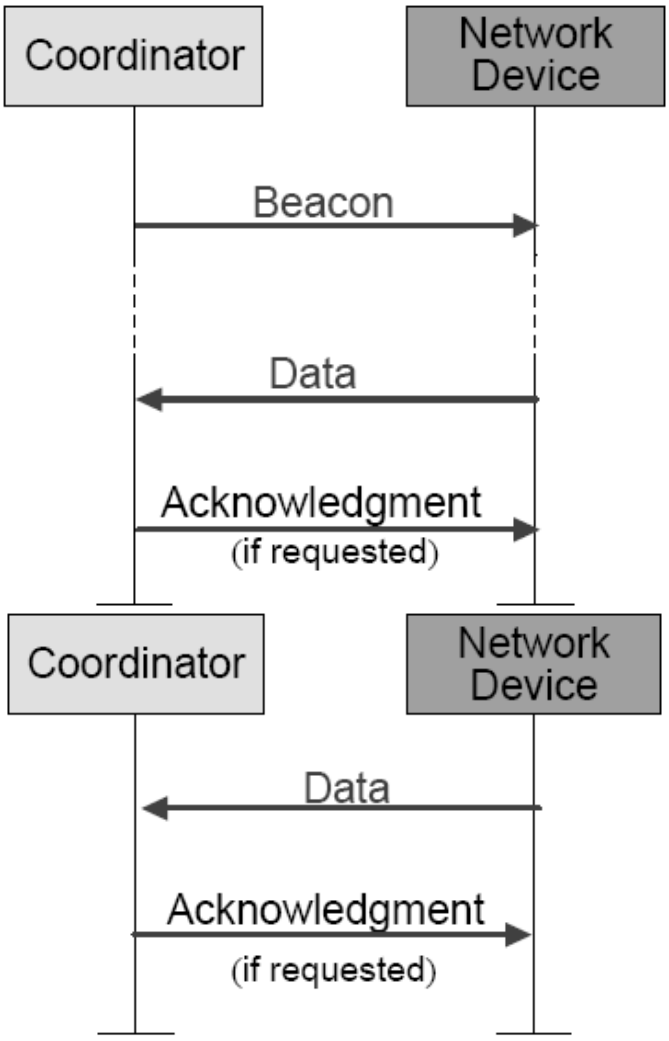


Рисунок 1.4 – Схема передачі даних координаторові з використанням і без використання маяка. Coordinator – координатор мережі; Network Device – мережевий пристрій; Data – данні; Beacon – запит; Acknowledgment – підтвердження.

Пересилка даних координаторові відбувається в наступному порядку (рис. 1.4):

- пристрій шукає маяк, інформація про який посилається координатором. Коли маяк знайдений пристрій синхронізується;
- далі в певний момент часу (по механізму CSMA - CA) вирушають самі дані;
- отримавши дані, координатор відправляє пристрою підтвердження про успішний прийом даних.

У разі, якщо маяк не використовується, дані відразу пересилаються координаторові по механізму CSMA - CA. При отриманні даних він також відправляє підтвердження.

Пересилка даних від координатора (рис. 1.5) :

- координатор інформує пристрій в маяку про наявність даних;
- пристрій, отримавши маяк, відправляє MAC команду запиту даних;
- у відповідь координатор відправляє підтвердження про успішний прийом;
- відразу за підтвердженням пересилаються самі дані;
- по прибуттю даних пристрій відправляє координаторові підтвердження про успішне отримання.

Якщо маяк не використовується, то координатор накопичує дані і при отриманні запиту від пристрою відправляє їх.

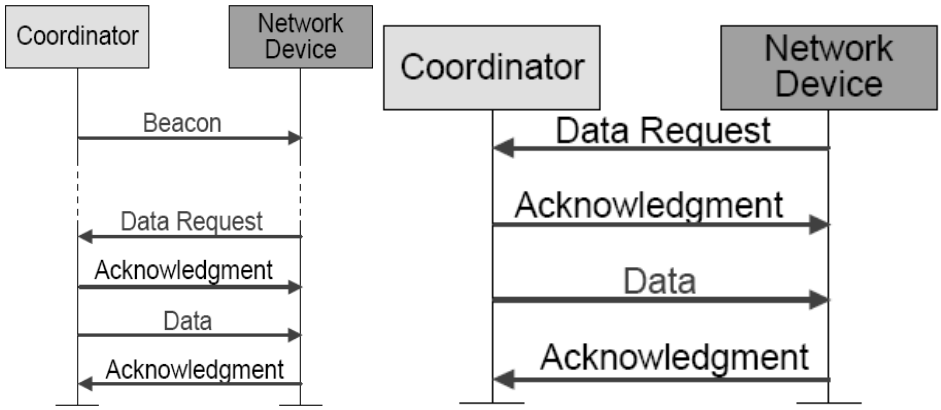


Рисунок 1.5 – Схема передачі даних від координатора з використанням і без використання маяка. Coordinator – координатор мережі; Network Device – мережевий пристрій; Data – данні; Beacon – запит; Acknowledgment – підтвердження

При передачі даних між рівноправними пристроями дані можуть передаватися, як і в перших двох випадках, після синхронізації.

Стандартом визначається чотири типи пакетів :

- сигнальний пакет (beacon frame), використовуваний координатором, щоб передавати маяки;
- пакет даних (data frame), використовуваний для передачі даних;
- пакет підтвердження (acknowledgment frame), використовуваний для підтвердження успішного прийому;
- командний пакет, використовуваний для управління об'єкту MAC.

Сигнальний пакет має наступну структуру (рис. 1.6).

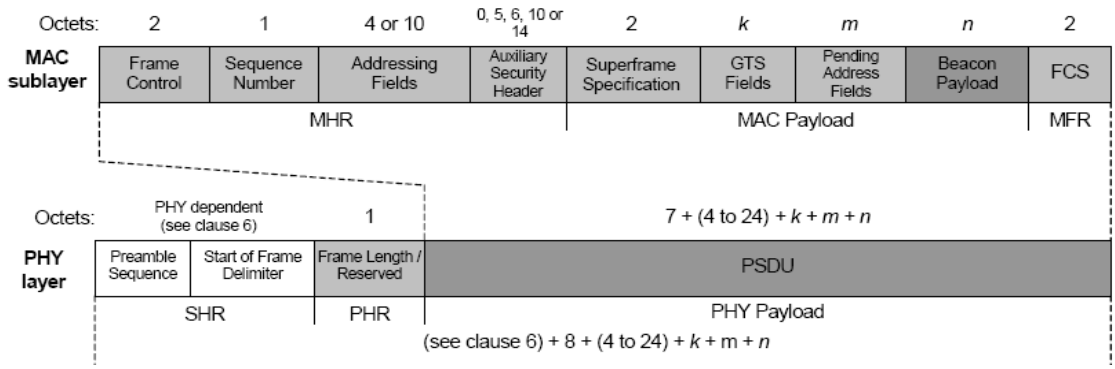


Рисунок 1.6 – Структура сигнального пакета

Пакет даних має наступну структуру (рис. 1.7).

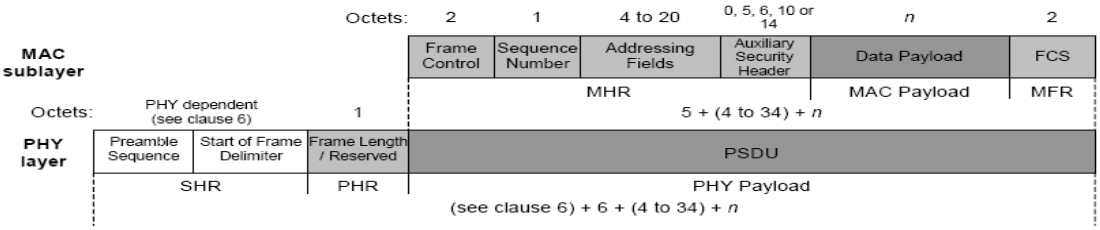


Рисунок 1.7 – Структура сигнального пакету

Пакет підтвердження має наступну структуру (рис. 1.8).

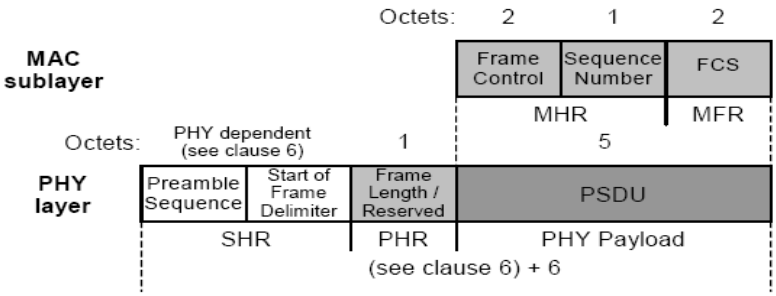


Рисунок 1.8 – Структура пакету підтвердження

Командний пакет має наступну структуру (рис. 1.9).

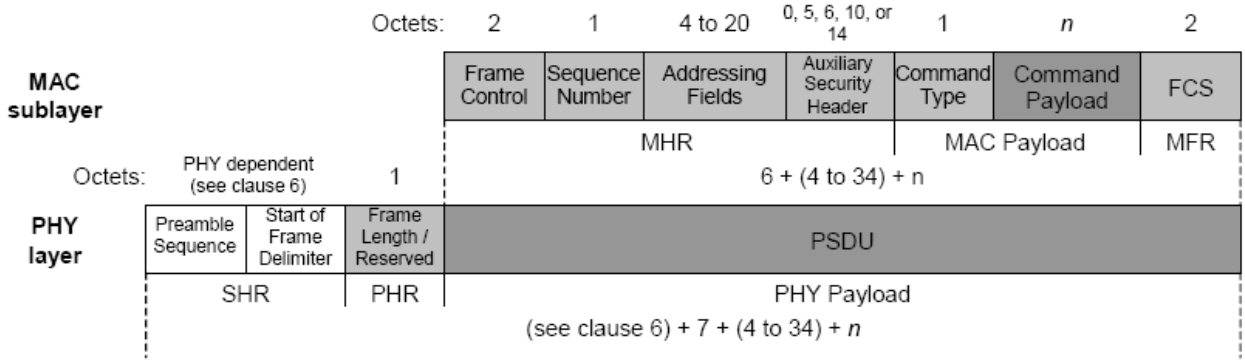


Рисунок 1.9 – Структура командного пакету

Після проходження усього потоку, в слові залишається залишок, який і є контрольною сумою.

- У цьому стандарті 802.15.4 передбачається захист даних за допомогою симетричних ключів шифрування.

1.5 Технологія безпровідного доступу до мережі Інтернет LTE

Створення конкурентної технології побудови мереж мобільного зв'язку на основі мобільного зв'язку стандарту IEEE 802.16e, що збільшило зусилля учасників проекту 3GPP по розробці на основі технології OFDM наступного варіанту мережі UMTS – LTE.

Ці удосконалення підвищують ефективність, понижають витрати, розширяють і удосконалюють послуги, що вже робляться, а також інтегруються із вже існуючими протоколами.

Мережа LTE складається з мережі радіодоступу і базовій мережі (рис 1.10). Радіус дії базової станції LTE у оптимальному випадку – до 5 км, при необхідності – до 90 км.

Виклик або сеанс передачі даних, ініційований в зоні покриття LTE, технічно може бути переданий без розриву в мережу 3G (WCDMA), CDMA2000 або в GSM/GPRS/EDGE [4].

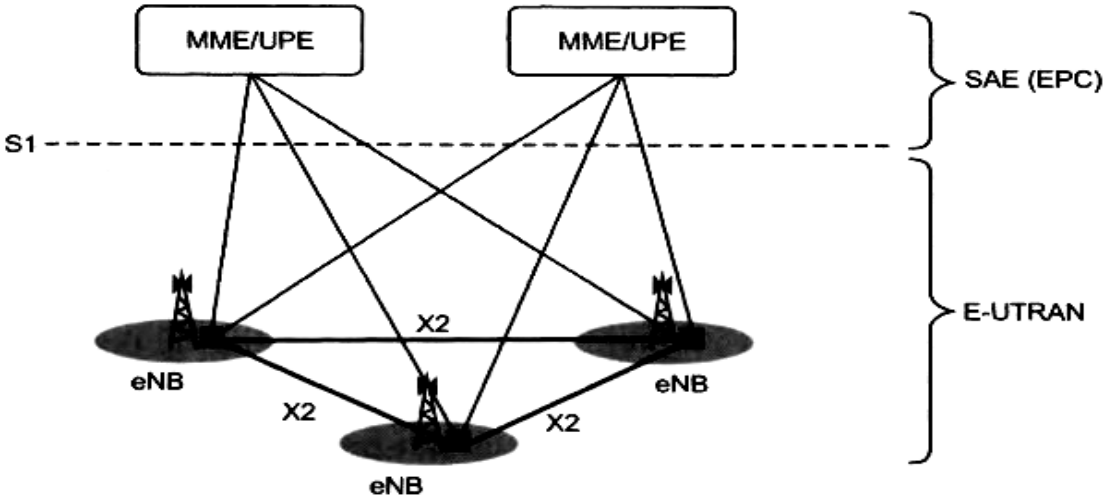


Рисунок 1.10 – Взаємодія мережі радіодоступу і базової мережі SAE

LTE краще використовує частотний спектр, відрізняється підвищеною місткістю і меншими значеннями затримки (latency), яка для невеликих пакетів може знижуватися до значення всього в 5 мс. Збільшення швидкості передачі даних сприяє підвищенню якості послуг, що надаються, прискорює

поширення нових мультимедійних сервісів (розраховані на багато користувачів ігри, соціальні мережі, відеоконференції, системи моніторингу і M2M, інтерактивні он-лайн додатка та ін.).

Ще одна перевага - на відміну від WCDMA (вимагаючої смуги в 5 Мгц), LTE здатна працювати з різними смугами частот - від 1.5 Мгц до 20 Мгц.

Стандарт Rel.8 передбачає можливість одночасної роботи до 200 активних користувачів в кожній соте, що використовує смугу в 5 Мгц:

– сильно віддалених від базової станції (десятки кілометрів) користувачів можна забезпечити як телефонним зв'язком, так і доступом в Інтернет з досить високою швидкістю, для цього потрібна наявність зовнішньої спрямованої антени на стороні користувача в зоні прямої видимості базової станції, причому антена може бути використана як точка колективного доступу;

– не сильно віддалених від базової станції (від 5 до 20 км) користувачів можна забезпечити широкосмуговим доступом до послуг зв'язку з використанням зовнішньої антени, для цього потрібна наявність зовнішньої антени на стороні користувача в зоні прямої видимості базової станції, причому антена може бути використана як точка колективного доступу;

– що знаходяться досить близько до базової станції (до 5 км) користувачів можна забезпечити широкосмуговим доступом до послуг зв'язку з використанням внутрішньої антени, при цьому користувач може бути обмежено мобільним - залежно від рівня сигналу.

Необхідно помітити, що як представлено на рис.2.4, усе три представлених вище за сценарій можуть бути розширені шляхом використання технології дротяної (LAN) або безпровідної локальної мережі (WLAN) для організації доступу призначеного для користувача устаткування до точки колективного доступу. В цьому випадку з одного боку, вартість послуги для крайового користувача буде істотно понижена, а з іншої - навантаження на устаткування створюватиметься безліччю користувачів, тобто час окупності устаткування може бути істотно понижений.

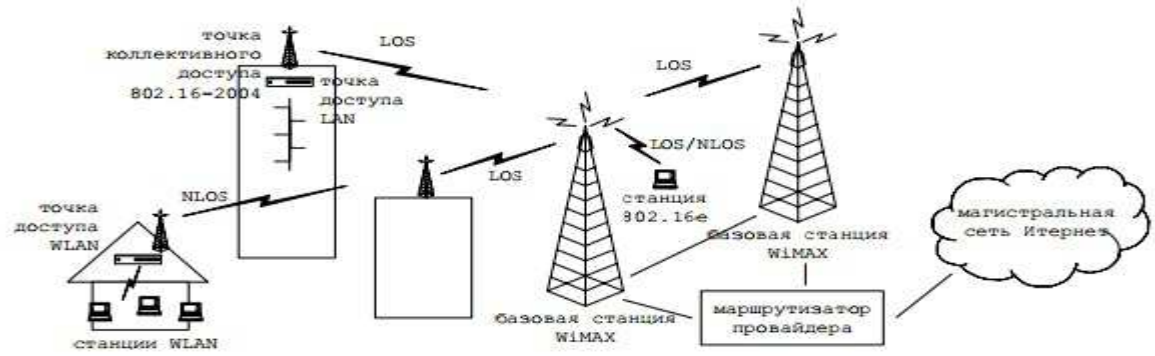


Рисунок 1.11 – Мережева структура організації безпровідного широкосмугового доступу в мережі WiMAX

Таким чином, при проектуванні широкосмугового доступу на основі технології WiMAX потрібне проведення планування мережі з обліком, як мінімум, наступних параметрів:

- відстань від базової станції до антени користувача/групи користувачів;

- кількість користувачів, їх тип і послуги якими вони користуватимуться, тобто необхідно провести оцінку навантаження на базову станцію.

Далі відмітимо, що, у свою чергу, базові станції можуть з'єднуватися з іншими базовими станціями як з використанням фіксованих мереж (наприклад, оптичний кабель), так і з використанням технології WiMAX (необхідно щоб базові станції знаходилися в зоні прямої видимості LOS). У обох випадках також необхідно проводити планування розміщення базових станцій з метою визначення оптимального, як з точки зору вартості, так і з точки зору якості широкосмугового доступу, що надається, розміщення базових станцій WiMAX.

WiMAX має високу якість сервісу, забезпечує мультисервісність, гнучкий розподіл частот, завдання пріоритетів різним видам трафіку, можливість забезпечення різного рівня якості (QoS), підтримка інтерфейсів IP, TDME1/T1.

Висновки до розділу

1. Для якісного надання будь-якої послуги оператори зв’язку повинні мати ресурсну базу (маршрутизатори, канали зв’язку та інше обладнання), технічні характеристики якої задовольняють всім вимогам цієї послуги. При цьому різні типи сервісів мають різні вимоги до технічних характеристик мережі зв’язку.

2. Зростання складності структури мережі, зростання кількості активних учасників в мережі обумовлює складність виконання розробки первинної топології мережі та визначення швидкісних параметрів на етапі проектування.

3. Мережа на основі бездротових елементів мережі вимагає особливого підходу, оскільки вузли мережі можуть взаємодіяти між собою з підтримкою передачі як "зірка" так і "вузол – вузол". Стандарт IEEE 802.15.4 дозволяє реалізувати мережу, яка може динамічно змінюватись в роботі, а тому процес моделювання такої мережі є одною з найбільш складних задач.

РОЗДІЛ 2 ЗАГАЛЬНІ ПРИНЦИПИ ФОРМУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2.1 Узагальнена мережева інфраструктура

Усі структурні блоки мережевої інфраструктури повинні мати підключення до зарезервованого ядра мережі, яке і забезпечуватиме високошвидкісне з'єднання між ними. Надалі будуть розглянуті особливості підключення кожного із структурних блоків.

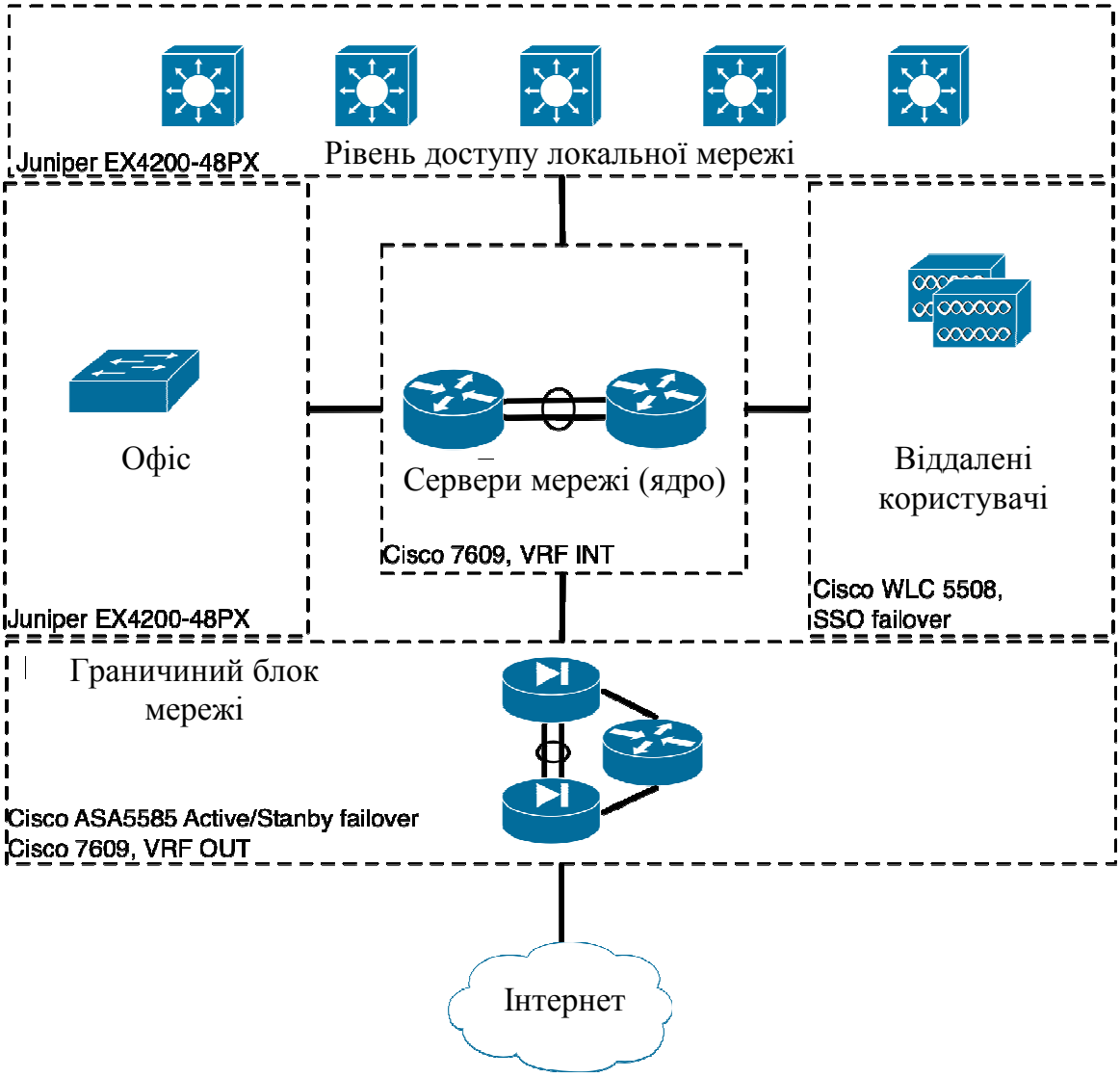


Рисунок 2.1 – Схема зв'язків між структурними блоками мережі (приклад) [8, 9]

Для вирішення завдань створення мереж розробляється мережеве устаткування різного призначення (рис. 2.1): комутатор - мережеве устаткування для об'єднання комп'ютерів в одну або декілька локальних мереж; маршрутизатор - пристрій, призначений для взаємодії комп'ютерів, що знаходяться в різних локальних мережах і надання доступу в мережу Інтернет; міжмережевий екран - пристрій, що забезпечує безпеку в мережі і так далі. На сьогодні існує безліч компаній, що виробляють мережеве устаткування, і компанія Cisco Systems вважається безумовним фаворитом на ринку мережевого устаткування (займає близько 70% ринку) і пропонує пристрої для створення обчислювальних мереж від невеликого офісу до великих корпорацій [4].

Компанія Cisco Systems є виробником мережевого устаткування з 1984 року і до цього часу є лідером в цій галузі. Мережеве устаткування компанії помітно виділяється на тлі конкурентів і має багато переваг:

1) Надійність - мережеве устаткування, що випускається компанією, функціонує на базі операційної системи Cisco IOS і включає величезний спектр налаштування і конфігурації пристрою;

2) Гнучкість - мережеві пристрої під управлінням Cisco IOS можу одночасно виконувати абсолютно різні функції: маршрутизації, захисні, налагоджувальні і так далі;

3) Інтелектуальність - пристрої компанії містять широкий спектр різних технологій і протоколів, як стандартних, так і розроблених власне компанією Cisco;

4) Централізація - для управління пристроями можуть використовуватися потужні комплекси управління і відлагодження устаткування, наприклад, такі, як Cisco Security Manager та ін.

З недоліків, можна лише виділити вартість устаткування. Проте, варто відмітити те, що висока вартість устаткування компанією Cisco, що випускається, окупається за рахунок надійності і терміну служби цього устаткування.

Враховуючи широке поширення мережевого устаткування під управлінням Cisco IOS (**Internetwork Operating System — Міжмережева Операційна** Система), а також високу вартість цього устаткування, ще яснішою стає необхідність в застосуванні програмних емуляторів мережевого устаткування для створення моделей обчислювальних мереж [18].

Саме на устаткуванні цього виробника проектуватимуться майбутні моделі обчислювальних мереж.

2.2 Технології, що використовувані при побудові захищених корпоративних мереж

Вибираючи технологію, яка використовуватиметься при реалізації проекту, необхідно відразу обертати уваги на декілька моментів. По-перше – технологія повинна задовольняти вимогам проекту – забезпечувати необхідну пропускну спроможність, масштабованість, захищеність переданої інформації і так далі. По-друге, технологія має бути стандартизована, і широко поширена – це дозволить уникнути проблем в ході впровадження і експлуатації (наприклад, припинення підтримки вибраної технології виробниками устаткування). Ще один аргумент на користь рішень на основі стандартних протоколів – незалежність від виробника устаткування, і гарантія можливості подальшої модернізації мережі з використанням актуальних рішень.

Фізичний рівень визначає середовище передачі даних і протокол. Для ЛВС під вимоги актуальності для завдання проекту і поширеності підходить оптичне середовище передачі даних і вита пара. Для безпровідної – тільки радіоканал, причому в частотних діапазонах не вимагаючи додаткових дозволів на використання.

Виходячи з вищесказаного, слід розглянути набір протоколів передачі даних IEEE 802, і вибрати найбільш відповідні стандарти для реалізації проекту :

- 802.3 Ethernet;
- 802.4 Token bus;
- 802.5 Token ring;
- 802.6 Distributed Queue Dual Bus;
- 802.9 “isoEthernet";
- 802.10 SDE;
- 802.11 Wi – Fi;
- 802.12 100BaseVG;
- 802.15 Bluetooth;
- 802.16 WMAN;
- 802.17 RPR.

Технологія, використовувана при побудові мережі, як дротяної так і безпровідної, має бути поширеною і використовуваною. З перерахованих, з деякими обмовками, такими є 802.3 (широко поширена), 802.11 (широко поширена), 802.15 (широко розповсюджена), 802.16, 802.5. Спочатку необхідно визначиться із стандартом для безпровідної мережі:

- IEEE 802.15 (Bluetooth) був спочатку створений як протокол для безпровідного зв'язку мобільних пристроїв, і не забезпечує ні належної пропускної спроможності, ні масштабованості для вирішення завдань.

- IEEE 802.16 (WMAN, також широко використовується найменування WiMAX) – безпровідне рішення, розроблене для покриття великих площ, використовує діапазон частот від 1,5 до 11 ГГц. Спочатку розроблялося як стандарт «Останньої милі» для безпровідних ятерів, вимагає дозволу на використання частотного діапазону базових станцій, не забезпечує належної пропускної спроможності за наявності безлічі абонентів, і для реалізації проекту не підходить.

- IEEE 802.11 (Wi – Fi) – набір стандартів, найбільш поширені 802.11b, 802.11a, 802.11g, 802.11n. Припускає роботові в частотних діапазонах 2.4 ГГц і 5 ГГц, 11b забезпечує пропускну спроможність в 11 Мбіт/з на канал, стандарти 11a і 11g – забезпечують пропускну спроможність

в 54 Мбіт/с, працюючи в діапазонах 2.4 і 5 ГГц відповідно. Найбільш сучасний IEEE 802.11n забезпечує теоретичну пропускну спроможність до 600 Мбіт/с, використовуючи MIMO (multiple input multiple output, наявність декількох передавальних і приймаючих антен на пристрої) і channel bonding (об'єднання частотних каналів). Допустима робота пристроїв 11n як в діапазонах 2.4-2.5 ГГц, так і в 5 ГГц. Стандарт назад сумісний з 11a/b/g. У даний момент прийнята чорнова редакція стандарту 802.11ac, що забезпечує швидкість безпровідної передачі даних до 6 Гбіт/з, в деру чергу за рахунок використання MIMO з великою кількістю антен і розширення каналу. Це сімейство стандартів найбільше підходить для реалізації проекту, враховуючи вимоги масштабованості і пропускної спроможності рішення.

У виборі протоколів канального рівня для дротяної мережі – з поширених під вимогу поширеності, доступності і забезпечення пропускної спроможності підходить тільки сімейство IEEE 802.3, Ethernet. У другу чергу:

- 802.3ae, 10 Гбіт/з по оптичному волокну
- 802.3ab, GigabitEthernet по витій парі
- 802.3af, Power over ethernet
- 802.3ad, агрегація каналів

Для виконання завдань проекту на мережевому і вище рівнях МВОС потрібно використання стека протоколів TCP/IP.

2.3 Існуючі рішення побудови корпоративної локальної мережі

Здавалося б, навіщо проектувати мережі «з нуля», коли будь-який виробник устаткування готовий надати декілька варіантів типових рішень, універсальних і повністю закінчених? Проекти, розміщені в якості прикладів в секції «SRND» сайту виробника, як правило мають декілька загальних рис:

- Орієнтованість на устаткування одного виробника, що відразу знижує гнучкість і відмовостійкість рішення. Частенько на усій лінійці мережевого устаткування використовується одна і та ж, або близька

програмна платформа, яка не ідеальна (Приклад – Juniper Networks і JunOS, Cisco Systems і IOS, IOS – XR). І у разі виявлення критичної уразливості, або нестабільної поведінки постраждає уся мережа відразу.

- Широке застосування пропріетарних протоколів, і, як наслідок, складність подальшої модернізації мережі з використанням устаткування іншого виробника.
- Максимально загальні рішення, які потрібно було б серйозно переглядати для відповідності вимогам цього проекту (multicast routing, канали в зовнішні офіси, відмовостійкість, можливе використання вже наявного у компанії устаткування, покриття БЛВС в ліфтах).

Подібні рішення не відповідають вимогам що пред'являються до мережевої інфраструктури, і не можуть бути використані без внесення змін, по масштабності порівнянних з розробкою «з нуля», проте запозичення з незначними змінами тихий або інших складених блоків типових вендорских проектів може бути цілком виправдане.

Перш ніж приступати до проектування структури майбутньої мережі передачі даних, вимагається вибрати технології, які використовуватимуться. Визначившись з ключовими для проекту характеристиками, по яких відбуватиметься вибір стандарту, можна вибрати відповідну технологію для фізичного, канального і мережевого рівня моделі взаємодії відкритих систем (МВОС, ISO OSI). Не дивлячись на деяку умовність цієї моделі у сучасному світі і неоднозначність трансляції цієї моделі на найбільш поширений стек протоколів – TCP/IP, цей підхід дозволить визначиться з набором стандартів для реалізації проекту, і, надалі, з використовуваним устаткуванням.

2.4 Класифікація емуляторів

Усі емулятори мережевого устаткування можна розділити на дві основні групи:

1. Апаратно-реалізовані емулятори.
2. Програмно-реалізовані емулятори.

До першої групи відносять, як правило, вузько спеціалізоване устаткування, що дозволяє при підключенні до нього реального телекомунікаційного устаткування імітувати роботу реальної телекомунікаційної мережі, або якійсь її частині (як правило - каналів зв'язку). У апаратних емуляторах на апаратному рівні реалізовані процеси, що протікають в реальних мережах, - виникнення затримок, втрат пакетів, спотворення переданих даних і тому подібне подій. Основна мета розробки і застосування апаратних емуляторів - дослідження роботи реального телекомунікаційного устаткування в різних умовах і при різних характеристиках каналів [12].

До другої групи емуляторів відносять спеціально розроблені програми, що дозволяють імітувати роботу устаткування і каналів зв'язку, а також роботу командних інтерфейсів активного мережевого устаткування [13]. Основна мета використання програмних емуляторів - застосування в якості науково-дослідної діяльності, для постановки наукових експериментів. Також, ці програми часто використовуються як повчальні системи для підготовки персоналу в роботі з мережевим устаткуванням [16].

2.4.1 Програмні емулятори мережевого устаткування

Повсюдне створення комп'ютерних мереж обумовлює різкий розвиток у сфері передачі інформації. Комп'ютерні мережі створюються для забезпечення користувачів видаленим доступом до ресурсів мережі. Тому фактично усі компанії, що мають більше за один комп'ютер, об'єднують їх в локальні мережі. Дуже принципово, щоб мережа компанії працювала безперебійно, була надійною, якнайкраще справлялася з обробкою інформації, циркулюючої між співробітниками компанії, і дозволяла приймати їм значимі і оптимальні рішення [1, 2].

Складні складені мережі складаються з великої кількості елементів - маршрутизаторів, концентраторів, комутаторів, модемів, мостів і тому подібне телекомунікаційного устаткування [9].

При розробці складних складених мереж нерідко встає завдання попереднього моделювання такої мережі з метою перевірки використовуваних технічних рішень [1]. Аналіз роботи створеної моделі мережі дозволяє до її фізичної реалізації оцінити характеристики проектованої мережі, а також розробити необхідну конфігурацію інтелектуальних мережевих пристроїв.

Це завдання, при усій її уявній простоті, є досить складним із-за великої різноманітності вживаного устаткування.

Найбільш простим рішенням для створення моделей майбутніх обчислювальних мереж є програмні емулятори устаткування. Вони не вимагають великих витрат, оскільки немає необхідності придбавати мережеве устаткування, усе, що необхідно, це персональний комп'ютер і програмний емулятор [4].

Програмні емулятори мережевого устаткування - це програмні продукти, функції, що дозволяють з'єднати в собі, і параметри реальної обчислювальної мережі. Вони були розроблені для проектування, моделювання і тестування роботи мережі. [7]

Більшість емуляторів досить зручна у використанні, оскільки надають графічний інтерфейс для управління мережевою інфраструктурою, що буває набагато зручніший чим управління підключеннями реальних пристроїв [4].

Серед засобів імітаційного моделювання окремих подій і станів безпровідних сенсорних мереж на базі стандарту IEEE 802.15.4-2006 найбільше поширення отримала наступні середовища:

1. OPNET Modeler (поточна версія 16.0);

2. OMNET++ (поточна версія 4.1);

3. NS-2 (поточна версія 2.34).

2.4.2 NS-2 (Network Simulator Version 2)

NS-2 - об'єктно-орієнтоване середовище імітаційного моделювання дискретних подій і станів з відкритим початковим кодом, яка розроблена у

рамках проекту VINT. Середовище моделювання написане на C++ і TCL. NS-2 використовує TCL для генерації сценаріїв - це дозволяє генерувати комплексні сценарії за допомогою скриптів.

Спочатку NS-2 підтримував моделювання тільки статичних комп'ютерних мереж TCP/IP. Проте зараз мобільні вузли підтримуються, що дозволяє моделювати мобільні мережі ad-hoc. Підтримуються протоколи маршрутизації ad-hoc AODV, DSDV, DSR і TORA, але вони вимагають доопрацювання для коректної роботи з мобільними вузлами.

Для NS-2 існує модель, що реалізовує стандарт IEEE 802.15.4, розроблена Джинлиан Женгом та ін. Структура компонентів моделі LR - WPAN і основні її функції представлені на рис. 1.12.

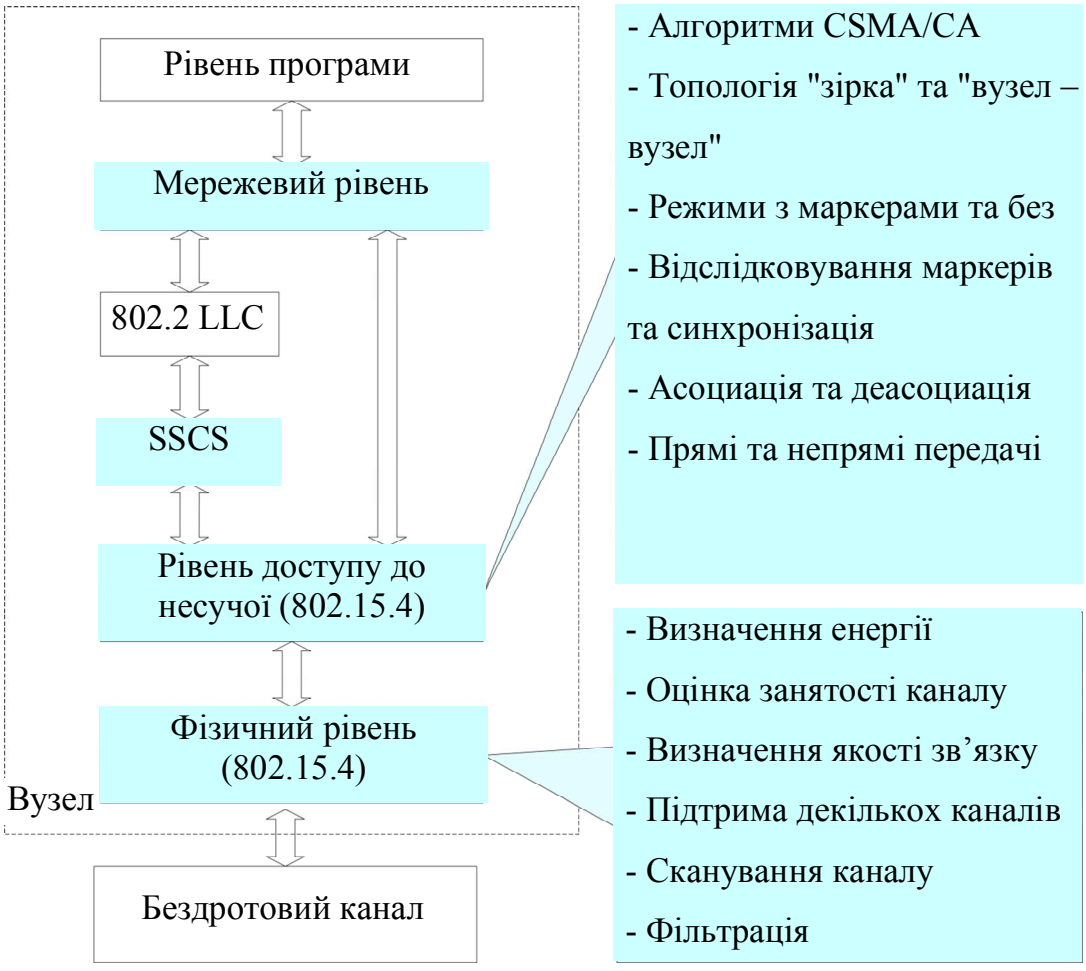


Рисунок 2.2 – Структура компонентів моделі LR-WPAN NS-2

Слід згадати, що в перших версіях моделі були реалізовані базові функції мережевого рівня ZigBee, але пізніше вони були виключені із загального доступу, оскільки не повною мірою відповідали цьому стандарту. У зв'язку з цим на даний момент можна використати тільки існуючі в NS-2 протоколи маршрутизації, які не до кінця враховують особливості безпровідних сенсорних мереж.

Документація по моделі явно недостатньо, автор в основному пропонує звертатися до презентації доступної разом з початковим кодом моделі, до списку питань, що часто ставляться, і аналізувати початковий код моделі.

2.4.3 OPNET Modeler (Optimized Network Engineering Tools)

OPNET Modeler - потужне середовище імітаційного моделювання дискретних подій і станів. Вона включає безліч бібліотек мережевих технологій і протоколів зв'язку, таких як TCP/IP, протокол передачі гіпертексту (HTTP), технологія асинхронного режиму передачі (ATM) і FrameRelay, IP - QoS, 802.11 (Wi - Fi), ZigBee та ін. Ці бібліотеки поставляють блоки для побудови моделей мереж. Одним з безлічі модулів, доступних в OPNET Modeler, є безпровідним модуль. Він розширює функціональність середовища для імітаційного моделювання і аналізу безпровідних мереж.

У версії OPNET Modeler 14.0 доступні моделі вузлів ZigBee, розроблені самою компанією OPNET. При цьому початковий код моделі мережевого рівня і рівня додатків прихований від користувачів. Доступний тільки код моделі нижнього рівня 802.15.4.

Також існує модель вузлів-сенсорів з відкритим початковим кодом, що відповідає стандарту IEEE 802.15.4, розробкою, якою займається співтовариство OPEN - ZB. Різні версії цієї моделі працюють з OPNET Modeler 10.5 і вище (табл. 2.1).

Таблиця 2.1 – Існуючі моделі OPEN – ZB для OPNET

OPEN – ZB модель	**Дата випуску**	**Версія OPNET**
OPNET Simulation Model v 3.0b	20.11.2009	15.0
OPNET Simulation Model v 2.1	31.03.2009	14.5
OPNET Simulation Model v 2.0	22.05.2007	11.5
OPNET Simulation Model v 1.0	06.04.2006	10.5

Розглянемо детальніше найбільш популярні емулятори, що дозволяють створити віртуальні копії мережевого устаткування виробництва компанії Cisco Systems.

2.4.4 Cisco Packet Tracer

Найпопулярнішим емулятором мережевого устаткування є Cisco Packet Tracer, це емулятор, розроблений самою компанією Cisco Systems для навчання початкуючих фахівців. Packet Tracer отримав велике поширення за рахунок необхідності його застосування для проходження навчання у рамках програм Cisco Network Academy, мережевої академії, в якій щорічно проходять навчання десятки тисяч початкуючих фахівців [6].

Створення мережевої інфраструктури і подальша модифікація відбуваються через графічний інтерфейс, який є інтуїтивно зрозумілим і найбільш зручних з графічних інтерфейсів управління, що надаються даними програмними засобами емуляції мережевого устаткування. Інтерфейс добре адаптований для початкуючих фахівців і дуже сильно спрощує процес створення нових мережевих інфраструктур або запуск і налаштування необхідних для проведення практичних занять сервісів. Приклад інтерфейсу відображений на рис. 2.2.

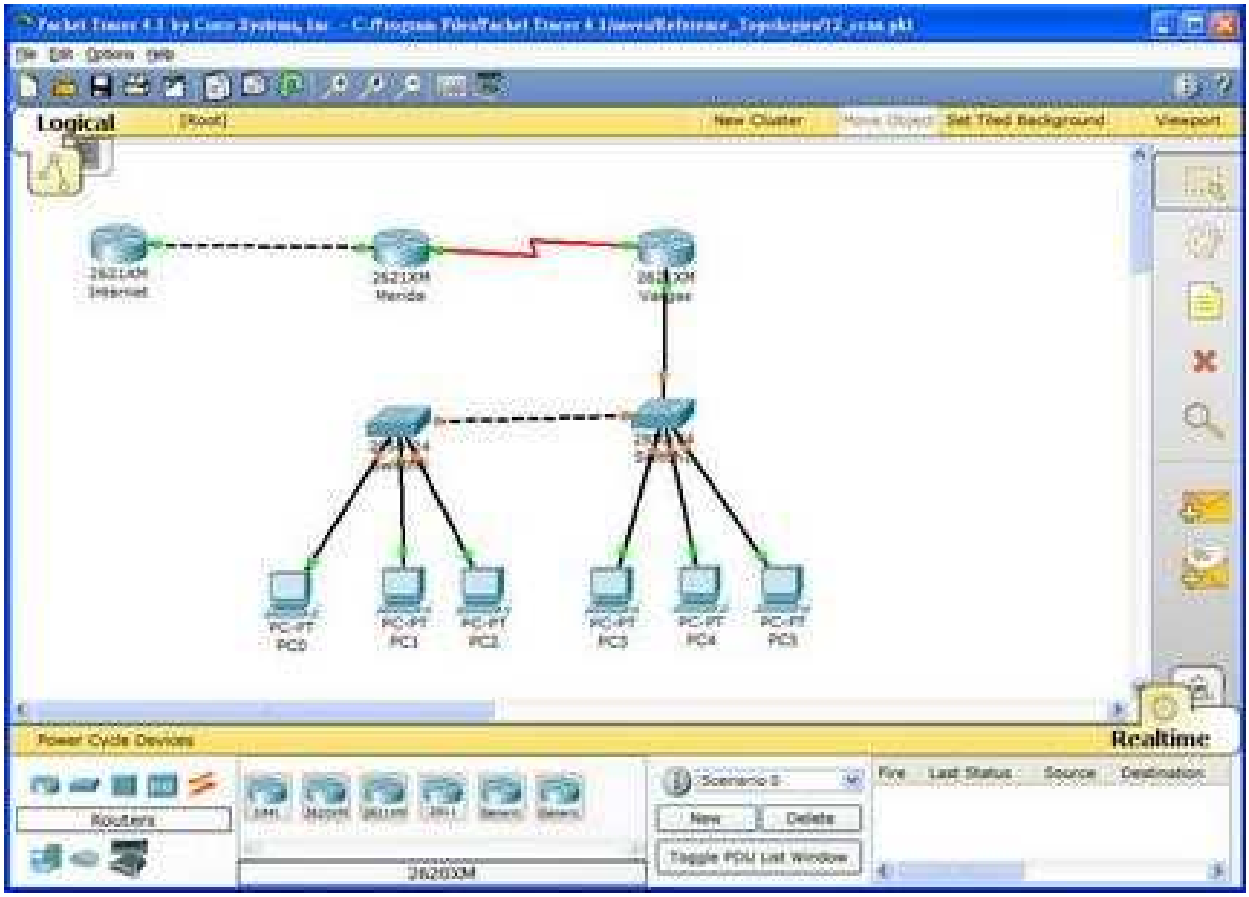


Рисунок 2.3 – Графічний інтерфейс емулятора Cisco Packet Tracer [17]

Основне призначення емулятора Packet Tracer в створенні віртуальних мереж для проведення практичних робіт для підготовки до сертифікаційних іспитів CCNA (Cisco Certified Network Associate) і CCNA Security (Cisco Certified Network Associate Security). Окрім стандартних маршрутизаторів і комутаторів Packet Tracer підтримує емуляцію IP-телефонів, безпровідних точок доступу і серверів з набором стандартних служб [7].

У Packet Tracer вбудована безліч засобів, що спрощують вивчення роботи мережевої інфраструктури, таких як снифери, що дозволяють отримати детальну інформацію про усі блоки даних переданих тому або іншому пристрою, генератори мережевого трафіку, що дозволяють штучно створювати навантаження, і засоби відображення потоків даних, що дозволяють простежити маршрут проходження мережі будь-яким пакетом або процес зміни пакету при проходженні різних пристроїв .

Packet Tracer є зручним засобом емуляції мережевого устаткування не лише для того, що навчається, але і для викладача. У емулятор вбудовані засоби автоматичної перевірки виконання завдання. Викладач може розробити лабораторну роботу для Packet Tracer, яка автоматично перевірятиме міру виконання завдання, і замість перевірки вручну правильності роботи усіх протоколів і коректності введених команд, досить скористатися автоматичною перевіркою, яка визначить відсоток виконання завдання і працездатність основних сервісів [9].

Cisco Packet Tracer робить емуляцію як апаратної, так і програмної частини мережевого устаткування. Таким чином, Packet Tracer дозволяє створювати копії великих мережевих інфраструктур, ось тільки емульовані пристрої не підтримують дуже велику кількість технологій, використовуваних в реальних великих мережах, багато функцій, доступних в реальних пристроях просто відсутні. Головна перевага Cisco Packet Tracer – безкоштовність цього продукту [6, 7].

Таким чином, емулятор Cisco Packet Tracer є оптимальним інструментом для проведення практичних занять при навчанні по базових курсах компанії Cisco і при підготовці до іспитів рівня фахівця. Але для вирішення складнішим завдань моделювання обчислювальних мереж дане ПО не підходить, оскільки є симулятором і не надає усіх можливостей реального устаткування, і далі розглядатися не буде.

2.4.5 Graphical Network Simulator 3

GNS3 або Graphical Network Simulator 3 – це незалежний безкоштовний програмний емулятор маршрутизаторів Cisco. GNS3 підтримується у більшості операційних систем Linux, Windows і Mac OS X, при цьому цей програмний емулятор дає можливість емулювати апаратну частину маршрутизаторів Cisco, для цього він завантажує і використовує реальний образ операційної системи Cisco IOS [8].

GNS3 - це графічна оболонка, що об'єднує в собі ряд різних програмних засобів емуляції. Графічний інтерфейс середовища емуляції, зображений на рис. 2.3, не адаптований для початкуючих фахівців, він швидше розрахований на тих, хто вже має досвід роботи із засобами емуляції, мережевим устаткуванням і знайомий з основними принципами функціонування мережевих пристроїв. Але наявність графічних засобів управління значно полегшує процес створення мережевої інфраструктури і робить роботу з нею зручнішою.

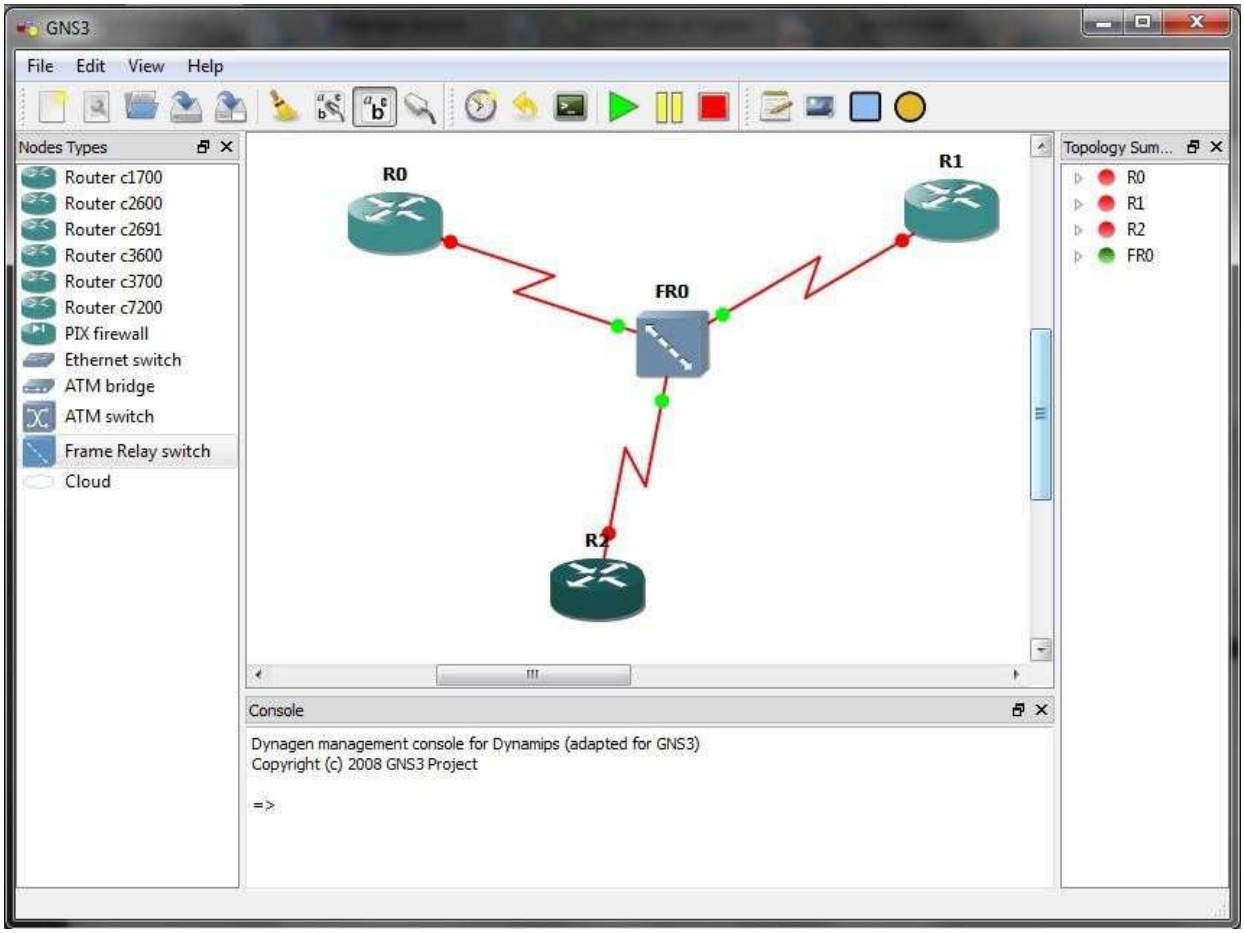


Рисунок 2.4 – Графічний інтерфейс емулятора GNS3 [18]

GNS3 включає три окремі програмні емулятори. Перший з них Dynamips. Багато фахівців, що вивчають мережеві технології, застосовують Dynamips виключно в середовищі GNS3, оскільки відпадає необхідність роботи з конфігураційними файлами і командним рядком. Другим є Qemu,

який дозволяє емулювати міжмережеві екрани Cisco PIX і ASA і системи запобігання вторгненням Cisco IPS, наявність підтримки цих пристроїв значно розширює можливість застосування GNS3 в навчанні по напрямах, пов'язаних із забезпеченням безпеки мережевих інфраструктур [5]. Третім елементів являється система віртуалізації VirtualBox, яка дозволяє інтегрувати в мережеву інфраструктуру з емульованих пристроїв віртуальні сервера або віртуальні персональні комп'ютери, які дозволять точніше відтворити реальну інформаційну інфраструктуру, а означати вивчити більший ряд технологій.

GNS3 є дуже вимогливою до ресурсів системою емуляції. Оскільки запускаються одночасно декілька незалежних систем емуляції, а поверх них контролююче середовище, що забезпечує ще і графічний інтерфейс, що постійно відображають зміни в стані інфраструктури, потрібно серйозні обчислювальні потужності. Хоч GNS3 і дає нам функціональні можливості створити досить точну копію реальних інформаційних інфраструктур з їх мережевим, серверним устаткуванням і комп'ютерами кінцевих користувачів, обчислювальної потужності персонального комп'ютера вистачить на емуляції лише дуже маленької інформаційної інфраструктури. В результаті, практичні заняття на GNS3 можуть проводитися на штучно створених сегментах мережі, але не на копіях реальних інфраструктур [6, 8].

2.4.6 UNetLab

Unified Networking Lab (UNetLab, UNL) - мережевий емулятор, який є розрахованою на багато користувачів платформою для моделювання і створення віртуальних мереж, різних лабораторій, підтримує переконливий список телекомунікаційного устаткування. Таким чином, концептуальною новизною продукту UNetLab є можливість запуску і використання програми між різними платформами і різними виробниками пристроїв. Приклад графічного інтерфейсу відображений на рисунку 2.4.

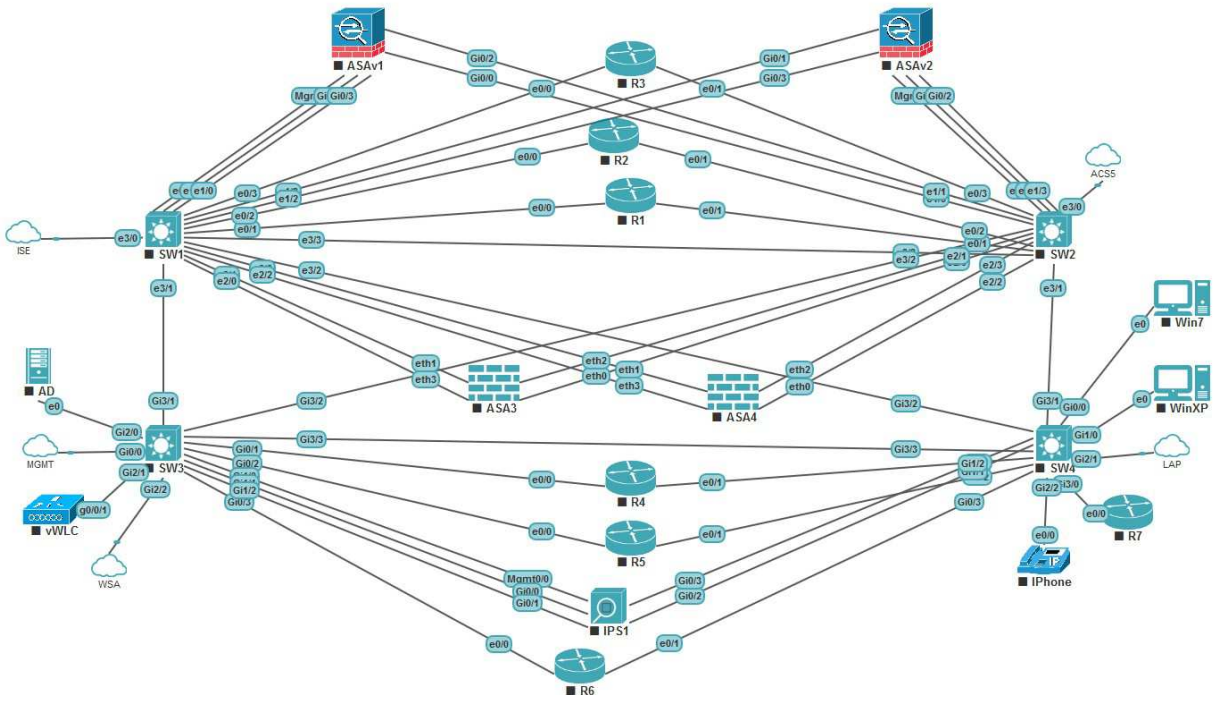


Рисунок 2.5 – Графічний інтерфейс емулятора UNL

Нині емулятор UNetLab є не лише платформою для моделювання віртуальних мереж, але і інструментом для підготовки до різних сертифікацій Cisco (для новачків до CCNA/CCNP, так і для професіоналів для підготовки CCIE Routing and Switching, CCIE Security та ін.). Крім того, UNL використовується в мережевому інженерінзі, у тому числі і для системного підходу у виявленні і усуненні причин проблеми неполадки мереж (troubleshooting) [8].

Проект UNetLab стартував у березні 2014 року, але за такий короткий термін став серйозним конкурентом для таких відомих емуляторів як GNS3 і Cisco Packet Tracer, маючи у своєму багажі ряд величезних переваг. При цьому розробка продукту здійснюється і до цього дня, виявляються помилки і виходять різні оновлення для розширення функціонала програми і списку підтримуваних пристроїв [7].

Використання цього підходу дозволяє UNL відійти від концепції використання автономних віртуальних машин для емуляції відповідних мережевих пристроїв, і створювати цифрові мережеві лабораторії на основі

програмних емуляторів IOU/IOL, Dynamips і вузлів QEMU, об'єднуючи усі необхідні програмні модулі і сценарії у вигляді одного файлу у рамках однієї платформи.

Таблиця 2.2 - Порівняльний аналіз функціональних характеристик платформ

Властивість	**UNetLab**	**GNS3**
Графічний інтерфейс	Зручний єдиний графічний інтерфейс користувача на основі технології WEB автоматично встановлюється разом з платформою.	Графічний інтерфейс користувача у вигляді спеціалізованого клієнта платформи встановлюється користувачем на ПК і окремо від платформи.
Спеціалізоване ПО	Немає необхідності в окремих клієнтах для використання платформи.	Вимагає установки спеціалізованого клієнта для подальшого використання платформи.
Функціо-нальність	Повноцінна підтримка емуляції канального і мережевого рівнів (L2 і L3) без обмежень.	Часткова підтримка емуляції канального і мережевого рівнів (L2 і L3).
Підтримка розрахованого на багато користувачів режиму	Розрахований на багато користувачів функціонал, можливість роботи декількох користувачів одночасно.	Строго розрахована на одного користувача система.
Обмеження ОЗП	Немає обмежень ОЗП під емуляцію QEMU - пристроїв.	QEMU підтримує використання до 2 Гб ОЗУ.
Кількість з'єднань	Відсутність обмежень по кількості з'єднань між пристроями в умовах віртуалізації QEMU.	Обмеження в 16 з'єднань між пристроями у рамках віртуалізації QEMU.
Масшта-бованість	Образи запускаються і працюють у рамках однієї віртуальної машини або фізичного сервера.	Необхідність в створенні окремих віртуальних машин для запуску образів у GNS3.
Нативна підтримка графічних позначень	Інтерфейс користувача забезпечує нативну підтримку призначених для користувача графічних позначень пристроїв.	Підтримка організації власних значень пристроїв частково є присутнім.

Вигідною перевагою емулятора UNetLab є те, що він повністю безкоштовний, і тому може використовуватися не лише для комерційних цілей, але і для навчання звичайними користувачами.

З достоїнств так само слід зазначити можливість запуску необмеженої кількості екземплярів устаткування (роутеров, комутаторів, облаштувань безпеки і так далі), кількість обмежена тільки апаратними можливостями робочого місця.

Підтримка устаткування в UNetLab дуже широка. UNL дає можливість запуску образів з VIRL (vIOS - L2 і vIOS - L3), образів ASA, Cisco IOL - образов, образів Cisco IPS, образів XRv і CSR1000v, образів dynamips з емулятора GNS, образів Cisco vWLC і vWSA. Окрім перерахованих образів підтримується переконливий список з устаткування інших вендоров : Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX virtual, Checkpoint Firewall, HP VSR1000, Juniper Olive (porting), Juniper Networks vMX router, Juniper vSRX, S - Terra Firewall, MS Windows і ін. [15].

Виходячи із загального порівняльного аналізу програмних платформ емулятора мережевого устаткування, можна виділити UNetLab і GNS3 як найбільш актуальні і ефективні. Слід зазначити, що UNetLab порівняно з GNS3 має ряд технічних переваг, за допомогою яких досягається підвищення функціонала і, як результат, розширення портфеля надання послуг в області мережевого проектування. Порівняльний аналіз функціональних характеристик платформ емулятора мережевого устаткування UNL і GNS3 приведений в таблицю 2.1 [4, 6, 7].

Виходячи з аналізу усіх вищеперерахованих програмних продуктів, явним фаворитом є UNetLab, в силу свого безкоштовного поширення, величезного функціонала, великої кількості підтримуваних емульованих пристроїв, а також в зручності створення тестових стендів мережевого устаткування в проектування обчислювальних мереж, саме UNetLab буде вибраний в якості програмного емулятора мережевого устаткування для розробки моделей обчислювальних мереж.

Висновки до розділу

1. Для роботи в мережі використовується широке різноманіття мережевих пристроїв. Проте, найбільшу частку в мережевих рішеннях має обладнання фірми Cisco та Міжмережева Операційна Система Cisco IOS. При розробці складних складених мереж нерідко встає завдання попереднього моделювання такої мережі з метою перевірки використовуваних технічних рішень

2. Виходячи зі складності топології мережі, важливою задачею стає моделювання мережі до початку її впровадження. Для цієї задачі все більше використовуються апаратні та програмні засоби емуляції роботи мережевого обладнання.

3. Серед засобів імітаційного моделювання окремих подій і станів безпровідних сенсорних мереж на базі стандарту IEEE 802.15.4-2006 найбільше поширення отримала наступні середовища: OPNET Modeler; OMNET++; NS-2, Graphical Network Simulator 3, UNetLab.

РОЗДІЛ 3 МОДЕЛІ МЕРЕЖІ ТА ЇЇ ПРИСТРОЇВ

3.1 Модель організації безпечного зв'язку між структурними підрозділами

Як правило, корпоративні мережі характеризуються не лише підвищеними вимогами до безпеки і відмовостійкості системи, але так само і необхідністю організації каналів зв'язку між віддаленими один від одного територіально підрозділами компанії. Можна виділити три основні механізми побудови таких каналів :

- Виділені канали, що орендуються у операторів зв'язку.
- Мережа зв'язку на основі технології VPN (Virtual Private Network)
- Побудова власних мереж зв'язку, що називаються так само технологічним, виділеними.

Немає ніяких перешкод для комбінування описаних вище підходів, використання найбільш доцільного методу в кожній конкретній ситуації.

Побудова власної мережі, або ж оренда каналів у операторів раціонально використати в межах міста – для цього проекту це може бути застосовне для зв'язку між датацентром і головним офісом компанії. Для зв'язку ж з видаленими офісами залишається тільки організація віртуальних з'єднань – ця технологія передбачає побудову корпоративної мережі поверх мереж загального користування, наприклад Інтернету. Захист переданих даних від несанкціонованого доступу повинен здійснюватися за допомогою механізмів шифрування і використання відповідних для побудови таких мереж протоколів. Найбільше поширення отримали протоколи IPSec, PPTP, L2TP, іноді ці протоколи так само інкапсулюються в GRE. Розглянемо протоколи окремо:

- IPSec (IP Security) – набір протоколів для забезпечення захисту переданих даних, що дозволяють здійснювати перевірку цілісності, підтверджена достовірності і шифрування IP-пакетов. Таке саме включає

протоколи обміну ключами. Є «надбудовою» над IP, для роботи досить підтримки стандарту тільки від встановлюючих VPN-тунель пристроїв. Може працювати як в тунельному так і в транспортному режимі. При передачі даних використовуються три основні протоколи: ESP (Encapsulating Security Payload) або AH (Authentication Header), при первинному налаштуванні з' єднання (узгодження шифрування, ключів, взаємної аутентифікації) використовується ISAKMP (Internet Security Association and Key Management Protocol). Стандарт не накладає обмежень на використовувані алгоритми шифрування трафіку і довжину ключа.

- PPTP (Point – to – point Tunneling Protocol) – протокол, що таке саме дозволяє встановити захищене з'єднання поверх громадських ятерів. Встановлюється звичайна PPP сесія з протилежною стороною, кадри PPP інкапсулюються в GRE для передачі до точки призначення. Підтримує 128 і 40 бітове кодування, в цілому вважається менш безпечним чим IPSec. В силу використання двох різних протоколів, у тому числі GRE, є складнощі проходження PPTP трафіку через міжмережеві екрани і трансляцію адреса і портів, що вирішуються включенням механізмів інспекції PPTP пакетів на міжмережевому екрані. Повноцінна підтримка протоколу PPTP реалізована у більшості популярних призначених для користувача операційних систем, але відсутній у частини виробників мережевого устаткування.

- L2TP (Layer 2 Tunneling Protocol) – протокол тунелювання іншого рівня, який може працювати не лише в IP-сетях. Є протоколом сеансового рівня, сумісний з IPSec.

- GRE (Generic Routing Encapsulation) – протокол використовуваний для передачі пакетів однієї мережі через іншу ятір. Тунель представляє з собі з' єднання точка-точка, і може розглядатися як різновид VPN з' єднання без шифрування. Для забезпечення захисту переданих по такому тунелю даних від несанкціонованого доступу вимагається використати поверх тунелю інші механізми шифрування, наприклад IPSec в транспортному режимі.

З розглянутих варіантів для встановлення постійних каналів зв'язку між офісами поверх громадський ятерів найбільш відповідним є IPSec – це стандартний протокол, підтримуваний більшістю виробників мережевого устаткування і не обмежуючий адміністратора у виборі алгоритму шифрування переданих даних. Таке саме на вибір використовуваного для вирішення завдання протоколу значне обмеження накладає вже існуюча інфраструктура у видалених офісах і датацентрах – канали у більшості своїй будуються на основі технології IPSec в тунельному режимі і супутнього криптографічного устаткування.

3.2 Топології побудови корпоративної мережі

Визначившись з протоколами і стандартами, на основі яких буде будується мережа головного офісу, – 802.11, ethernet, TCP/IP, відразу ж вимагається розглянути і вибрати відповідне рішення по структурі безпровідної мережі.

Мережа на основі стандарту 802.11 може бути організована по одній з трьох топологий:

- **BSS** (Basic Service Sets) – група працюючих за стандартом 802.11 станцій, з центральним пунктом зв'язку – точкою доступу. Клієнтські станції не зв'язуються один з одним, відправляючи увесь трафік точці доступу, яка у свою чергу доставляє кадри адресатові.
- **IBSS** (Independent Basic Service Sets) – децентралізована, ad – hoc топологія. Відсутній центральний вузол зв'язку, безпровідні станції передають трафік, зв'язуючись безпосередньо один з одним. Розподіл часу в течії якого віщає кожна станція так само відбувається децентрализовано.
- **ESS** (Extended Service Sets) – об'єднання декількох інфраструктур BSS з метою збільшення зони покриття і розподілу мережевого трафіку. Для з'єднання між BSS використовується незалежний

канал, який може бути як безпровідним, так і дротяним.

Для здійснення цілей проекту підходить тільки остання з перерахованих топологій, оскільки у випадку з BSS одна загальна точка доступу є єдиною точкою відмови, фізично не може забезпечити покриття в усій будівлі, а так само має на увазі під собою ділення пропускної спроможності між усіма підключеними абонентами. IBSS так само не підходить із-за топології мережі, відсутності централізованого керування, низької швидкості передачі даних (не більше 11Мбит/із згідно із стандартом 802.11), що динамічно міняється, і слабкою захищеністю – єдиний підтримуваний спосіб шифрування WEP.

Визначившись з топологією, необхідно розглянути можливі варіанти об'єднання безлічі точок доступу в єдину систему. Точки доступу можуть бути:

1) Автономні (децентралізовані, «розумні»). Автономні точки доступу повністю самостійно відповідають за доставку трафіку абонентів, застосування політик безпеки, моніторинг ефіру і вибір каналу.

2) Працюючі під керуванням контролера безпровідної мережі (так звані lightweight AP, «легковагі»). Можливо як рішення в якому увесь трафік безпровідних користувачів спочатку передається точкою доступу контролеру, так і підхід при якому контролер здійснює тільки контроль за одноманітністю налаштувань фактично автономних точок доступу.

Так само, стандарт 802.11 не дає вказівок за способом організації і керування радіоканалами, тому має місце бути як використання точками доступу для роботи статично заданих діапазонів частот, так і динамічне налаштування каналу.

Перевага автономних точок доступу очевидна – відсутність єдиної точки відмови (контролера безпровідної мережі), відсутність в мережі надмірного трафіку, що управляє, між контролером і точками доступу. Це рішення прекрасно підходить для невеликих проектів.

Проте, коли з'являється необхідність в загальній конфігурації і політиці безпеки для безлічі точок доступу, узгодженні каналів кожної з точок доступу, автоматичній реакції на інтерференцію, розгортанні додаткових сервісів – таких як, наприклад, визначення місця розташування абонентів – набагато ефективніше використати рішення на основі зв'язки «легковагих» точок доступу і контролера безпровідної мережі. Головну проблему цього підходу можна усунути використовуючи декілька контролерів і механізми резервування.

Може відрізнятися поклад від завдання і спосіб з'єднання точок між собою – це може бути безпровідним канал зв'язку (так саме реалізований за стандартом 802.11, але в іншому частотному діапазоні) – така побудова БЛВС таке саме часто називають mesh, або локальна ятір. Точки доступу підтримують mesh-сети, значно дорожче, складніше в конфігурації – особливо якщо коштує вимога відмовостійкості. Зазвичай безпровідною канал зв'язку використовується при організації БЛВС за межами будівель, в місцях де використання дротяної мережі неможливе або недоцільне. Для офісної мережі цілком підійде підключення точок через загальну локальну ятір на основі Ethernet.

3.3 Моделі вузлів мереж

3.3.1 Модель OPEN-ZB

Модель реалізує фізичний рівень і рівень доступу до середовища, і відповідає стандарту IEEE 802.15.4. Версія моделі 2.1 підтримує тільки топологію зірка, де комунікації відбуваються між кінцевими пристроями через центральний пристрій, що називається координатором приватної мережі.

У моделі версії 2.1 існує два типи вузлів :

1) wpan_analyzer_node - вузол, який збирає глобальні для приватної мережі статистичні дані;

2) wpan_sensor_node - вузол, який реалізує протоколи зв'язку стандарту IEEE 802.15.4-2003

Структура вузла-сенсора, використана в моделі, полягає і чотирьох функціональних блоків (мал. 12) :

1. Фізичний рівень складається з радіопередавача (tx) і приймача (rx), які відповідно до специфікації IEEE 802.15.4 працюють на частоті 2,4 ГГц із швидкістю обміну даними 250 Кбит/сек. Потужність передавача встановлена в 1мВт з модуляцією QPSK (Quadrature Phase Shift Keying). Фізичний рівень реалізований за допомогою вже існуючого в OPNET Modeler безпровідного модуля з вказівкою параметрів, що відповідають стандарту IEEE 802.15.4.

Рисунок 3.1 – Модель OPEN-ZB 2.1

2. Рівень доступу до середовища реалізує алгоритм CSMA/CA з фіксованими тимчасовими слотами очікування передачі (slotted CSMA/CA) і механізм гарантованих тимчасових слотів (GTS). GTS трафік (тобто трафік чутливий до швидкості доставки) приходить від рівня додатка зберігається у буфері певної місткості і передається в мережу, коли відповідний часовий слот активний. Нечутливі до часу доставки кадри даних зберігаються в необмеженому буфері і передаються в мережу впродовж періоду активної конкуренції, відповідно до алгоритму CSMA/CA з фіксованими тимчасовими слотами очікування передачі. Цей рівень також може генерувати кадри маркери для синхронізації пристроїв в мережі, якщо вузол працює в режимі координатора.

3. Рівень додатка - складається з двох генераторів трафіку (Traffic Source і GTS Traffic Source) і одного одержувача (Traffic Sink). Джерело звичайного трафіку (Traffic Source) генерує кадри даних з прапором підтвердження доставки і без, які передаються впродовж періоду конкурентного доступу (CAP). Джерело трафіку (GTS Traffic Source) з гарантованими тимчасовими слотами, може використовуватися для створення кадрів даних з прапором підтвердження доставки і без, які чутливі до затримок в мережі. Модуль одержувача приймає кадри від нижніх рівнів і рахує мережеву статистику.

4. Модуль батареї - обчислює споживаний рівень енергії, що залишився. Значення за умовчанням для моделі встановлені відповідно до специфікації MICAz.

Модель досить добре документована, продовжує допрацьовуватися і підтримуватися. Детальніша характеристика моделі приведена в технічному описі.

У версії, що нещодавно вийшла, 3.0 (beta) також реалізовані наступні функції:

- Мережевий рівень ZigBee;
- Ієрархічна маршрутизація по дереву ZigBee;

- Перевірка адрес вузлів для підтримки адресної схеми дерева кластерів ZigBee.

3.3.2 Вбудована в OPNET модель ZigBee

Вбудована в OPNET Modeler 14.0 реалізує не лише фізичний рівень і рівень доступу до середовища стандарту IEEE 802.15.4-2006, але і мережевий рівень ZigBee. Модель підтримує топології: зірка, дерево, і комірчаста мережа.

Модель містить три типи вузлів відповідно до специфікації ZigBee :

1. Координатор (Coordinator);
2. Маршрутизатор (Router);
3. Кінцевий пристрій (End Device).

Структура вузла-сенсора, використана в моделі, представлена чотирма функціональними блоками (рис.2.3) :

1. Фізичний рівень складається з радіо передавача (wireless_tx) і приймача (wireless_rx), які відповідно до специфікації IEEE 802.15.4-2006 можуть працювати на частотах 868МГц, 915 Мгц і 2,4 ГГц. Фізичні характеристики мережі задаються на координаторові. Потужність передавача встановлена в 5мВт.

2. Рівень доступу до середовища реалізує алгоритм CSMA/CA без фіксованих тимчасових слотів очікування передачі, і частину інших функції цього рівня відповідно до стандарту IEEE 802.15.4.

3. Мережевий рівень реалізує функції відповідно до специфікації ZigBee. Початковий код блоку недоступний, поставляється у виді, що компілює.

4. Рівень додатка дозволяє генерувати трафік і ініціювати пошук і приєднання до мережі. Початковий код блоку недоступний, поставляється у виді, що компілює.

Рисунок 3.2 – Вбудована модель OPNET Modeler 14.0

3.3.3 OMNeT++ (Objective Modular Network Testbed in C++)

OMNeT++ - середовище імітаційного моделювання дискретних подій і станів з відкритим початковим кодом, заснована на компонентах, яка стає усе більш популярною. Основна сфера застосування - моделювання мереж передачі даних, ИТ систем і бізнес процесів. Компоненти OMNeT++ написані на C++.

На базі середовища моделювання OMNeT++ 4.1 побудований симулятор різних протоколів безпровідних сенсорних мереж Castalia (поточна версія 3.1). У нім також реалізована модель що відповідає стандарту IEEE 802.15.4.

На базі даного середовища моделювання існують бібліотеки INETMANET і MiXiM, які дозволяють створювати моделі безпровідних сенсорних мереж, але на даний момент готові моделі відсутні.

3.3.4 Castalia

Castalia - симулятор мереж, який орієнтований на мережі з низьким енергоспоживанням. Особливістю цього симулятора є те, що не тільки створені моделі рівнів передачі даних, але і моделюються фізичні процеси, дані про яких збираються у вузлах. В результаті виходить, що безпровідні сенсори пов'язані між собою не лише безпровідними каналами зв'язку, але і фізичним процесом параметри якого вони вимірюють.

Внутрішня структура вузла представлена на рис.3.3. Суцільні стрілки означають проходження повідомлень між модулями, а пунктирні - інтерфейс між ними з викликом простих функцій.

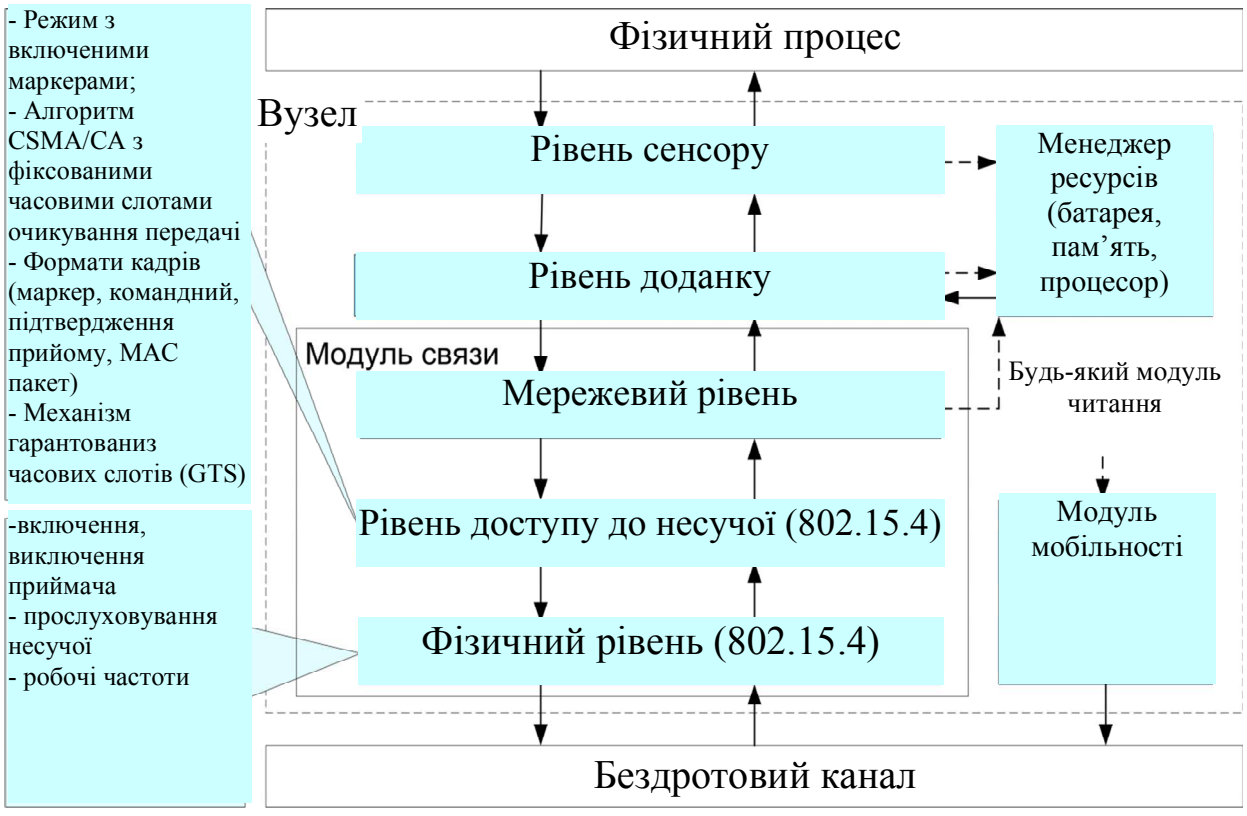


Рисунок 3.3 – Внутрішня структура вузла в середовищі Castalia

Модель вузла представлена наступними модулями:

1. Модуль управління сенсорами - дозволяє генерувати реальніший трафік у БСМ, ніж просто використання генераторів пакетів даних, пропонованих іншими моделями.

2. Модуль додатка найчастіше використовується користувачами симулятора для реалізації тестованих алгоритмів. У симуляторі вже існує декілька простих модулів додатка. Наприклад, додаток оцінки пропускної спроможності мережі.

3. Модуль зв'язку - складається з трьох рівнів:

- Мережевий рівень - дозволяє реалізувати різні алгоритми маршрутизації у безпровідній сенсорній мережі. На даний момент є готові прості алгоритми маршрутизації (наприклад, маршрутизація по дереву).

- Рівень управління доступом до середовища, у тому числі IEEE 802.15.4. У версії 3.1 реалізована основна частина завдань рівня, описана в стандарті IEEE 802.15.4-2006.

- Фізичний рівень. Розробники Castalia приділили особливу увагу моделюванню фізичного рівня безпровідного сенсора. У симуляторі вже задані параметри наступних модулів : Mica2_CC1000 і TelosB_CC2420.

4. Модуль мобільності - зберігає положення інших вузлів в мережі і надає дані про положення вузла моделі радіоканалу.

5. Модуль управління ресурсами управляє різними ресурсами вузла і найбільш важливим з них - споживаною енергією.

6. Модель радіоканалу враховує середні втрати при поширенні, зміни сигналу в часі, інтерференцію. Також є можливість використати модель ідеального радіоканалу.

3.4 Процес моделювання обчислювальних мереж в середовищі UNetLab

Для запуску UNetLab необхідно створити віртуальну машину, на якій і буде розгорнута наша система. Для створення віртуальної машини використовувалося Microsoft Virtual PC. Цей програмний продукт віртуалізації дозволяє встановити на фізичний комп'ютер одну або декілька віртуальних машин. Процес розгортання UNetLab відбувається шляхом установки початкових файлів на створеній віртуальній машині. Після завершення установки, UNetLab готовий до роботи і стає доступний по IP - адресі, вказаній в ході інсталяції.

Процес моделювання в UNetLab відбувається в графічному інтерфейсі програми, який стає доступний через веб-браузер. Користувачеві необхідно перейти по веб-адресі у браузері, на якому було розгорнуто програмне забезпечення. Після чого, він побачить наступне вікно аутентифікації користувача, зображеного на рис. 3.5.

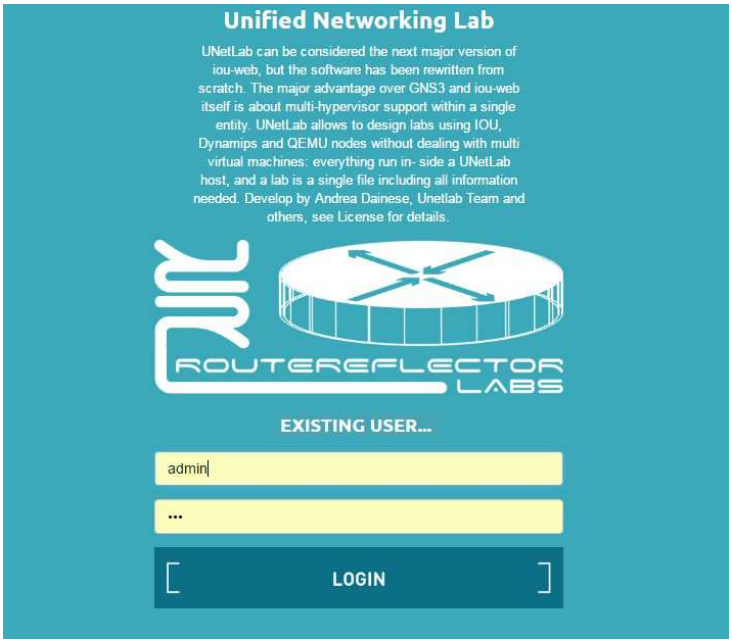


Рисунок 3.4 – Аутентифікація користувача в системі UNetLab

Після успішної аутентифікації, користувач побачить наступне меню, рис.3.6. На якому відображений список усіх проектів і панель управління. За допомогою панелі управління можна управляти вже створеними проектами (видаляти, перейменовувати, переміщати, імпортувати), так і створювати нові. Так само, в меню "Users" можна створити нового користувача системи і призначити йому права.

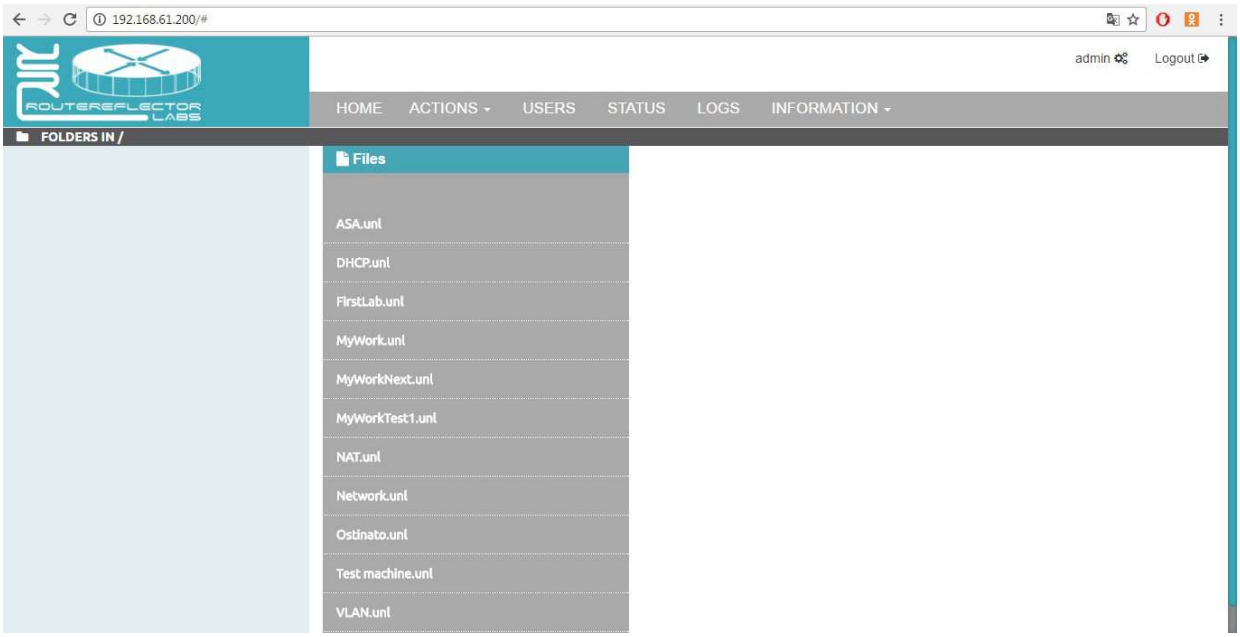


Рисунок 3.5 - Головне меню системи UNetLab

У меню "Status", рис.3.7, можна проглянути поточну статистику використовуваних ресурсів системою (завантаження ЦП і ОЗП, кількість використовуваної пам'яті і так далі) і кількість запущених образів.

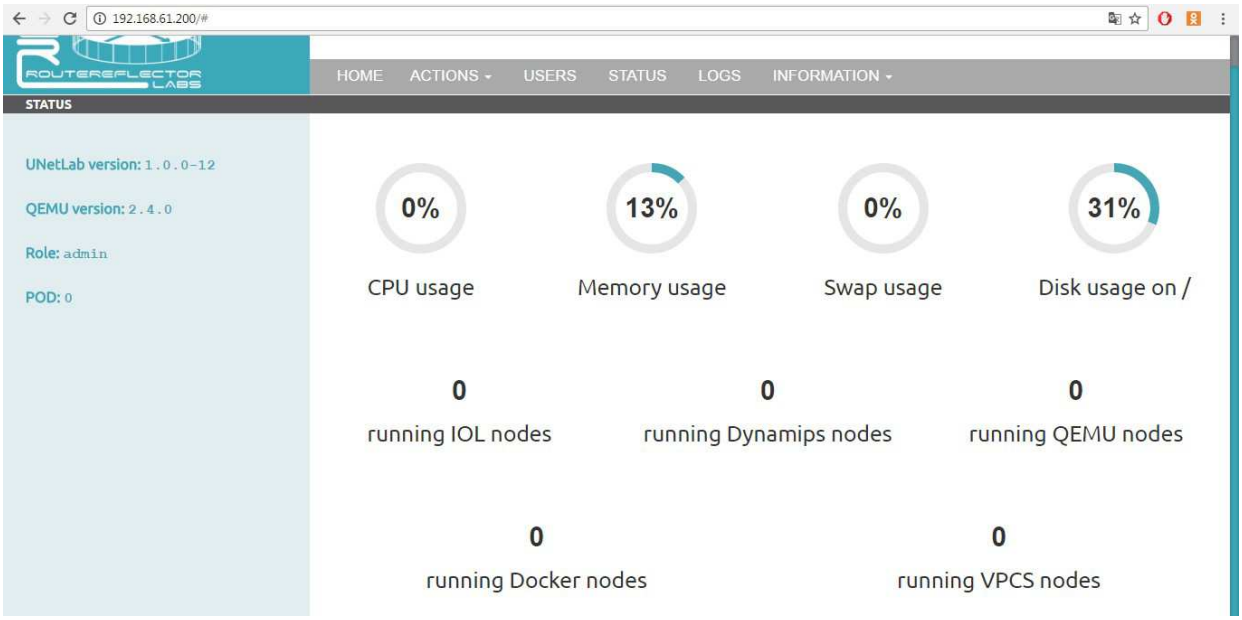


Рисунок 3.6 – Інформація про використовувані ресурси системою UNetLab

Створивши новий проект, користувач потрапить на вікно робочого місця, рис.3.8. Проектування майбутніх обчислювальних мереж відбувається шляхом додавання мережевих пристроїв на робочу область.

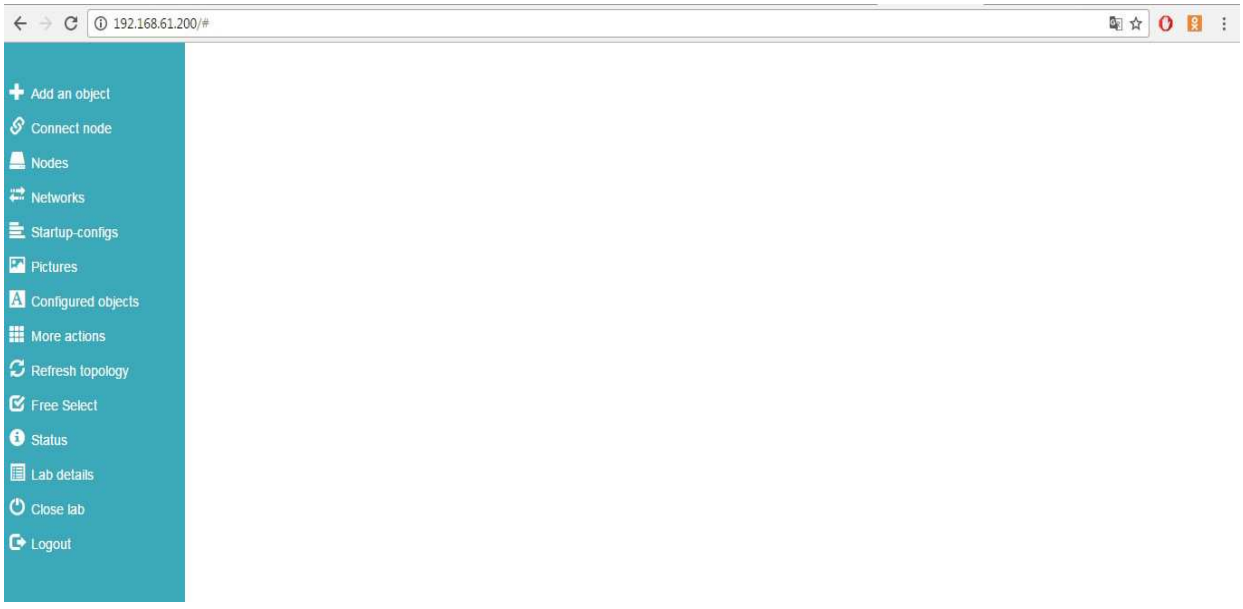


Рисунок 3.7 – Робоче місце в UNetLab

У вкладці "Add an object" користувачеві доступний список мережевих облаштувань різних виробників. Вибравши конкретний пристрій, з'являється

можливість завдання характеристик пристрою : завдання імені, вибір емульованого образу пристрою, об'єм оперативної і флэш пам'яті, кількість груп Ethernet портів (у кожній групі по 4 Ethernet порту) і так далі, рис.3.9. Система надає можливість користувачеві самому настроїти вибраний мережевий пристрій. На прикладі облаштувань компанії Cisco, користувач вибирає емульований образ мережевого пристрою, який емулює програмну оболонку пристрою (Cisco IOS) і шляхом завдання параметрів, сам конфігурує майбутній фізичний пристрій. Таким чином, варіюючи параметрами, користувач може імітувати роботу різних, реальних пристроїв.

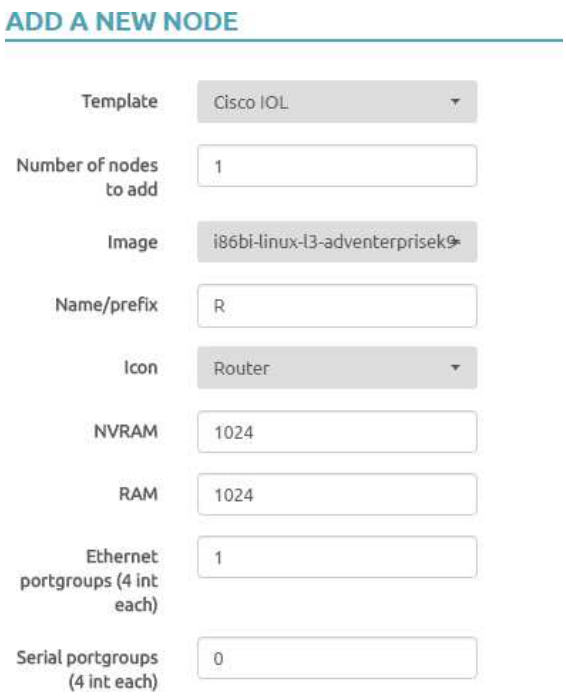


Рисунок 3.8 – Конфігурація пристрою, що додається

Після того, як пристрій заданий, воно відображається на робочому полі. Таким чином, користувач, додаючи на робоче поле мережеві пристрої, конфігурує майбутню архітектуру обчислювальної мережі.

Для зв'язку пристроїв між собою необхідно вибрати пункт в меню "Connect node" і з'єднати необхідні пристрої між собою, таким чином зімітувати фізичне підключення між ними.

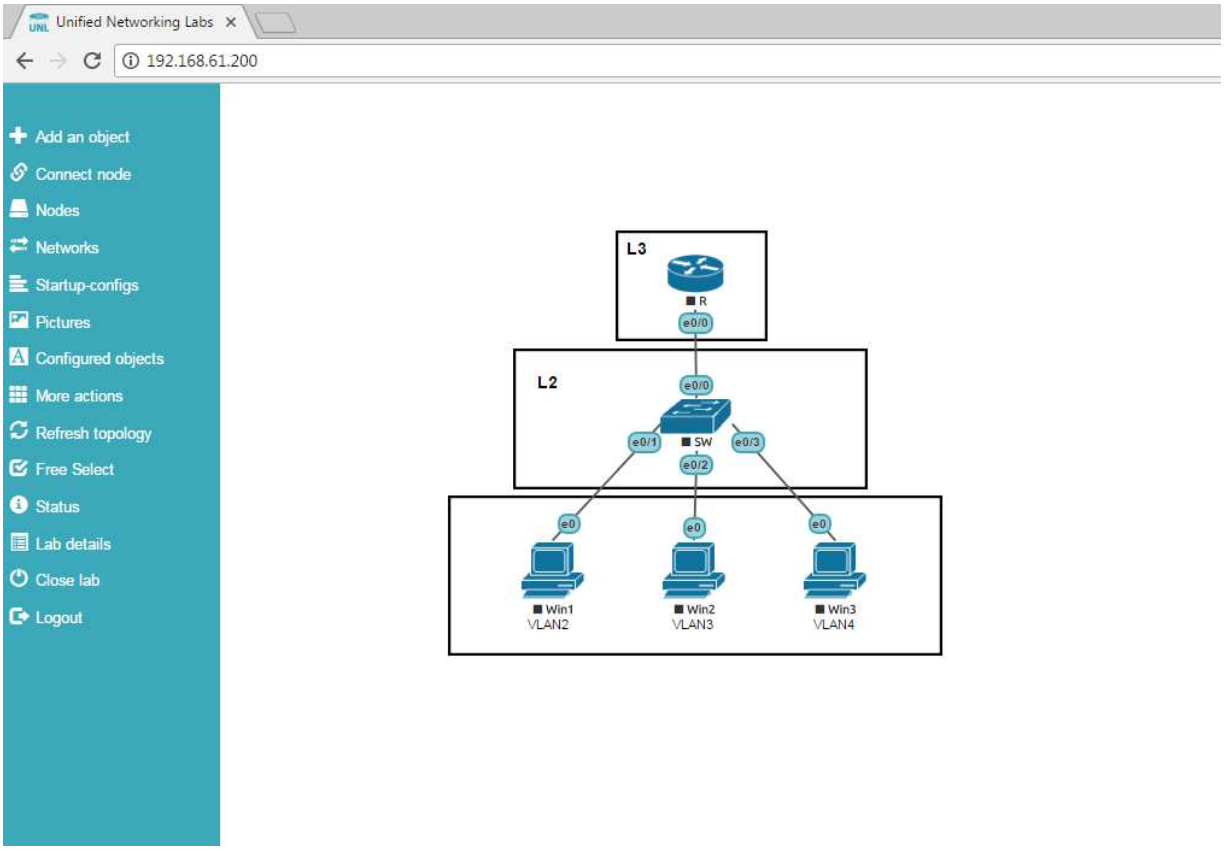


Рисунок 3.9 – Створення моделі обчислювальної мережі

Так само користувачеві доступне додавання різних об'єктів на робоче поле, таких як: геометричні об'єкти, зображення, написи і їх настоянка, для організації моделей обчислювальних мереж.

Для налаштування і конфігурації доданих на робоче поле пристроїв, в UNetLab вбудовано ПО PuTTY. PuTTY - це клієнт для видаленого доступу до пристроїв. Після запуску пристрою, якщо натиснути на нього лівою кнопкою миші, то відбувається автоматичне підключення до консолі пристрою через PuTTY, в якому користувач робить налаштування пристрою.

Також, в UNetLab вбудовано додатково ПО WireShark, що є програмою-аналізатором трафіку, за допомогою якої можна перехоплювати і аналізувати мережевий трафік (переглядати вміст мережевих пакетів) того, що протікає між пристроями при їх взаємодії.

3.5 Сучасні технології, що застосовуються для моделей мереж

У розроблених раніше концепціях було сформульовано безліч різних завдань, від логічного розбиття на підмережі, формування IP - адрес, для можливості роботи в мережі, створення повідомляючих тунелів до можливості виходу в мережу Інтернет робочих станцій підприємства. Крім того, для коректного функціонування обчислювальної мережі, необхідно маршрутизувати увесь протікаючий трафік усередині мережі для можливості мережевої взаємодії між комп'ютерами компанії. Для досягнення усіх цих завдань, а також завдань по підвищенню відмовостійкості і захисту інформації, що протікає по повідомляючих тунелях, необхідно використати різні мережеві протоколи, за допомогою яких і буде організована уся робота усередині обчислювальної мережі.

Розглянемо ці технології детальніше.

3.5.1 VLAN

Для вирішення завдання логічної структуризації мережі використовуватиметься технологія VLAN (Virtual Local Area Network, віртуальна локальна мережа) — це технологія, що дозволяє на одному фізичному мережевому інтерфейсі створювати декілька віртуальних локальних мереж, таким чином, розбивай мережу на логічні підмережі [13]. Технологія дозволяє пристроям діяти так між собою, хоча фізично вони можуть бути підключені до різних мережевих комутаторів.

Відмітимо основні достоїнства цієї технології :

- **Гнучке розділення пристроїв на групи** як правило, одному VLAN відповідає одна підмережа. Комп'ютери, що знаходяться в різних VLAN, будуть ізольовані один від одного;
- **Зменшенням широкомовного трафіку в мережі** Кожен VLAN є окремий широкомовний домен. Широкомовний трафік не транслюватиметься між різними VLAN;

- **Збільшення безпеки і керованості мережі** в мережі, розбитій на віртуальні підмережі, зручно застосовувати політики і правила безпеки для кожного VLAN. Політика буде застосована до цілої підмережі, а не до окремого пристрою;

- **Зменшення кількості устаткування і мережевого кабелю** для створення нової віртуальної локальної мережі не потрібно купівля комутатора і прокладення мережевого кабелю [12].

3.5.2 DHCP

Для роботи комп'ютера в мережі йому потрібний IP-адрес. Привласнення IP - адреси комп'ютеру може бути зроблено як статичним методом (ручне завдання IP-адреса користувачем), так і динамічно (автоматичне привласнення IP-адреса). Оскільки в нашій мережі кількість робочих станцій може обчислюється десятками, то безперечно необхідно використати саме другий спосіб.

DHCP (Dynamic Host Configuration Protocol — протокол динамічного налаштування вузла). Технологія DHCP дозволяє комп'ютерам автоматично отримувати IP-адрес і інші параметри, необхідні для роботи в мережі. Цей протокол працює по моделі «клієнт-сервер», де клієнтом виступає комп'ютер, запитуючи у DHCP-сервера конфігурації для роботи в мережі [5]. Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережевого пристрою звертається до так званого сервера DHCP і отримує від нього потрібні параметри. Мережевий адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі і зменшує кількість помилок.

3.5.3 EIGRP

Для коректного функціонування обчислювальної мережі, необхідно маршрутизувати увесь протікаючий трафік усередині мережі для можливості мережевої взаємодії між комп'ютерами. Маршрутизація - це процес визначення маршруту в мережі [4].

Маршрутизація буває 2 видів:

- статична маршрутизація;
- динамічна маршрутизація.

При статичній маршрутизації маршрути задаватимуться адміністратором мережі. Цей вид маршрутизації дуже зручний для реалізації маленької мережі, але непрактичний у великій мережі, оскільки усі маршрути задаються при конфігурації маршрутизатора. Мережа, побудована на статичній маршрутизації, є нестійкою, а також погано масштабованою. Цей вид маршрутизації дуже неефективний для реалізації обчислювальної мережі для підприємства, що розвивається [12].

У мережі, налагодженій за допомогою динамічної маршрутизації, таблиця маршрутизації редагується програмно, тобто здійснення динамічної маршрутизації відбувається за рахунок протоколів маршрутизації.

EIGRP (Enhanced Interior Gateway Routing Protocol) — це протокол динамічної маршрутизації, розроблений фірмою Cisco Systems в 1994 році. Принцип робота протоколу полягає в трьох основних кроках. Спочатку маршрутизаторами відбувається виявлення сусідніх пристроїв, потім відбувається обмін топологічною інформацією між сусідами і у кінці маршрутизатори аналізують отриману інформацію і вибирає з неї маршрути з найменшою метрикою до кожної мережі [6, 8].

Після того, як ці три етапи будуть виконані, в маршрутизаторі зберігатиметься 3 таблиці: таблиця сусідніх пристроїв; таблиця топології, отримана від сусідніх пристроїв; таблиця маршрутизації, з оптимальними маршрутами до усіх відомих підмереж.

3.5.4 NAT

Для вирішення завдання доступу в мережу Інтернет облаштуванням компанії, через виділений IP-адрес провайдером, використовуватиметься технологія NAT. NAT (Network Address Translation — «перетворення мережевих адрес») це технологія в TCP/IP мережах, за допомогою якого

декілька комп'ютерів або облаштувань приватної мережі (з приватними адресами з таких діапазонів, як 192.168.x.x, 172.x.x.x) можуть спільно користуватися однією адресою IPv4, що забезпечує вихід в глобальну мережу [7]. Головна причина зростаючої популярності NAT пов'язана з дефіцитом адрес протоколу IPv4, що усе більш загострюється, — поточного протоколу інтернету.

Відмітимо основні достоїнства цієї технології :

- **Економія публічних IP-адресів**
  через одну адресу, можна випустити більше 65000 сірих адрес;
- **Перешкоджає зовнішнім з'єднанням доходити до кінцевих комп'ютерів**
  якщо ззовні на облаштування с включеною технологією NAT приходить пакет, який не дозволений, він просто відкидається;
- **Приховує від сторонніх очей внутрішню структуру мережі** при трасуванні маршруту ззовні, нічого далі пристрою з включеним NAT доступно не буде;
- **Зменшення кількості устаткування і мережевого кабелю** для створення нової віртуальної локальної мережі не потрібно купівля комутатора і прокладення мережевого кабелю [5, 6].

3.5.5 STP

Для вирішення завдання відмовостійкого доступу до сервера, відображеного в останній концепції, використовуватиметься мережевий протокол STP, а саме його поліпшена версія RSTP, версія протоколу STP з прискореною реконфігурацією топології.

STP (Spanning Tree Protocol, протокол остовного дерева) — основне завдання STP — запобігти появі петель на канальному рівні. Робота протоколу полягає у блокування дублюючого маршруту, тим самим запобігаючи появу петель [8]. У нашій концепції робота протоколу полягатиме в "резервуванні" одного маршруту до сервера. При виникненні

несправності в одному з діючих маршрутів ведучого до сервера, він буде продубльований зарезервованим маршрутом, в інший час, "зарезервований" маршрут буде заблокований, щоб уникнути петель в топології [4, 7].

3.5.6 VPN/GRE/IPsec

Завдання створення повідомляючого тунеля між територіально віддаленими філіями, для можливості мережевої взаємодії, не тривіальне і має різні варіанти рішення. У запропонованих, в главі 2.3, концепціях було запропоновано різне рішення цієї задачі.

Перше, це створити повідомляючий тунель між маршрутизаторами філій, друге - це створення двох повідомляючих тунелів, один з яких знаходитиметься в резервному стані і використовуватиметься тільки при виникненні несправності основного.

Крім того, оскільки ці повідомляючі тунелі виходитимуть за рамки внутрішньої мережі і проходитимуть через мережу Інтернет, виникає необхідність захисту протікаючої інформації, від сторонніх користувачів, по таких тунелях.

Для вирішення першого завдання використовуватиметься технологія VPN.

VPN (Virtual Private Network — віртуальна приватна мережа) — технологію, яка використовується для організації постійного двостороннього каналу між двома офісами, при цьому не потрібно установка якогось додаткового програмного забезпечення.

Використання Інтернету як каналу зв'язку між основними філіями є економічно ефективною альтернативою дорогих орендованих приватних ліній [1, 13].

Технологія VPN має на увазі використання складного шифрування переданих по тунелю даних для забезпечення безпеки і запобігання їх перехопленню.

Шифрування тих, що протікають по VPN тунелю відбуватиметься по мережевому протоколу захищеного доступу IPSec.

IPsec (скорочення від IP Security) —протоколи для забезпечення захисту даних, що передаються по протоколу IP. Він призначений для аутентифікації, тунелювання і шифрування IP-пакетів. IPSec прозорий і дуже зручний тим, що може працювати практично в усіх мережах. Протокол IPSec передбачає стандартні методи ідентифікації, стандартні способи шифрування, а також стандартні методи обміну і управління ключами шифрування між кінцевими точками [6, 9].

Таким чином, для вирішення першого завдання по створенню захищеного повідомляючого тунелю буде створений VPN тунель з шифруванням даних протоколом IPSec.

Оскільки друге завдання має на увазі наявність двох повідомляючих тунелів і автоматичної їх конфігурації у разі відмови одного з них, то для вирішення завдання відмовостійкого тунелю використовуватиметься вже раніше описаний протокол EIGRP.

Проте, оскільки робота протоколу EIGRP ґрунтується на широкомовній розсилці пакетів на етапі виявлення найближчих сусідів, то вже раніше описаний протокол побудови повідомляючого тунеля VPN не підходить для вирішення цього завдання, одного з особливості роботи протоколу VPN полягає в непропусканні широкомовного трафіку. Тому, для побудови повідомляючого тунеля для вирішення другого завдання використовуватиметься протокол GRE.

GRE (Generic Routing Encapsulation — загальна інкапсуляція маршрутів) протокол туннелирования мережевих пакетів, розроблений компанією Cisco Systems. Цей протокол використовується для передачі пакетів однієї мережі, через іншу. GRE тунель є з'єднанням точка — точка і його можна вважати одним і різновидів VPN-тунеля, без шифрування даних.

Основна перевага GRE - це можливість передачі широкомовного трафіку, що дозволяє пропускати через створений тунель протоколи

маршрутизації, що використовують його [1, 7]. Таким чином, для вирішення другого завдання, по побудові відмовостійких повідомляючих тунелів, використовуватиметься протокол GRE з протоколом динамічної маршрутизації EIGRP.

Оскільки протокол GRE, на відміну від VPN, за умовчанням не вимагає шифрування даних, що протікають по тунелю, то необхідно додатково настроїти його. Для цього використовуватиметься вже раннє згаданий набір протоколів для забезпечення захисту даних IPSec. У результаті, будуть створені 2 повідомляючих GRE тунеля з динамічною маршрутизацією EIGRP і захищених за допомогою IPSec.

Висновки до розділу

1. Проектування мережі базується на виконанні декількох етапів проектування. На початку приймається рішення щодо технології безпечного зв’язку між структурними вузлами. Наступним кроком є обрання топології крупних частин мережі: BSS, IBSS, ESS. Третім кроком є розгляд можливих варіантів об'єднання безлічі точок доступу в єдину систему, згідно стандарту 802.11

2. Оскільки бездротові елементи можуть підключатись та відключатись до координатора мережі, то розглянуто моделі бездротових пристроїв. Для цього розглядаються моделі OPEN-ZB 2.1; модель OPNET Modeler 14.0; Castalia. Моделі в цих середовищах володіють достатньо потужним набором параметрів, включаючи як протоколи фізичного рівня, так і протоколи мережевого рівня. Підтримуються робота з такими режимами модулів, як режим з включеними маркерами; алгоритм CSMA/CA з фіксованими часовими слотами очікування передачі; формати кадрів (маркер, командний, підтвердження прийому, MAC пакет); Механізм гарантованих часових слотів (GTS) та інші властивості модулів як пам’ять, батарея.

3. Розглянуто створення робочого середовища в UNetLab від Cisco. Потужне середовище моделювання підтримує роботу з Cisco IOS і шляхом завдання параметрів, сам конфігурує майбутній фізичний пристрій. Таким чином, варіюючи параметрами, користувач може імітувати роботу різних, реальних пристроїв Cisco. Застосування такого рішення дозволяє не тільки створити мережу, а також і використати сучасні технології – VLAN, DHCP, EIGRP, NAT, STP, VPN, GRE, IPsec.

РОЗДІЛ 4 ПРОЕКТУВАННЯ ТА МОДЕЛЮВАННЯ РОБОТИ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

4.1 Застосування принципу модульності

Одним з головних принципів в архітектурі обчислювальних мереж є принцип модульності. Принцип модульності має на увазі те, що усю архітектуру обчислювальної мережі можна розбити на окремі модулі, що, у свою чергу, дозволяє зосередитися на функціоналі кожного модуля окремо, при цьому, такий підхід спрощує її впровадження і управління.

Розбиття великої мережі на маленькі модулі сприяє, в першу чергу, стійкості мережі, оскільки при виникненні неполадок або збоїв в мережі можна локалізувати наявну проблему. При цьому інші модулі мережі, які працюють стабільно, не зачіпаються. Ще однією перевагою модульності мережі є можливість спрощеної і безболісної масштабованості, яка досягається за рахунок введення додаткових модулів при виникаючій необхідності розширення обчислювальної мережі [1].

У архітектурі мереж використовується ієрархічна модель мережі, зображена на рис.4.1, яка уперше була запропонована інженерами компанії Cisco Systems. Згідно цієї моделі обчислювальна мережа підрозділяється на три рівні ієрархії, кожен з яких виконує свою певну функцію [3]. До рівнів ієрархічної моделі відносяться: рівень доступу (Access Layer), рівень розподілу (Distribution Layer) і рівень ядра або ядро мережі (Core Layer).

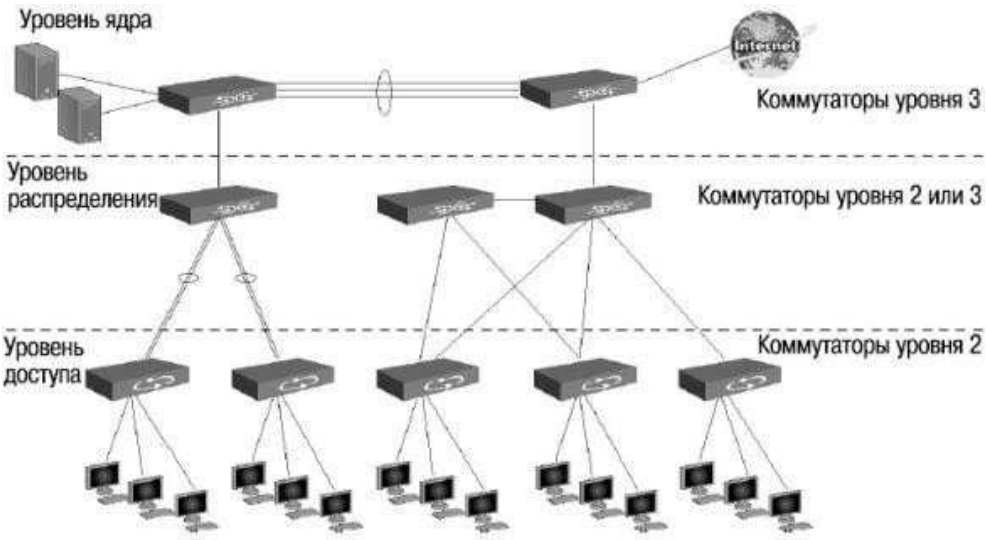


Рисунок 4.1 – Трирівнева ієрархія обчислювальної мережі [3, 12, 13]

На рівні доступу (Access Layer) надається доступ до ресурсів мережі користувачам або пристроям, таким як сканер, принтер, IP-телефони та ін. Таким чином основне завдання цього рівня - це створення точок входу користувачів в об'єднану мережу. Рівень доступу частенько представлений в мережі комутаторами другого рівня мережевій моделі OSI (Open System Interconnection), в окремих випадках використовуються L3-комутатори [3, 12, 13].

Наступним рівнем є рівень розподілу (Distribution Layer), основною функцією якого є агрегація рівнів доступу і рішення завдань маршрутизації. На цьому рівні використовуються облаштування третього рівня L3 - комутатори (маршрутизатори), що здійснюють маршрутизацію різного трафіку між різними сегментами мережі. Також на рівні розподілу виконуються функції фільтрації і доступу до глобальних мереж. Об'єднання комутаторів в одну мережу дозволяє зменшити кількість з'єднань [2, 7, 8].

Рівень ядра (Core Layer) використовується, як правило, у великих мережах, що об'єднують декілька офісів або будівель. Цей рівень відповідає за швидку і своєчасну передачу великих об'ємів трафіку. Крім того, слід зазначити, що рівень ядра об'єднує рівні розподілу, тому відмовостійкість

цього рівня має важливе значення. Помилка на рівні ядра впливатиме на усіх користувачів мережі. Ядро мережі є сукупністю потужних комутаторів і маршрутизаторів.

При побудові обчислювальної мережі окрім ієрархічної структури мережі треба керуватися наступними основними принципами:

- обчислювальна мережа має бути мультисервісною, що припускає передачу усіх типів трафіку, використовуючи єдині канали;
- обчислювальна мережа повинна будуватися на базі відкритих стандартів і інтерфейсів з метою забезпечення можливості нарощування мережі і об'єднання її з іншими мережами;
- принцип мінімізації усіх витрат, пов'язаних із створенням і експлуатацією обчислювальної мережі. Цей принцип має на увазі, що найбільш ефективною з економічної точки зору буде мережа, що використовує комутацію пакетів, яка дозволить ефективно використати канали зв'язку.

Модульність обчислювальної мережі, про яку згадувалося вище, припускає під собою створення окремих модулів під різні функції. До основних модулів обчислювальної мережі можна віднести модуль мережі Інтернет, модуль територіальних мереж і серверний модуль [9].

4.2 Опис проектованих обчислювальних мереж

На основі вибраної онлайн-платформи віртуалізації UNetLab, будуть розроблено декілька моделей складних обчислювальних мереж. Моделі обчислювальних мереж, що розробляються, ґрунтуються на використанні мережевого устаткування компанії Cisco Systems, що є безумовним фаворитом на ринку мережевого устаткування і що пропонує пристрої для створення обчислювальних мереж від невеликого офісу до великих корпорацій.

Саме шлях становлення компанії від невеликого офісу до великої компанії, що має територіально віддалені філії, потребує високих

обчислювальних ресурсів і їх захисту, буде відбитий в проектованих моделях обчислювальних мереж.

Уся робота буде розділена на декілька етапів, на кожному з яких буде спроектована обчислювальна мережа, відображаючи розвиток компанії і вирішуючи нові завдання.

На першому етапі будуть спроектовані моделі обчислювальних мереж початкового рівня, для підприємства малого рівня. Офіси такого підприємства можуть розташовуватися в одному або декількох сусідніх будівлях. Ця модель обчислювальної мережі відображатиме схему об'єднання робочих станцій підприємства до мережі, для надання можливості мережевої взаємодії між собою, а також продемонструє різні варіанти цих підключень. Будуть розглянуті як варіанти об'єднання робочих станцій підприємства в єдину мережу, що знаходяться в одній будівлі (на різних поверхах), так і можливість об'єднання в мережу робочих станцій, розташованих в різних будівлях, що знаходяться зблизька один від одного.

На наступному етапі буде спроектована модель обчислювальних мереж, що відображає розвиток підприємства. На прикладі розвитку буде відображено збільшення робочих станцій, що підключаються, до мережі, а також буде зроблена їх градація на різні підрозділи, включаючи різні методи підключення робочих станцій до мережі продемонстрованих в попередній моделі. Крім того, для усіх робочих станцій підприємства буде наданий доступ в мережу Інтернет. Буде змодельована ситуація, при якій, підприємство, для доступу в мережу Інтернет, орендуватиме у провайдера "білий" IP-адрес і тільки один. Т. е. доступ в глобальну мережу для усіх робочих станцій підприємства здійснюватиметься тільки через один, виділений провайдером, IP-адрес, що значно скорочує фінансові витрати підприємства. Такий спосіб доступу в глобальну мережу хороший ще і тим, що приховує внутрішню структуру організації обчислювальної мережі від сторонніх.

На завершальному етапі будуть спроектовані моделі обчислювальних мереж, на яких буде відбитий ріст підприємства і ділення на територіально віддалені філії. Будуть розглянуті різні варіанти побудови повідомляючого тунеля для об'єднання філій. При виникненні необхідності мережевої взаємодії філій, увесь інформаційний трафік протікатиме через цей тунель. Оскільки передача інформації між філіями відбуватиметься за рамками внутрішньої структури обчислювальної мережі, то цю інформацію необхідно буде захистити від несанкціонованого доступу. Тому необхідно буде настроїти шифрування усього протікаючого трафіку "завертаного" в цей повідомляючий тунель.

При рості підприємства його логічним розвитком являється поява у свого серверного устаткування. Будь то файловий, поштовий або ж веб-сервер. У проектованій моделі буде розглянутий випадок, при якому сервер організації, що знаходиться у внутрішній структурі обчислювальної мережі, прихованої від сторонніх користувачів, матиме відкритий доступ. Т. е. будь-який користувач, що навіть знаходиться за межами мережі підприємства, міг мати доступ до сервера підприємства.

У моделі також буде розглянуто питання про відмовостійкість мережі філії компанії. Топологія обчислювальної мережі, в якій розташовано серверне устаткування, буде спроектована таким чином, що при виникненні порушення фізичної цілісності з'єднання (розрив передавального середовища, кабелю) робота усієї мережі не припиниться. Модель обчислювальної мережі, при виявленні несправності, автоматично перебудується так, щоб її функціональність не була порушена, тим самим не перериваючи роботу підприємства.

4.3 Розробка концепцій обчислювальних мереж

Перед тим, як приступити до розробки моделей обчислювальних мереж в UNetLab, необхідно спочатку спроектувати концепцію майбутніх моделей.

Спроектована концепція відображатиме майбутню топологію обчислювальних мереж. Таким чином будуть спроектовані усі вузли майбутньої обчислювальної мережі. Буде зроблено розбиття сегментів на підмережі і розподіл адрес для них, а також буду спроектовані усі з'єднання між пристроями.

Розробка такої концепції дозволяє враховувати усі нюанси майбутніх мереж, а також уникнути помилок на етапі моделювання мереж в емуляторі.

Перша концепція, зображена на рис.4.2, відображатиме просту обчислювальну мережу, головною метою якої є об'єднання в єдину мережу обчислювальні машини підприємства і створення можливості мережевої взаємодії між ними.

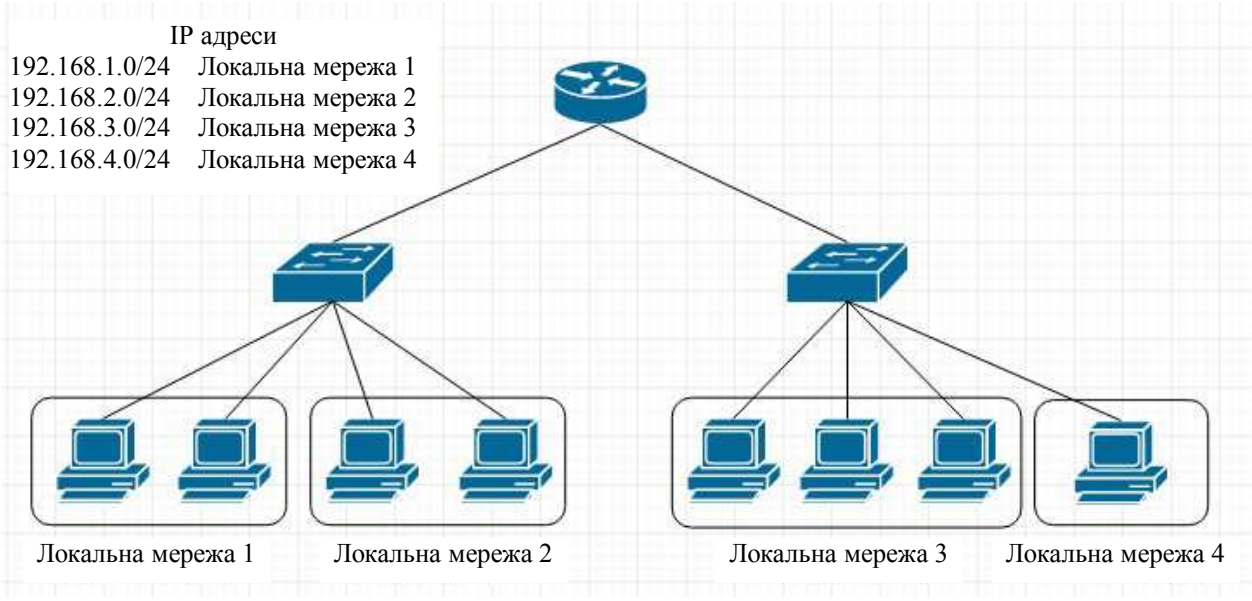


Рисунок 4.2 – Концепція, що відображає просту обчислювальну мережу

Ця мережа складатиметься з декількох комутаторів для розбиття групи комп'ютерів на різні локальні мережі, розбиття може відбуватися за будь-яким принципом (наприклад, по відношенню комп'ютерів до певного підрозділу компанії), і маршрутизатора, для забезпечення можливості мережевої взаємодії між робочими станціями компаніями, що знаходяться в

різних локальних мережах. Побудована обчислювальна мережа цим способом може припускати різне видалення комп'ютерів, що знаходяться в одній локальній мережі. Наприклад, на різних поверхах однієї будівлі. Таким чином, з'являється можливість логічного об'єднання комп'ютерів на підмережі, що значно спрощує в майбутньому управління такою мережею і логічно структурує її.

Наступна концепція, зображена на рис. 4.3., є логічною продовження попередньої концепції.

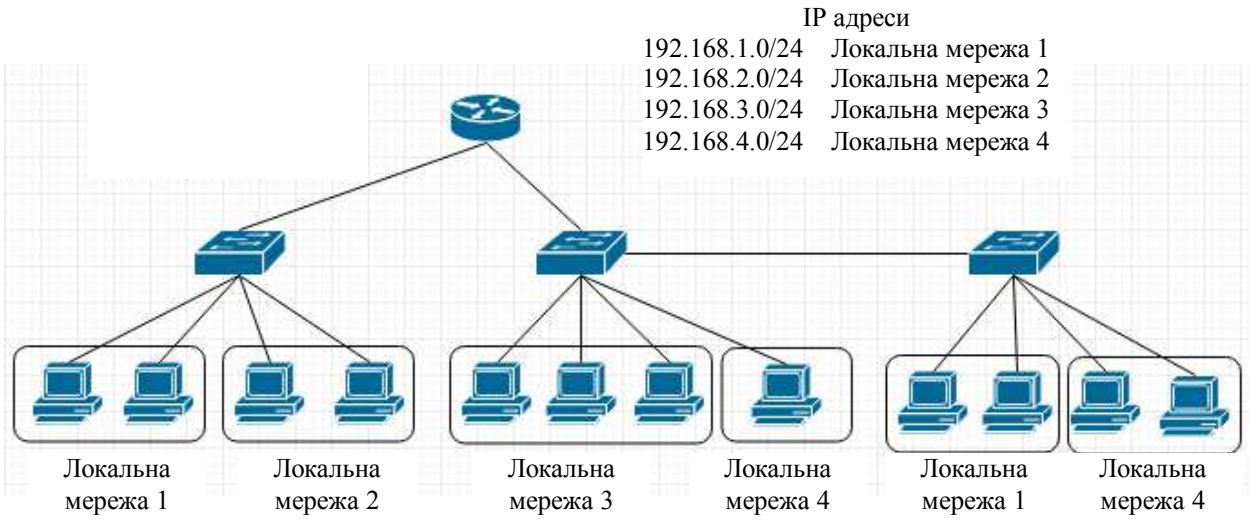


Рисунок 4.3 – Логічне продовження попередньої концепції

На ній продемонстрований випадок, при якому виникає завдання логічного об'єднання обчислювальних машин в єдину локальну мережу, але фізично підключених до різних комутаторів. В даному випадку, комп'ютери, що логічно знаходяться в четвертій локальній мережі, але фізично підключені до різних комутаторів матимуть можливість мережевої взаємодії навіть без урахування маршрутизатора. Проте ситуація з комп'ютерами тих, що логічно знаходяться в першій локальній мережі протилежна, взаємодія можливо тільки за наявності маршрутизатора.

Далі, спроектуємо концепцію обчислювальної мережі, що зображену на рис.4.4, відображає ріст підприємства. Збільшується як кількість робочих

станцій, так кількість мережевих пристроїв для створення обчислювальної мережі. Ця концепція включає обидва методи підключення робочих станцій з попередніх концепцій. Також в концепції відбито логічне ділення комп'ютерів на локальні мережі по відношенню до підрозділів на підприємстві. Так, наприклад, локальна мережа "Офис2" складається з комп'ютерів, фізично підключених до різних комутаторів.

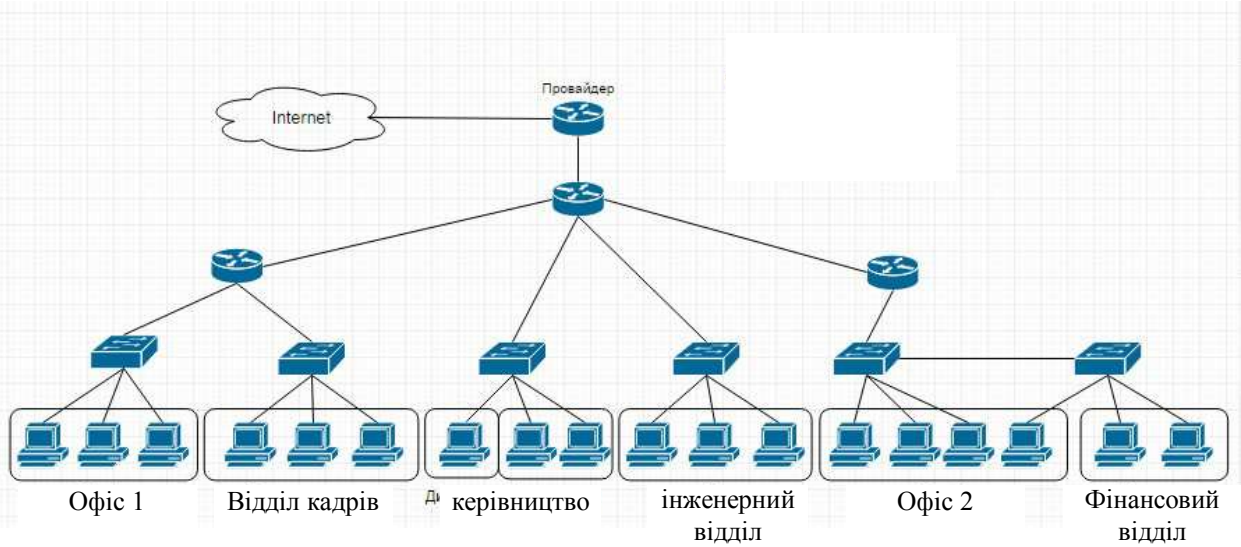


Рисунок 4.4 – Концепція обчислювальної мережі підприємства, що розвивається

У концепції також почав фігурувати провайдер - постачальник "білого" IP-адреса. Т. е. доступ в глобальну мережу для усіх робочих станцій підприємства буде здійснюється тільки через один, виділений провайдером, IP-адрес. Що у свою чергу приведе до економії фінансових коштів компанії при оренді тільки одного IP-адреса.

У наступній концепції, зображеній на рис.4.5, відбито ділення на територіальні філії. Розглянутий випадок, коли у компанії з'являється територіально віддалена філія і з'являється необхідність в створенні загальної обчислювальної мережі для можливості мережевої взаємодії між об'єктами різних філій. Оскільки, кожна філія має доступ в інтернет через виділений IP-

адрес своїм провайдером, то між цими IP-адресами буде створений спеціальний тунель, через який і протікатиме уся інформація між філіями.

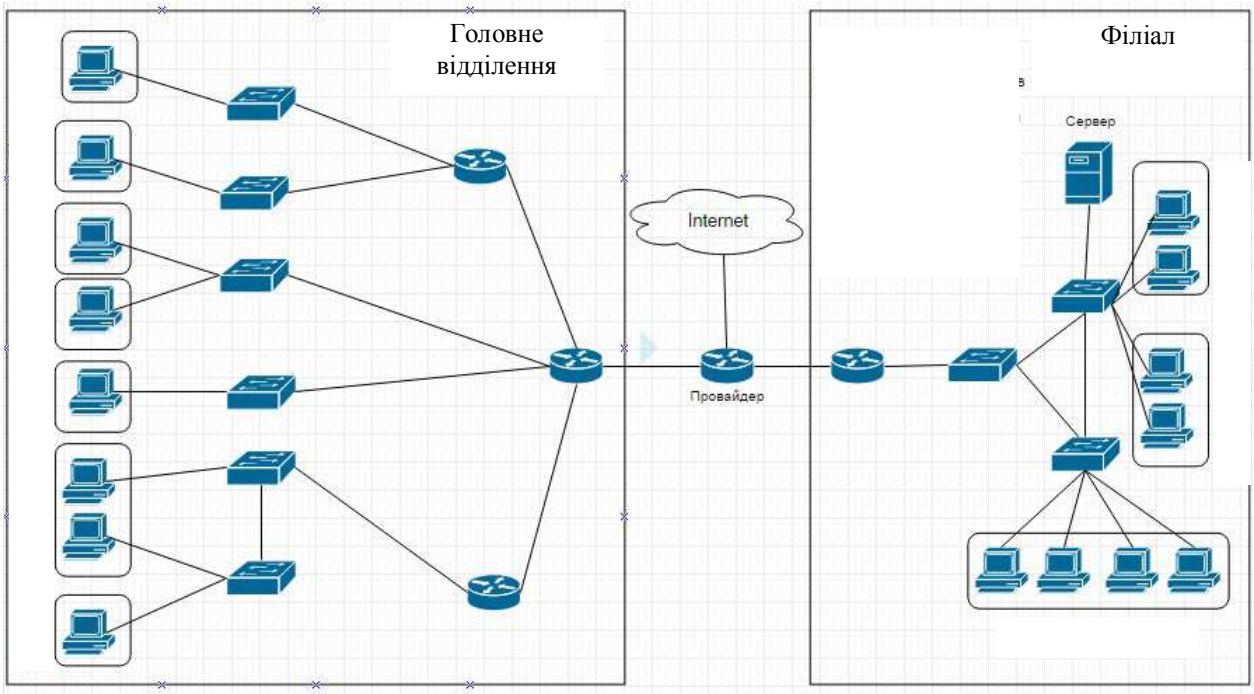


Рисунок 4.5 – Концепція обчислювальної мережі з діленням на територіально віддалені філії

Ще в концепції з'явився новий об'єкт - сервер підприємства. Для будь-якого підприємства серверне устаткування є найважливішим об'єктом в його інфраструктурі. Це досягається не лише вартістю цього устаткування, але і об'ємом і значущості інформації, що зберігається на нім. Вихід з ладу такого устаткування може привести до повної зупинки функціонування усього підприємства, тому дуже важливою метою є забезпечити відмовостійкий доступ до нього. Для цього топологія мережі філії була сформована таким чином, що при виникненні фізичного обриву одного із з'єднання між комутаційними пристроями, зв'язок з сервером не порушувався, тим самим не перериваючи роботу підприємства.

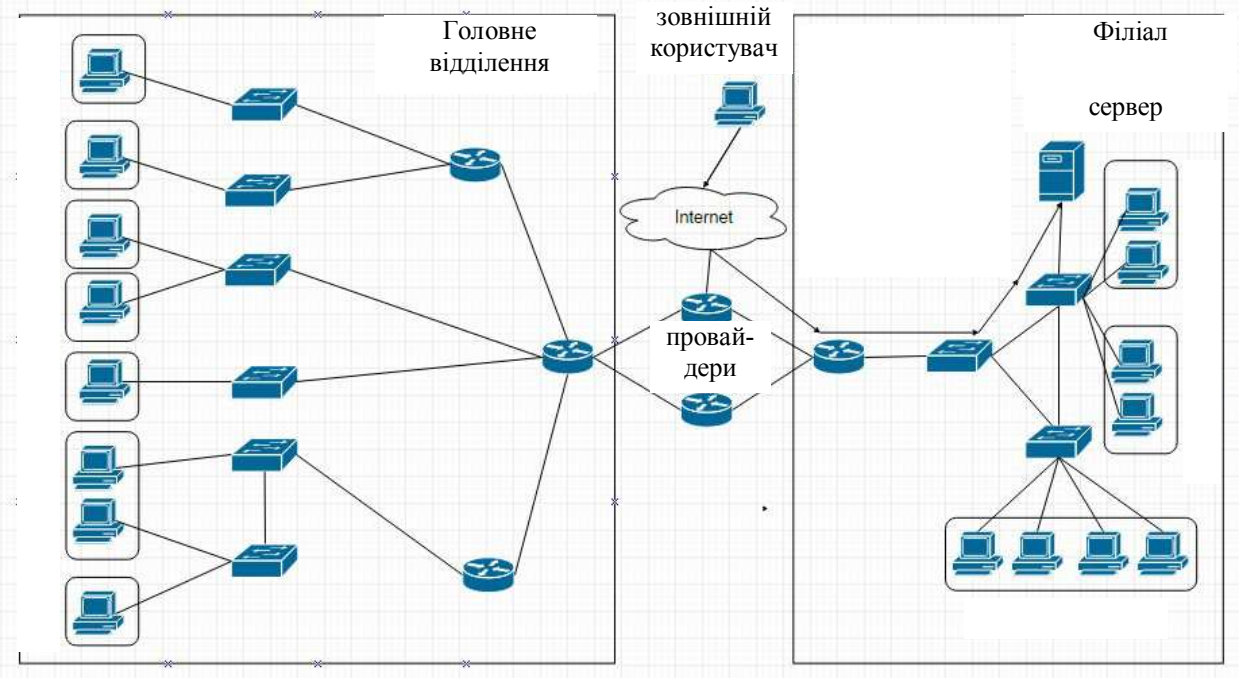


Рисунок 4.6 – Концепція обчислювальної мережі
з діленням на територіально віддалені філії і відмовостійкістю

У завершальній концепції, зображеній на рис.4.6, буде розглянутий інший варіант побудови повідомляючого тунеля між філіями компанії. Цей варіант мати на увазі, що кожна філія орендує як мінімум два "білих" IP-адреса у провайдерів. Через кожну пару IP-адресов буде проведений повідомляючий тунель, один основний і один резервний. У разі обриву з'єднання з будь-якого боку між основним провайдером ("Провайдер 1") топологія мережі буде в автоматичному режимі перебудована і активізується другий тунель, що повідомляється, через резервного провайдера ("Провайдер 2"). Таким чином досягається відмовостійкість зв'язку між філіями, що у свою чергу, веде до надійності функціонування усього підприємства.

Також в концепції відбита можливість доступу до сервера підприємства користувачам з мережі Інтернет, що знаходяться за межами внутрішньої структури обчислювальної мережі підприємства. Т. е. доступ до сервера стає публічним і доступний будь-яким користувачам, незалежно від приналежності до підприємства.

Таким чином були сформовані концепції майбутніх моделей обчислювальних мереж. Далі, на основі вибраної онлайн-платформи віртуалізації UNetLab, будуть розроблені моделей складних обчислювальних мереж на основі цих концепцій і проведені дослідження їх ефективності.

4.4 Вибір засобу моделювання

Найбільш перспективними в плані подальшої підтримки і розвитку видаються моделі OPEN - ZB і Castalia. Особливу увагу необхідно звернути на модель Castalia, оскільки команда розробників спочатку ставила перед собою завдання змоделювати усі аспекти роботи безпровідних сенсорних мереж, її початковий код є відкритим і, що особливо важливо, середовище моделювання на основі, якою вона побудована, має також відкритий початковий код і поширюється безкоштовно для некомерційного використання.

Модель OPEN-ZB, побудована на базі комерційного продукту OPNET Modeler 10.5 і вище, проте доступного на безкоштовній базі для навчальних закладів.

Таблиця 4.1 – Основні можливості розглянутих моделей БСМ

Параметр	**OPNET**		**NS-2**	**OMNET++**
	OPNET Modeler 14.0	**OPEN - ZB 3.0 (beta)**	**Zheng**	**Castalia**
Завдання фізичного рівня (IEEE 802.15.4)				
Включення та виключення приймача	-	+	-	+
Вибір частотного каналу	+	-	+	-
Підтримка частотних діапазонів 868/915/2450	+/+/+	-/-/+	+/+/+	+/+/+
Визначення енергії в поточному каналі	+	+	+	+
Індикація якості з'єднання для отриманих пакетів (LQD)	+	+	+	+
Оцінка чистоти каналу (CCA) для механізму CSMA - CA	+	+	+	+

Параметр	OPNET		NS-2	OMNET++
	OPNET Modeler 14.0	**OPEN - ZB 3.0 (beta)**	**Zheng**	**Castalia**
Завдання рівня доступу до середовища (IEEE 802.15.4)				
Підтримка топологій зірка/точка-точка	+/+	+/+	+/+	+/+
Режим прямих передач	+	-	+	+
Режим непрямих передач	-	+	+	-
Підтримка асоціації і дизасоціації з приватною мережею (PAN)	+	+	+	+
Координатор	-	+	+	+
Режим роботи без маркерів	+	-	+	-
Синхронізація маркерами мережі	-	+	+	+
Підтримка безпеки пристроїв	-	-	-	-
Реалізація механізму slotted CSMA - CA	-	+	+	+
Реалізація механізму unslotted CSMA - CA	+	-	+	-
Управління і підтримка механізму GTS	-	+	-	+
Підтримка надійного з'єднання між двома рівнями MAC	+	+	+	+
Мережевий рівень				
Наявність протоколів маршрутизації	+	+	-	+
Відповідність специфікації ZigBee	+	-	-	+
Додаткові можливості моделі				
Мобільність вузлів	+	-	-	+
Розрахунок споживаної вузлами енергії	-	+	-	+

Таблиця 4.2 – Вибір найкращої моделі бездротової мережі

	OMNET++ &Castalia	**NS-2**	**OPNET Academic Modeler**
Визначення енергії в поточному каналі	+	+	+
Відкритий код	+	+	-
Відповідність специфікації ZigBee	+	-	-
Мобільність вузлів	+	-	-
Наявність протоколів маршрутизації	+	-	+
Розрахунок споживаної вузлами енергії	+	-	+

Для досягнення поставленої мети необхідно вибрати засіб імітаційного моделювання за наступними критеріями і визначити найбільш відповідне (таблиця 4.2).

Оскільки планується некомерційне використання засобу моделювання, то програмний комплекс OPNET Modeler не підходить через дорожнечу. Network Simulator NS-2 не підходить через невідповідність специфікації ZigBee. Програмний комплекс OMNET++ і Castalia є найкращим варіантом. Базуючись на ОС Linux так само портовані і на OS Windows.

4.5 Моделювання обчислювальних мереж в UNetLab

На основі вибраної сучасної онлайн-платформи віртуалізації мережевого устаткування UNetLab, було розроблено декілька моделей складних обчислювальних мереж. У спроектованих моделях відображений шлях становлення компанії від невеликого офісу до великої компанії, що має територіально віддалені філії, потребує високих обчислювальних ресурсів і їх захисту.

Процес моделювання обчислювальних мереж з використанням устаткування компанії Cisco Systems відбувався шляхом емуляції операційної системи Cisco IOS комутуючого і маршрутизуючого устаткування. Параметри емульованих пристроїв були задані: для комутаторів - 128 MByte для оперативної пам'яті (RAM) і флэш пам'яті (NVRAM) відповідно; для маршрутизаторів - 128 Mbyte для флэш пам'яті (NVRAM) і 256 Mbyte для оперативної пам'яті (RAM). При створенні моделей обчислювальних мереж з використанням технології перетворення мережевих адрес - NAT і технологій побудови повідомляючих тунелів VPN/GRE, налагоджених на пристрої, що маршрутизується, кількість оперативної пам'яті (RAM) була збільшена до 512 Mbyte. Це збільшення кількості оперативної пам'яті обумовлене роботою вищеперелічених протоколів.

Для моделювання роботи серверного устаткування, на платформі UNetLab був розгорнутий веб-сервер.

Таким чином, при фізичному відтворенні спроектованих моделей в UNetLab, вибір типу і серії устаткування, може бути обумовлено вказаними характеристиками і необхідною кількістю портів для підключення устаткування.

В результаті, в платформі UNetLab на основі розроблених концепціях обчислювальних мереж і використанням вибраний мережевих технологій, були спроектовані моделі обчислювальних мереж.

4.6 Опис змодельованих обчислювальних мереж

Модель №1, зображена на рис.4.6, є моделлю, що складається з двох комутаторів SW1 і SW2 і маршрутизатора R, і відображає просту обчислювальну мережу, головною метою якої є об'єднання в єдину мережу обчислювальні машини підприємства і створення можливості мережевої взаємодії між ними.

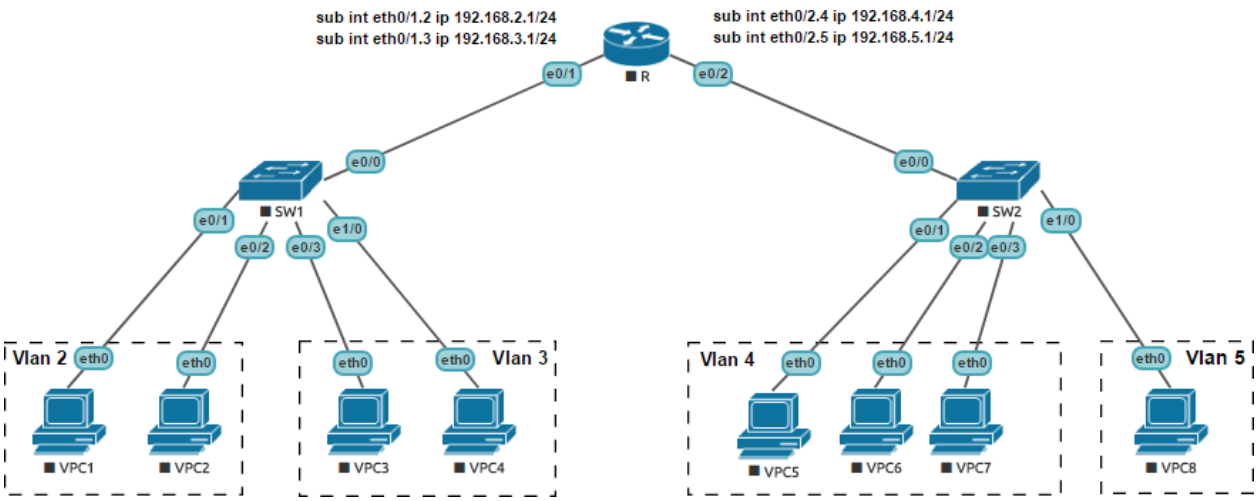


Рисунок 4.7 – Спроектована модель обчислювальної мережі №1

На кожному комутаторі налагоджені віртуальні локальні мережі (VLAN). На комутаторі SW1 налагоджені локальні мережі VLAN2 і VLAN3, а на комутаторі SW2 - VLAN4 і VLAN5. Визначення відношення робочих станцій до локальних мереж відбувається шляхом розподілу на комутаторі

інтерфейсів підключення. Цей розподіл інтерфейсів по локальних мережах на комутаторі SW1 продемонстрований на рис.4.7.

У моделі є присутнім маршрутизатор R, завдання якого організовувати можливість мережевої взаємодії між робочими станціями, що знаходяться в різних локальних мережах. Так само на маршрутизаторі налагоджений DHCP -сервер, завдання якого полягає в автоматичному привласненні IP-адресов комп'ютерам-агентам, необхідних для роботи робітників станцій в мережі. Для цього, на маршрутизаторі були створені DHCP - пули з параметрами, переданих для кожної локальної мережі, необхідних комп'ютерам для роботи в мережі. Модель, зображена на рис.4.8, має схожу архітектуру обчислювальної мережі, що і модель №1, оскільки є логічним продовження попередньої.

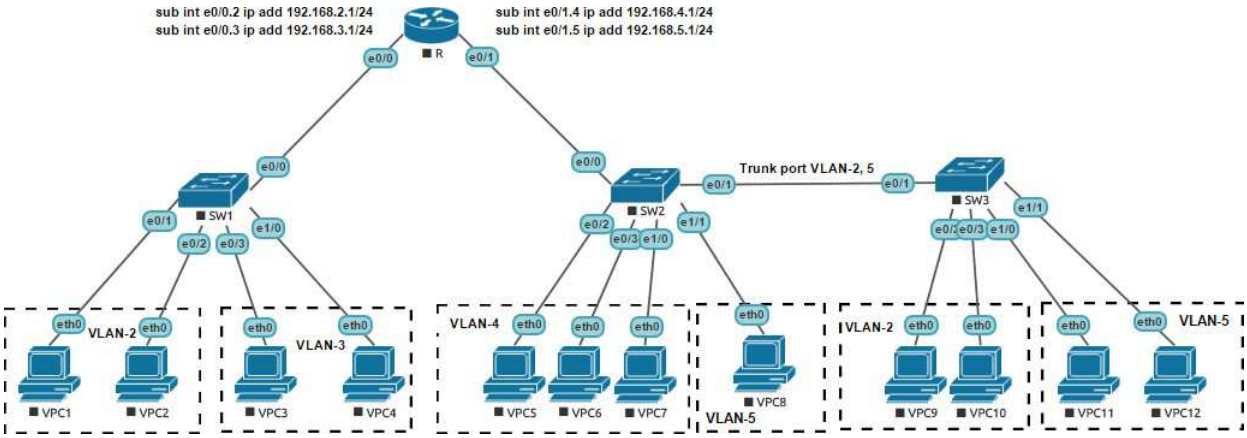


Рисунок 4.8 – Спроектована модель обчислювальної мережі №2

На ній продемонстрований випадок, при якому виникає завдання логічного об'єднання обчислювальних машин в єдину локальну мережу, але фізично підключених до різних комутаторів. В даному випадку, комп'ютери, що логічно знаходяться в п'ятій локальній мережі, але фізично підключені до різних комутаторів (SW2 і SW3) матимуть можливість мережевої взаємодії навіть без урахування маршрутизатора R. Проте ситуація з комп'ютерами тих, що логічно знаходяться в другій локальній мережі протилежна, взаємодія можливо тільки за наявності маршрутизатора. Таке логічне

об'єднання стало можливим шляхом з'єднання комутаторів SW2 і SW3 магістральним портом (Trunk port). Цей магістральний порт служить для передачі трафіку локальних мереж (VLAN) між пристроями.

Модель №3, продемонстрована на рис.4.9, відображає зростання підприємства. Збільшується як кількість робочих станцій, так кількість мережевих пристроїв для створення обчислювальної мережі. Ця концепція включає обидва методи підключення робочих станцій з попередніх моделей. Також в моделі відбито логічне ділення комп'ютерів на локальні мережі по відношенню до підрозділів на підприємстві.

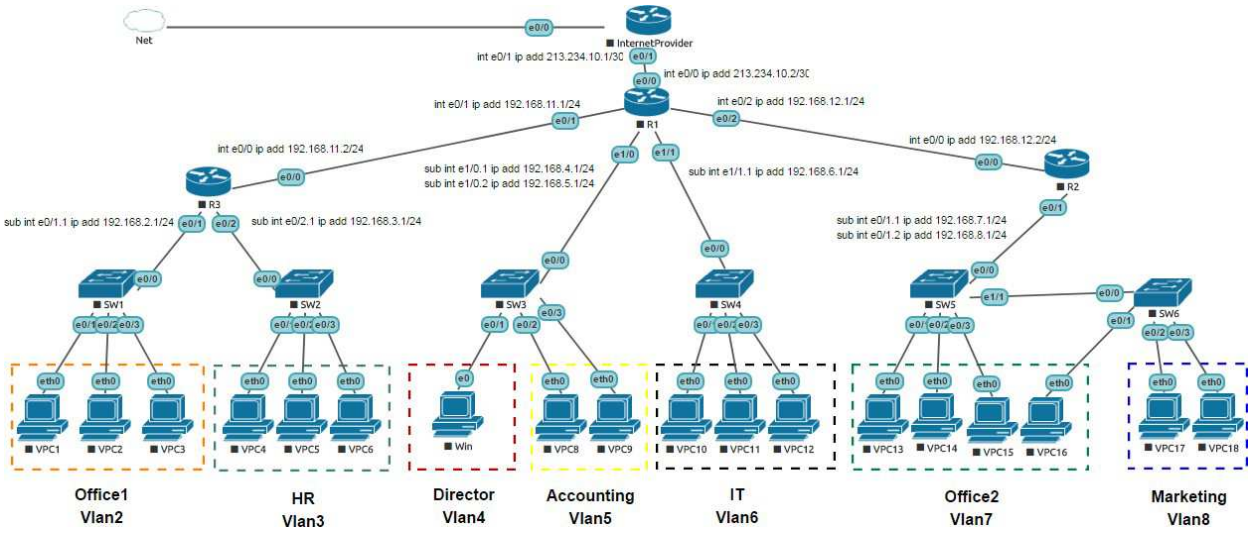


Рисунок 4.9 – Спроектована модель обчислювальної мережі №3

Оскільки в цій моделі є присутнім три маршрутизатори (R1, R2 і R3), з'являється необхідність в маршрутизації трафіку, що протікає в мережі. Для цього був використаний протокол динамічної маршрутизації EIGRP, робота якого полягає в обміні, сусідніх маршрутизаторів, інформацією про відомих їм мережам. Налаштування цього протоколу на маршрутизаторі R1 продемонстроване на рис.4.10.

```
router eigrp 1
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.6.0
 network 192.168.11.0
 network 192.168.12.0
 network 213.234.10.0
```

Рисунок 4.10 – Налаштування протоколу динамічної маршрутизації EIGRP на маршрутизаторі R1

У моделі також фігурує провайдер (InternetProvider) - постачальник "білого" IP-адреса. За допомогою протоколу NAT, через виділений IP-адрес провайдером, був відкритий доступ усім вузлам мережі доступ в мережу Інтернет. Для цього, на маршрутизаторі R1, був створений лист-доступа з переліком IP-адресов локальних мереж, необхідних перетворювати у виділений провайдером IP, - адреса. Т. е. при виникненні звернення в мережу Інтернет вузлом з локально мережі зі списку-доступу, відбувалася трансляція його "сірого" IP-адреса в "білий". Створений лист-доступа на маршрутизаторі R1 відображений на рис.4.11.

```
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
 permit 192.168.5.0 0.0.0.255
 permit 192.168.6.0 0.0.0.255
 permit 192.168.7.0 0.0.0.255
 permit 192.168.8.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.12.0 0.0.0.255
```

Рисунок 4.11 – Лист доступу з переліком трансльованих IP-адресів локальних мереж протоколом NAT на маршрутизаторі R1

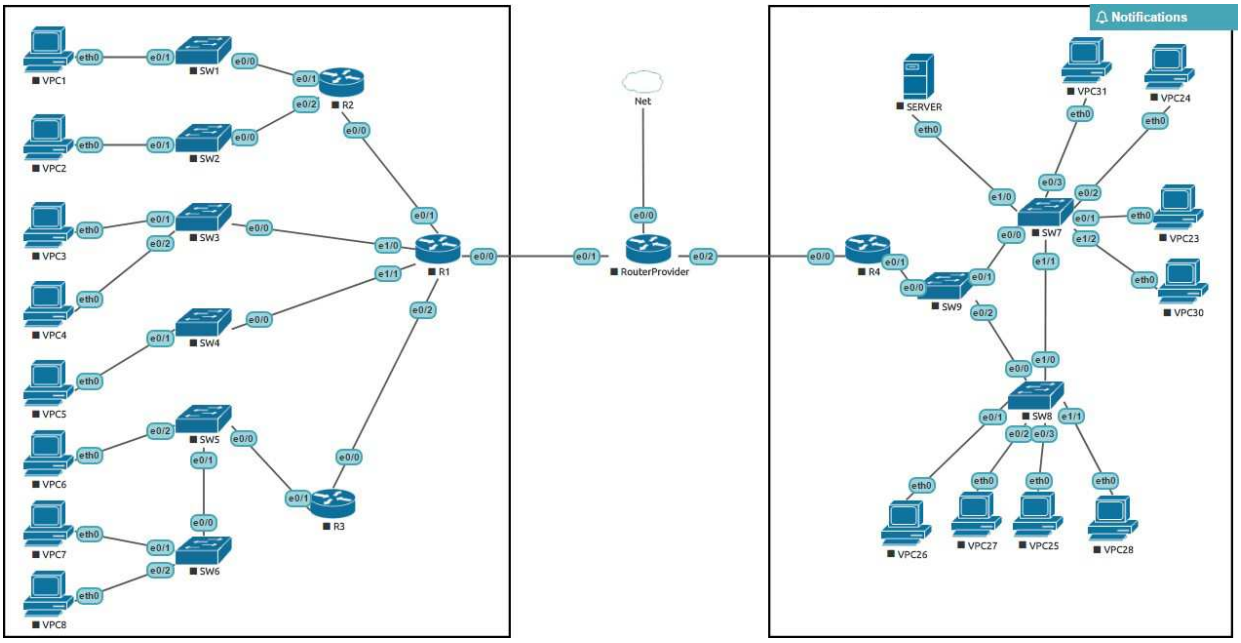


Рисунок 4.12 – Спроектована модель обчислювальної мережі №4

Модель №4, зображена на рис.4.12, відображає структурне ділення підприємства на територіальні філії. Змодельований випадок, коли у компанії з'являється територіально віддалена філія і з'являється необхідність в створенні загальної обчислювальної мережі для можливості мережевої взаємодії між об'єктами різних філій.

Оскільки кожна філія має доступ в Інтернет, через виділений IP-адрес своїм провайдером, то між цими IP-адресами був створений повідомляючий VPN тунель. Т. е. створювалося явне з'єднання типу точка-точка між зовнішніми інтерфейсами маршрутизаторів R1 і R4. Потім, на створеним VPN тунель, накладалися політики шифрування з протоколу IPSec.

Проте, з'являється необхідність маршрутизації трафіку, що виходить за межі локальної мережі. Необхідно робити сортування трафіку. Трафік, що йде в локальну мережу філії, має бути спрямований по VPN тунелю, а увесь інший трафік необхідно перетворювати у виділений провайдером IP-адрес. Для вирішення цього завдання використовувався розширений список-доступу, в якому явно був вказаний, який трафік необхідно направляти по VPN тунелю, а якій транслювати в "білий" IP-адрес.

Для забезпечення відмовостійкого доступу до серверного устаткування, в топології обчислювальної мережі філії, на комутаторах SW7, SW8 і SW9 був налагоджений мережевий протокол STP, а саме його поліпшена версія RSTP, що має менший час перестроювання топології, у разі виникнення несправності.

У завершальній моделі №5, зображеною на рис.4.13, був змодельований інший варіант побудови повідомляючого тунеля між філіями компанії.

Цей варіант мати на увазі, що кожна філія орендує як мінімум два "білих" IP-адреса у провайдерів. Через кожну пару IP-адресов проведені повідомляючі GRE тунелі, один основний і один резервний. Для реалізації відмовостійкості тунелів, на маршрутизаторах філій R1 і R4 був налагоджений, вже раніше використаний, протокол динамічної маршрутизації EIGRP. У разі виникнення несправності основного GRE тунеля, топологія автоматично перебудується і активізується зарезервований GRE тунель.

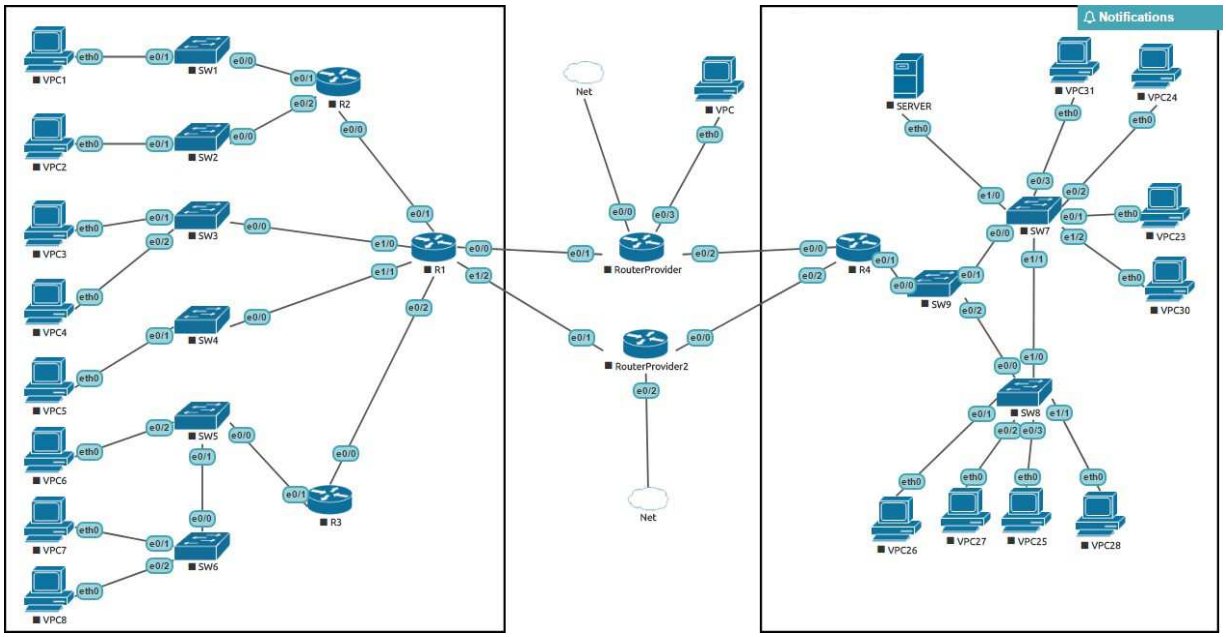


Рисунок 4.13 – Спроектована модель обчислювальної мережі №5

Також в моделі налагоджений доступу до сервера підприємства користувачам з мережі Інтернет, що знаходяться за межами внутрішньої структури обчислювальної мережі підприємства. При зверненні користувачем з мережі Інтернет на IP-адрес, виділений провайдером на маршрутизаторі R4, за допомогою технології NAT відбувається трансляція в IP-адрес сервера. Таким чином, доступ до сервера стає публічним і доступний усім користувачам з мережі Інтернет.

4.7 Проведення досліджень ефективності змодельованих обчислювальних мереж

4.7.1 Дослідження тестування навантаження змодельованих обчислювальних мереж

Для проведення досліджень ефективності спроектованих моделей обчислювальних мереж необхідно провести симуляцію роботи цієї мережі, піддавши її навантаженням, тобто зробити генерацію великого об'єму трафіку усередині неї. Для цього завдання, в UNetLab передбачений генератор трафіку Ostinato, яким ми і скористаємося. Ostinato є пристроєм - дрон, який фізично підключається до моделі обчислювальної мережі. Управління ж відбувається з комп'ютера користувача, шляхом запуску на нім графічного інтерфейсу. Користувачеві доступне налаштування типу генерованого трафіку, його об'єму, джерела і призначення.

Для проведення досліджень, дрон Ostinato був підключений до спроектованих моделей замість робочих станцій, таким чином, відбуватиметься імітація роботи користувачів в мережі шляхом генерації трафіку дроном Ostinato. Приклад підключення дрона Ostinato до моделі обчислювальної мережі продемонстрований на рис.4.14.

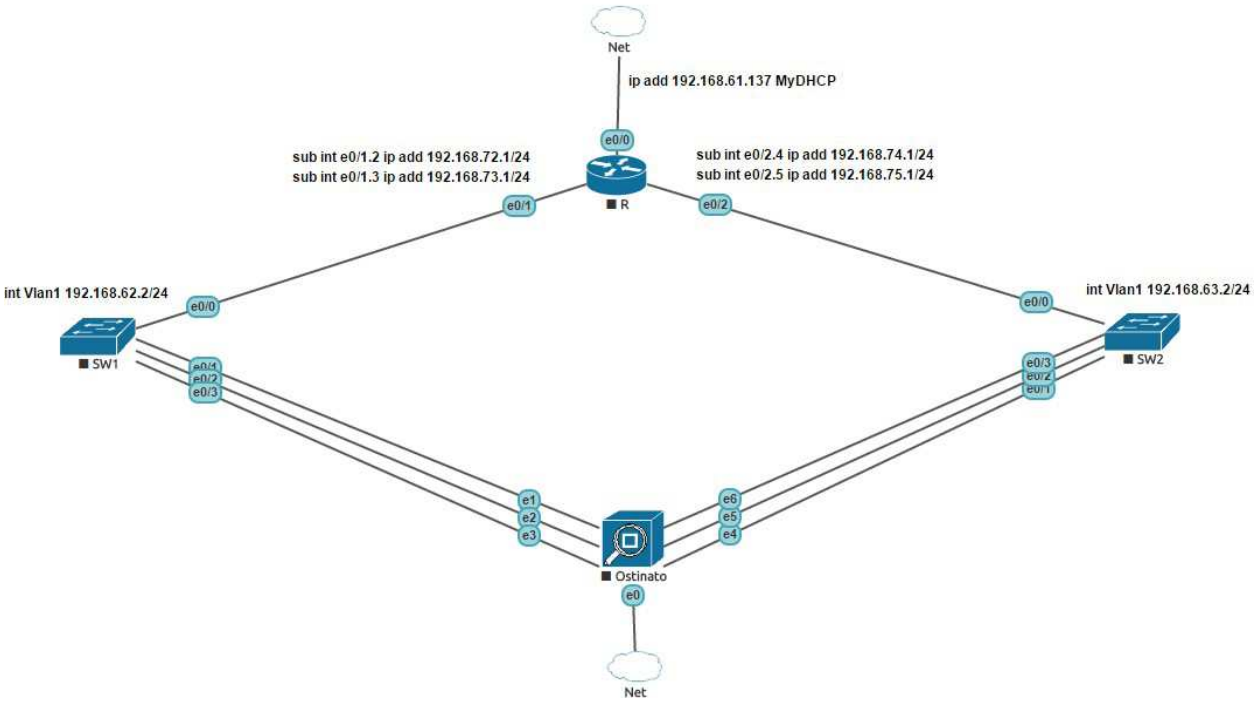


Рисунок 4.14 – Приклад підключення дрона Ostinato до спроектованої модель обчислювальної мережі.

Для аналізу роботи моделей обчислювальних мереж під навантаженням необхідно збирати інформацію з пристроїв. Зробити це можна за допомогою протоколу SNMP (Simple Network Management Protocol, простий протокол мережевого управління). Для цього, було використано програмне забезпечення PRTG Network Monitor, за допомогою якого, по протоколу SNMP, збиралася статистика роботи мережевого устаткування.

Тестування проводилося шляхом генерації нескінченного трафіку дроном Ostinato, що передається між локальними мережами.

В результаті такого тестування навантаження, були отримані наступні результати, рис.4.15, рис.4.16:

- Максимальна завантаженість каналів на комутаторах SW1 і SW2 дорівнювала 147 кб/с;
- Максимальна завантаженість каналів на маршрутизаторі дорівнювала 5,33 кб/с;
- Завантаження процесора маршрутизатора не перевищувало 2%.

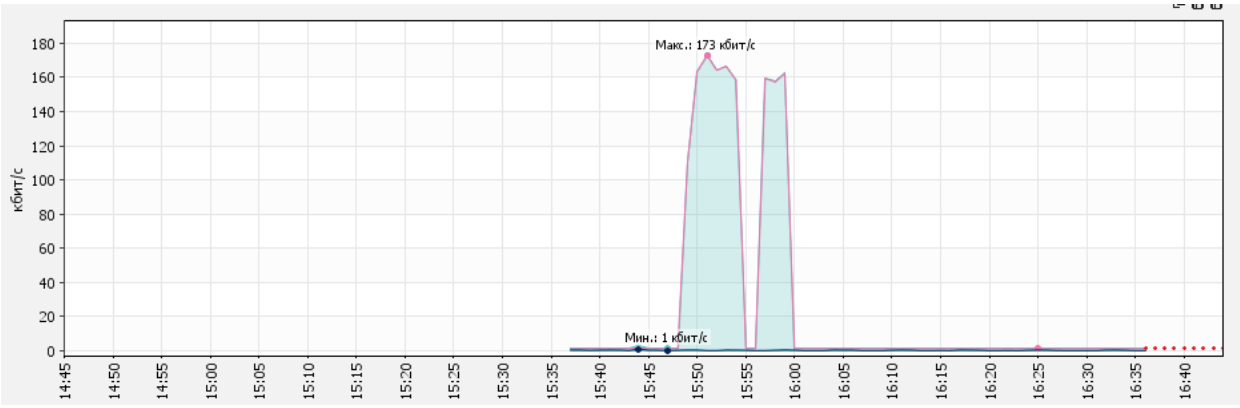


Рисунок 4.15 – Результати тестування навантаження для комутаторів

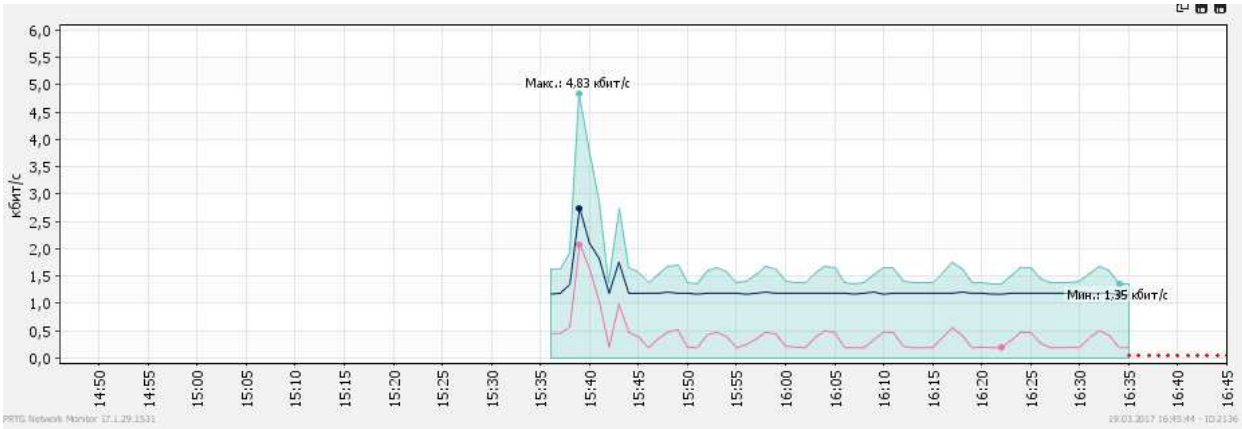


Рисунок 4.16 – Результати тестування навантаження для маршрутизатора

Отримані результати виявилися не репрезентативними і навіть близько не відповідають параметрам реального устаткування, заявлених виробником устаткування. Такі результати обумовлені тим, що мережеве устаткування, що випускається компанією Cisco Systems, це передусім устаткування, що складається як з програмного забезпечення (Cisco IOS), так і апаратного забезпечення. При моделюванні роботи цього устаткування в платформі UNetLab, відбувається емуляція тільки програмного забезпечення, оболонки Cisco IOS, а усе емуляція апаратного забезпечення лягає на устаткуванні обчислювальної машини, на якій ця платформа встановлена.

Таким чином, при фізичному відтворенні спроектованих моделей в UNetLab, вибір типу і серії устаткування, може бути обумовлено заданими характеристиками при моделюванні роботи і необхідною кількістю портів для підключення устаткування.

Висновки до розділу

1. В середовищі UNetLab проведено покрокове створення моделей складних обчислювальних мереж. Модель обчислювальної мережі відображає схему об'єднання робочих станцій підприємства до мережі, для надання можливості мережевої взаємодії між собою, а також продемонструє різні варіанти цих підключень. Показано створення моделей згідно представлених технологій забезпечення підключення

2. Проведено тестування роботи мережі у випадку підключення додаткового користувача. В якості такого користувача використано дрон Ostinato, що дозволяє генерувати певний трафік в мережу. Тестування проводилося шляхом генерації нескінченного трафіку дроном Ostinato, що передається між локальними мережами.

ВИСНОВКИ

1. В роботі проведено аналіз проблематики побудови телекомунікаційних мереж різної складності. Особлива увага приділена мережам, в яких учасники мережі є мобільними пристроями, що характерно для мереж із застосуванням безпровідних пристроїв (ZigBee, LTE).

2. Проаналізовані існуючі принципи створення топології мережі. Встановлено, що існує цілий клас програм – емуляторів мережевого устаткування. Визначено, що ці емулятори дозволяють в різній мірі виконати побудову топології мережі, що включає в собі моделі маршрутизаторів, комутаторів, серверів, локальних користувачів. Особлива увага в аналізі присвячена моделям бездротових пристроїв – ZigBee пристроям. А також показано, які технології забезпечення зв’язку через тунелі між сегментами мережі використовуються.

3. Виконано віртуалізацію мережевого устаткування в середовищі UNetLab від компанії Cisco. А також проведено моделювання роботи мережі при взаємодії з бездротовим вузлом, в якості якого використано дрон – генератор трафіку.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифе – Учебник. – СПб: Изд-во «Питер», 2016. – 992 с.

2. Локальные сети: архитектура, алгоритмы, проектирование. / Ю.В. Новиков, С.В. Кондратенко – М.: ЭКОМ, 2001. – 312 с.

3. Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 468 с.

4. Вычислительные сети и сетевые протоколы / Д. Девис, Д. Барбер, У. Прайс – М.: Мир, 1982. – 562с.

5. Компьютерные сети. Книга 1: High-Performance Networking. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 432 с.

6. Корпоративные сети связи / Т.И. Иванова. Пособие. – Москва 2001, – 297 с.

7. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е издание. / А. Мысник – М.: Издательский дом «Вильямс», 2005. – 1168 с.

8. CCNP маршрутизация / Т.Лэммсл, Ш.Одом, К. Уоллес. Изд. «Лори», 2015. – 444 с.

9. Компьютерные сети / Э. Таненбаум – СПБ.: «Питер», 2002. – 248 с.

10. Основы построения виртуальных частных сетей. / С.В. Запечников. – М.: Мир, 2003. – 249 с.

11. Информационная безопасность компьютерных систем и сетей. / В. Шаньгин. – Изд.: Инфра-М, 2011. – 416 с.

12. Использование программных средств эмуляции оборудования в обучении сетевым технологиям / Е.Ф. Попов, А.А. Захаров // Сборник научных трудов по материалам Международной заочной научно-

практической конференции «Теоретические и прикладные проблемы науки и образования в 21 веке». Часть 8. – Тамбов, Изд-во ТРОО «Бизнес-Наука-Общество», 2012.

13. Использование программных средств эмуляции оборудования при модификации сетевой инфраструктуры / Е.Ф. Попов// Сборник научных трудов по материалам всероссийскую научно-практической конференции студентов, аспирантов и молодых ученых «Новые технологии – нефтегазовому региону». Тюмень, 2012.

14. Тестирование и применение эмуляторов Cisco для моделирования гетерогенной IPсети / А.М. Горячев // Гагаринские чтения – 2016: XLII Международная молодежная научная коференция: Сборник тезисов докладов Т.ё. Московский авиационный институт (национальный исследовательский университет). – 2016. – стр.277-278

15. UNetLab: List of supported images [Электронный ресурс] / A. Dainese. URL: http://www.unetlab.com/documentation/supported-images/index.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

16. Razvan Beuran, Intorduction to network emulation – Taylor & Francis Group, 2012. -389стр.

17. Introduction to Cisco IOS Netflow:A Technical Overview / URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

18. Cisco IOS Flexible NetFlow [Электронный ресурс] / URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-fnetflow.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

ISSN 2307-5732
DOI 10.31891/2307-5732

НАУКОВИЙ ЖУРНАЛ

5.2020

ВІСНИК

Хмельницького національного університету

Том 1

Технічні науки

Technical sciences

SCIENTIFIC JOURNAL
HERALD OF KHMELNYTSKYI NATIONAL UNIVERSITY

2020, Issue 5, Volume 289

Хмельницький

ВІСНИК
ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
серія: Технічні науки

Затверджений як фахове видання (перереєстрація)
Категорія «Б», РІШЕННЯ АТЕСТАЦІЙНОЇ КОЛЕГІЇ № 1643 ВІД 28.12.2019

Засновано в липні 1997 р. ***Виходить 6 разів на рік***

Хмельницький, 2020, № 5(289)

Засновник і видавець: Хмельницький національний університет
(до 2005 р. – Технологічний університет Поділля, м. Хмельницький)

Включено до науково-метричних баз:

Google Scholar	http://scholar.google.com.ua/citations?hl=uk&user=aIUP9OYAAAAJ
Index Copernicus	http://jml2012.indexcopernicus.com/passport.php?id=4538&id_lang=3
Polish Scholarly Bibliography	https://pbn.nauka.gov.pl/journals/46221

Технічний редактор Горященко К. Л., к.т.н.
Редактор-коректор Броженко В. О.

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 3 від 29.10.2020 р.

Адреса редакції: редакція журналу "Вісник Хмельницького національного університету"
Хмельницький національний університет
вул. Інститутська, 11, м. Хмельницький, Україна, 29016

☎ (038-2) 67-51-08 **web:** http://journals.khnu.km.ua/vestnik
http://lib.khnu.km.ua/visnyk_tup.htm

e-mail: visnyk.khnu@gmail.com

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 9722 від 29 березня 2005 року

УДК 621

О.О. ПОЛЬНОВ, К.Л. ГОРЯЩЕНКО, В.В. МІШАН
Хмельницький національний університет

ТЕХНІЧНІ ЗАСОБИ МОДЕЛЮВАННЯ РОБОТИ МЕРЕЖ

Сучасна телекомунікаційна мережа складається з великої сукупності елементів. В мережу можуть входити як вузли, що стаціонарні, так і мобільні засоби. Розробка топології такої мережі вимагає критичного аналізу роботи за умов можливої динамічної зміни навантаження. В роботі показано аналіз сучасних програмних засобів моделювання роботи мережі. Емулятори NS-2, Riverbed OPNET Modeler, Cisco Packet Tracer є представниками великої сукупності таких технічних засобів. В пакетах моделювання мережі доступно використання різноманітного обладнання. Cisco Packet Tracer орієнтовано на моделювання із застосуванням обладнання фірми Cisco. OPNET Modeler навпаки – орієнтований на створення моделі із застосуванням як існуючого обладнання різних виробників, так і моделей обладнання без прив'язки до виробника.

Ключові слова: силова лінія, передача даних, перетворення Фур'є.

O.O. POLNOV, K.L. HORIASHCHENKO, V.V. MISHAN
Khmelnitsky national university, Ukraine

MODERN NETWORK MODELLING SOFTWARE

Modern telecommunication network consist of large amount of components like servers, routers, switches, end-point computers. Fibre channels and usual gigabit lines used as a medium. Modern network can combine not only static elements but mobile components like mobile phones, ZigBee modules, Wi-Fi access points, Bluetooth. High speed equipment like satellites can be added to network structure too.

So, selecting of correct equipment for network, estimating characteristics of such network can be hard task to be done in most cases. The analysis of modern programmatic facilities of design of work of network is in-process shown. Emulators of NS - 2, Riverbed OPNET Modeler, Cisco Packet Tracer are the representatives of large aggregate of such technical equipments. In the packages of design of network accessible the use of various equipment. It is oriented Cisco Packet Tracer to the design with application of equipment of firm Cisco. OPNET Modeler vice versa - oriented to creation of model with application of both existent equipment of different producers and models of equipment without attachment to the producer.

Keywords: power line, data transmission, Fourier transform.

Вступ

Сучасні технології дозволяють використовувати мережі зв'язку не тільки для звичайного перегляду web - сторінок і відправки електронних листів, але і для передачі голосу і відео. Трафік пакетних даних досяг таких обсягів, що для телекомунікаційних компаній будь-якого типу він став помітним джерелом доходів, тому мережі IP експлуатуються все активніше. З метою збільшення прибутку оператори намагаються підвищити ефективність використання мережі, а значить, методи оптимізації мереж IP набувають все більшої значущості. Максимальний комерційний ефект від мережі IP не може бути отриманий без раціонального використання всіх мережевих ресурсів - в першу чергу маршрутизаторів і каналів зв'язку. Функціонування пакетної мережі можна вважати ефективним тільки тоді, коли кожен ресурс завантажений, але водночас не перевантажений.

Кілька років тому послуги телебачення і телефону надавалися користувачам по різних мережах доступу. В кінці 90-х - початку 2000 року в телекомунікації почався новий етап розвитку індустрії, а саме конвергенція трафіку. Тепер по одним і тим же мереж доступу користувачі можуть отримувати послуги і телебачення, телефонії, доступу в Internet та ін. Види сервісів. Однак методи маршрутизації, які застосовувалися для трафіку єдиного типу сервісу, стали неефективними для трафіку пакетів різних сервісів.

У зв'язку з цим виникла потреба створення систем маршрутизації, які при побудові шляху враховували б не тільки технічні характеристики обладнання

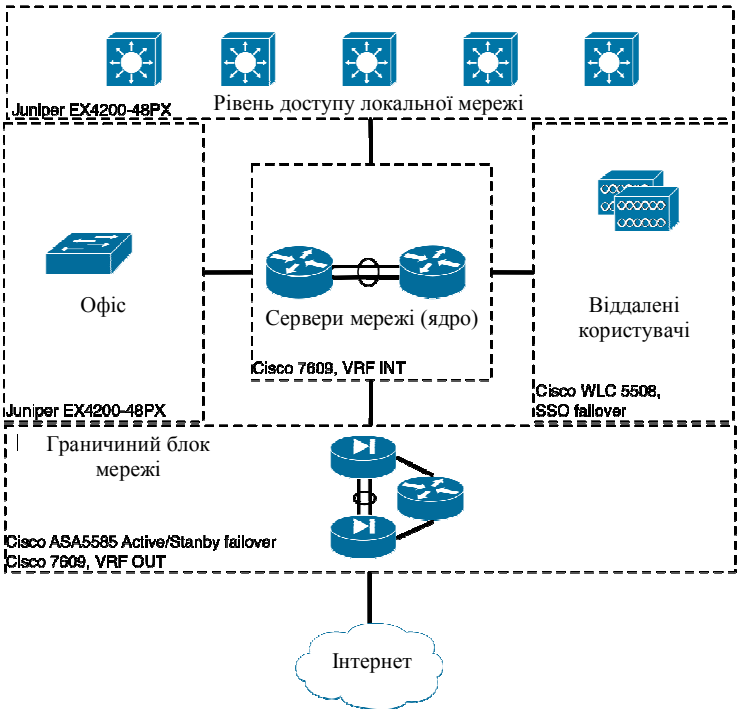


Рис. 1. Мережеве устаткування різного призначення

і каналів, а й його вартість.

Проблеми надання послуг необхідної якості

Для якісного надання будь-якої послуги оператори зв'язку повинні мати ресурсну базу (маршрутизатори, канали зв'язку та інше обладнання), технічні характеристики якої задовольняють всім вимогам цієї послуги. При цьому різні типи сервісів мають різні вимоги до технічних характеристик мережі зв'язку. Так, для простої передачі даних (пересилання електронної пошти або файлів) критична тільки ширина пропускання каналів зв'язку, тоді як для IP-телефонії найбільшим пріоритетом є мінімальний час затримки обробки IP пакетів на шляху проходження до адресата.

На різних ділянках мережі може перебувати різне обладнання зі своїм набором характеристик. Для деякого сервісу не всі пристрої мережі можуть задовольняти вимогам до ресурсів. Тому такі пристрої не повинні входити в маршрут прямування IP пакетів цього сервісу. Таким чином, не всі послуги можуть надаватися по деяких дільницях мережі.

Для вирішення завдань створення мереж розробляється мережеве устаткування різного призначення (рис. 1): комутатор - мережеве устаткування для об'єднання комп'ютерів в одну або декілька локальних мереж; маршрутизатор - пристрій, призначений для взаємодії комп'ютерів, що знаходяться в різних локальних мережах і надання доступу в мережу Інтернет; міжмережевий екран - пристрій, що забезпечує безпеку в мережі і так далі.

Технології, що використовувані при побудові захищених корпоративних мереж

Вибираючи технологію, яка використовуватиметься при реалізації проекту, необхідно відразу обертати уваги на декілька моментів. По-перше – технологія повинна задовольняти вимогам проекту – забезпечувати необхідну пропускну спроможність, масштабованість, захищеність передаваної інформації і так далі. По-друге, технологія має бути стандартизована, і широко поширена – це дозволить уникнути проблем в ході впровадження і експлуатації (наприклад, припинення підтримки вибраної технології виробниками устаткування). Ще один аргумент на користь рішень на основі стандартних протоколів – незалежність від виробника устаткування, і гарантія можливості подальшої модернізації мережі з використанням актуальних рішень.

Фізичний рівень визначає середовище передачі даних і протокол. Для ЛВС під вимоги актуальності для завдання проекту і поширеності підходить оптичне середовище передачі даних і вита пара. Для безпровідної – тільки радіоканал, причому в частотних діапазонах не вимагаючих додаткових дозволів на використання.

У виборі протоколів канального рівня для дротяної мережі – з поширених під вимогу поширеності, доступності і забезпечення пропускної спроможності підходить тільки сімейство IEEE 802.3, Ethernet. У другу чергу:

- 802.3ae, 10 Гбіт/з по оптичному волокну;
- 802.3ab, GigabitEthernet по витій парі;
- 802.3af, Power over ethernet;
- 802.3ad, агрегація каналів.

Емулятори мережевого обладнання

Усі емулятори мережевого устаткування можна розділити на дві основні групи:

1. Апаратно-реалізовані емулятори.
2. Програмно-реалізовані емулятори.

До першої групи відносять, як правило, вузько спеціалізоване устаткування, що дозволяє при підключенні до нього реального телекомунікаційного устаткування імітувати роботу реальної телекомунікаційної мережі, або якійсь її частині (як правило - каналів зв'язку). У апаратних емуляторах на апаратному рівні реалізовані процеси, що протікають в реальних мережах, - виникнення затримок, втрат пакетів, спотворення передаваних даних і тому подібне подій. Основна мета розробки і застосування апаратних емуляторів - дослідження роботи реального телекомунікаційного устаткування в різних умовах і при різних характеристиках каналів [**Ошибка! Источник ссылки не найден.**].

До другої групи емуляторів відносять спеціально розроблені програми, що дозволяють імітувати роботу устаткування і каналів зв'язку, а також роботу командних інтерфейсів активного мережевого устаткування [**Ошибка! Источник ссылки не найден.**]. Основна мета використання програмних емуляторів - застосування в якості науково-дослідної діяльності, для постановки наукових експериментів. Також, ці програми часто використовуються як повчальні системи для підготовки персоналу в роботі з мережевим устаткуванням [**Ошибка! Источник ссылки не найден.**].

Більшість емуляторів досить зручна у використанні, оскільки надають графічний інтерфейс для управління мережевою інфраструктурою, що буває набагато зручніший чим управління підключеннями реальних пристроїв [**Ошибка! Источник ссылки не найден.**].

Серед засобів імітаційного моделювання окремих подій і станів безпровідних сенсорних мереж на базі стандарту IEEE 802.15.4-2006 найбільше поширення отримала наступні середовища:

1. OPNET Modeler (поточна версія 16.0);
2. OMNET++ (поточна версія 4.1);
3. NS-2 (поточна версія 2.34).

NS-2 - об'єктно-орієнтоване середовище імітаційного моделювання дискретних подій і станів з

відкритим початковим кодом, яка розроблена у рамках проекту VINT. Середовище моделювання написане на C++ і TCL. NS-2 використовує TCL для генерації сценаріїв - це дозволяє генерувати комплексні сценарії за допомогою скриптів.

Спочатку NS-2 підтримував моделювання тільки статичних комп'ютерних мереж TCP/IP. Проте зараз мобільні вузли підтримуються, що дозволяє моделювати мобільні мережі ad-hoc. Підтримуються протоколи маршрутизації ad-hoc AODV, DSDV, DSR і TORA, але вони вимагають доопрацювання для коректної роботи з мобільними вузлами.

Для NS-2 існує модель, що реалізовує стандарт IEEE 802.15.4, розроблена Джинлиан Женгом та ін. Структура компонентів моделі LR - WPAN і основні її функції представлені на рис. 2.

Рис. 2.Структура компонентів моделі LR-WPAN NS-2

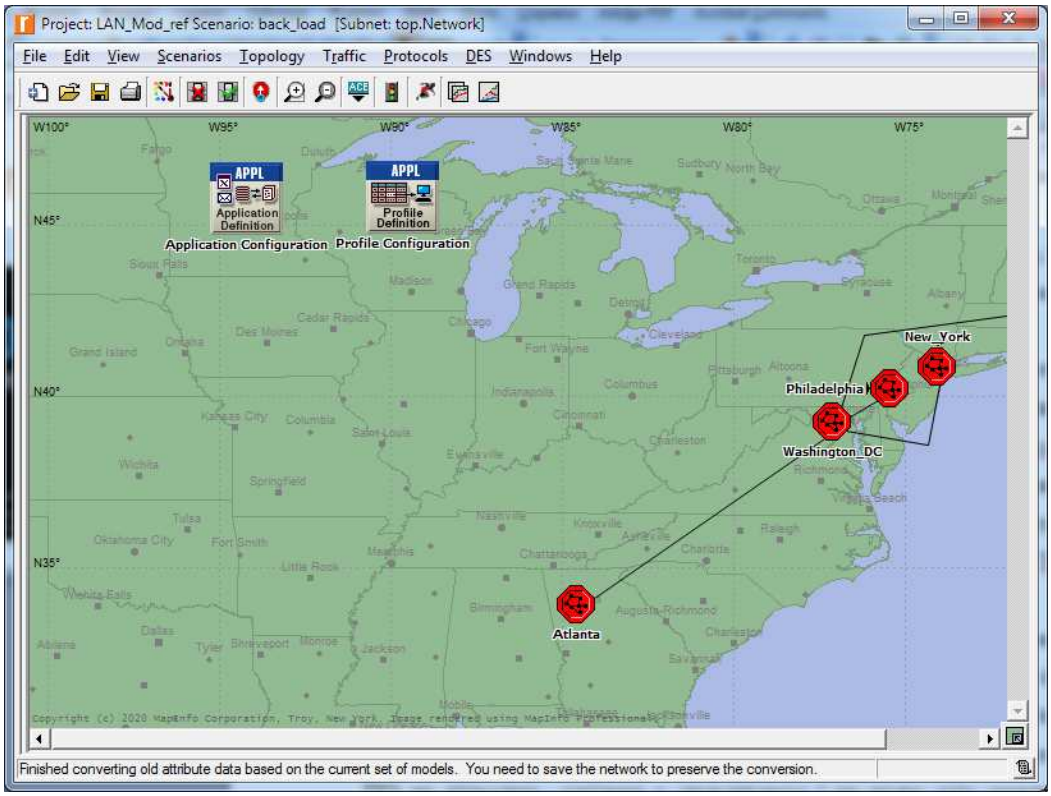


Рис. 3. Вікно програми проекту в середовищі OPNET Modeler 17.5

OPNET Modeler - потужне середовище імітаційного моделювання дискретних подій і станів. Вона включає безліч бібліотек мережевих технологій і протоколів зв'язку, таких як TCP/IP, протокол передачі гіпертексту (HTTP), технологія асинхронного режиму передачі (ATM) і FrameRelay, IP - QoS, 802.11 (Wi -

Fi), ZigBee та ін. (рис 3). Ці бібліотеки поставляють блоки для побудови моделей мереж. Одним з безлічі модулів, доступних в OPNET Modeler, є безпровідним модуль. Він розширює функціональність середовища для імітаційного моделювання і аналізу безпровідних мереж.

У версії OPNET Modeler 14.0 доступні моделі вузлів ZigBee, розроблені самою компанією OPNET. При цьому початковий код моделі мережевого рівня і рівня додатків прихований від користувачів. Доступний тільки код моделі нижнього рівня 802.15.4.

Найпопулярнішим емулятором мережевого устаткування є Cisco Packet Tracer, це емулятор, розроблений самою компанією Cisco Systems для навчання початкуючих фахівців. Packet Tracer отримав велике поширення за рахунок необхідності його застосування для проходження навчання у рамках програм Cisco Network Academy, мережевої академії, в якій щорічно проходять навчання десятки тисяч початкуючих фахівців [**Ошибка! Источник ссылки не найден.**].

Створення мережевої інфраструктури і подальша модифікація відбуваються через графічний інтерфейс, який є інтуїтивно зрозумілим і найбільш зручних з графічних інтерфейсів управління, що надаються даними програмними засобами емуляції мережевого устаткування. Інтерфейс добре адаптований для початкуючих фахівців і дуже сильно спрощує процес створення нових мережевих інфраструктур або запуск і налаштування необхідних для проведення практичних занять сервісів.

Висновок

5. Присутні на ринку програмних засобів технічні реалізації середовищ з моделювання параметрів телекомунікаційних мереж мають широкий спектр властивостей.

6. Для сучасного ПО властиво забезпечення моделювання мережевого устаткування відомих виробників. Так OPNET Academic Modeler містить моделі як відомих виробників так і моделі для маніпуляцій з налаштуваннями. UNetLab, навпаки моделює роботу обладнання Cisco, проте надає можливість емуляції роботи середовища операційної системи Cisco IOS.

7. Засоби емуляції також підтримують створення моделей мереж із застосуванням мобільних вузлів – ZigBee, LTE, Wi-Fi.

8. В пакетах моделювання мережі доступно використання різноманітного обладнання. Cisco Packet Tracer орієнтовано на моделювання із застосуванням обладнання фірми Cisco. OPNET Modeler навпаки – орієнтований на створення моделі із застосуванням як існуючого обладнання різних виробників, так і моделей обладнання без прив'язки до виробника.

Література

9. Локальные сети: архитектура, алгоритмы, проектирование. / Ю.В. Новиков, С.В. Кондратенко – М.: ЭКОМ, 2001. – 312 с.

10. Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя: пер. с англ. / А. Марк, Д. Спортак и др. – К.: Изд-во «ДиаСофт», 1999. – 468 с.

11. UNetLab: List of supported images [Электронный ресурс] / A. Dainese. URL: http://www.unetlab.com/documentation/supported-images/index.html – свободный. – Загл. с экрана. – Яз. Англ. Дата обращения: 16.03.2017 г.

References

1. Lokal'nye seti: arhitektura, algoritmy, proektirovanie. / Ju.V. Novikov, S.V. Kondratenko – M.: JeKOM, 2001. – 312 s.

2. Komp'juternye seti. Kniga 2: Networking Essentials. Jenciklopedija pol'zovatelja: per. s angl. / A. Mark, D. Sportak i dr. – K.: Izd-vo «DiaSoft», 1999. – 468 s.

3. UNetLab: List of supported images [Jelektronnyj resurs] / A. Dainese. URL: http://www.unetlab.com/documentation/supported-images/index.html – svobodnyj. – Zagl. s jekrana. – Jaz. Angl. Data obrashhenija: 16.03.2017 g.

Рецензія/Peer review : 09.10.2020 р. Надрукована/Printed :06.12.2020 р.

Повні вимоги до оформлення рукопису
http://journals.khnu.km.ua/vestnik/support.htm

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 3 від 29.10.2020 р.

Підп. до друку 29.10.2020 р. Ум.друк.арк. 36,51 Обл.-вид.арк. 34,74
Формат 30х42/4, папір офсетний. Друк різографією.
Наклад 100, зам. № ____

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу "Вісник Хмельницького національного університету"
редакційно-видавничим центром Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1. тел (0382) 72-83-63

Дипломна робота

магістра із спеціальності 172 Телекомунікації та радіотехніка

тема роботи: **МЕТОД МАКСИМІЗАЦІЇ ПРОПУСКНОЇ ЗДАТНОСТІ МЕРЕЖІ ЗАДАНОЇ ТОПОЛОГІЇ**

Студент: **Польнов Олексій Олегович, гр. ТРм-19-2**

Керівник **к.т.н., доц. Горященко Костянтин Леонідович**

Мета роботи: Дослідження сучасних програмних засобів моделювання телекомунікаційних мереж при сталому розміщенні вузлів в просторі та можливості визначення варіантів підключення між собою на прикладі бездротових мереж

Об’єкт дослідження: Засоби моделювання телекомунікаційних мереж

Предмет дослідження: Методи моделювання передачі інформації в мережах при взаємодії з бездротовими пристроями стандарту ZigBee

ЗАДАЧІ ДОСЛІДЖЕННЯ

1. Виконати аналіз проблематики створення телекомунікаційної мережі різної складності. А особливо проаналізувати взаємодію телекомунікаційних мереж, що складаються зі стаціонарних елементів та мобільних пристроїв.

2. Проаналізувати існуючі принципи створення топології мережі. Для цього розглянути програмне забезпечення з емуляції роботи мережевого устаткування.

3. Провести дослідження роботи мережі у віртуальному середовищі програми емулятора мережі з використанням моделі бездротового пристрою для визначення конфігурацій з найкращими параметрами роботи.

Науково-практичне значення отриманих результатів

Розглянуто існуючі безкоштовні та умовно-безкоштовні програмні засоби, що дозволяють виконувати задачі моделювання схеми, зв’язків та визначення фізичних параметрів телекомунікаційних мереж.

СТАН ПРОБЛЕМАТИКИ НАДАННЯ ШИРОКОСМУГОВОДУ ДОСТУПУ

Для **якісного надання** будь-якої послуги оператори зв’язку повинні мати **ресурсну базу** (маршрутизатори, канали зв’язку та інше обладнання), технічні характеристики які задовольняють всім вимогам цієї послуги.

З метою **збільшення прибутку** оператори намагаються **підвищити ефективність використання мережі**, а значить, методи оптимізації мереж IP набувають все більшої значущості.

Максимальний комерційний ефект від мережі IP **не може** бути отриманий без раціонального використання всіх мережевих ресурсів - в першу чергу маршрутизаторів і каналів зв'язку. Функціонування пакетної мережі можна вважати ефективним тільки тоді, коли кожен ресурс завантажений, але водночас не перевантажений.

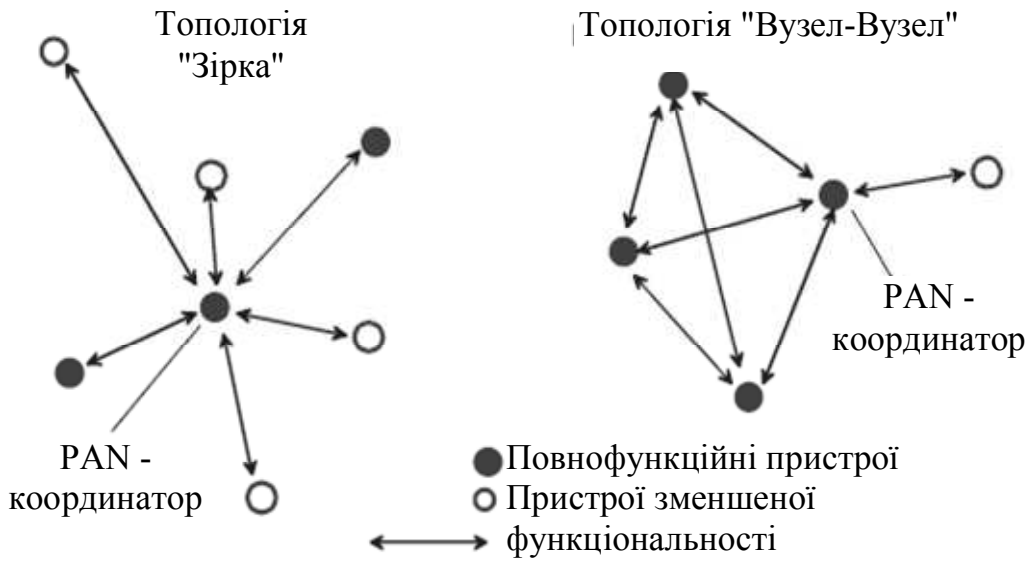


Рисунок 3.1 – топологія мережі

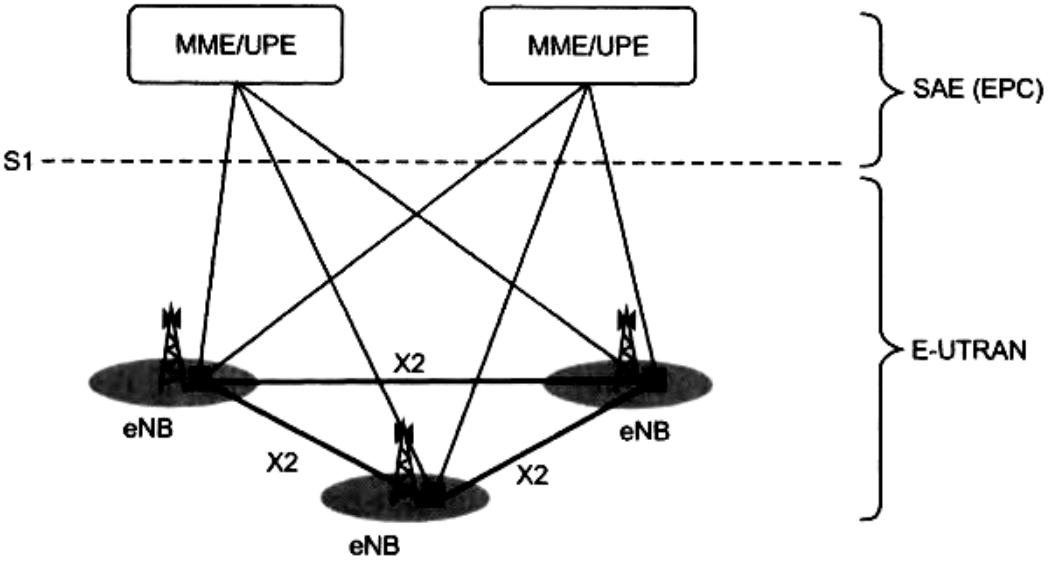


Рисунок 3.2 – взаємодія мережі радіодоступу і базової мережі SAE

УЗАГАЛЬНЕНА МЕРЕЖЕВА ІНФРАСТРУКТУРА

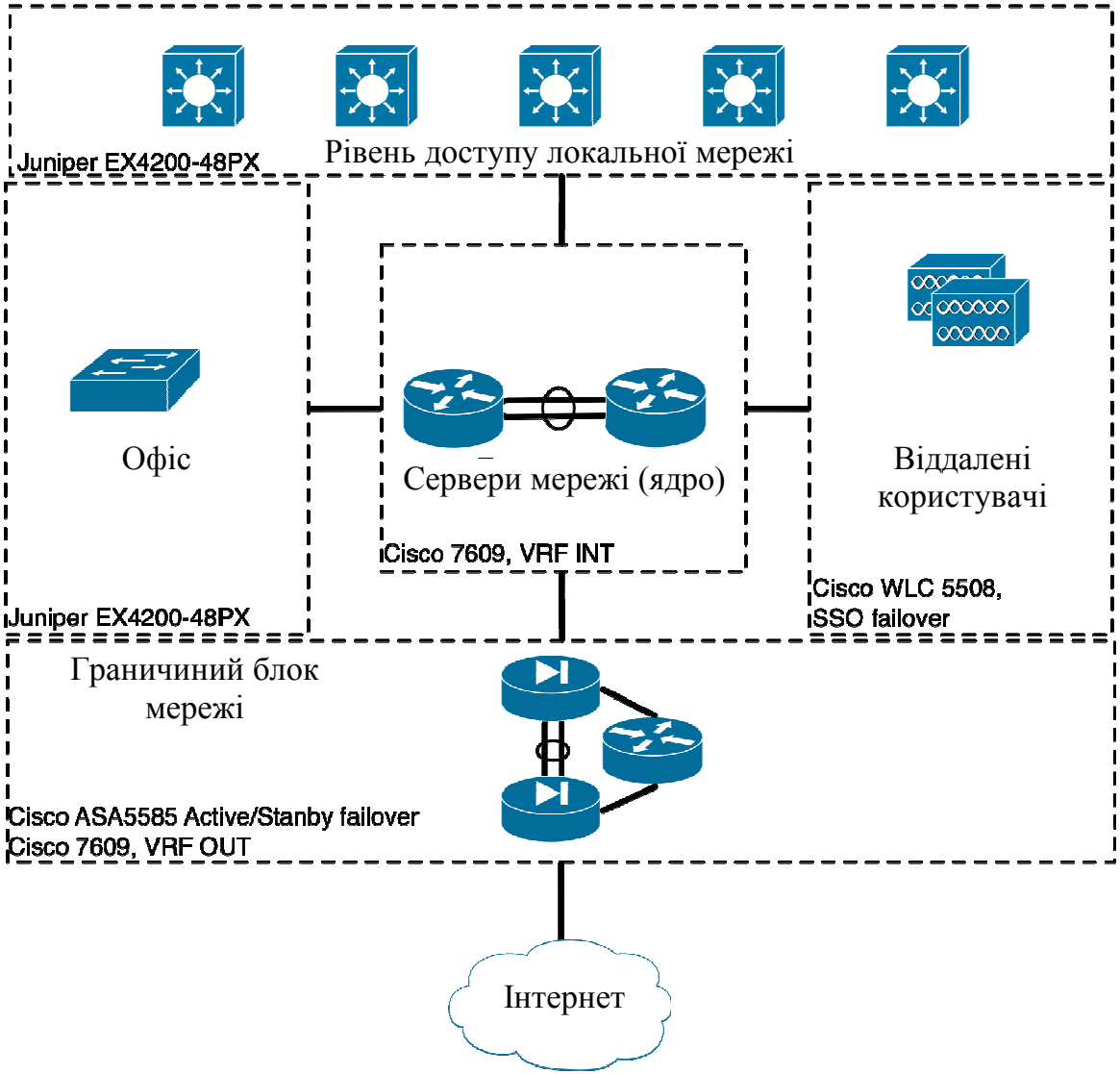


Рисунок 4.1 – схема зв'язків між структурними блоками мережі (приклад)

На сьогодні існує безліч компаній, що виробляють мережеве устаткування, і компанія Cisco Systems вважається безумовним фаворитом на ринку мережевого устаткування (займає близько 70% ринку) і пропонує пристрої для створення обчислювальних мереж від невеликого офісу до великих корпорацій.

Враховуючи широке поширення мережевого устаткування під управлінням Cisco IOS (Internetwork Operating System — Міжмережева Операційна Система), а також високу вартість цього устаткування, ще яснішою стає необхідність в застосуванні програмних емуляторів мережевого устаткування для створення моделей обчислювальних мереж

ТЕХНОЛОГІЇ ДЛЯ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

Набір протоколів передачі даних IEEE 802

- 802.3 Ethernet;
- 802.4 Token bus;
- 802.5 Token ring;
- 802.6 Distributed Queue Dual Bus;
- 802.9 “isoEthernet";
- 802.10 SDE;
- 802.11 Wi – Fi;
- 802.12 100BaseVG;
- 802.15 Bluetooth;
- 802.16 WMAN;
- 802.17 RPR.

Стандарти для безпровідної мережі:

- IEEE 802.15 (Bluetooth)
- IEEE 802.16 (WMAN, WiMAX)
- IEEE 802.11 (Wi – Fi) – набір стандартів, найбільш поширені 802.11b, 802.11a, 802.11g, 802.11n.

Протоколи канального рівня для проводової мережі

сімейство IEEE 802.3, Ethernet.

Що складається з:

- 802.3ae, 10 Гбіт/з по оптичному волокну
- 802.3ab, Gigabit Ethernet по витій парі
- 802.3af, Power over ethernet
- 802.3ad, агрегація каналів

ЕМУЛЯТОРИ МЕРЕЖЕВОГО УСТАТКУВАННЯ ТА МОДЕЛІ БЕЗДРОТОВИХ КОМПОНЕНТ МЕРЕЖІ ЗА IEEE 802.15.4

NS-2 (Network Simulator Version 2)

NS-2 - об'єктно-орієнтоване середовище імітаційного моделювання дискретних подій і станів з відкритим початковим кодом, яка розроблена у рамках проекту VINT. Середовище моделювання написане на C++ і TCL. NS-2 використовує TCL для генерації сценаріїв - це дозволяє генерувати комплексні сценарії за допомогою скриптів.

Рисунок 6.1 – Структура компонентов модели LR-WPAN

OPNET MODELER (OPTIMIZED NETWORK ENGINEERING TOOLS)

OPNET Modeler - потужне середовище імітаційного моделювання дискретних подій і станів. Вона включає безліч бібліотек мережевих технологій і протоколів зв'язку, таких як TCP/IP, протокол передачі гіпертексту (HTTP), технологія асинхронного режиму передачі (ATM) і FrameRelay, IP - QoS, 802.11 (Wi - Fi), ZigBee та ін.

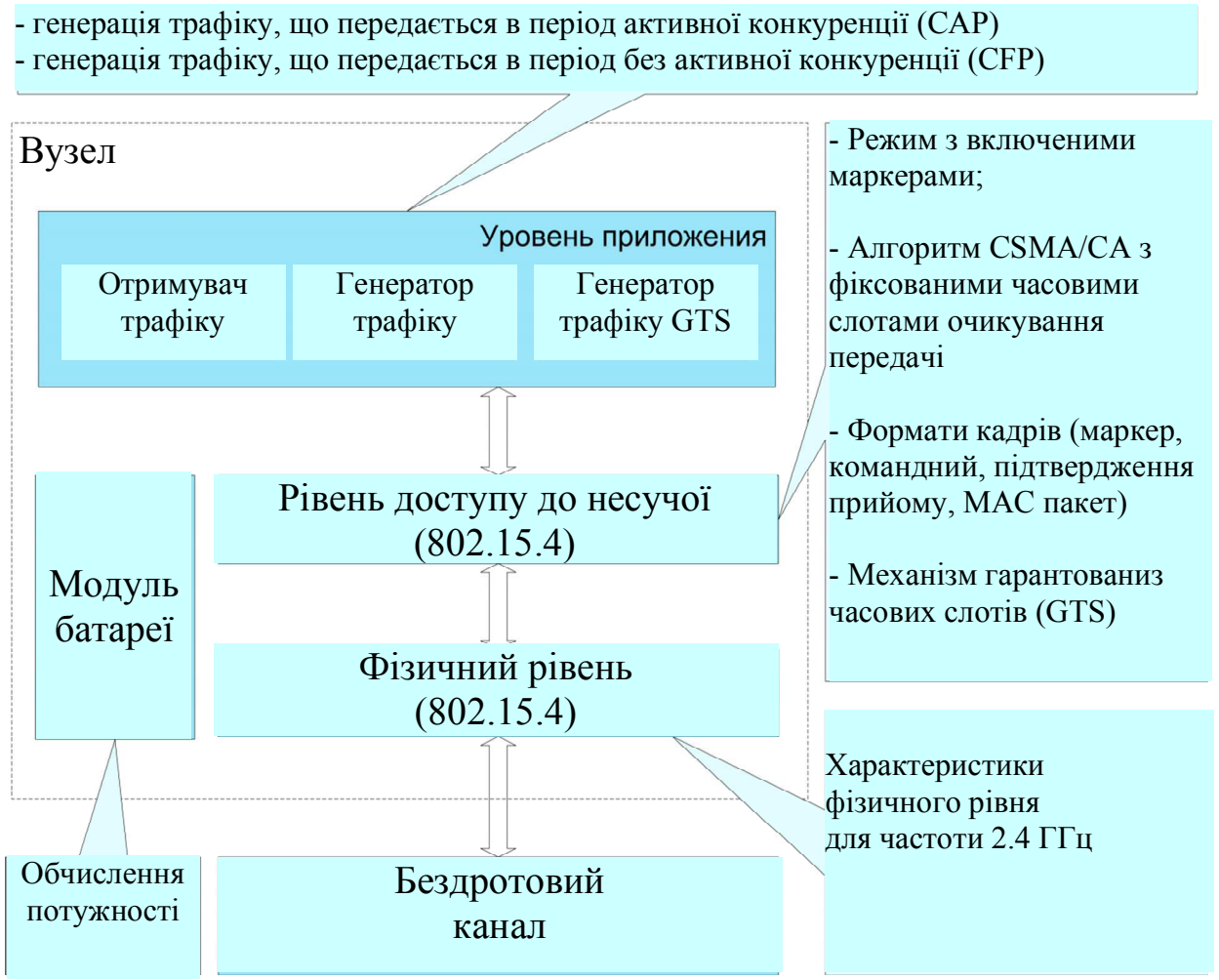


Рисунок 7.1 – Модель OPEN-ZB 2.1

OPNET MODELER (OPTIMIZED NETWORK ENGINEERING TOOLS) (продовження)

Вбудована в OPNET Modeler 14.0 реалізує не лише фізичний рівень і рівень доступу до середовища стандарту IEEE 802.15.4-2006, але і мережевий рівень ZigBee. Модель підтримує топології: зірка, дерево, і комірчаста мережа.

Модель містить три типи вузлів відповідно до специфікації ZigBee :

1. Координатор (Coordinator);
2. Маршрутизатор (Router);
3. Кінцевий пристрій (End Device).

Рисунок 8.1 – Вбудована модель OPNET Modeler 14.0

ДОСЛІДЖЕННЯ МЕРЕЖЕВОЇ СТРУКТУРИ У СЕРЕДОВИЩІ UNETLAB ВІД CISCO

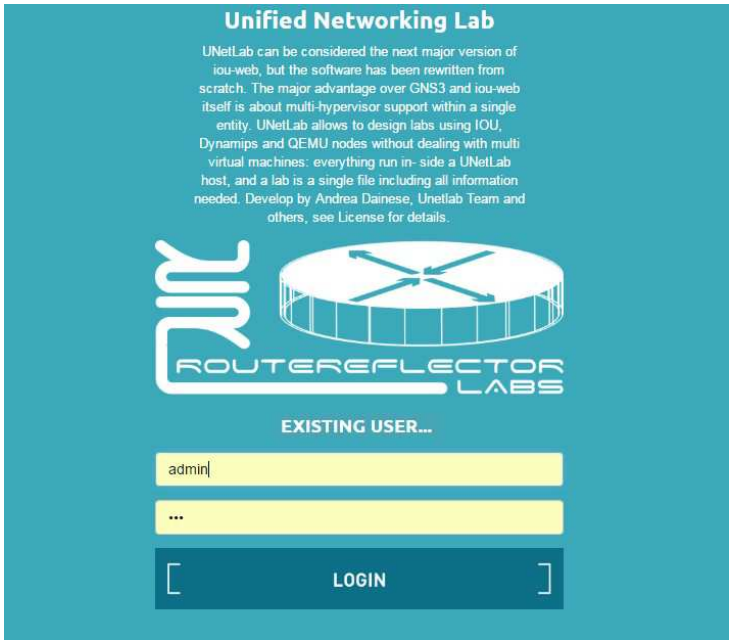


Рисунок 9.1 – аутентифікація користувача в системі UNetLab

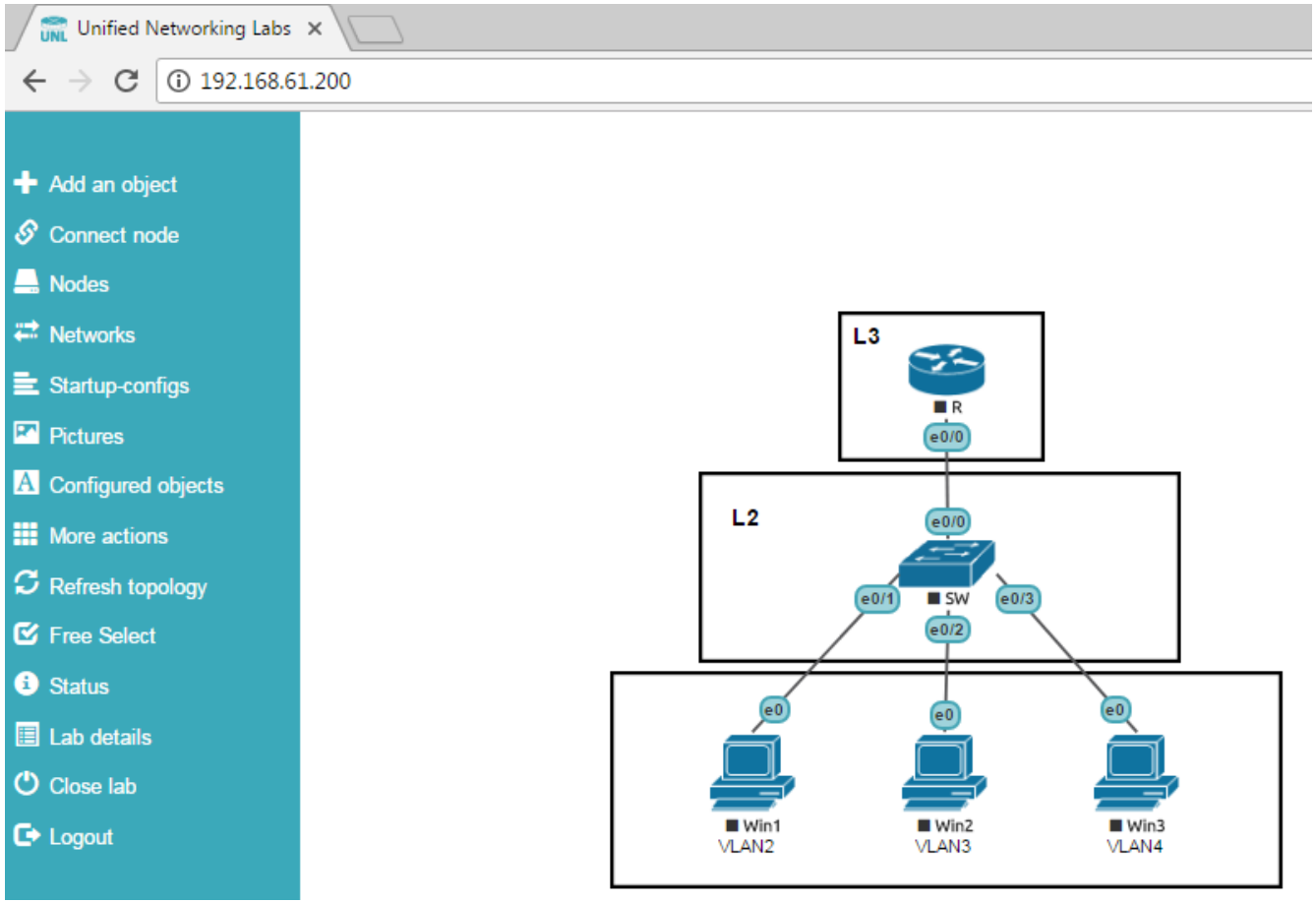


Рисунок 9.2 –модель обчислювальної мережі

ПРОЕКТУВАННЯ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

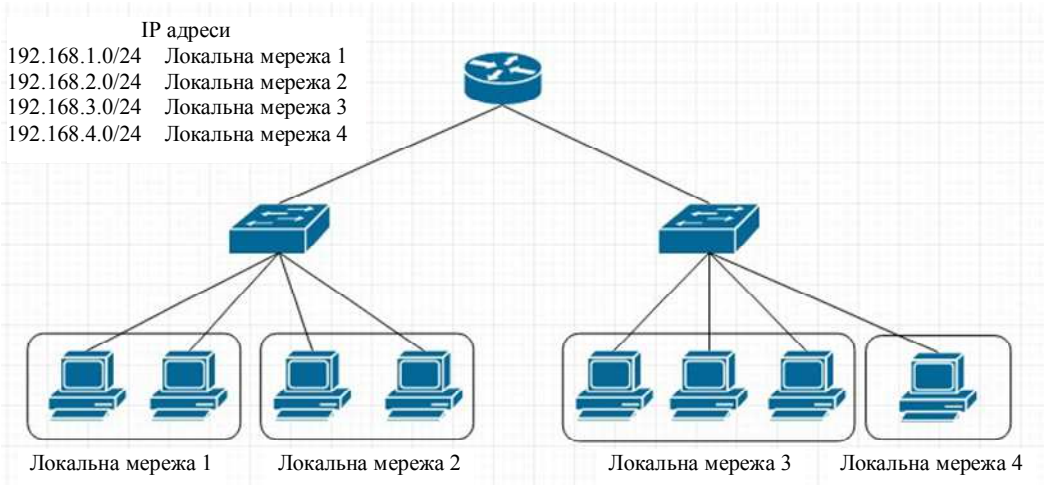


Рисунок 10.1 – Концепція, що відображає просту обчислювальну мережу

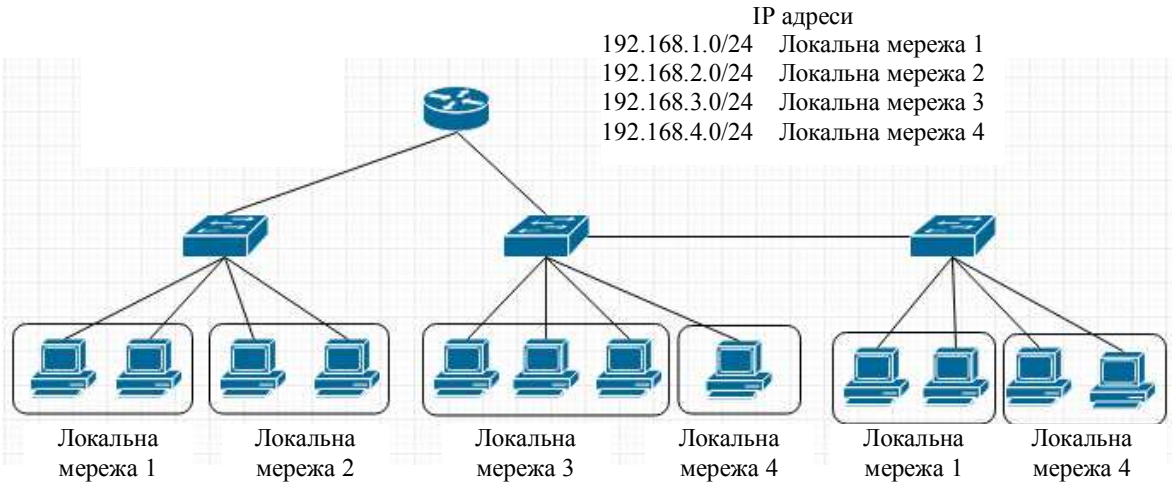
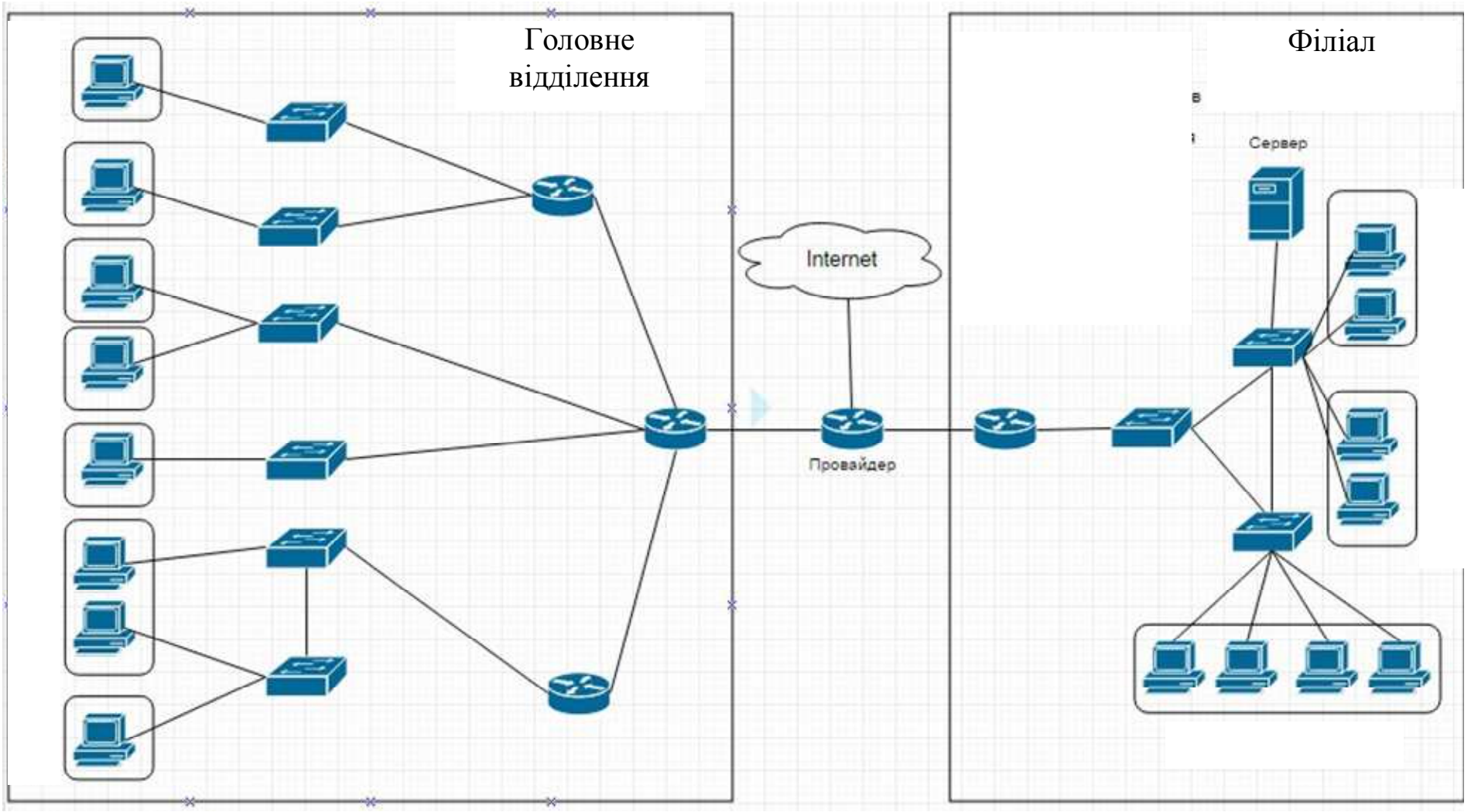


Рисунок 10.2 – Логічне продовження попередньої концепції – завдання логічного об'єднання обчислювальних машин в єдину локальну мережу, але фізично підключених до різних комутаторів.

Одним з **головних принципів в архітектурі** обчислювальних мереж **є принцип модульності**. Принцип модульності має на увазі те, що усю **архітектуру обчислювальної мережі** можна **розбити на окремі модулі**, що, у свою чергу, дозволяє зосередитися на функціоналі кожного модуля окремо, при цьому, такий підхід спрощує її впровадження і управління.

ПРОЕКТУВАННЯ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ. Розвиток концепції



Випадок, коли у компанії з'являється територіально віддалена філія і з'являється необхідність в створенні загальної обчислювальної мережі для можливості мережевої взаємодії між об'єктами різних філій. Оскільки, кожна філія має доступ в інтернет через виділений IP-адрес своїм провайдером, то між цими IP-адресами буде створений спеціальний тунель, через який і протікатиме уся інформація між філіями

Моделювання обчислювальних мереж в UNetLab

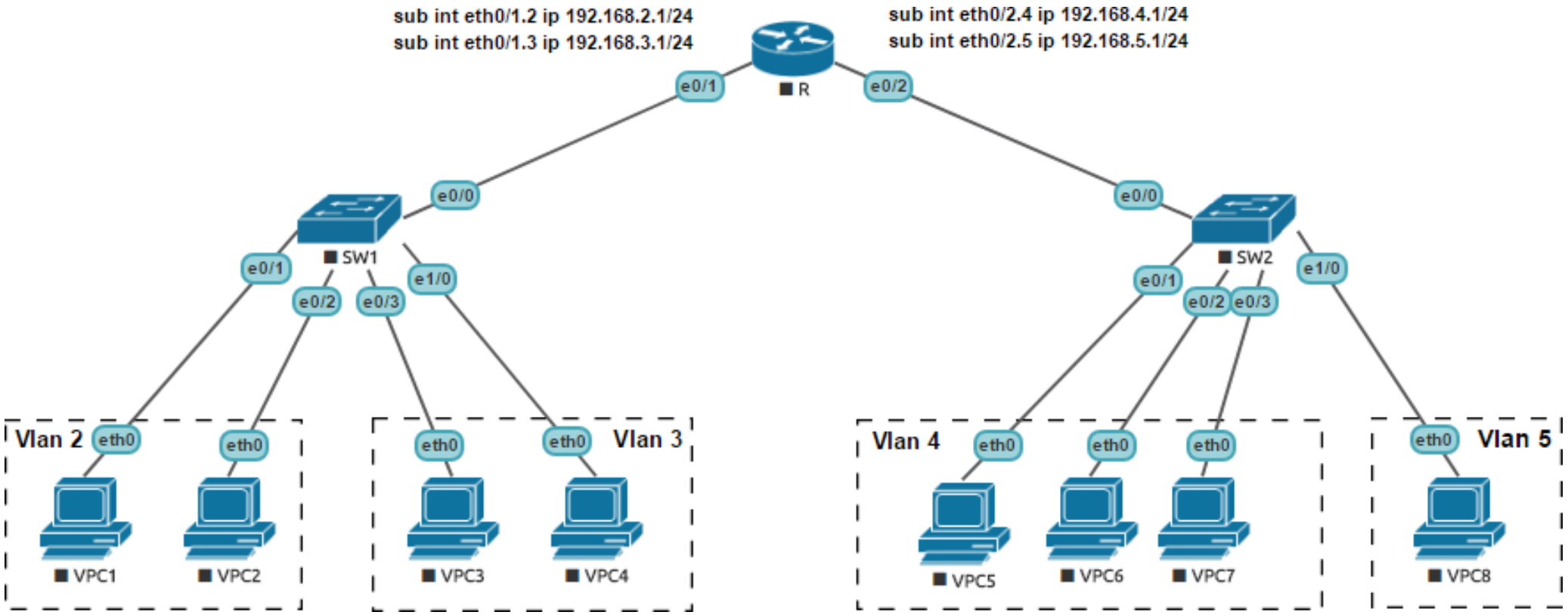


Рисунок 12.1 – Спроектована модель обчислювальної мережі №1

Модель, зображена на рис. 12.1, є моделлю, що складається з двох комутаторів SW1 і SW2 і маршрутизатора R, і відображає просту обчислювальну мережу, головною метою якої є об'єднання в єдину мережу обчислювальні машини підприємства і створення можливості мережевої взаємодії між ними.

ТЕСТУВАННЯ НАВАНТАЖЕННЯ ЗМОДЕЛЬОВАНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Результат

– Максимальна завантаженість каналів на комутаторах SW1 і SW2 дорівнювала 147 кб/с;
– Максимальна завантаженість каналів на маршрутизаторі дорівнювала 5,33 кб/с;
– Завантаження процесора маршрутизатора не перевищувало 2%.

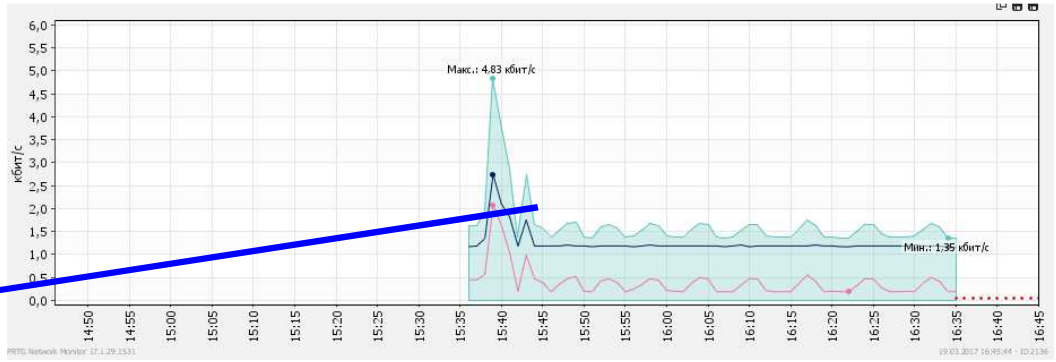
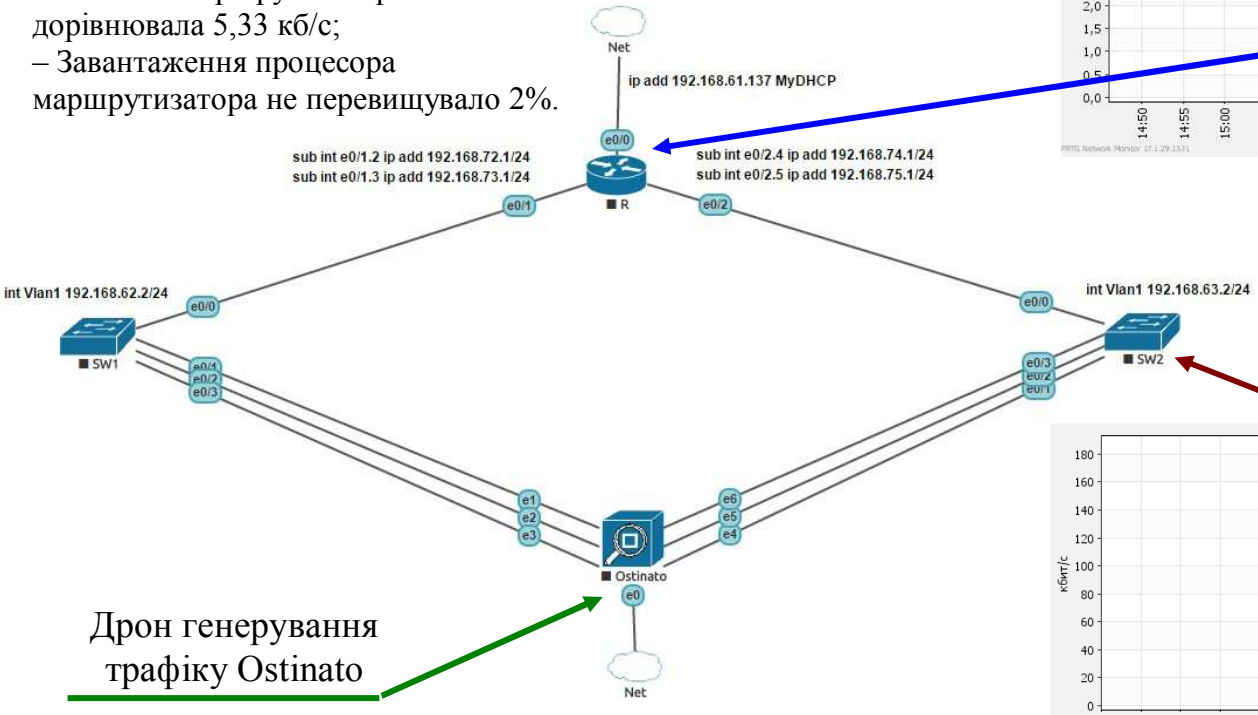


Рисунок 13.1 – Результати тестування навантаження для маршрутизатора



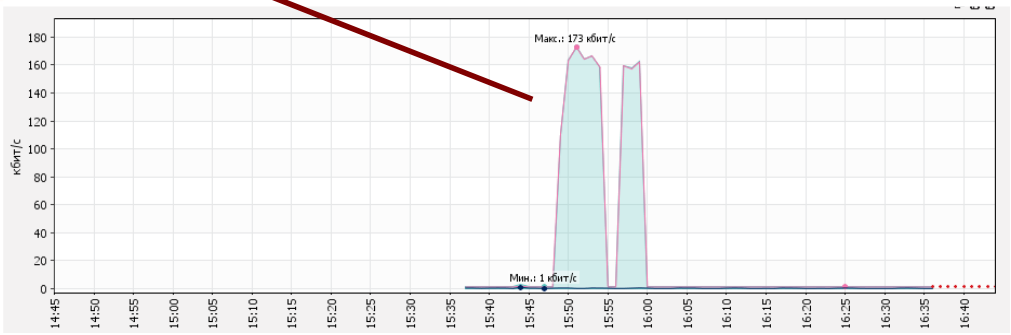


Рисунок 13.2 – Результати тестування навантаження для комутатора

Рисунок 13.1 – Модель із підключенням дрона Ostinato

до спроектованої модель обчислювальної мережі для генерації трафіку

ВИСНОВКИ

1. В роботі проведено аналіз проблематики побудови телекомунікаційних мереж різної складності. Особлива увага приділена мережам, в яких учасники мережі є мобільними пристроями, що характерно для мереж із застосуванням безпровідних пристроїв (ZigBee, LTE).

2. Проаналізовані існуючі принципи створення топології мережі. Встановлено, що існує цілий клас програм – емуляторів мережевого устаткування. Визначено, що ці емулятори дозволяють в різній мірі виконати побудову топології мережі, що включає в собі моделі маршрутизаторів, комутаторів, серверів, локальних користувачів. Особлива увага в аналізі присвячена моделям бездротових пристроїв – ZigBee пристроям. А також показано, які технології забезпечення зв’язку через тунелі між сегментами мережі використовуються.

3. Виконано віртуалізація мережевого устаткування в середовищі UNetLab від компанії Cisco. А також проведено моделювання роботи мережі при взаємодії з бездротовим вузлом, в якості якого використано дрон – генератор трафіку.

ДЯКУЮ

ЗА

УВАГУ !

Завідувачу
кафедри телекомунікацій,
медійних та інтелектуальних
технологій (ТМІТ)
Підченко С.К.
здобувача вищої студента
Польнова Олексія Олеговича
2 курсу, гр. ТРм-19-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

02.12.20 Польнов О. О.

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 11%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 83556 Название: Метод максимізації пропускної здатності мережі заданої топології Добавлено в БД: 2020-12-10 Авторы: Польнов Олексій Олегович Руководители: Горященко Костянтин Леонідович Консультанты: Оппоненты:	Символы	Лексемы	Символы	Лексемы
	94722	1484	2829 (3%)	52 (4%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Имя пользователя:
Kafedra TMIT KhNU

ID проверки:
1005418747

Дата проверки:
10.12.2020 10:17:48 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
10.12.2020 10:22:15 EET

ID пользователя:
100005657

Название файла: Польнов_ТРм-19-2

Количество страниц: 90 Количество слов: 15579 Количество символов: 126709 Размер файла: 3.45 MB ID файла: 1005710506

829 слов помечены как "исключенные" и не учитываются в подсчете слов

5.63% Совпадения

Наибольшее совпадение: 3.24% с Интернет-источником (http://dspace.wunu.edu.ua/bitstream/316497/28051/1/%D0%9...

5.34% Источники из Интернета 109 ..... Страница 92

0.45% Источники из Библиотеки 4 ..... Страница 93

0.98% Цитат

Цитаты 5 ..... Страница 94

Не найдено ни одной ссылки

0% Исключений

Нет исключенных источников

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы 15

РЕЦЕНЗІЯ

на дипломну роботу студента групи ТРм-19-2

Польнова Олексія Олеговича

"Метод максимізації пропускної здатності мережі заданої топології"

Дипломна робота присвячена розгляду питань побудови та моделювання параметрів телекомунікаційної мережі. Розвиток систем телекомунікацій, поява послуг з передачі відео, аудіо призвело до появи мережі нового покоління – NGN-мережі. Одночасно з цим, обсяги мережі, її учасники стрімко зросли. Сучасна мережа представляє собою динамічно формовану мережу. Пріоритетними завданнями стає збільшення ширини пропускання каналів зв'язку і зменшення загасання сигналу на одиницю довжини каналу.

В дипломній роботі магістра ставиться та виконується декілька завдань, а саме:

- проведено аналіз проблематики створення телекомунікаційний мереж різної складності з врахуванням особливостей проаналізувати взаємодію телекомунікаційних мереж з мобільними пристроями;
- показано існуючі принципи створення топології мережі, проведено докладний аналіз програмного забезпечення з емуляції роботи мережевого устаткування;
- виконано дослідження роботи мережі у віртуальному середовищі програми емулятора мережі з використанням моделі бездротового пристрою для визначення конфігурацій з найкращими параметрами роботи.

Робота складається з 4-х розділів, кожен з яких відповідає суті поставлених задач. Загальний обсяг роботи – 90 сторінок. В роботі 19 посилань на літературні джерела, а також 41 рисунок та 4 таблиці.

В роботі виконано достатнє дослідження щодо програмних рішень як з моделювання самої мережі на прикладі обладнання фірми Cisco, так і показані параметри моделей бездротових модулів ZigBee, що моделюють в них. Робота містить посилання на літературу з посиланням на джерела відповідних запозичень.

Викладення матеріалу в розділах є послідовним та пов'язаним між собою. В роботі міститься достатня кількість власних та запозичених ілюстрацій. Припущення та висновки мають достатнє обґрунтування та детальне пояснення. Мова викладення роботи є технічно грамотною, зрозумілою. Оформлення пояснювальної записки знаходиться на належному рівні, граматичних та стилістичних помилок дуже обмежена кількість.

Серед позитивних сторін магістерської роботи слід відмітити наступне:

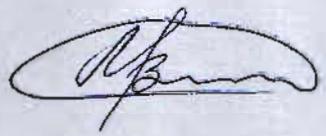
1. В роботі проведено аналіз проблематики побудови телекомунікаційних мереж різної складності з врахуванням мережам з безпровідними пристроями –(ZigBee, LTE).

2. Проаналізовані існуючі принципи створення топології мережі. Розглянуті сучасні програми – емуляторів мережевого устаткування, такі як OPNET Modeler, NG-2 та інші.

3. Показано покрокове створення мережі від найпростішої до складної в середовищі UNetLab від компанії Cisco. А також проведено моделювання роботи мережі при взаємодії з бездротовим вузлом.

В цілому дипломна робота магістра Польнова Олексія Олеговича "Метод максимізації пропускної здатності мережі заданої топології" повністю відповідає вимогам до кваліфікаційних робіт магістра та заслуговує на оцінку "відмінно", а її автор – на присвоєння кваліфікаційного рівня магістра зі спеціальності 172 – "Телекомунікації та радіотехніка".

Рецензент:

д.т.н., проф., зав.каф. АКІТ  Мартинюк В. В.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ

ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Технологія передачі сигналів мережею електроживлення
Автор: Польнов Олексій Олегович
Спеціальність: 172 Телекомунікації та радіотехніка
Освітня програма Телекомунікації та радіотехніка
Науковий керівник к.т.н., доц. Горященко Костянтин Леонідович
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнуті. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: В роботі виявлені запозичення зі сторонньої літератури, загальним обсягом у розмірі 5,63%. Виявлені запозичення мають місце в 1, 2, 3 розділах. Виявлені запозичення співпадають із визначеннями зі стандартів та типових виразів з літератури в галузі телекомунікацій із застосуванням спеціальної термінології. Цитати та запозичення містять посилання на відповідні джерела літератури, що використані в роботі. Результати досліджень не містять запозичень. Висновки по роботі є унікальними та також не містять запозичень. Робота приймається до захисту.

10.12.2020 р.

Науковий керівник роботи: К.Л. Горященко

Зав. каф. ТМІТ С.К.Підченко