Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: *Оцінювання ефективності роботи мультисервісної мережі зв'язку засобами імітаційного моделювання*

Виконав(ла): студент(ка) *6* курсу, групи *РРм-61*
спеціальності *172 Телекомунікації та радіотехніка*
(шифр і назва спеціальності)

(підпис) *Николин О.І.* (прізвище та ініціали)

Керівник (підпис) *Яськів В.І.* (прізвище та ініціали)

Нормоконтроль (підпис) *Хвостівська Л.В.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Дунець В.Л.* (прізвище та ініціали)

Рецензент (підпис) *Хвостівський М.О.* (прізвище та ініціали)

Тернопіль
2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *прикладних інформаційних технологій та електроінженерії*
(повна назва факультету)

Кафедра *радіотехнічних систем*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Дунець В.Л.*
(підпис) (прізвище та ініціали)
« »
2020 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *172 Телекомунікації та радіотехніка*
(шифр і назва спеціальності)

студенту *Николину Оресту Ігоровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Оцінювання ефективності роботи мультисервісної мережі зв'язку засобами імітаційного моделювання*

Керівник роботи *Яськів Володимир Іванович, к.т.н., доц.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*24*» *листопада* 20*20* року № *4/7-870*

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Об'єкт дослідження: процес оцінювання ефективності роботи мультисервісної мережі; Предмет дослідження:: засоби імітаційного моделювання

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналітична частина
2. Основна частина
3. Науково-дослідна частина
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та	*Зелінський І.М., доц. каф. ПВ*		
безпека в надзвичайних	*Клепчик В.М., стар. викл. каф. ОХ*		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*		
2	*Аналіз завдання*		
3	*Виконання розділу 1*		
4	*Виконання розділу 2*		
5	*Виконання розділу 3*		
6	*Виконання розділу 4*		
7	*Оформлення пояснювальної записки*		
8	*Оформлення графічного та презентаційного матеріалу*		
9	*Перевірка роботи на антиплагіат*		
10	*Попередній захист*		
11	*Захист*		

Студент _____ *Николин О.І.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Яськів В.І.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Оцінювання ефективності роботи мультисервісної мережі зв'язку засобами імітаційного моделювання» // Кваліфікаційна робота // Николин Орест Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, група РРм-61 // Тернопіль, 2020 // с. – 70, рис. – 38, табл. – 5, додат. – 1, бібліогр. – 63.

КЛЮЧОВІ СЛОВА: МУЛЬТИСЕРВІСНА МЕРЕЖА, IPV4, IPV6, VLAN, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ, RIVERBED MODELER.

В кваліфікаційній роботі здійснено процес оцінювання ефективності мультисервісної мережі засобами комп'ютерного імітаційного моделювання LabView.

Розроблено імітаційну модель мультисервісної мережі для моделювання її поведінки при різних сценаріях із використанням технології Riverbed Modeler. Оцінено ефективність мультисервісної мережі із застосуванням засобів імітаційного моделювання з різними параметрами мережі при використанні протоколів IPv4 та IPv6. На підставі отриманих результатів моделювання мережевих сценаріїв здійснено процедуру порівняння ефективності роботи протоколів IPv4 і IPv6.

Оцінено ефективність мультисервісної мережі із застосуванням засобів імітаційного моделювання при різних параметрів мережі при використанні VLAN.

ANNOTATION

Theme of qualification work: " Evaluation of the efficiency of the multiservice communication network by means of simulation modeling" // Qualification work // Nykolyn Orest Ihorovych // Ternopil Ivan Puluj National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, group RRm-61 // Ternopil, 2020 // p. – 70, fig. – 38, tab. – 5, Add – 1, Ref. – 863.

Keywords: MULTISERVICE NETWORK, IPV4, IPV6, VLAN, SIMULATION MODELING, RIVERBED MODELER.

In the qualification work the process of evaluating the efficiency of the multiservice network by means of computer simulation modeling LabView is carried out.

A simulation model of a multiservice network has been developed to model its behavior in different scenarios using Riverbed Modeler technology.

The efficiency of the multiservice network with the use of simulation tools with different network parameters using IPv4 and IPv6 protocols is evaluated. Based on the obtained results of network scenario modeling, the procedure of comparing the efficiency of IPv4 and IPv6 protocols was carried out.

The efficiency of the multiservice network with the use of simulation tools at different network parameters when using VLAN is evaluated.

ЗМІСТ

ВСТУП

Актуальність роботи. Інтенсивний розвиток мереж зв'язку та інформаційних технологій призвело до розробки та впровадження сучасних інформаційно-комунікаційних мереж зв'язку, які сумісні з більшістю послуг сфер діяльності людини. Практично на сьогодні мережі зв'язку різних організацій, а також мультисервісні мережі мікрорайонів, можуть досягати сягати великих розмірів, підтримувати широкий спектр послуг та мати гарну масштабованість. Така організація мереж не можлива без об'єднання великої кількості активних мережевих пристроїв в окремі мережеві сегменти, що призводить до появи великого обсягу службового трафіку в мережі, що зумовлює додаткові затримки трафіку, збільшення часу перебування пакетів в мережі і складності адміністрування таких мереж. Найчастіше прагнення операторів зв'язку до збільшення ефективності роботи мультисервісних мереж зводитися до оптимізації таких параметрів як пропускна здатність, часові затримки пакета в мережі, завантаження серверів, швидкості роботи вузлового мережевого обладнання. На сьогодні дану задача вирішують за рахунок застосування нових технологій таких як організація віртуальних локальних мереж VLAN і використання протоколу IPv6, які дають змогу збільшити ефективність роботи мережі. Проте, не всі нові підходи можуть бути досить ефективними в тому чи іншому випадку. Таким чином, для того щоб вирішити застосовувати ту чи іншу технологію в інфокомунікаційних мережах в конкретному випадку вдаються до імітаційного моделювання, яке дає змогу на ранній стадії проектувати та досліджувати мережі.

Отже, оцінювання ефективності мультисервісної мережі з точки зору часу затримки пакетів, пропускної здатності, завантаження мережевих вузлів, за допомогою засобів імітаційного моделювання при впровадженні технологій є актуальною задачею.

Мета і завдання дослідження. Метою дослідження є оцінювання ефективності в роботі мультисервісної мережі із застосуванням засобів імітаційного моделювання.

Досягнення цієї мети вимагає розв’язання таких задач:

1. Проведено аналіз існуючих протоколів мультисервісних мереж зв'язку з метою обґрунтування напряму дослідження

2. Розробити імітаційну модель мультисервісної мережі для моделювання її поведінки при різних сценаріях.

3. Оцінити ефективність мультисервісної мережі із застосуванням засобів імітаційного моделювання з різними параметрами мережі при використанні протоколів IPv4 та IPv6.

4. Оцінити ефективність мультисервісної мережі із застосуванням засобів імітаційного моделювання при різних параметрів мережі при використанні VLAN.

Об’єкт дослідження: процес оцінювання ефективності роботи мультисервісної мережі

Предмет дослідження: засоби імітаційного моделювання

Новизна отриманих результатів. Застосування засобів імітаційного моделювання на базі технології Riverbed Modeler дало змогу визначити показники ефективність мультисервісної мережі при використанні протоколів IPv4, IPv6 та технології VLAN.

Публікації.

Викладені в роботі результати апробовано на 3-ій Всеукраїнській науково-практичній конференції молодих вчених та студентів «Сучасні інформаційні системи та технології» (м.Херсон, 30 листопада 2020 р.).

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1. Протокол IPv4

Мережеві протоколи, еквівалентні третьому рівня моделі OSI , визначають те, яким чином пакети доставляються від комп'ютера, який їх створив до комп'ютера, який повинен отримати. У сучасних мережах єдиним широко використовуваним протоколом третього рівня є стек протоколів TCP/IP, а здебільшого це протокол IP. Невід'ємною частиною IP є IP-адреси. Протоколи IP-адрес версії 4 - це найбільш поширений тип адрес, який застосовують на мережевих рівнях моделі OSI, для реалізації процесу передачі пакетів між мережами. Конструктивно IP-адреси складаються з 4-ох байт, наприклад 194.167.102.112 [1-3].

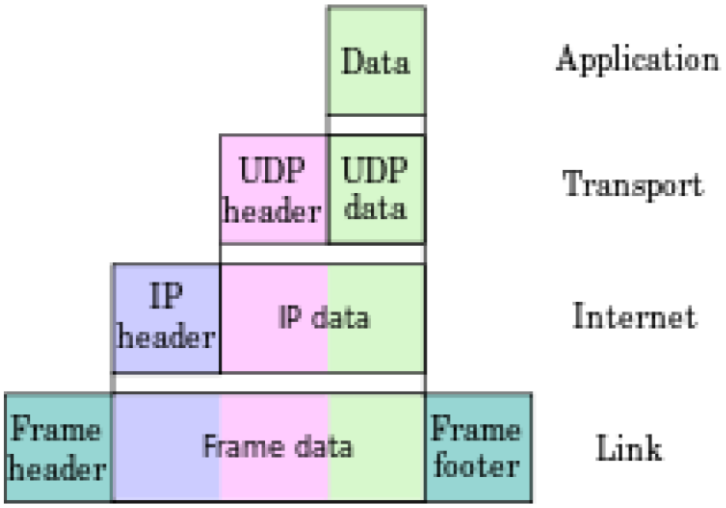

Рис. 1.1. Додавання частин заголовка пакета на кожному рівні OSI перед передачею його в мережу

IP-адреси присвоюються хостам двома методами:

- вручному режимі, налаштування здійснюється адміністратором в процесі налаштування мережі;

- в автоматичному режимі при використанні протоколів спеціального типу за допомогою протоколу DHCP (протокол динамічного налаштування хостів).

Протокол IPv4 було розроблено в 1981 року як частина протоколу IP, з метою присвоїти адресу кожному пристрою в мережі, щоб передавати пакети безпосередньо адресату [4].

Основною задачею протоколу IPv4 є реалізація процесу передачі блоків дейтаграм від відправляючого хоста до одержувача хоста, де одержувачами і відправниками є ПК з ідентифікаторами адресами обмеженої довжини (IP - адрес). Також протокол IP здатний виконувати, у випадку необхідності, процес фрагментації і збір відправляюючих дейтаграм для передачі пакетів іншими мережами з меншим їх розміром [5,7-9].

До недоліків протоколу IPv4 віднесено їх ненадійність, яка зумовлена тим, що в процесі передачі не встановлюється з'єднання і не здійснюється підтвердження про доставку пакетів, які не здійснюють процес контролю правильності отриманих даних (із використанням контрольних сум) і не здійснюється процедура квитирування (синхрообмін повідомлення службовими з хостом-призначення та повна готовністю до приймання пакетів) [6].

Кожна дейтаграма відправляється і обробляється протоколом IP окремо, не враховуючи інші дейтаграми при передаванні даних через мережу [7].

Відправник не контролює наступні дії з дейтаграмою після того як вона була відправлена IP протоколом. Якщо дейтаграма недосягла адресата, то вона не має змоги бути переданою далі по мережі з різних причин, та підлягає знищенню. Вузол, що здійснив процес знищення дейтаграми, має змогу повідомити відправника про відповідні збої за зворотнім адресом (зокрема використовуючи протокол ICMP). Функція гарантованої доставки інформаційних даних є покладеною на транспортний рівень протоколу, який має в своєму арсеналі спеціальні механізми (TCP протокол) [5-10].

На мережевому рівні моделі OSI працюють усі маршрутизатори. Однією з найголовнішим завданням IP протоколу - це організація процесу дейтаграмної маршрутизації, або інакше, процес визначення найкращого шляху проходжень дейтаграм із застосування алгоритму маршрутизації від відправника мережі до інших вузлів мережі за даними IP адреси [1-10].

Алгоритм працездатності IPv4 протоколу на будь-якому з вузлів мережі, який приймає дейтаграму з мережі, зображено на рис.1.1.

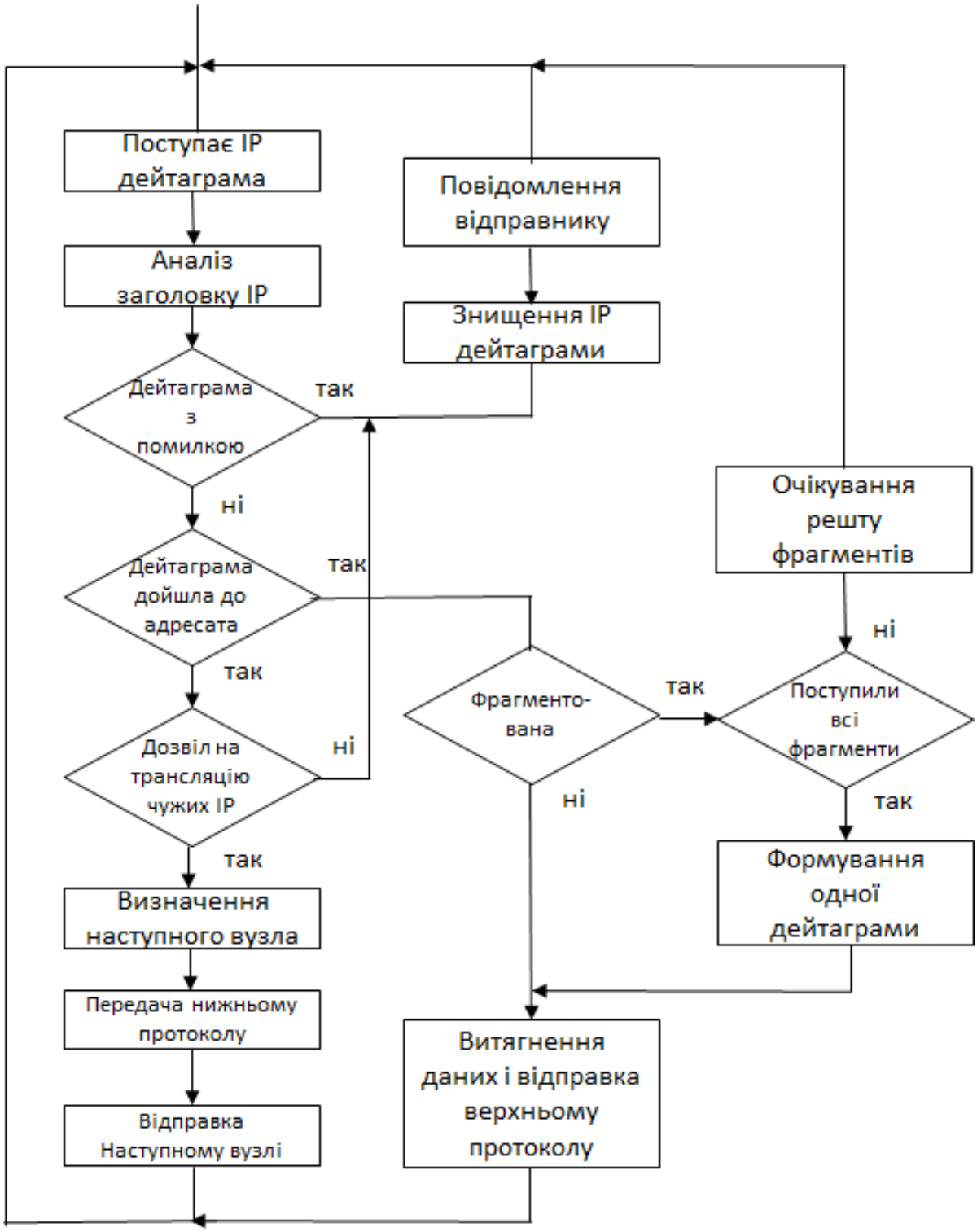

Рис. 1.2. Алгоритм роботи протоколу IPv4

Структуру IPv4 подано на рис. 1.3.

Октет	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31					
0	Версія	Розмір	Диференціювання послуг	ПП	Довжина пакету	
4	Ідентифікатор				Прапори	Зміщення фрагменту
8	Час життя		Протокол		Контрольна сума заголовка	
12	IP-адрес відправника					
16	IP-адрес отримувача					
20	Параметри від 0-я до 10-и 32-х бітових слів					
20 або 24+	Дані					

Рис.1.4. Структура пакету IPv4

Структура пакета IPv4, яку зображено на рис.1.4, складається з таких полів:

– Версія - для IPv4 значення поля має бути рівним 4.

– Розмір заголовка - (Internet Header Length) довжина заголовку пакету IP. У цьому полі вказується початок блоку даних в пакеті. Мінімум значення поля рівний 5 (5x32=160 біт, 20 байт), максимальне – 15 (60 байт).

– Точка коду диференційованих послуг (DSCP) - 6 біт, що використовуються для вказання класу обслуговування.

– ПП (покажчик перевантаження, Explicit Congestion Notification , ECN) - попереджує про перевантаження мережі без втрати пакетів. Є необов'язковою функцією.

– Довжина пакета -довжина, що складається з заголовку та даних. Мінімум значення цього поля рівний 20, максимум - 65535.

– Ідентифікатор - значення, котре ідентифікує відправника пакету і є призначеним для складання пакетів в заданій послідовності. В межах пакету фрагменти характеризуються єдиними значенням ідентифікатора.

– Три біта прапорів. 1-ий біт завжди рівний 0, 2-ий біт DF (don't fragment) вказує на здатність процесу фрагментування пакета та 3-ій біт MF (more fragments) вказує на місце пакету, а саме на його кінцеву локалізацію.

– Зміщення фрагмента – це значення вказує на місце локалізації фрагментів в повідомленнях. Зміщення повинне задаватися в розмірі 8-ми байт-блоків, оскільки це необхідно при множенні на 8 в процесі трансформації в байти.

– Тривалість життя (TTL) - кількість маршрутизаторів, котрі має пройти пакет даних. В процесі проходження через маршрутизатор TTL зменшується рівно на 1. При умові що значення TTL рівне 0 пакет має бути відкинутим і відправнику надсилається повідомлення Time Exceeded (ICMP код 11 тип 0).

– Протокол - ідентифікатор інтернет - протоколу кожного наступного рівня , який вказує на факт присутності в пакеті TCP чи ICMP.

– Контрольна сума заголовка - числиться у відповідності з RFC [11]

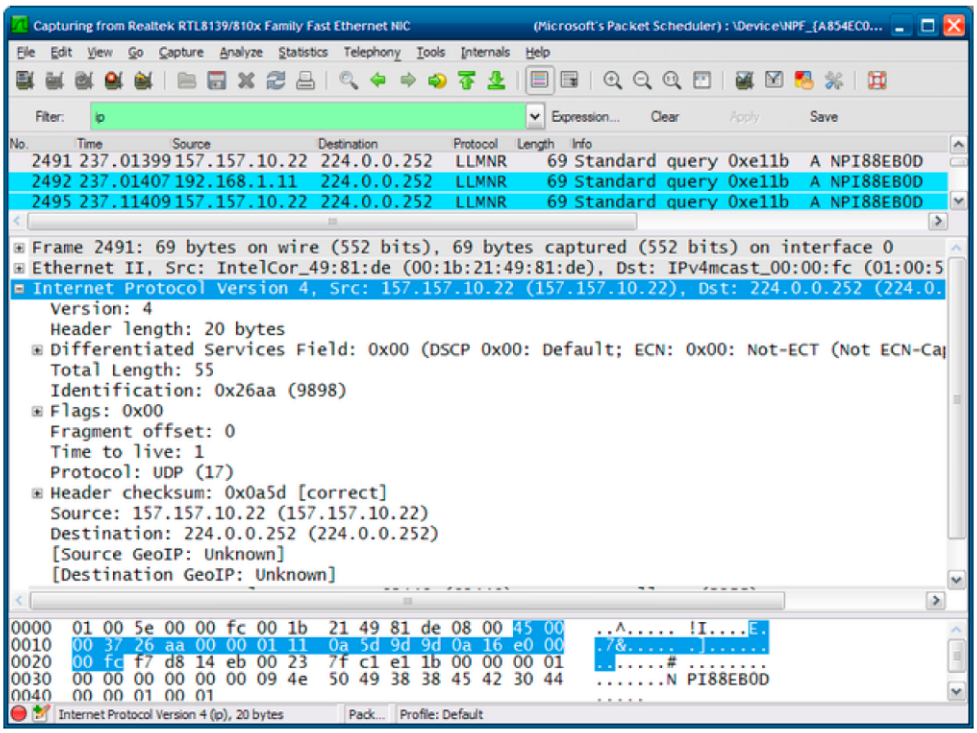

Рис. 1.4. Перехоплений IPv4 пакет із використанням сніффер Wireshark

Здатність протоколу IP здійснювати процес фрагментації пакетів є головною особливістю на відміну від мережевого протоколу IPX. Передача пакетів через мережі локального та глобального характеру різноманітних типів призводить до проблеми різнодопустимих об'ємів полів даних кадрів на канальному рівні (MTU). Мережі Ethernet здатні здійснювати процес передачі кадрів, які переносять до 1500 байт інформаційних даних, що є характерним для мережі X.25 з розміром поля даних до 128 байт. FDDI мережі спроможні передавати дані об'ємом 4500 байт, а в мережах інших видів є власні обмеження. IP протокол здатен здійснювати процес передачі дейтаграм шляхом

фрагментації, тобто розбиття "громіздкого пакету" на меншу кількість фрагментів з розміром, який відповідає MTU проміжних мереж. Після здійснення процесу передачі усіх пакетів фрагментованих через проміжні мережі, де вони складуться зворотно в один пакет. Слід відзначити, що процедуру складання пакету з кусків (фрагменті) організовує лише одержувач, а не будь-який проміжний маршрутизатор. В такому випадку маршрутизатори здатні здійснювати лише процес фрагментації пакетів, проте не складати їх. Такий факт є пов'язаний з тим, що різні куски єдиного пакету не завжди будуть проходити через спільні маршрутизатори [12].

За допомогою поля «Ідентифікація» визначається приналежність фрагменту до певного пакету з метою не переплутання з фрагментами інших пакетів в процесі їх складання. Значення вказаного поля має бути ідентичним в межах одного пакету для усіх фрагментів в процесі усього часу життя. Об’єм фрагментів в процесі розділу пакету має бути кратно 8-ми. Така процедура забезпечує процедуру відведення меншого об’єму в заголовку підполя «Зміщення».

Коли 2-ий біт поля «Прапори» рівний 1 то це свідчить про те, що фрагмент не є останнім в межах пакету. Пакет буде відправлено без процедури фрагментування, якщо прапор "More fragments" рівний 0, а в полі «Зміщення» усі біти будуть рівні нулям.

Якщо біт перший в полі «Прапори» (Don't fragment) рівний 1 то заборонено процес фрагментації пакету. В такому випадку пакет завжди буде відкинутий маршрутизатором при спробі його передачі.

Цей прапор використовують тоді, коли є відомим факт того, що отримувач не зможе відновити пакет в себе [12-16, 35].

IP-адреси складаються з двох логічних частин - номера мережі та вузла цієї мережі. Перші біти вказують на номер мережі та її вузла, а загалом є можливість визначення за бітами приналежність до конкретного класу IP-адреси.

На рис . 1.5 зображено конструктивне подання IP усіх класів.

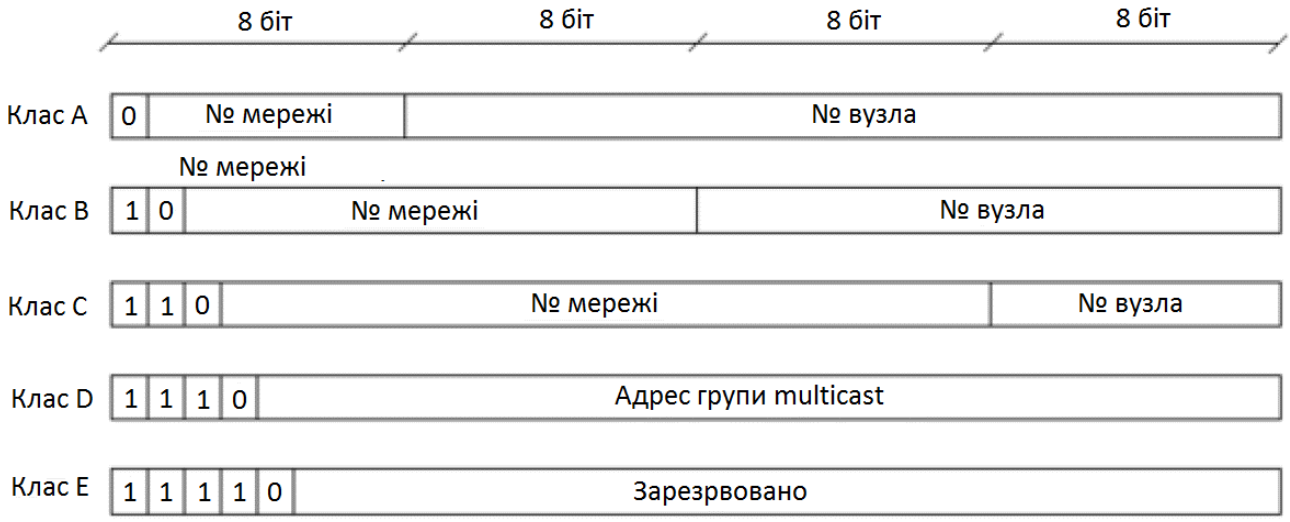

Рис. 1.5. Конструктивне подання IP усіх класів

Якщо початком адреси є 0, то таку мережу класифікують класом А і відповідно номер такої мережі локалізується в межах одного байту, а решту 3 байт відводяться для номерів вузлів в мережі. Клас А має номери діапазону 1-126. (0 не застосовується, а 127 є зарезервованим). Передбачена кількість вузлів класом А сягає 2^{24}, що складає 16777216 вузли.

У випадку коли два перших біт адресу є рівними 10, то мережа є класу класу В. У цій мережі для ідентифікації мереж та вузлів виділено рівно по 16 біт. Для такої мережі загальне число вузлів рівне 2^{16}, що складає 65536.

Для випадку коли початком ідентифікації є значення 110, то така мережа класифікується як С клас. В такому класі 24 біта відведено для ідентифікації мережі, а для вузлів виділено 8 біт. Такий клас набув найбільшого поширення в яких загальна кількість вузлів рівна 256.

Якщо адрес розпочинається з 1110 то він класифікується як клас D (multicast) як груповий, який забезпечує широкомовну передачу пакетів в мережі

Мережа з початковими значеннями 11110 класифікується як клас Е і є пріоритетною для майбутнього [5,7,11, 26].

У табл. 1.1 відображено числові діапазони кожного з класів мереж.

Таблиця 1.1

Класи мереж

Клас	Початок	min номер мережі	max номер мережі	max вузлів в мережі
«A»	0	1.0.0.0	126.0.0.0	2^{24}-2
«B»	10	128.0.0.0	191.255.0.0	2^{16}-2
«C»	110	192.0.0.0	223.255.255.0	2^{8}-2
«D»	1110	224.0.0.0	239.255.255.255	Multicast
«E»	11110	240.0.0.0	247.255.255.255	Зарезервований

Давніше більшість підприємств для отримання діапазону IP-адрес здійснювали заповнювання реєстраційної форми, де необхідно було вказати кількість ПК і запланований приріст кількості ПК. В результаті підприємству надавалися класи A-C у відповідності до форми, де прописано параметри мережі.

Така методика була адекватною до тієї пори, доки загальне число ПК було не велике. Із тенденціями розвитку інтернет та технологій мережевих загальне число робочих місць, які підключені до мережі, сягало декілька сотень. Такий приріст зобов'язував здійснювати реєстрацію класу B, оскільки мережа не мала змоги ідентифікувати таку кількість робочих місць (хостів) (max=254).

Для гнучкого встановлення меж між номерами мереж та вузлів було розвинуто застосування маски мережі. Маска забезпечує ідентифікацію області мережі за рахунок кількості одиниць, які займали ліву цілісну частину адреси. Маска має вигляд цілісної послідовності з двійковими одиницями та нулями. Одиниці вказують діапазон мережі, а нулі – вузлів.

У випадку класів стандартного типу мереж маски мають вигляд:

- клас A - 11111111.00000000.00000000.00000000 (255.0.0.0)
- клас B - 11111111.11111111.00000000.00000000 (255.255.0.0);
- клас C - 11111111.11111111.11111111.00000000 (255.255.255.0).

Забезпечивши кожну IP-адресу відповідною маскою є можливість відмови від загальних класів адресного простору та забезпечити гнучкість системи адресації.

Якщо адресу 185.23.44.206 покладемо у відповідність маску 255.255.255.0, тоді номер мережі стане 185.23.44.0, а не 185.23.0.0 при застосуванні системи класів.

Обмеження щодо кратності кількості одиниць маски є відсутньою, аби відтворювати ділення адресного простору.

Наприклад IP-адрес 129.64.134.5 має маску 255.255.128.0, то двійковій формі буде мати такий вигляд:

– IP-адрес 129.64.134.5 - 10000001.01000000.10000110.00000101
– Маска 255.255.128.0 - 11111111.11111111.10000000.00000000

При ігноруванні маски при врахуванні системи класів адрес 129.64.134.5 буде класифіковано як клас B, і відповідно, ідентифікатором мережі будуть перші два байта - 129.64.0.0 та ідентифікатором - 0.0.134.5.

При використанні маски ідентифікатор мережі буде 17 послідовних одиниць в масці, що накладають на IP-адрес за принципом логічного «І». В такому випадку номер в двійковому форматі має вигляд:

$$\begin{array}{r} 10000001.01000000.10000110.00000101 \\ \& \quad 11111111.11111111.10000000.00000000 \\ \hline 10000001.01000000.10000000.00000000 \end{array}$$

В десятковій формі мережі буде ідентифікуватися як 129.64.128.0 і вузол як 0.0.6.5.

Також застосовується коротка форма запису у вигляді префіксу або короткої маски. Мережа 80.255.147.32 при масці 255.255.255.252 має вигляд 80.255.147.32/29, де «/28» характеризує число кількості одиниць в масці, тобто 29 одиниць зліва на право [10 20].

В табл.1.2 відображено відповідності префіксів з маскою.

Таблиця 1.2

Відповідності префіксів з масками мережі

Маска	Префікс	Кількість вузлів
255.255.255.252	/30	4-2
255.255.255.248	/29	8-2
255.255.255.240	/28	16-2
255.255.255.224	/27	32-2
255.255.255.192	/26	64-2
255.255.255.128	/25	128-2
255.255.255.0	/24	256-2
255.255.0.0	/23	512-2

Застосування масок є найбільш застосованим в IP-маршрутизаціях, зокрема маски мають змогу до застосування в різних цілях. За допомогою масок адміністратор має змогу провести структурування своєї мережі, без необхідності додаткових номерів від постачальників. Постачальники маж змогу здійснювати процес об'єднання адрес простих мереж через відповідні префікси при мінімізації таблиць маршрутизації з підвищеними параметрами продуктивності. Окрім цього, запис маски із використанням префіксу є значно коротшим [19, 30].

У протоколі є декілька інтерпретацій адрес:

– 0.0.0.0 0.0.0.0 - адрес шлюзний (за замовчуванням), тобто адрес ПК, на який надсилаються пакети у випадки коли не знайдено адресата в межах локальної мережі;

– 255.255.255.255 - адрес широкомовний. Усі надісланні повідомлення за цією адресою будуть в результаті отримувати усі хости мережі локального характеру.

– «Номер мережі».«Всі нулі» - адрес мережі;

– «Всі нулі». «номер вузла» - вузол мережі. Застосовується для передачі пакету визначеному вузлу в межах мережі локального характеру;

– Якщо області номеру вузла є лише одиниці, то пакет з такою адресою, здійснює розсилання усім вузлам мережі з вказаним номером мережі. Наприклад, пакет даних з адресом 192.191.22.255 буде доставлятися усім хостам мережі 192.191.22.0. Таке розсилання є широкомовним (broadcast).Номер мережі та вузла не можуть складатися лише з одних двійкових 0 та 1. Звідси

виходить, що максимальне число вузлів, які є наведеними в таблиці класів, на завжди зменшується на 2. Наприклад, в класі С для номеру вузла відведено 8 біт, які дають змогу здійснити процедуру задавання 256 номерів в діапазоні 0-255. В практичних ситуаціях пікове число вузлів класу С не перевищує 254, оскільки адреси 0 та 255 є спеціально призначеними. За таких же умов видно, що ідентифікатор останнього вузла не ідентифікуватися як 98.255.255.255 тому, що номер вузла в класі А складається з двійкових 1 [17].

– Особливим є IP-адрес в якому октет 1-ий рівний 127.x.x.x. Він застосовується при тестуванні ПЗ і процесових взаємодій для одної машини. Коли ПЗ здійснює надсилання даних по IP -адресі 127.0.0.1, то формується ніби «петля». Процес передачі таких даних не здійснюється в мережі, а здійснюється процес повернення до модулів верхніх рівнів як ніби їх тільки прийняли. В такому випадку присвоювати кожному ПК IP-адрес є забороненим, які адрес яких розпочинається на 127. Адрес з таким початок називається loopback. Адреса 127.0.0.0 відноситься до мережі внутрішньої відповідного блоку-модуля маршрутизатора вузла. Адрес 127.0.0.1 відноситься до модуля на внутрішньої мережі.

В протоколах IP відсутнє розуміння широкомовного в протоколах рівню канального мережах локального типу, коли пакети мають бути доставленими всім хостам. Лімітований широкомовний адрес IP та не лімітований мають границі їх що розповсюдження інтернет мережею, які є обмеженими самою мережею в якій локалізується пакет відправника, або мережею отримувача. В такому випадку ділення мережі із застосуванням маршрутизаторів на ланки локалізує широкі межі передачі пакетів з одною мережі в спільну мережу частин просто тому, що немає способу адресувати пакет одночасно всім вузлам. Такий спосіб виключає передачу пакетів усіх вузів по окремо, а здійснюється передача усіх одночасно в іншу мережу [18].

Таблиця 1.3

Опис адрес в мережі

Мережа (адрес)	Опис	Стандарт
0.0.0.0/8	Адреса поточної мережі	RFC 5735
10.0.0.0/8	Призначено для організацій приватного сектору	RFC 1918
100.64.0.0/10	Для провайдера	RFC 6598
127.0.0.0/8	Інтерфейсний комутатор всередині хоста	RFC 5735
169.254.0.0/16	Для автоматичного конфігурування	RFC 3927
172.16.0.0/12	Для приватних мереж	RFC 1918
192.0.0.0/24	Спеціально зарезервований IETF	RFC 5735
192.0.2.0/24	Тестувальна мережа 1 для документів	RFC 5735
192.88.99.0/24	Трансляція IPv6 в IPv4	RFC 3068
192.168.0.0/16	Організація мереж приватних	RFC 1918
198.18.0.0/15	Тестування продуктивних параметрів	RFC 2544
198.51.100.0/24	Тестувальна мережа 2 для документів	RFC 5737
203.0.113.0/24	Тестувальна мережа 3 для документів	RFC 5737
224.0.0.0/4	Для LGPL	RFC 5771
240.0.0.0/4	Для майбутніх застосувань	RFC 1700
255.255.255.255	Широкомовний адрес	RFC 919

Усі адреси в мережі Інтернет мають бути зареєстрованими, що забезпечує гарантування щодо їхньої унікальності в глобальних масштабах планети. Такий тип адрес є публічними або реальними.

Для мереж локального характеру, що комутовані з Інтернетом, процедура реєстрації адрес не є необхідною. Оскільки можна застосовувати будь-який адресний простір. Для недопущення можливості конфліктних ситуацій при кожних наступних підключеннях мережі до інтернету є рекомендованим щодо застосовування мережах локального характеру тільки діапазони IP-адрес приватного типу (в межах інтернету таких адрес не має та їх застосування не є можливим), які наведено в табл.1.4 [20].

Таблиця 1.4

Межі IP-адрес приватного типу

Межі адрес, які застосовуються в мережах локального характеру
10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0 -192.168.255.255

1.2. Протокол IPv6

В процесі розроблення IPv4 становище інформаційно-комунікаційної технології не було передбачено застосування великої кількості мережевих обладнань, які підключені до мережі Internet. Приблизно 4,23 мільярдів адрес повністю вистачає аби задіяти усе мережеве обладнання у світі в одну мережу. Проте на 2020 рік кількість користувачів підключених до Інтернет склала близько 15 мільярдів конектувань мережевих і прогресує в сторону зростання [21-23].

Застосування IPv4 здійснюється в штатному режимі, тому що застосовуються різні технологічні процеси щодо економічного застосування адрес мережеві, зокрема NAT (Network Address Translation трансформація адрес мережі). Апріорним є той факт, що використання IPv4 наближається до завершення тому, що передбачається підключення побутового обладнання до інтернет (холодильники, мікрохвильові печі) з метою їх віддаленого керування з різних місць планети.

Здійснення переходу на нові формати адресування є дуже гострою ситуацією. Проте більшість фахівців прогнозували проблематику не вистачання адрес мережі до 1990 р., і тоді вже розпочала роботу ціла група над розробкою нових технологій протоколів мережі Інтернет, зокрема IPv6 [22-27].

Основні розв'язувані завдання:

– Можливість доступу до глобальної мережі мільярдів хостів навіть при нераціональному використанні адресного простору.

– Скорочення розміру таблиць маршрутизації

– Спрощення протоколу для прискорення обробки пакетів маршрутизації

– Підвищення рівня безпеки протоколу

– Спрощення роботи багатоадресних розсилок за допомогою вказання областей розсилки.

– Перспективи подальшого розвитку протоколу в майбутньому

– Організація сумісності старого і нового протоколу

Протокол IPv6 розроблений в кінці 1992 року.

Протокол IPv6 є новою версією протоколу інтернет (IP), який розроблено для розв’язання проблематики, яка сформована в версіях IPv4 під її застосування інтернеті. Однією з головних причин є її обмеженість.

На сьогодні протокол IPv6 поки ще не набув такого широкого розповсюдження в Інтернеті, як IPv 4, але поступово частка в світовому масштабі зростає і на початок 2016 року пристрої, які використовують міжмережевий протокол IP версії 6 складає 10% (рис.1.8) [28 , 29].

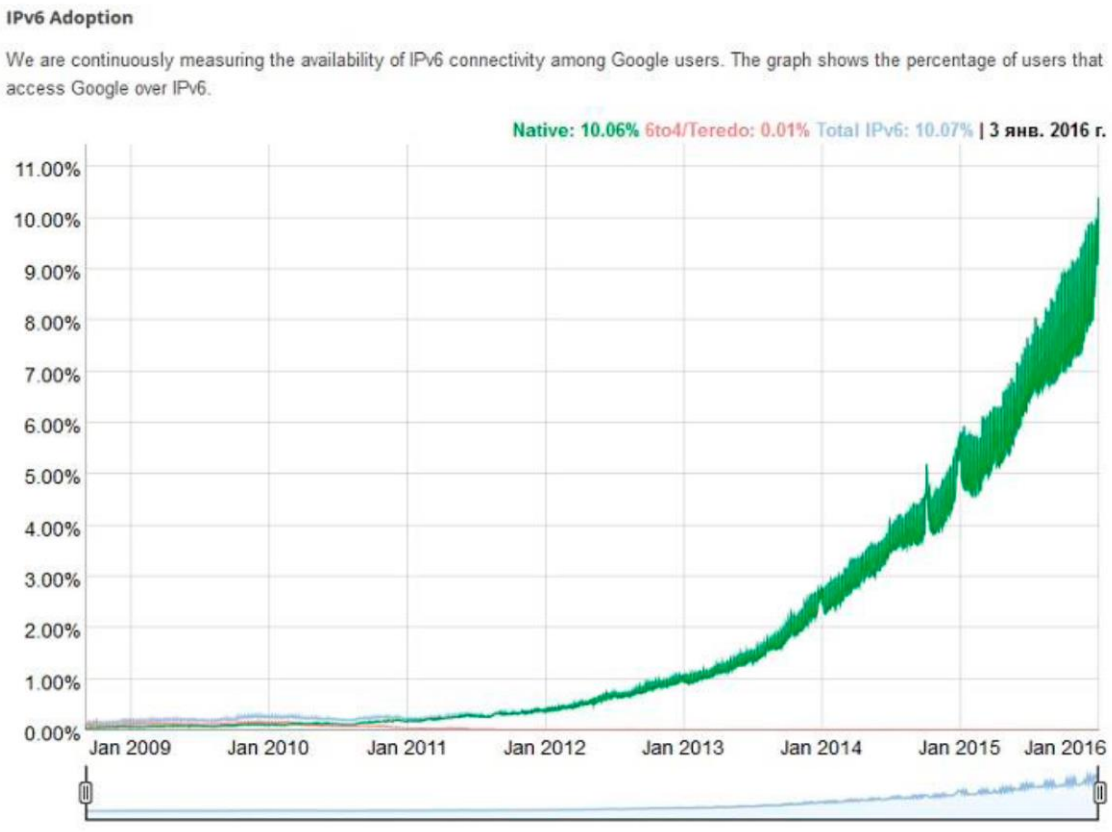

Рис. 1.6. Графік кількості пристроїв використовують IPv 6

Інтернет протокол IPv6 добре справлять з основними поставлений ними завданнями. Йому притаманні переваги інтернет протоколу IP і позбавлений деяких недоліків, до того ж володіє деякими новими здатностями. В загальному IPv6 протокол несумісним у відповідності до протоколу IPv4, проте є сумісним з іншими Інтернет протоколами, зокрема UDP, TCP, OSPF, ICMP, DNS для чого є необхідним вносити зміні.

Особливості IPv6 :

– Протокол IPv6 реалізовано довжиною в 16 байт, що забезпечує розв’язання проблеми щодо збільшення обсягу інтернет-адресацій.

– Протокол IPv6 у порівнянні до протоколу IPv4 має більшу структуру заголовку пакету. Отже, маршрутизатори мають здатність до швидшого оброблення пакетів, що збільшує показники продуктивності.

– Покращені показники підтримки параметрів, які є необов'язковими. Такі варіації є суттєвими, оскільки новому заготовці необхідні поля є необов'язковими.

– Суттєво підвищено безпеку, процес автентифікації і конфіденційності є базовими особливостями нового протоколу.

– Наділено значну увагу типу послуг, які надаються. Для цього в пакетному заголовку IPv4 було виділено поле восьми розрядне [30].

Заголовок IPv6 наведено на рис. 1.7.

<table>
<tr><td>Октет</td><td colspan="4">0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31</td></tr>
<tr><td>0</td><td colspan="2">Версія</td><td colspan="2">Пріоритет</td><td colspan="2">Мітка потоку</td></tr>
<tr><td>4</td><td colspan="3">Довжина корисного навантаження</td><td>Наступний заголовок</td><td>Макс. число транзитних вузлів</td></tr>
<tr><td>8-20</td><td colspan="5">IP-адреса відправника</td></tr>
<tr><td>24-36</td><td colspan="5">IP-адреса одержувача</td></tr>
<tr><td></td><td colspan="5">додатковими заголовок</td></tr>
<tr><td></td><td colspan="5">дані</td></tr>
</table>

Рис.1.7. Структура заголовку IPv6

– Поле у випадку IPv6 рівне 6.
– Пріоритет застосовується з метою розрізнення пакетів з різноманітними вимогами щодо доставлення пакетів реального часу.

- Мітка потоку є застосовною при установленні з’єднання між хостами відправлення та отримання випадкового до з’єднання з заданими параметрами та вимогами. Пакетований потік двох процесів різних хостів може мати суттєві вимоги до часових затримок, що вимагає резерву до здатності пропускної.
- Загальна довжина навантаження корисного типу здійснює повідомлення про те яка кількість байт поступає в черзі за заголовком 40-байтної довжини.
- Із використанням наступного заголовку здійснюється повідомлення про те, який саме з заголовків додаткових чергується вслід за базовим.
- Максимальна кількість транзитів як вузлів ідентичний параметру TTL.
- Заголовки додаткового характеру:
- Маршрутизаційні параметри відображають різну сформовану інформацію маршрутизаторам;
- Параметри щодо отримання відображають додаткову інформацію отримувачу;
- Маршрутизація є частинним списком маршрутизаційних транзитів в напрямку переміщення пакета;
- Фрагментація здійснює керування дейтаграмними фрагментами;
- Автентифікація здійснює процес перевірки вірогідності відправника;
- Шифровані дані відображають інформацію щодо зашифрованого вмісту [31-34].

Існує низка типів адрес в IPv6, які наведено нижче по тексту.

Unicast є ідентифікатором інтерфейсу одиночного типу. Надісланий пакет унікастному адресу буде доставлено до інтерфейсу, який будо вказано при адресуванні.

Anycast є ідентифікатором множини інтерфейсів, які є належними кожному окремому вузлу. Надісланий пакет за енікастною адресою буде доставлено інтерфейсу, який зазначено в адресі (найближчий за відстанню маршрут згідно до таблиці).

Multicast є ідентифікатором множини інтерфейсів, які є належними до різноманітних вузлів. Надісланий пакет за даними мультикастинг-адресою буде доставлено усім інтерфейсам, які були зазначенні в адресі.

В IPv6 не передбачено адрес широкомовних, а їх функціональність передано адресам-мультикастинг.

В IPv6 передбачено будь-які конфігурації 0 та 1 для різних полів, за умови їх обмеженості [35].

IPv6 адресація є асоційованою не з вузлами, а з інтерфейсами. Оскільки окремо взятий інтерфейс є належним тільки до одного вузлу, а адрес унікастний відповідного інтерфейсу призначений для ідентифікування вузла.

IPv6 є унікастним адресом, який є співвідносений тільки для одного інтерфейсу. Відповідно одному з інтерфейсів можуть відповідати множина IPv6 адресацій різних типів (енікастні, унікастні та мультикстні). На сьогодні можна виділити лише два винятки з правил:

– Адрес одиночного типу може бути підписаний декількома фізичним інтерфейсам лише тоді, коли додаток здійснює розгляд кількох інтерфейсів як єдиних цілей при представлені його на рівнях в Інтернет мережах.

– Маршрутизатори можуть не мати нумерованих інтерфейсів для комутацій точка-точка з метою виключення необхідності ручної конфігурації та оголошення цих адрес. Адреси тепер не потрібними у випадку для з'єднання точка-точка з маршрутизаторами у випадку коли ці інтерфейси не застосовуються як точки відправника або отримувача при передачі IPv6 дейтограм. Тут маршрутизація виконується у відповідності до схеми, яка є наближена до схеми є застосовною протоколом CIDR у IPv4.

IPv6 є відповідним моделі IPv4, де підмережа є асоційована з каналом. Виділеному каналу ставиться у відповідність кілька підмереж [36].

Є наступні форми подання IPv6:

- Форма 16-их чисел і двокрапок.

Така форма є найкращою і має вид n:n:n:n:n:n:n:n. Знак n є відповідним 4-х значному 16-му числу (8 16-их чисел відведено кожному числі відведено 16 біт). Приклад: 1FA8:FFFF:2622:ACDB:2255:BF88:3422:4267.

- Форма стиснута.

Через велику довжину адреси переважно міститься багато 0 підряд. Для спрощеного подання адрес застосовується форма стислого характеру, де суміжно характерні 0 блоків буду замінені на пара символьних двокрапок (::). Проте таке символьне подання зустрічатися може один раз.

- Змішана форма.

Така форма здійснює поєднування адресних протоколів IPv4 з IPv6. В такій ситуації адрес буде мати наступний формат n:n:n:n:n:n:d.d.d.d, де символ n є відповідними 4-ох значному 16-ому числу (6 16-их чисел відведено 16 біт), ad.ddd - адресні частина, які записано в виді IPv4 (32 біти) [36-39].

Таблиця 1.5

Адреси IPv6 спеціального призначення

Мережа (адрес)	опис	резервність
::/128	Поточна мережа	зарезервовано
::1/128	Комутаційний хостовий інтерфейс	зарезервовано
64:ff9b::/96	Трансформоація IPv4-IPv6	не зарезервовано
::ffff:0:0/96	Адрес IPv4 відображається у IPv6	зарезервовано
100::/64	Відмова	не зарезервовано
2001:10::/28	ORCHID	не зарезервовано
2002::/16	Трансляція протоклу 6 в 4	не зарезервовано
fc00::/7	Local-Unique	не зарезервовано
fe80::/10	Unicast Scoped-Linked	зарезервовано
2001::/23	Зарезервований IETF при потребі протоколу	не зарезервовано
2001::/32	TEREDO	не зарезервовано
2001:2::/48	Тестування показників продуктивності	не зарезервовано
2001:db8::/32	Для документації	не зарезервовано

1.3. Мережі VLAN

На сьогодні більшість організації та підприємств з практичної сторони не застосовують корисну можливість що процесу організації віртуальної мережі локального характеру (VLAN) як єдину інфраструктури, яку надають сучасні комутатори. Це є необхідним з більшості факторів, оскільки необхідно проаналізувати таку технологію з точки зору можливостей її застосування [40-42].

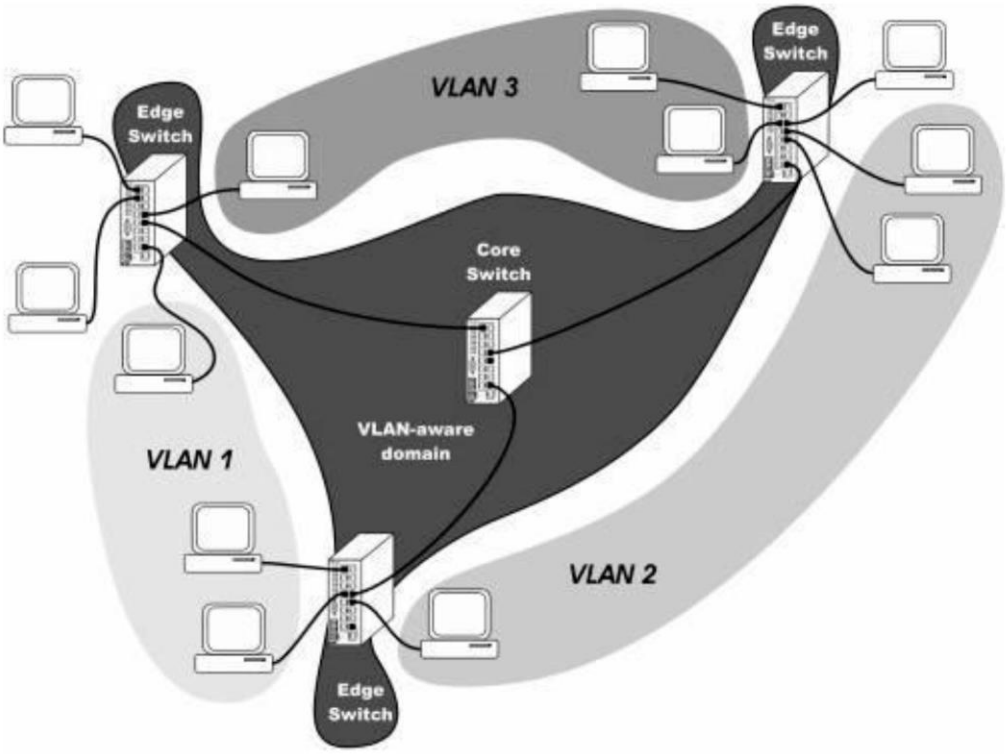

Рис. 1.8. Приклад розподілення мережі локального типу за VLAN

Під VLANs розуміють групу ПК, які підключено до мережі з логічним об'єднанням їх в домен розсилання інформаційних повідомлень з ознаками широкомовності. Групи при VLAN мають змогу бути виділеними в залежності від структурних особливостей підприємств або за видом їх діяльності. VLAN мережі мають низку переваг. Такі мережі мають більш суттєво ефективніше використання пропускних здатностей на відміну від традиційних мереж, підвищений ступінь захищеності передаючої інформації і спрощена схема здійснення процесу адміністрування.

При застосуванні VLAN здійснюється розбивання усього простору мережевого на домени широкомовного типу. Інформаційні потоки в мережі з такою структурою передаються лише між її учасниками-хостами, а не між усіма ПК фізичної мережі. Генерований серверами широкомовний трафік є обмежений виділеним доменом, тобто процес трансляції не відбувається між усіма станціями в мережі. За таких умов досягнуто оптимального розподілення пропускних здатностей мережі між групами ПК, які є віддаленими: сервери та робочі станції з VLAN не мають змоги бачити одна одного [40-45].

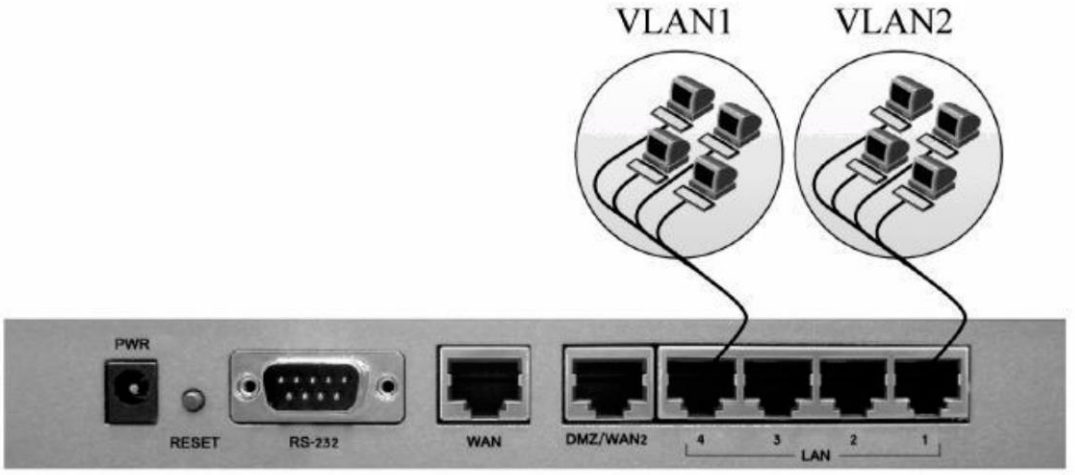

Рис. 1.9. Вид поділення мережі на VLAN на технічному обладнані, зокрема комутаторі

Така мережа забезпечує захищеність інформації від будь-якого доступу, оскільки обмін інформаційними потоками реалізовується в межах одної виділеної групи комп'ютерів, тобто їм ненадана здатність отримання трафіку генерованим в інші ідентичні структурі. Для VLAN є характерною особливістю як процедура спрощеного мережевого адміністрування. Ця процедура вимагає розв’язання завдання додавання нових компонентів в мережу, зміна їх локалізації та видалення. У випадку коли користувачі VLAN переїжджають в інші місця локалізації, адміністратору мережі не є необхідним здійснювати процес нової комутації кабелів. Він має здійснити лише налаштування обладнання мережеві з власних робочих місця адміністратора. Також в таких мережах є передбачено процедура автоматичного режиму налаштування параметрів користувачі, які здійснюють відповідні переміщення. Адміністратору є лише необхідним здійснення лише процедури налаштування VLAN з метою проведення усіх необхідних операцій. Адміністратор здатний створити логічні групи користувачів без потреби його переміщення на місця налаштування. Це є вкрай важливим щодо економії робочого часу, що є необхідним при вирішенні інших важливих завдань [42-45,47].

На сьогодні є три варіанти: на основі використання портів, протоколів 3-го рівня та MAC-адресу. Кожен варіант є відповідний одному з 3-ох нижче стоячих

рівнів OSI моделі: мережевий, фізичний та канальний. В VLAN використовується також 4-ий спосіб із використанням правил, який рідко застосовується, проте він володіє високими показниками гнучкості.

В VLAN передбачено процедуру логічного об'єднання портів комутатора, які є обраними при взаємодії. Адміністратор має змогу визначати порти, які формують VLAN1, VLAN1 та інші. Один комутаційний порт повністю може застосовуватися при підключенні з етою виявлення декількох комп'ютерів із використанням hub. Усі вони мають бути визначеними в якості учасників однієї мережі віртуального характеру які призначений порт обслуговування комутатора. Необхідно мати жорстку прив'язку членів мережі віртуального типу, що є вагомим недоліком вказаної організаційної схеми [43].

Базою цього способу є закладеними при застосуванні унікальних 16-х адрес рівня каналу, які передбачені мережевими адаптерами сервера або іншого обладнання мережі. Також необхідно відзначити такий спосіб як більш гнучкіший при порівнянні з іншими ранніми версіями для одного порту комутатора є повністю допущеним щодо комутації комп'ютерів різних мереж віртуального характеру. Так він здійснює автоматичне відстеження пересування ПК з портів, що забезпечує зберігання приналежності клієнтів до визначеної мережі без задіяння адміністраторів. За принципом роботи комутатори працюють у відповідності до таблиць MAC-адресів відповідних станцій мереж віртуального характеру. Після перемикання ПК на будь-який порт здійснюється процес порівняння полів MAC-адреси з показниками таблиці. Після цього процесу формується коректний висновок щодо належності ПК до конкретної мережі. Як недолік цієї технології є її складність VLAN при налаштуванні і облаштуванні, яка і є першопричиною прояву помилок. Враховуючи те, що комутатор здійснює процес самостійної побудови таблиці адресного простору, адміністратор мережі має здійснювати перегляд її в повному об’ємі для визначення адреси тих, хто є у віртуальних групах. Після цієї процедури адміністратор здійснює прописування тих хто в групі до відповідних VLAN. Якраз на цьому етапі і формуються помилки, які інколи є притаманними для

VLAN Cisco, налаштування яких є простим, але на наступних етапах процедура перерозподілення є складнішою, на відміну від застосування портів.

VLAN із протоколами 3-го рівня не часто застосовується в комутаційному обладнанні на рівнях робочих груп або відділень. Він є характерним у випадку магістралей, які є оснащеними інтегрованими технічними маршрутизаційними засобами базових протоколів мереж локального характеру – IPX, IP та AppleTalk. Цей спосіб враховує те, що груповані порти мережевого комутатора, які є належними до визначеної VLAN , будуть асоційованими з деякою підмережою IPX або IP. Гнучкість в такому випадку буде забезпечено тим, що користувацька переміщеність на будь-який інший порт цієї мережі віртуального характеру, завжди буде відстежена комутаційним обладнанням і не вимагатиме переконфігурації. Процес маршрутизації VLAN є досить простим, оскільки комутаційне обладнання здійснює аналіз мережевих адрес ПК, які є визначеними для кожної мережі. Такий спосіб здійснює підтримку та взаємодію між різноманітними VLAN не використовуючи додаткові засоби. Є вагомий недопрацювання цього способу, яка пов’язані із високими вартісними показниками щодо вартості комутаційного обладнання. VLAN у більшості існуючих провайдерів забезпечують роботу мережі на рівні, який зображено на рис.1.10 [45].

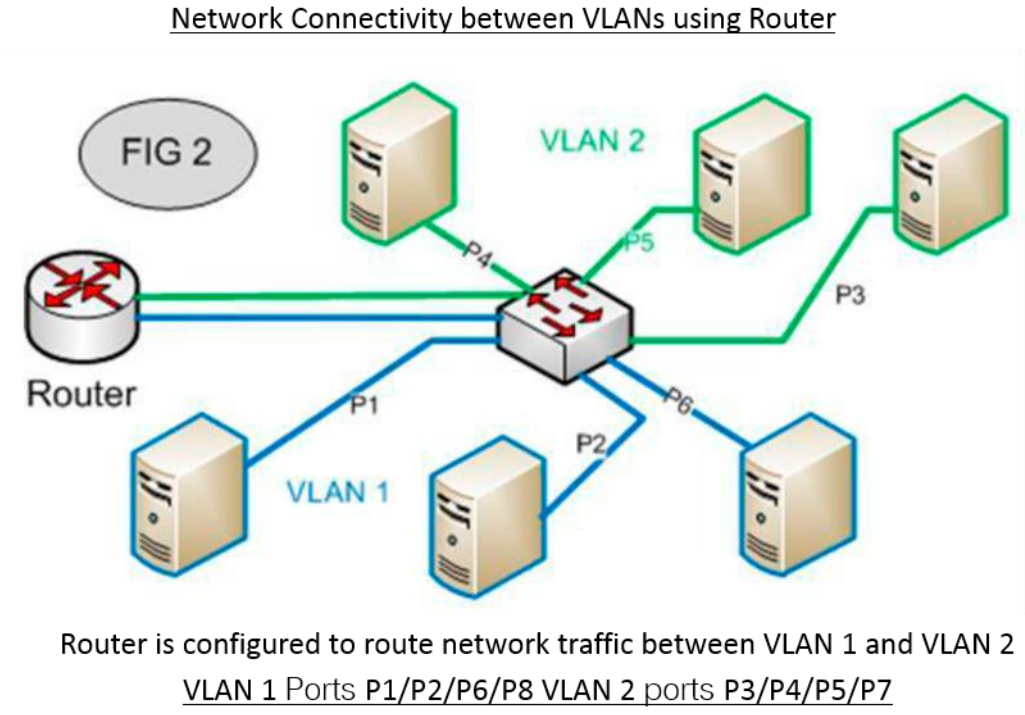

Рис. 1.10. Процес формування VLAN на основі MAC-адрес

1.4. Висновки до розділу 1

У розділі проаналізовані існуючи протоколи IP, які є реалізованими в сучасних мультисервісних мережах. На підставі аналізу визначено їх переваги та недоліки, що дало змогу обґрунтувати шляхи дослідження.

РОЗДІЛ 2
ОСНОВНА ЧАСТИНА

2.1. Типова схема досліджуваної мультисервісної мережі зв'язку

Одна з цілей дослідження було визначення ефективності роботи мультисервісної мережі за часом затримки проходження пакетів в мережі і завантаження сервера обробляючими пакетами даних при різних налаштуваннях. Основний інтерес в даній роботі приділено дослідженню характеристик мультисервісної мережі при використанні мережного протоколу IPv4, а також IPv6 та здійснити їх порівняння. IP протокол є одним з найважливіших на сьогоднішній день в організації будь-якої мережі. Цей протокол, об'єднуючи сегменти мережі, забезпечує доставку пакетів між будь-якими мережевими вузлами через довільне число проміжних вузлів. Інформаційна частина пакетів з даними істотно впливає на роботу мережі. Залежно від інформації, що міститься в заголовках IP пакета буде залежати доставка даних за призначенням, якомога швидше і ефективніше. Чим швидше IP-пакет буде оброблятися на вузлах (маршрутизаторах) тим швидше буде працювати і вся мережа. IP протокол версії 6 сприяє ефективній роботі мережі за рахунок декількох особливостей в порівнянні з IPv4 [48-50].

В якості експерименту була взята типова схема мультисервісної мережі житлового району. У цій мережі знаходиться 4000 абонентів, які підєднанні до різних Web, VoIP, відео, аудіо сервісів через комутатори і маршрутизатори по деревовидній топології. Маршрутизатори між собою з'єднані оптоволоконним кабелем, а також з комутаторами доступу, від яких використовуючи UTP кабель за технологією FastEhternet передається трафік до кожного абонента. Для того щоб відстежити, як впливає кількість абонентів і вузлів (маршрутизаторів) в мережі при використанні двох досліджуваних протоколів, було вирішено побудувати 3 моделі різного масштабу і вмісткості. Перша модель включає в себе 1000 абонентів, які підключені до комутатора, і далі через маршрутизатор отримують послуги від групи серверів. Друга модель має в два рази більше

абонентів і на один більше маршрутизатор, ніж в першій моделі. Також весь трафік проходить через маршрутизатори до групи серверів, які надають послуги підключеним абонентам. Третя модель має в 4 рази більший розмір підключених клієнтів, які отримують послуги і об'єднані між собою з доступом до серверів через три маршрутизатора.

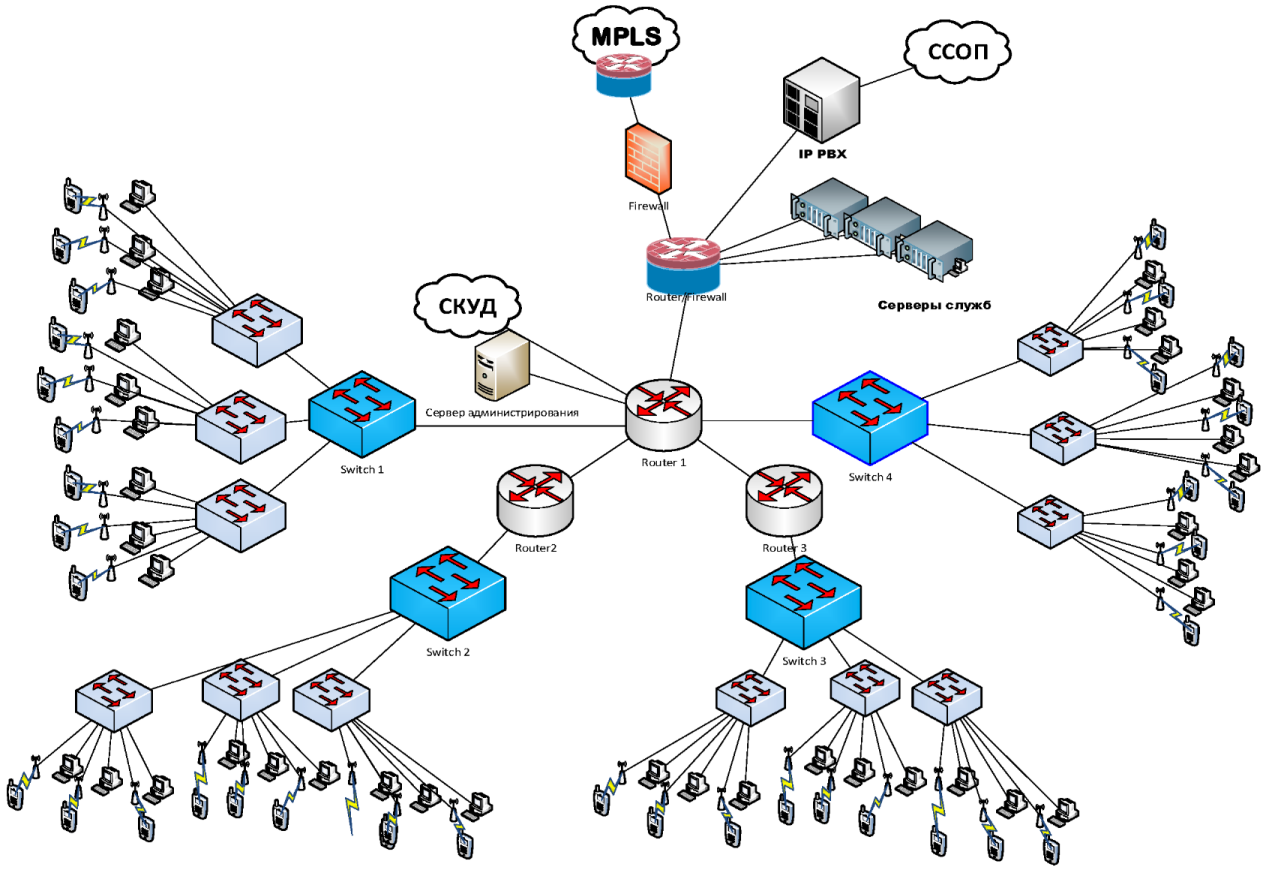

Рис. 2.1. Типова схема мультисервісної мережі району

2.2. Технологія Riverbed Modeler

Під технологією Riverbed Modeler розуміється сукупність дій для створення моделі мережі і проведення на ній імітаційних експериментів. Програмний пакет Riverbed Modeler надає широкі можливості для побудови моделей мережі, що дозволяють приділяти увагу аж до дрібниць в створенні будь-якого проекту мережевої інфраструктури. Вибір необхідної статистики, що збирається з кожного об'єкта мережі або з усієї мережі, запускаючи процес моделювання на задані часи симуляції роботи мережі і потім здійснюватися перегляд результатів - всі ці можливості, що надаються даним продуктом, несуть

величезний потенціал у вирішенні різних питань з організації ІТТ (інформаційно обчислювальних мереж).

Застосування високого рівня моделювання дає змогу забезпечити повноту і коректність виконування інформаційно-телекомунікаційною системою заданих функціональностей сформованих замовником.

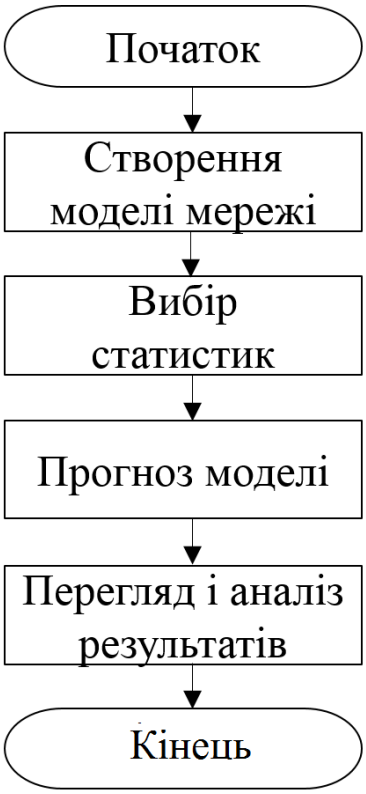

Рис. 2.2. Алгоритм роботи з програмною системою Riverbed Modeler

Програмна система Riverbed Modeler дає змогу моделювати мережі, та представити її графічному виді, що можна віднести до переваги, оскільки користувач має змогу візуалізувати усю мережу повністю, а також її ланко по окремо. Також можна враховувати розміри моделі мережі, створюючи проекти на шаблоні глобального масштабу, районного, кампусного або розміром офісу, враховуючи відстані між вузлами. Або використовувати схему будівлі, де розміщується або планується розмістити обчислювальну мережу, отримуючи готовий план-проект, який можна змінювати тільки в рамках обмежених середовищем розміщення мережі.

Riverbed Modeler є безкоштовною утилітою, яка призначена абсолютно в освітніх цілях для студентів навчальних закладів. Установка проводиться після реєстрації, вказуючи дані студента і навчального закладу.

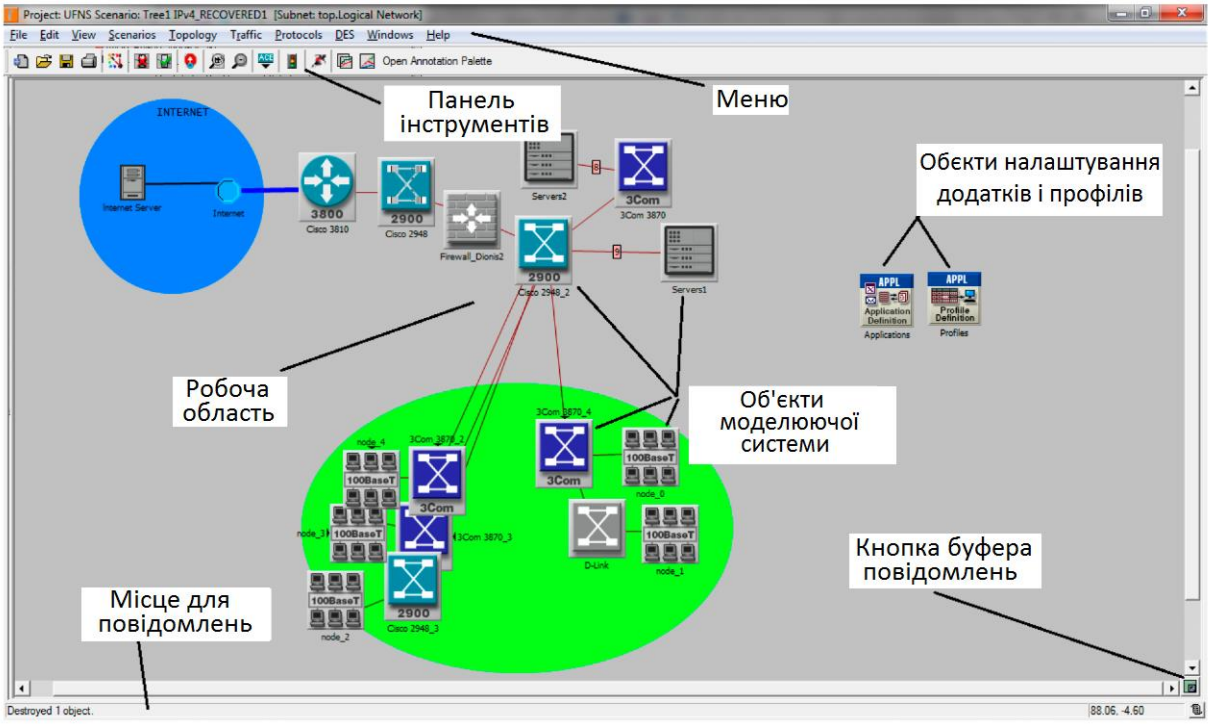

Рис. 2.3. Інтерфейс програми Riverbed Modeler

Riverbed Modeler надає собою віртуальне мережеве середовище, яка моделює поведінку мереж, включаючи маршрутизатори, комутатори, робочі станції, сервери, протоколи і конкретні програми. Дружній інтерфейс Modeler з технологією «перетягування» дає можливість ефективно моделювати, управляти, шукати і усувати нсправності в реальних мережевих структурах. Це середовище дозволяє IT менеджерам, проектувальникам мереж, систем і штату операторів більш ефективно вирішувати важкі проблеми, моделювати зміни перш, ніж вони здійснюються, і планувати майбутні сценарії, такі як зростання трафіку і вихід з ладу сегментів мережі. Створення самостійно унікальних всеможливих мережевих пристроїв, яких немає у великій базі Modeler, надає можливість найбільш точно спроектувати мережу, домагаючись необхідних результатів.

Можна проводити моделювання сценаріїв (окремих схем і планів дій) при проектуванні мереж. Програма дозволяє аналізувати механізми роботи додатків клієнт-сервер та новітніх технологічних розробок на функціонування мережі; моделювати ієрархічні мережі, багатопротокольні локальні і глобальні мережі з урахуванням алгоритмів маршрутизації; здійснювати оцінку та аналіз

продуктивності змодельованих мереж. Також за допомогою пакету можна здійснити перевірку протоколу зв'язку, аналіз взаємодій протоколу, оптимізацію і планування мережі. В процесі моделювання можна відстежити, як будуть змінюватися час запізнення відгуку і інші мережеві характеристики при різних підходах до конструювання мережі. За результатами моделювання користувач отримує повну інформацію про вузькі місця мережі (про пропускну здатність, завантаженність мережевого обладнання та ліній), дані трафіку, часові затримки та ін.

Щоб створити модель мережі (Modeler проект), необхідно визначитися з вузлами мережі: з комп'ютерами, комутаторами, маршрутизаторами і так далі, з’єднаннями між вузлами і додатками, які будуть працювати на тому чи іншому вузлі. Також можна згенерувати певний трафік зі специфікою, які є в реальній працюючій мережі, або навіть завантажити файл з характеристикою трафіку роботи реальної мережевої інфраструктури [58-60] .

2.3. Висновки до розділу 2

У розділі розроблено імітаційну модель мультисервісної мережі в середовищі Riverbed Modeler, яка дала змогу моделювати поведінку мережі при різних сценаріях, оцінювати її пропускну здатність, визначати рівень завантаження буферів мережевих пристроїв, затримки мережевого трафіку.

РОЗДІЛ 3
НАУКОВО-ДОСЛІДНА ЧАСТИНА

3.1. Порівняння ефективності роботи протоколів IPv4 і IPv6

Для моделювання мереж була використана програма Riverbed Modeler , що дозволяє створювати моделі мереж і отримувати характеристики у вигляді графіків тих чи інших параметрів: час затримки проходження пакета, про пропускну здатність на вузлі, завантаження серверів і т.д.

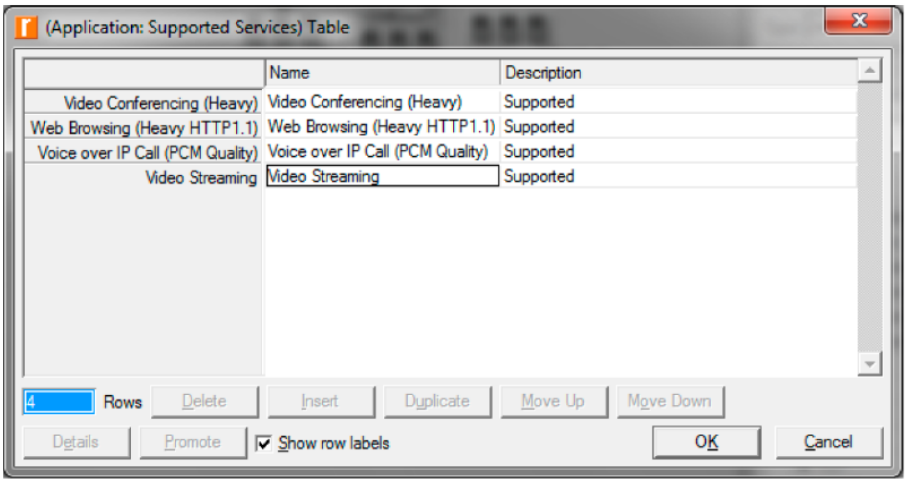

Рис. 3.1. Налаштування різних видів трафіку

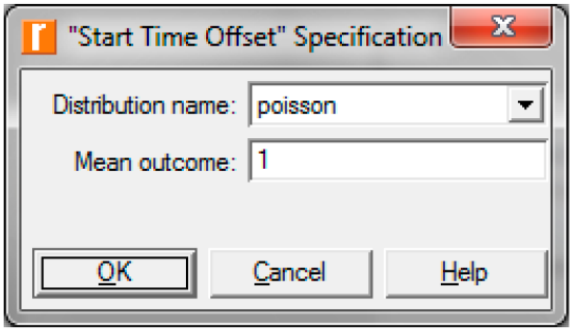

Рис. 3.2. Налаштування закону генерації трафіку

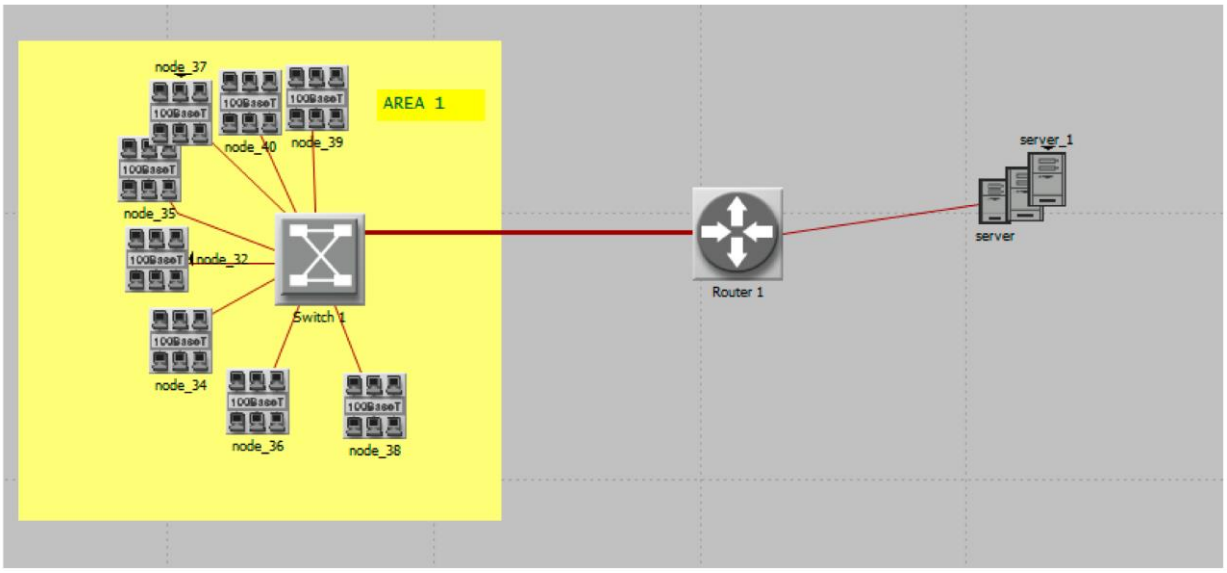

Рис.3.3. Схема моделі першого сценарію

Перша модель має до тисячі абонентів і один маршрутизатор через який проходить трафік до серверів, які обслуговують клієнтів надаючи різні послуги: Web , VoIP , відео, аудіо трансляції та інше. Були задані специфікації генерування трафіку за певним законом і з інтенсивністю 100 пакетів в секунду від підключеного пристрою. На кожному елементі мережі було присвоєно індивідуальний IP-адрес. Спочатку мережа була налаштована по протоколу IPv4, потім робочі станції і маршрутизатори були переналаштовані на роботу по протоколу IPv6.

Запустивши симуляцію роботи мережі тривалістю 15 хвилин, були отримані результати, досліджуваних характеристик. В якості критерію оцінки продуктивності мережі використовується середній час перебування пакета в мережі з декількома вузлами комутації, з'єднаними між собою дуплексними лініями зв'язку з пропускною спроможністю $d_{k,l}$ байт/с між k і l вузлами [44].

Кожен вузол комутації має буфер необмеженої ємності, середня довжина пакета дорівнює $L_p = 1/\mu$ байт. Потік даних, що виникає в вузлі i і призначений вузлу j , є найпростішим із середньою інтенсивністю $\lambda_{i,j}$ пакетів/с. Повна середня інтенсивність мережі визначається за формулою:

$$\lambda = \sum_{i=1}^{N} \sum_{j=1}^{N} \lambda_{ij}, \tag{3.1}$$

де N - загальне число вузлових комутаторів.

Вираз для середньої затримки пакета виглядає наступним чином:

$$T = \sum_{k=1}^{N} \sum_{l=1}^{N} \gamma_{kl} t_{kl}', \tag{3.2}$$

де γ_{kl} - середній час перебування повідомлень в лінії,

$$\gamma_{kl} = \sum_{i=1}^{N} \sum_{j=1}^{N} \lambda_{ij} x_{kl}^{(i,j)}, \tag{3.3}$$

де $x_{kl}^{(i,j)}$ - частка потоку, що проходить по лінії (k,l) [61-63].

Крім часу затримки порівняння проводиться за результатами завантаження серверів послуг пакетами і кількістю біт, що обробляються.

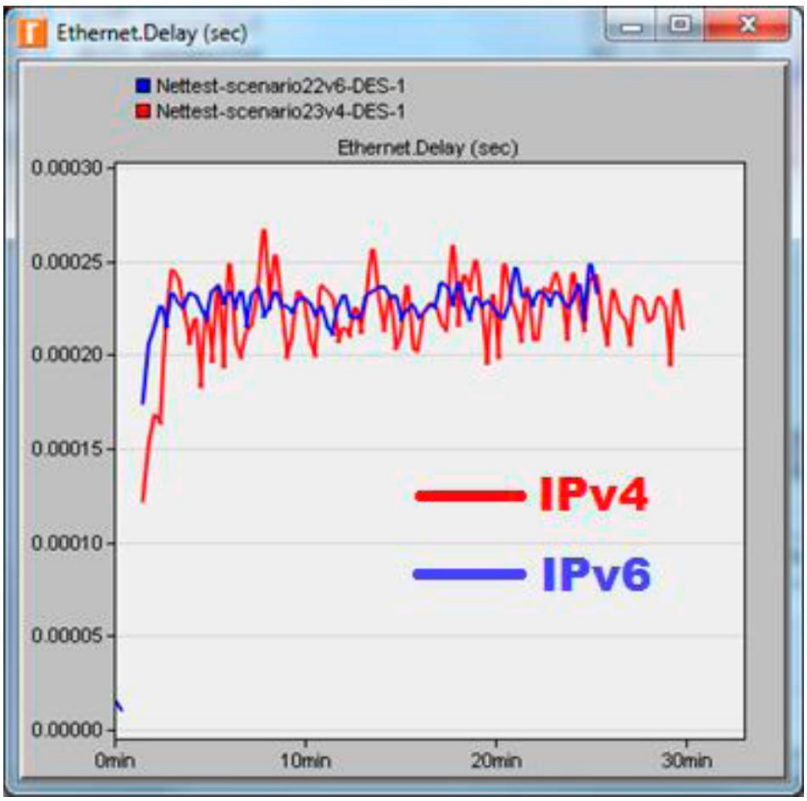

Рис. 3.4. Час затримки пакетів в першому сценарії

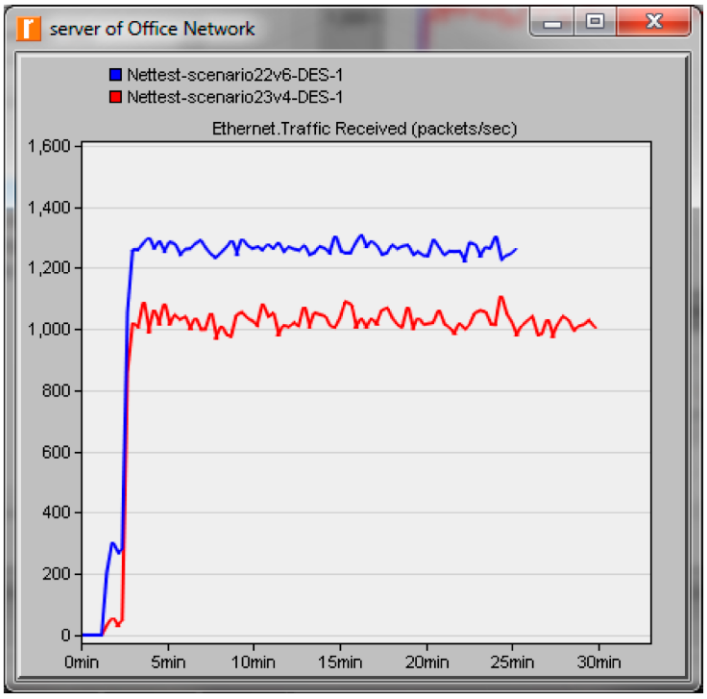

Рис.3.5. Кількість оброблюваних пакетів на сервері в першому сценарії

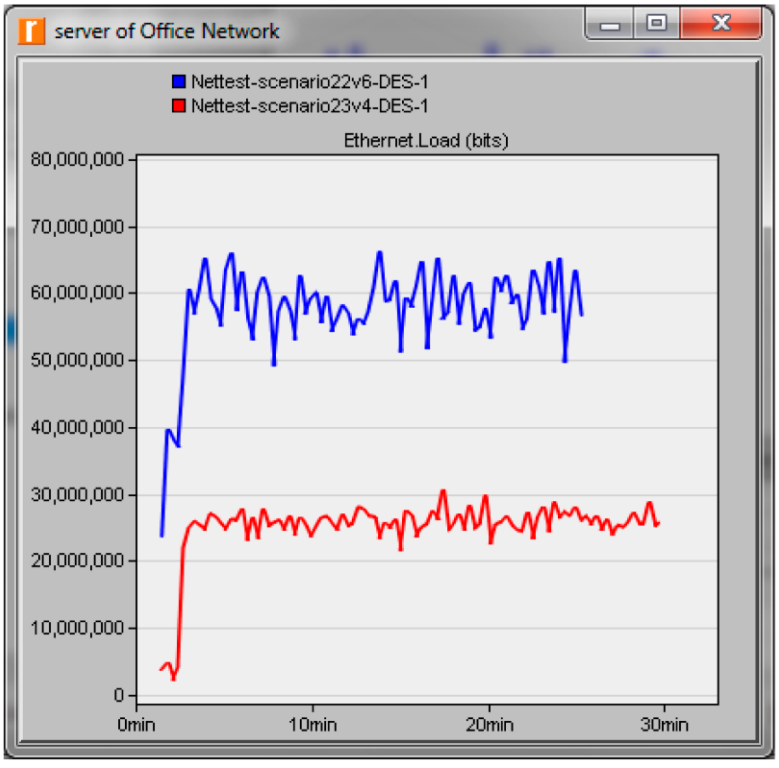

Рис. 3.6. Кількість байт оброблюваних сервером в першому сценарії

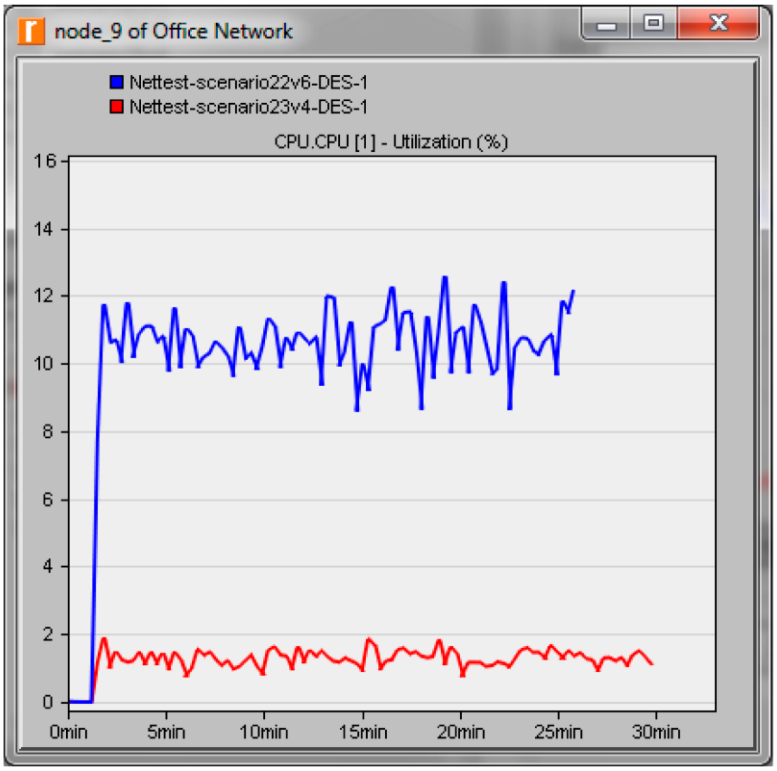

Рис. 3.7. Завантаження процесора маршрутизатора в першому сценарії

На отриманому графіку можна відстежити який час (в секундах) витрачається пакетом при проходженні всього шляху. Видно, що різниця в використанні IP протоколів різних версій несильно впливає на час затримки проходження пакета в малих мережах. В деякі моменти часу роботи мережі, мережева модель, яка зконфігурована по протоколу IPv4, працює швидше IPv6. Маршрутизатор в стані обробляти необхідну кількість пакетів, не вносячи значний час на затримку пакетів в черзі, тримаючи їх в пам'яті. Однак на графіку, що описує завантаження сервера на обробку запитів і передачу послуг, видно, що протокол IPv6 більше навантажує сервер за кількістю оброблених біт інформації, ніж IPv4. При цьому на графіку, який відображає обробляючі пакети даних, кількісно однакові у двох досліджуваних протоколах.

Це пояснюється тим, що протокол IPv6 спроектований розробниками, враховуючи сучасний розвиток технологій передачі даних, з можливістю формування пакетів з великою кількістю даних. Це скорочує кількість пакетів в мережі, що відповідно скорочує кількість біт технічної інформації, що передається, розвантажуючи канал передачі даних. При цьому збільшується навантаження на маршрутизатори, що можна відстежити на графіку

завантаження процесора. Також потрібна велика ємність буфера маршрутизатора, щоб зберігати великі пакети, які очікують у черзі на обробку.

Друга модель більш навантажена абонентами і проміжними вузлами. Вона має в два рази більше абонентів, плюс ще один маршрутизатор. Розширення мережі повинно збільшити час затримки в мережі, завантаження маршрутизатора і завантаженість серверів.

Як і з першою моделлю, також була проведена симуляція роботи мережі тривалістю 15 хвилин, спочатку з мережею, яка зконфігурована по протоколу IPv4, а потім по протоколу IPv6. Були отримані досліджувані параметри.

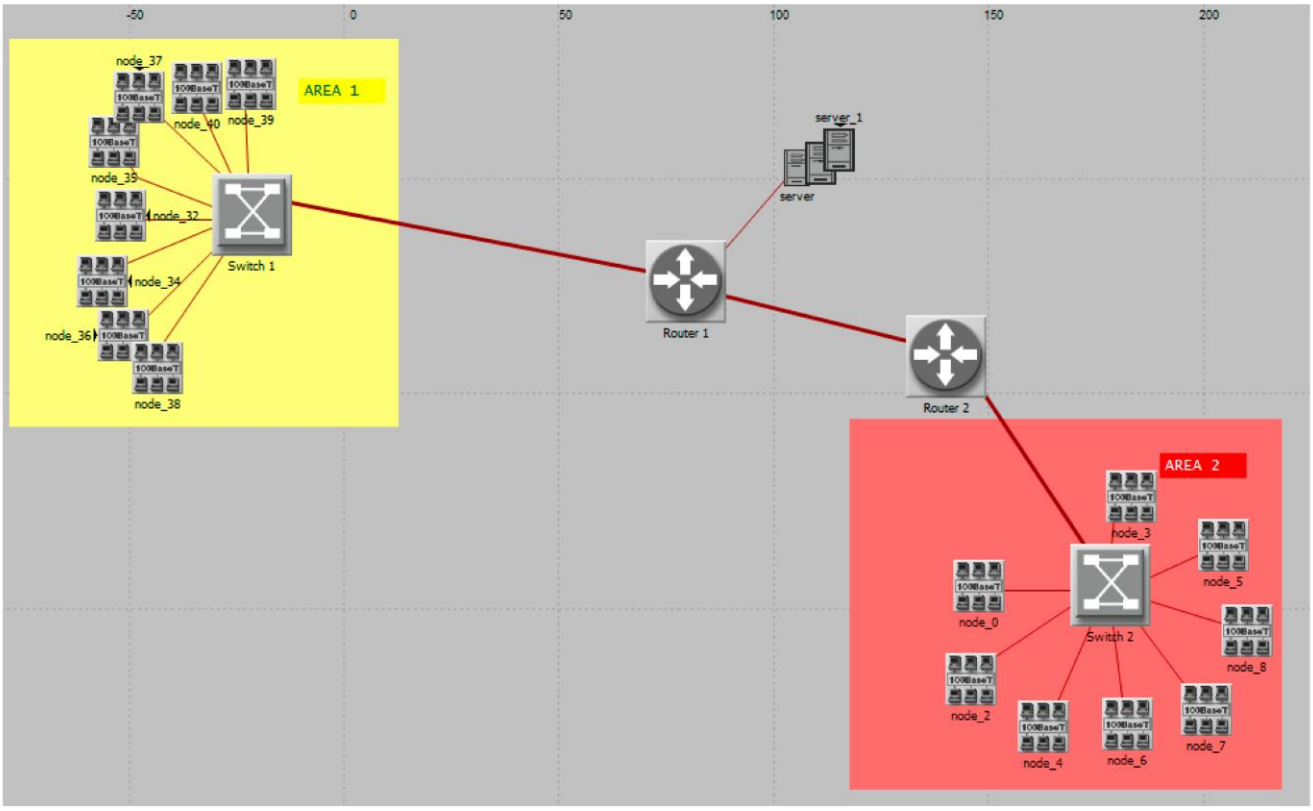

Рис. 3.8. Схема моделі другого сценарію

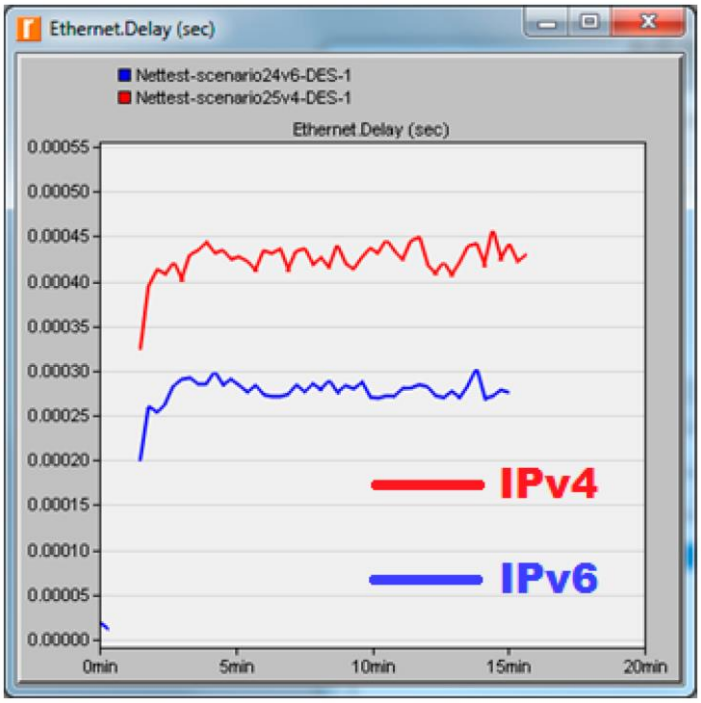

Рис. 3.9. Час затримки пакетів другого сценарію

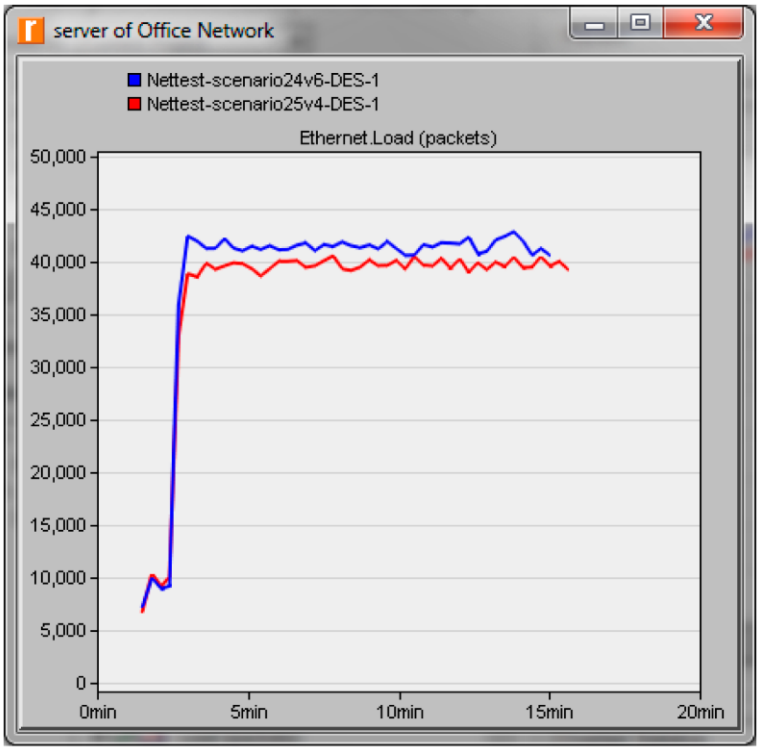

Рис. 3.10. Кількість оброблюваних пакетів сервером сценарію другого

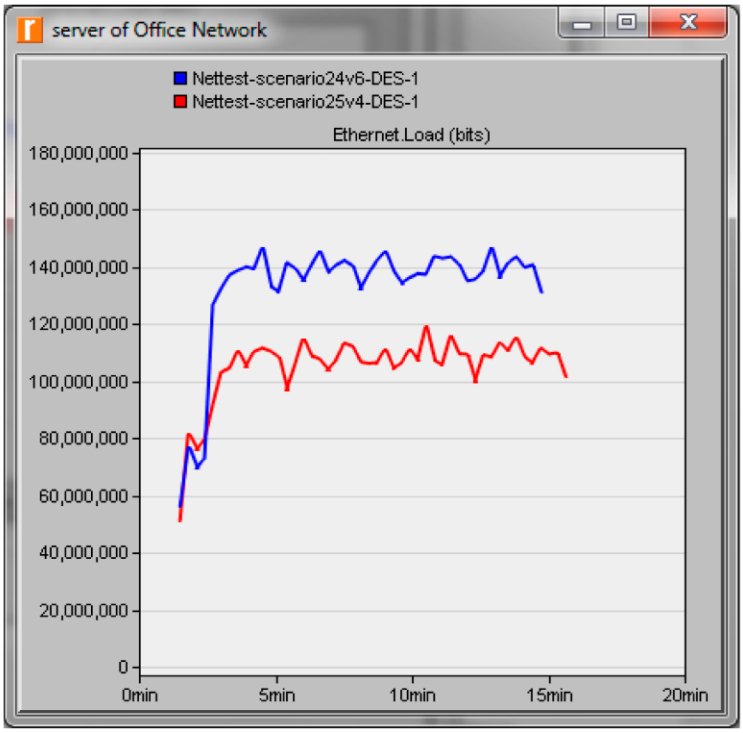

Рис. 3.11. Кількість біт оброблених сервером другого сценарію

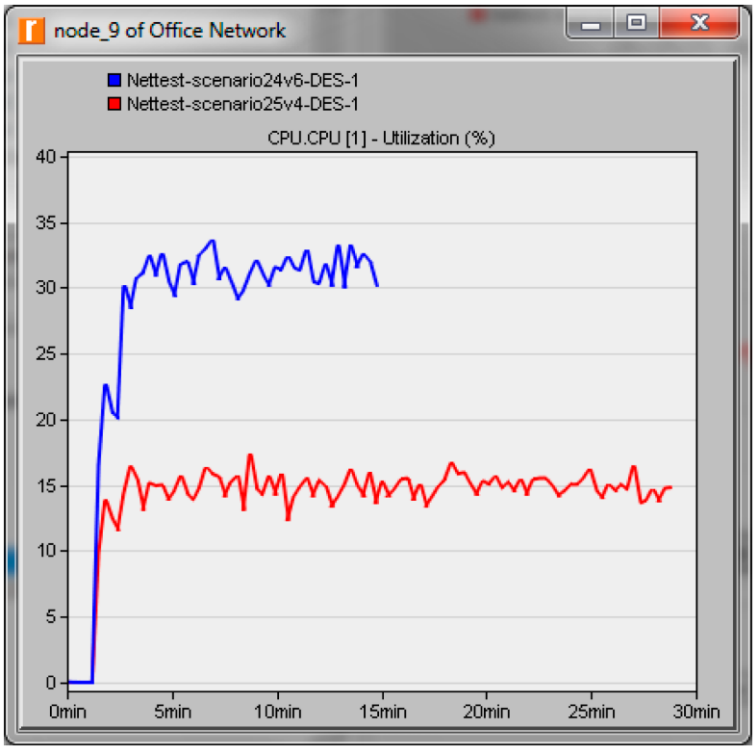

Рис. 3.12. Завантаження процесора маршрутизатора Router 1 в другому сценарії

За графіками затримки проходження пакета спостерігається збільшення часу, тому що на це впливає більша кількість абонентів. Збільшилася і кількість маршрутизаторів, які обробляють пакети. Час, за який проходить пакет від точки

до точки, використовуючи міжмережевий протокол IP версії 6 суттєво менший, ніж у IPv4. Пакет в навантаженій абонентами і маршрутизаторами проходить на 40-50% швидше при використанні IPv6, на відміну від мережі, яка налаштована по протоколу IPv4. Одна з причин збільшення швидкості передачі, при використанні мережевого протоколу IP версії 6 в порівнянні з IPv4, це спрощення заголовка. В результаті оптимізації заголовка число полів скоротилося з 14 до 8. З нього було вилучені поля «розмір» - він тепер фіксованого розміру і «контрольна сума» - її більше немає в IP пакеті, тому що більш високорівневі протоколи (наприклад TCP, UDP) ведуть свої контрольні суми, низькорівневі (наприклад Ethernet) свої. Сенсу в ще одній контрольній сумі не має, тому її вилучили. Тому маршрутизаторам не потрібно аналізувати пакет на предмет обчислення довжини заголовка або перераховувати контрольну суму при зміні TTL пакета, що в свою чергу скорочує час обробки IP пакета в маршрутизаторі, що дає змогу передавати більшу кількість пакетів за той же час.

У цьому сценарії також спостерігається збільшення оброблюваної інформації сервером. Сервера послуг формують пакети даних більшого обсягу по протоколу IPv6, завантажуючи канал передачі корисним навантаженням. При цьому на іншому графіку видно, що великі пакети даних надають більше навантаження на маршрутизатори відносно IPv4.

Третя модель побудована з максимальною кількістю підключених кінцевих пристроїв, пов'язана з обмеженням академічною версією програми Riverbed Modeler. У даній моделі в 4 рази більше абонентів, ніж в першій і в 2 рази відповідно, ніж у другій, а також мережу об'єднують три маршрутизатора з’єднаних між собою послідовно, надаючи доступ до послуг підключених абонентів. Велика кількість підключених робочих станцій вносить істотне навантаження на роботу мережі, обробку пакетів маршрутизаторами, завантаження серверів. Все це впливає на затримки в мережі, а також на пропускну здатність маршрутизаторів.

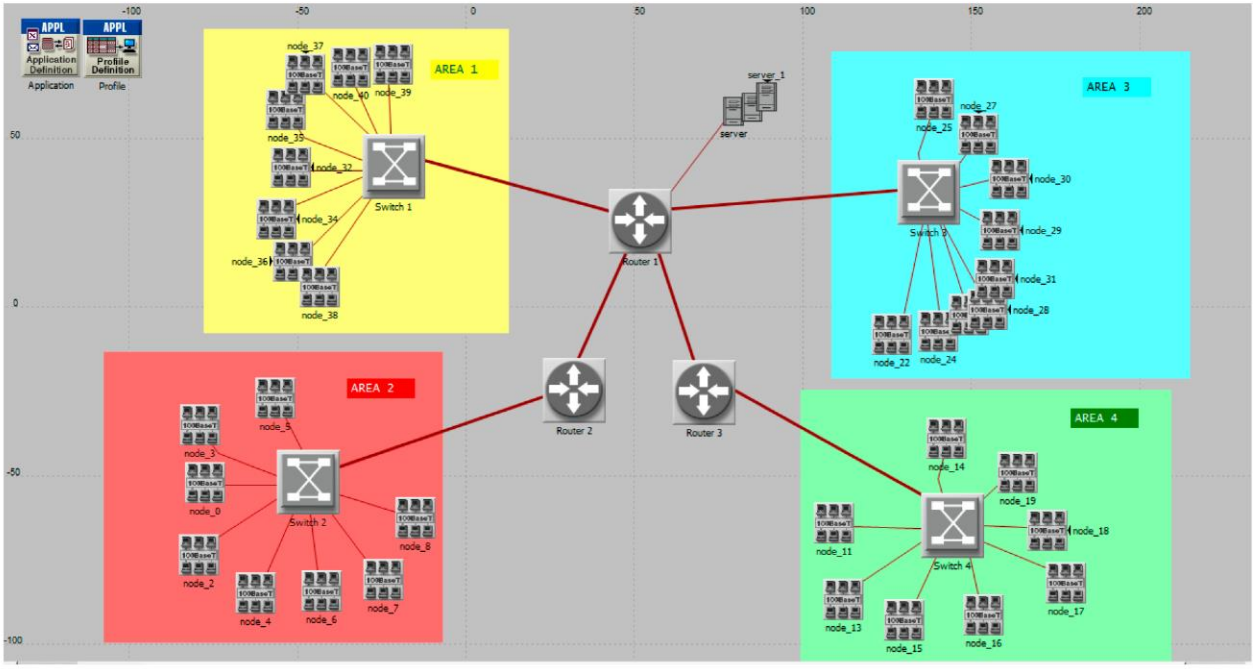

Рис. 3.13. Схеми моделі третього сценарію

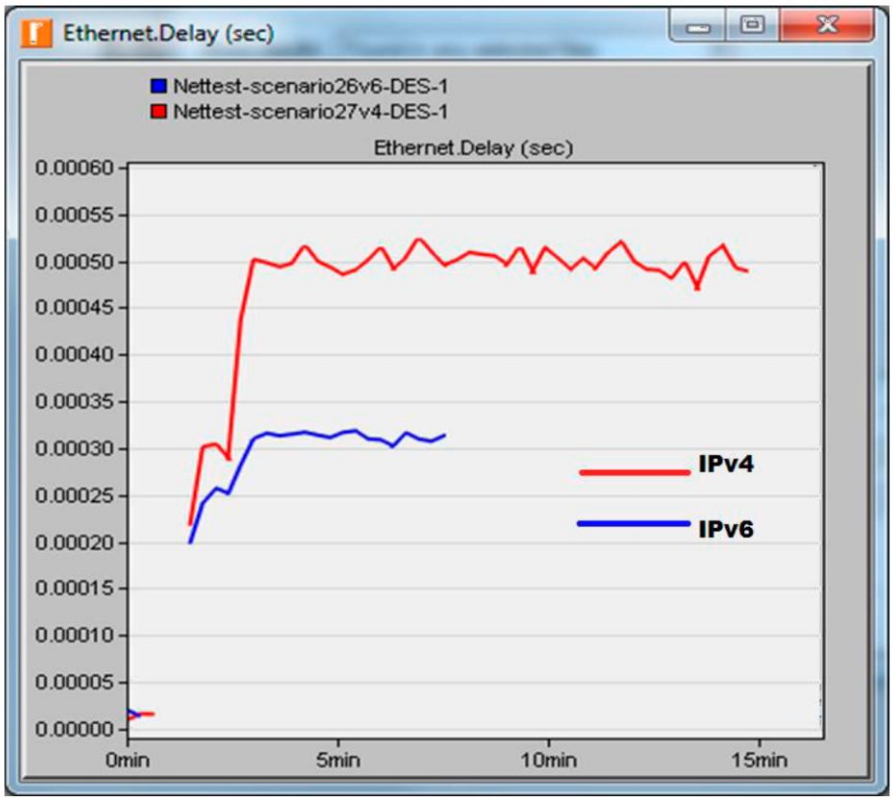

Рис. 3.14. Час затримки пакетів третього сценарію

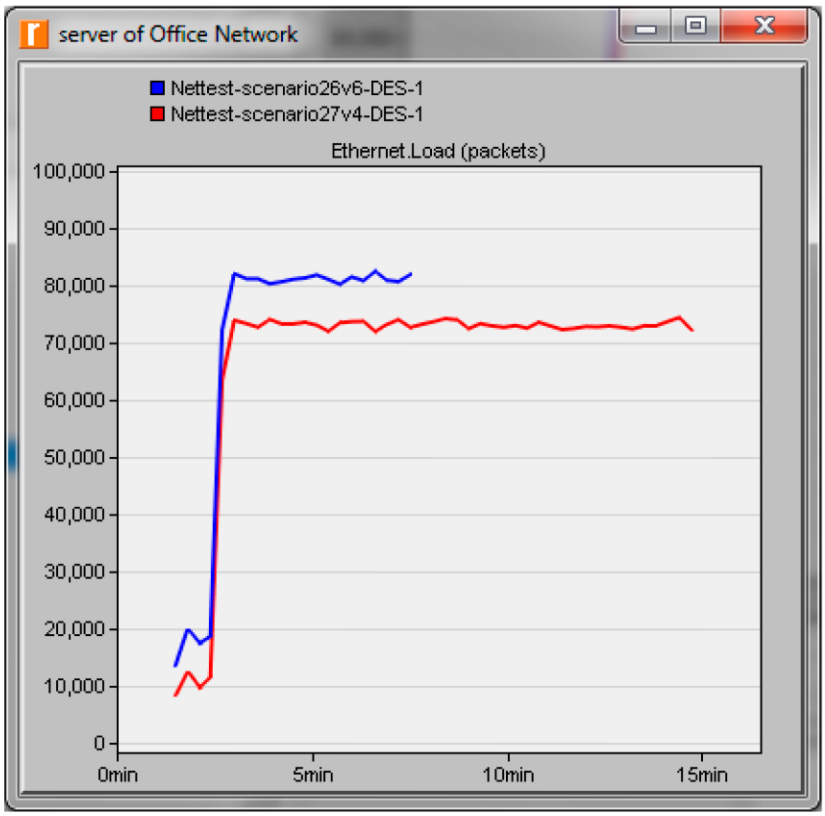

Рис. 3.15. Кількість оброблюваних пакетів сервером сценарію третього

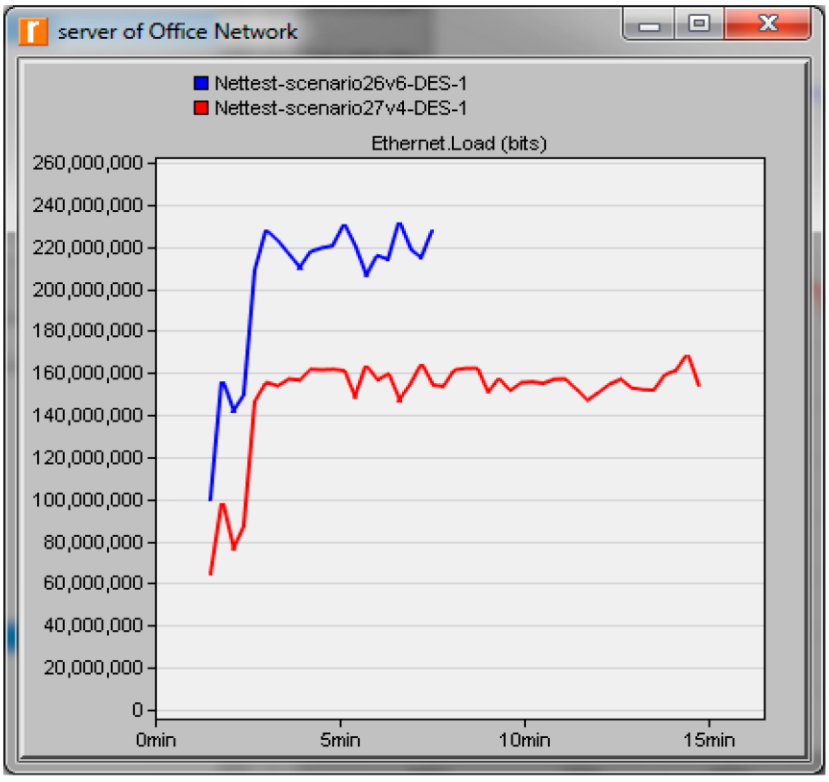

Рис. 3.16. Кількість біт оброблених сервером третього сценарію

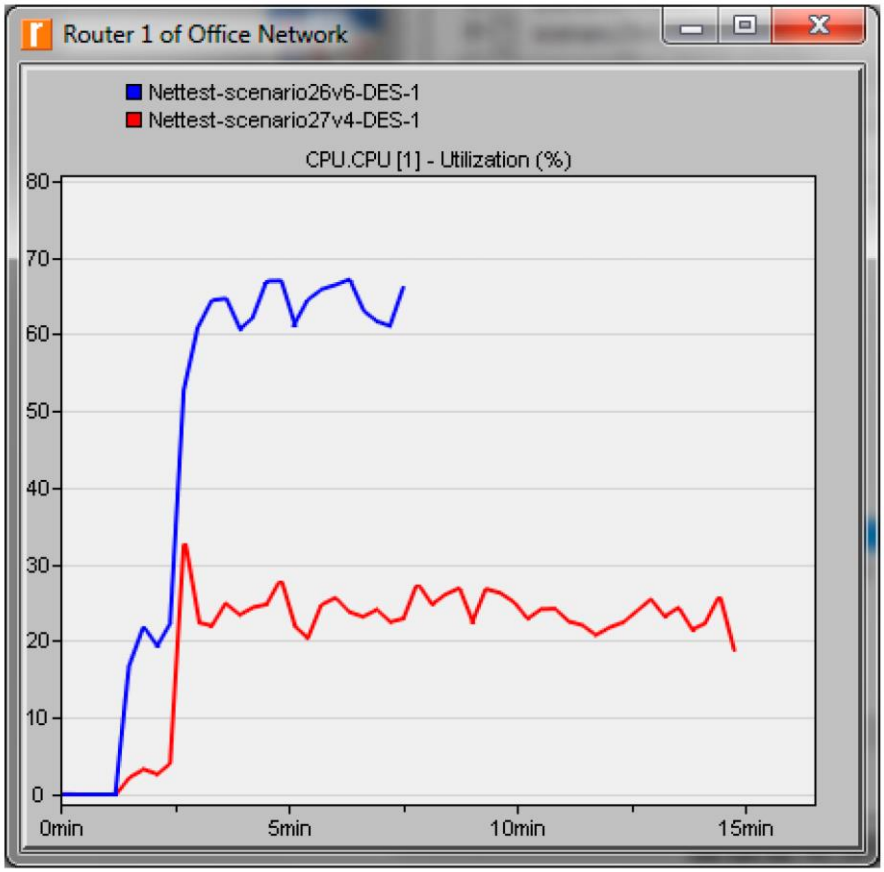

Рис. 3.17. Завантаження процесора маршрутизатора в третьому сценарії

Результат симуляції роботи мережі третьої моделі показує, що зростання часу затримки проходження пакетів при використанні мережевого протоколу IPv4 збільшується кратно, зі збільшенням кількості абонентів і числа вузлів маршрутизації. У тій же ситуації протокол IPv6 збільшує час затримки набагато менше при тій же кількості абонентів і маршрутизаторів. У третій моделі різниця досліджуваного параметра часу затримки проходження пакета від точки до точки з конфігурацією мережі IPv6 вже вище 50%, ніж з конфігурацією IPv4, що є суттєвим при роботі мережі.

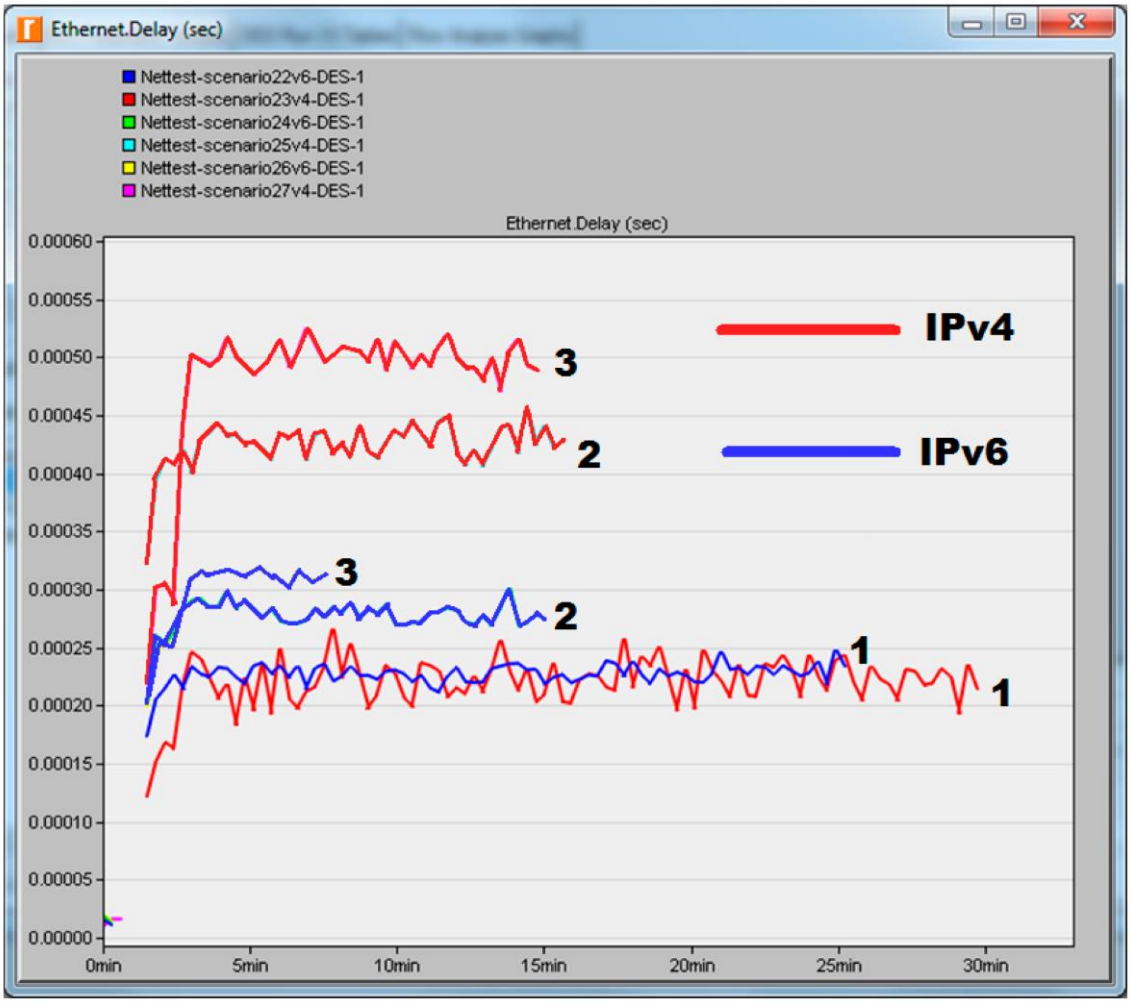

Рис. 3.18. Узагальнений графік порівняння часу затримки пакетів всіх 3 моделей

На порівняльному графіку протоколів IPv4 і IPv6 відображена залежність часу затримки проходження пакетів від розмірів мережі. З цієї порівняльної характеристики можна стверджувати, що використання протоколу IPv6 зі збільшенням розмірів мережі дає перевагу перед IPv4 .

3.2. VLAN-канали по послугах

У даній частині досліджуються характеристики мультисервісної мережі при використанні технології VLAN для надання послуг клієнтам. Для експерименту взята та ж типова схема мультисервісної мережі зв'язку.

У мережі є класичні послуги різних unicast-потоків:

- Internet-трафік (HSI - High Speed Internet);

- IP-телефонія (VoIP);
- VoD-сервіси (VoD);
- Відеоконференцзв’язок-сервіси ().

І Multicast-сервіси:

- Широкомовне телебачення (BTV);
- Музичні канали та ін.

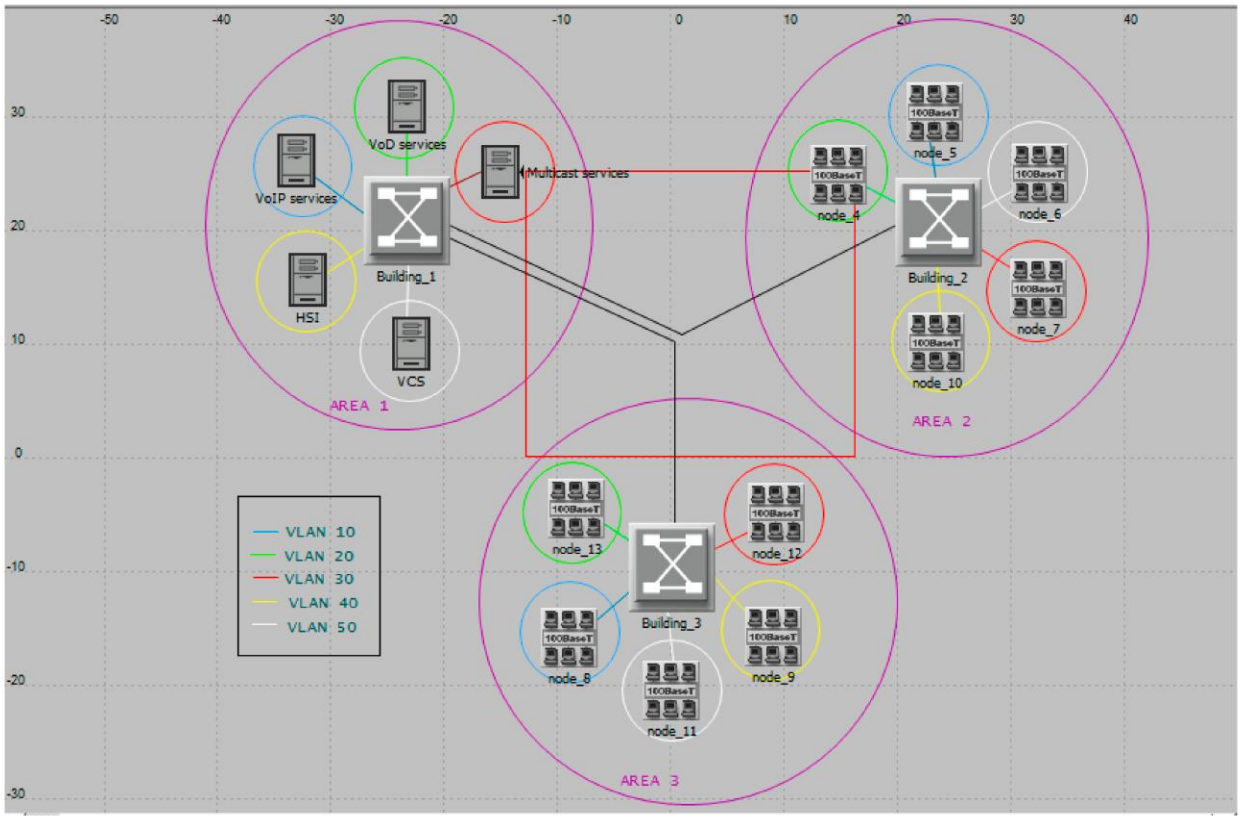

Рис. 3.19. Схема моделі з VLAN

Модель складається з трьох районів, об'єднаних трьома комутаторами. В одному районі зосереджені системи формування послуг, які поширюються по створеним на комутаторах VLAN-канали до абонентів в два інших району. У кожному районі по 1000 користувачів, які підключені до тих чи інших послуг. Дана технологія (що має назву Triple Play) має деякі переваги перед розповсюдженням послуг в загальному потоці даних. Використання VLAN каналів по послугах дозволяє в деякій мірі розвантажити комутатори, зменшивши кількість технічної інформації при передачі пакетів.

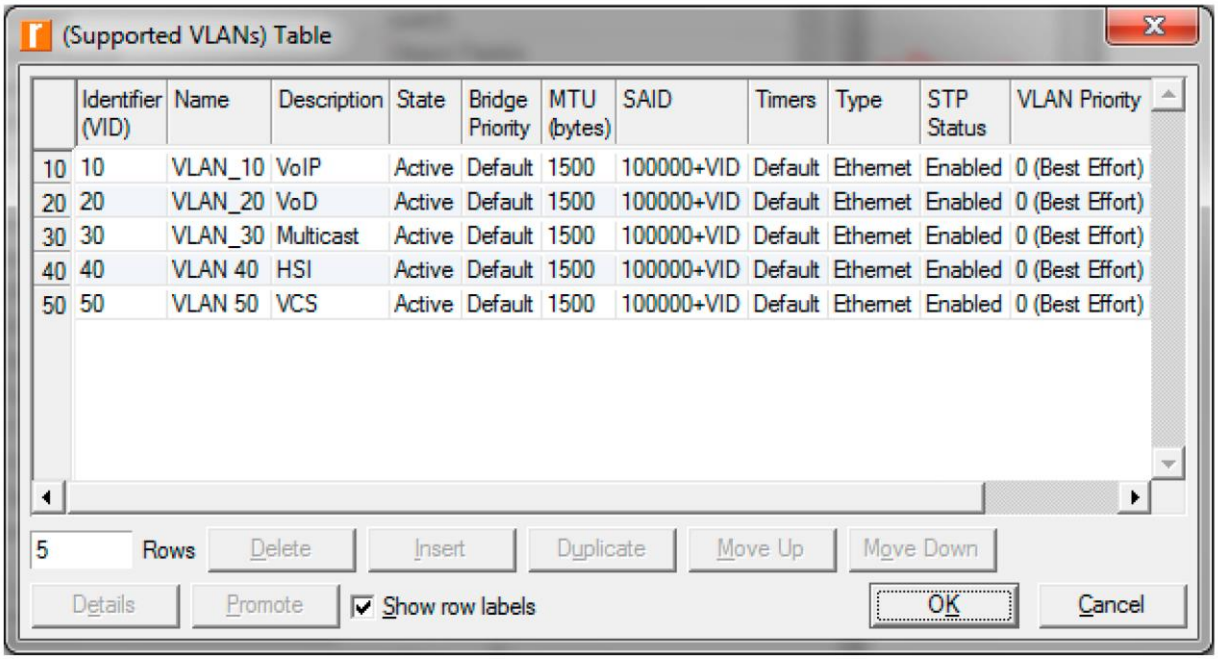

Рис. 3.20. Налаштування VLAN на комутаторі 1

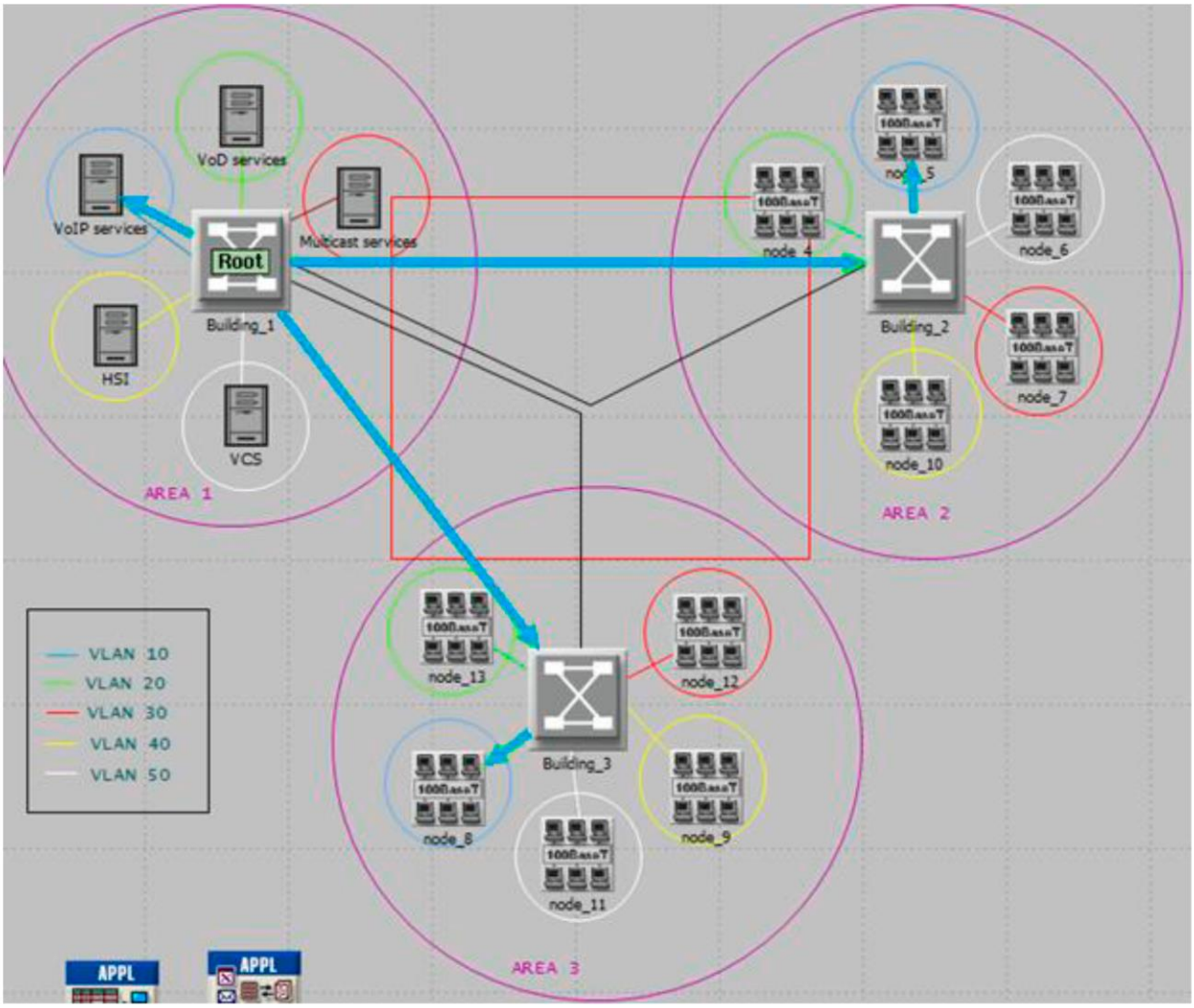

Рис. 3.21. VLAN-канал VoIP

Таблиця 3.1

План організації VLANs

Відділи організації	VoIP	VoD	Multicast-сервіси	HSI	Відеоконференц-зв'язок
Номера VLAN	10	20	ЗО	40	50

У програмі Riverbed Modeler була побудована модель і зконфігуровані 5 VLAN каналів за послугами. Також створені Trunk-канали між комутаторами. Імітація роботи моделі була проведена тривалістю 60 секунд з використанням VLAN каналів, а потім без них. Були отримані результати часу затримки проходження пакетів від точки до точки і завантаженість комутаторів в залежності від прийнятої інформації в байтах в кожен момент роботи мережі. За графіком час затримки пакетів спостерігається різниця, де мережа з використанням VLAN працює на чверть швидше. Також на іншому графіку, що описує завантаженість комутатора прийнятими байтами інформації, мережу з VLAN завантажує комутатори на чверть менше, ніж у мережі, де усі послуги передаються в загальному каналі передачі даних.

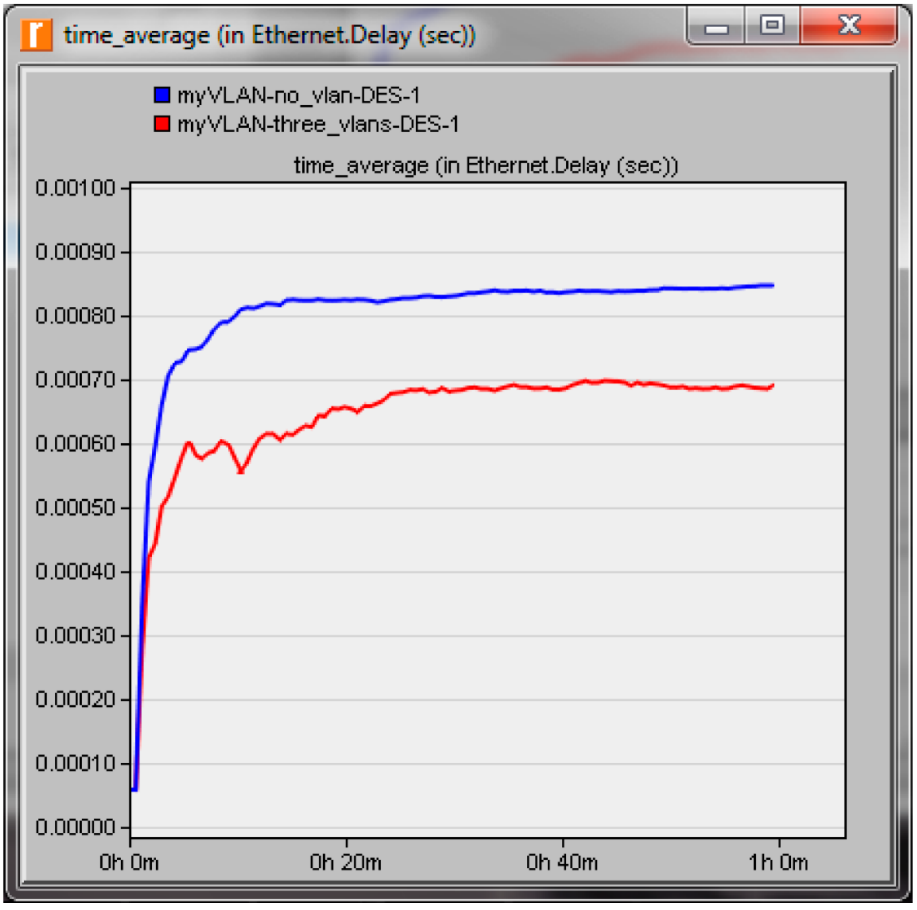

Рис. 3.22. Час затримки з VLAN та без її використання

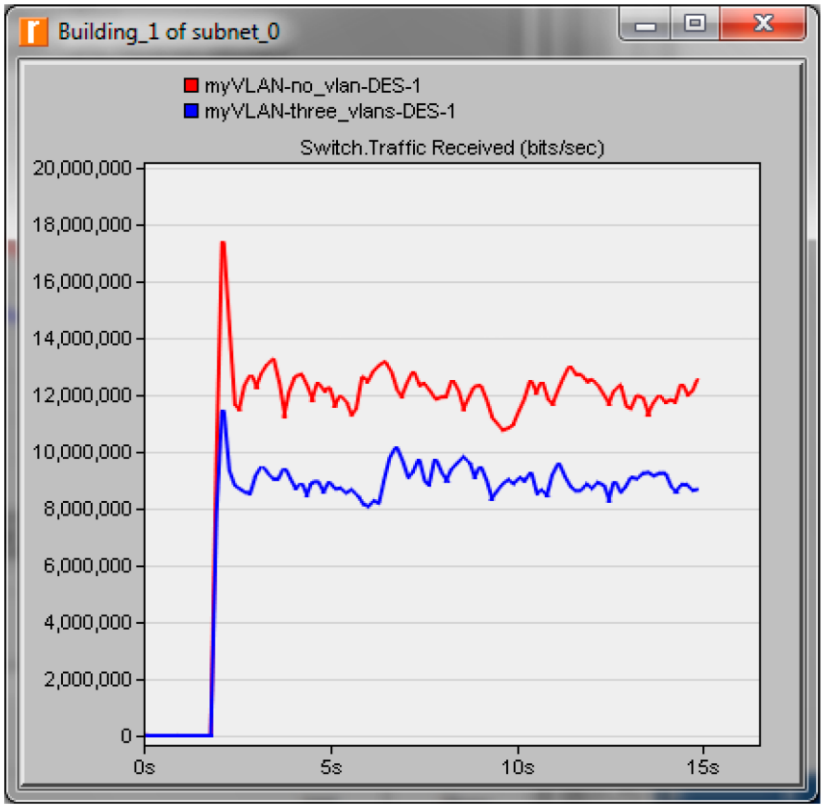

Рис. 3.23. Кількість біт в секунду прийнятих комутатором 1 з VLAN і без використання VLAN

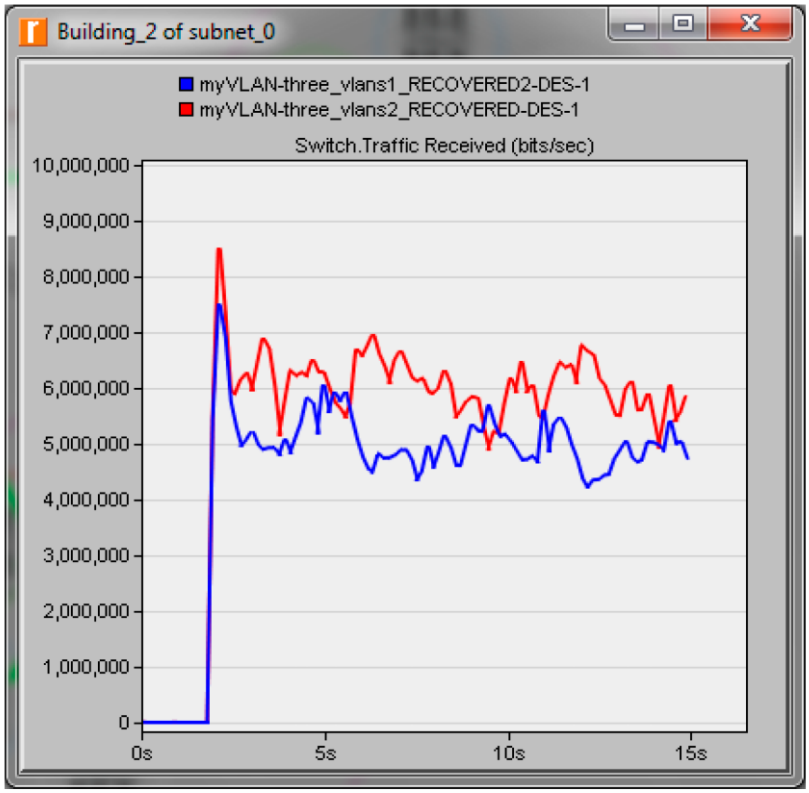

Рис.3.24. Прийнятий трафік на другому комутаторі

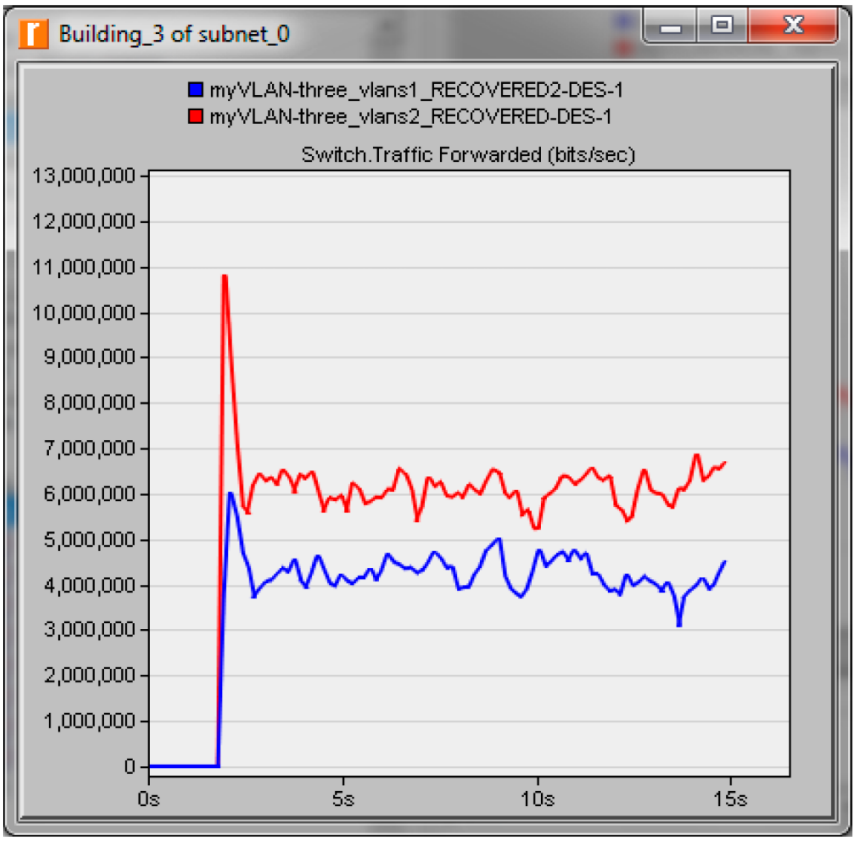

Рис. 3.25. Переданий трафік на третьому комутаторі

Як видно з наведених графіків, затримка значно зменшилася при використанні технології VLAN і завантаження комутаторів знизилося. Це пояснюється тим, що кількість пакетів в мережі скорочується, з огляду на те що відпадає необхідність масового розсилання широкомовних пакетів всім працюючим машинам. Широкомовлення обмежується межами VLAN і не виходить за його межі.

Результати комп'ютерного моделювання показали, що використання технології віртуальних локальних мереж (Virtual Local Area Network - VLAN) в мультисервісних мережах, дає змогу істотно знизити кількість пакетів, що знаходяться в мережі, а також зменшити затримку і середній час перебування в мережі, збільшуючи тим самим продуктивність мультисервісної мережі зв'язку.

3.3. Висновки до розділу 3

У розділі проведено оцінювання ефективності мультисервісної мереж

при застосуванні засобів імітаційного моделювання з різними параметрами мережі при використанні протоколів IPv4 та IPv6 чим встановлено, що:

- протокол IPv6 має менший час затримки пакетів, ніж при використанні протоколу IPv4;

- протокол IPv6 передає більшу кількість біт інформації в одному пакеті в порівнянні з IPv4;

- використання IPv6 сприяє швидкій роботі мережі і більшій пропускній здатності, перевершуючи протокол IPv4 за багатьма показниками.

- в мережах малого масштабу зконфігурованих по IPv4 або по IPv6, різниця в швидкості роботи мережі не спостерігається, в той же час завантаження мережевих вузлів зростає в мережах, налаштованих по IPv6 .

Також здійснено оцінювання ефективності мультисервісної мережі при застосуванні засобів імітаційного моделювання при різних параметрів мережі і типів послуг при використанні VLAN чим встановлено, що :

- використання VLAN-каналів знижує навантаження на вузли через зниження широкомовлення в мережі;

- використання технології VLAN при передачі послуг до абонентів по виділеним віртуальним каналам дає змогу знизити навантаження на активне мережеве обладнання та власне на всю мережу, дозволяючи обробляти більше корисної інформації.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Розробка програмного забезпечення для тестування комп'ютерних мереж, з різними протоколами IPv4, IPv6 та різними мережевими обладнаннями здійснювалась на персональному комп'ютері, тому дотримання вимог Державних санітарних правил і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98) (затверджено постановою Головного державного санітарного лікаря України від 10.12.98 р. №7) та Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, затверджених наказом Міністерства соціальної політики України 14.02.2018 № 207 (НПАОП 0.00-7.15-18), які розроблено на основі Директиви 90/270/ЄЕС від 29 травня 1990 року про мінімальні вимоги безпеки та здоров'я при роботі з екранними пристроями.

В процесі роботи з мережевим обладнанням щодо тестування роботи комп'ютерної мультисервісної мережі рівень безпеки та захист працюючого від випромінювання екранних пристроїв має бути зведено до гранично допустимого рівня (вібрації, шуму, температур), який не спричиняє соматичних розладів, а також інших патологічних змін стану здоров'я, працездатності відповідно до вимог безпеки та охорони здоров'я працівників.

Під час облаштування робочого місця необхідно підібрати таке устаткування, яке не створює додаткового шуму та не виділяє позанормованого тепла. Гранично допустимі рівні шуму повинні відповідати вимогам Санітарних норм виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.6.037-99), затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 37. Мікроклімат виробничого приміщення має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень (ДСН 3.3.6.042-99), затверджених постановою Головного державного санітарного лікаря України від 01 грудня

1999 року № 42.

Організація робочого місця при роботі із мережевим обладнанням повинно бути забезпечено відповідність усіх елементів місця та їх розташування повинне бути ергономічним, антропологічним, відповідати психофізіологічним вимогам, а також характеру роботу із комп’ютерним електрокардіографом при розробці програмного забезпечення. Освітлення в зоні роботи повинне створювати контраст між екраном і навколишнім середовищем та відповідати вимогам ДСанПІН 3.3.2.007-98.

Необхідно зауважити, що програмне забезпечення керує алгоритмами роботи системи при прийнятті рішень щодо прийому та передачі даних мережі, відноситься до класу інформаційно-телекомунікаційних виробів.

Відповідне програмне забезпечення розроблялось у такий спосіб, щоб у разі його застосування не було спричинено виникнення ризику для клінічного стану або безпеки споживачів чи для здоров’я і безпеки користувачів або інших осіб.

Відповідно до вимог мереже обладнання спроектоване таким чином, що забезпечує надійність, відтворюваність, та ефективність системи згідно з призначенням. В системі передбачено засоби для усунення або мінімізації спричинених ризиків у разі поодинокого збою.

Програмне забезпечення мережевого обладнання розроблено відповідно до поточного рівня знань з урахуванням принципів циклу розробки, управління ризиками, валідації та перевірки.

Конструкцією мережевого обладнання передбачено мінімізацію ризиків створення електромагнітних полів, які можуть погіршити роботу інших виробів або обладнання в звичайних умовах, а також, щоб уникнути ризиків випадкового ураження електричним струмом за умови належного використання, правильного встановлення, тобто має робочу ізоляцію і виконана таким чином, що підключити її до електричної мережі можна лише після під’єднання корпусу до заземлювача, а при від'єднанні від мережі - корпус відключається від заземлювача (нульового захисного провідника) в останню чергу. Рівень та стан

ізоляції струмопровідних частин системи відповідає правилам використання системи.

Таким чином, мережеве обладнання при розробці програмного забезпечення для тестування комп’ютерних мереж є безпечною з точки зору охорони праці та техніки безпеки.

4.2. Безпека в надзвичайних ситуаціях

Підприємтсво з випуску мережевого обладнання як базової складової мультисервісної мережі є пожежонебезпечним, тому акуальним є забезпечення протипожежного захисту робітників та службовців, які на них працюють. Заходи протипожежного захисту здійснюються з дотриманням вимог глави 13 Кодексу цивільного захисту України від 02.10.2012 р. №5403-VI.

Відповідно до Закону України “Про пожежну безпеку” забезпечення безпеки підприємств, установ покладено на керівників або уповноважених ними осіб; їх обов'язки щодо забезпечення пожежної безпеки обумовлені статтею 5 цього Закону.

Обов'язки керівників цехів і лабораторій з виготовлення мультисервісної мережі та посадових осіб щодо пожежної безпеки:

1. Розробляти комплекс заходів щодо забезпечення пожежної безпеки цехів і лабораторій з виготовлення мультисервісної мережі, в установі, організації;

2. Відповідно до державних нормативних актів з пожежної безпеки розробляти і затверджувати положення, інструкції, інші нормативні документи, що діють у межах цехів і лабораторій з виготовлення мультисервісної мережі; здійснювати контроль за їх виконанням;

3. Організовувати навчання працівників щодо пожежної безпеки;

4. Утримувати у справному стані засоби протипожежного захисту і зв'язку, пожежну техніку, обладнання та інвентар, не використовувати його не за призначенням;

5. Здійснювати службове розслідування випадків пожеж.

Загальні вимоги пожежної безпеки:

Кожний працівник повинен знати правила поведінки при пожежі, шляхи евакуації, вміти користуватися первинними засобами пожежогасіння, знати місце їх знаходження.

Легкозаймисті та горючі рідини необхідно зберігати у спеціально відведених місцях окремо від інших матеріалів.

У разі виникнення пожежі працівники повинні негайно повідомити про це пожежну охорону за телефоном 101 та керівництво підприємства, і негайно розпочати ліквідацію пожежі всіма наявними засобами.

Комплекс технічних, експлуатаційних, організаційних і режимних заходів щодо відвернення пожеж розробляє і здійснює Державний пожежний нагляд. Представники органів Державного пожежного нагляду мають право перевіряти стан протипожежного захисту будівель, споруд, складів, вимагати відповідні документи та інформацію, притягувати до відповідальності осіб, винних у порушенні постанов, правил, норм, інструкцій з пожежної охорони, частково чи повністю забороняти роботу цехів і лабораторій з виготовлення мультисервісної мережі при наявності небезпеки виникнення пожежі.

Протипожежна профілактика – комплекс організаційних і технічних заходів, спрямованих на забезпечення пожежної безпеки працівників, відвернення пожежі; створення умов для швидкого та ефективного гасіння пожежі.

Заходи з пожежної профілактики поділяються на організаційні, технічні, режимні, експлуатаційні.

Організаційні заходи передбачають правильну експлуатацію устаткування будівель, території, своєчасний інструктаж працюючих з пожежної небезпеки, проведення занять з пожежно-технічного мінімуму, створення добровільних пожежних дружин, перевірку їх готовності до пожежогасіння, тренування, створення пожежно-технічних комісій та ін. Підприємства повинні бути забезпечені загальнооб'єктової протипожежними інструкціями, що регламентують особливості утримання доріг, протипожежних розривів, під'їздів до будівель і джерел води, зберігання речовин і матеріалів, режим паління,

утримання засобів пожежогасіння у справному стані, виклик пожежної охорони.

До технічних заходів відноситься дотримання протипожежних норм і правил при конструюванні та проектуванні будівель, обладнання, утримання в справному стані устаткування, суворий контроль за дотриманням правил експлуатації обладнання та дотримання правил та інструкцій з протипожежної безпеки, застосування автоматичних пристроїв виявлення, оповіщення та гасіння пожеж.

До заходів пожежної профілактики при проектуванні і будівництві належать: підвищення вогнестійкості будівель та споруд; зонування території (планування з урахуванням ознак пожежної небезпеки); протипожежні розриви; протипожежні перешкоди; забезпечення безпечних шляхів евакуації (не менше двох виходів); видалення з приміщення диму при пожежі (застосування аераційних ліхтарів, димових люків, легкоскидних конструкцій); дотримання протипожежних вимог до систем опалення та кондиціонування повітря.

Заходи режимного характеру регулюють режим і правила роботи. Куріння допускається тільки у спеціально відведених місцях, обладнаних урнами і ємностями з водою. У цих місцях повинні бути вивішені написи "Місце для куріння".

Експлуатаційні заходи охоплюють своєчасне проведення профілактичних оглядів, випробувань, ремонтів технологічного та допоміжного устаткування, а також інженерного господарства (електромереж, електроустановок, опалення, вентиляції).

4.3. Висновки до розділу 4

У підрозділі з охорони праці обґрунтовано безпечність експлуатації мережевого обладнання як базового складової мультисервісної мережі з точки зору охорони праці.

У підрозділі з безпеки в надзвичайних ситуаціях проаналізовано заходи організаційно-технічного характеру протипожежного захисту на виробництві мережевого обладнання як базової складової мультисервісної мережі.

ЗАГАЛЬНІ ВИСНОВКИ

У роботі розв’язано актуальну задачу оцінювання ефективності мультисервісної мережі із застосуванням засобів імітаційного моделювання.

Отримано такі результати:

1. Проведено аналіз існуючих протоколів мультисервісних мереж зв'язку, що дало змогу обґрунтувати напрям дослідження.

2. Розроблено імітаційну модель мультисервісної мережі в середовищі Riverbed Modeler, яка дала змогу моделювати поведінку мережі при різних сценаріях, оцінювати її пропускну здатність, визначати рівень завантаження буферів мережевих пристроїв, затримки мережевого трафіку.

3. Оцінено ефективність мультисервісної мереж при застосуванні засобів імітаційного моделювання з різними параметрами мережі при використанні протоколів IPv4 та IPv6 чим встановлено, що:

- протокол IPv6 має менший час затримки пакетів, ніж при використанні протоколу IPv4;

- протокол IPv6 передає більшу кількість біт інформації в одному пакеті в порівнянні з IPv4;

- використання IPv6 сприяє швидкій роботі мережі і більшій пропускній здатності, перевершуючи протокол IPv4 за багатьма показниками.

- в мережах малого масштабу зконфігурованих по IPv4 або по IPv6, різниця в швидкості роботи мережі не спостерігається, в той же час завантаження мережевих вузлів зростає в мережах, налаштованих по IPv6 .

4. Оцінено ефективність мультисервісної мережі при застосуванні засобів імітаційного моделювання при різних параметрів мережі і типів послуг при використанні VLAN чим встановлено, що :

- використання VLAN-каналів знижує навантаження на вузли через зниження широкомовлення в мережі;

- використання технології VLAN при передачі послуг до абонентів по виділеним віртуальним каналам дає змогу знизити навантаження на активне мережеве обладнання та власне на всю мережу, дозволяючи обробляти більше корисної інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Камер, Д. Э. Сети TCP/IP, том 1. Принципы, протоколы и структура — М.:«Вильямс», 2003. — 880 с.

2. Семенов, Ю. А. Протоколы Internet. — 2-е изд., стереотип.. — М.: Горячая линия - Телеком, 2005. — 1100 с.

3. Общее описание RFC 793, 1981

4. Общее описание RFC 791, 1981

5. Общее описание RFC3330: Special-use IPv4 addresses (англ.); заменён RFC5735: Special-use IPv4 addresses (англ.), 2002

6. Общее описание RFC1700: Assigned Numbers, 1994

7. Общее описание RFC1122: Requirements for Internet Hosts — Communication Layers, 1989

8. Общее описание RFC1918: Address allocation for private internets, 1996

9. Общее описание RFC3927: Dynamic configuration of IPv4 link-local addresses, 2005

10. Новиков, Ю.В., Основы локальных сетей: курс лекций: учеб. пособие : для студентов вузов, обучающихся по специальностям в обл. информ. технологий / Ю. В. Новиков, С. В. Кондратенко. — М.: Интернет — Ун-т Информ. Технологий, 2005. - 360 с.

11. Олифер, В. Г., Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 4-е изд. — СПб.:Питер, 2010. — 944 с.: ил.

12. Олифер В. Г., Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 3-е изд. — СПб.:Пи-тер, 2006. — 958 с.: ил.

13. Гольдштейн, Б.С. Протоколы сети доступа [Текст]. Том 2. 2-е изд., перераб. и доп. / Б. С. Гольдштейн. - М.: Радио и связь, 2002.

14. Гольдштейн, Б. С. Протоколы сети доступа: Учеб. пособие / Б. С. Гольдштейн. - М.: Радио и связь, 2005. - 292 с.

15. Олифер В.Г., Основы сетей передачи данных: Учеб. пособие / В.Г.Олифер, Олифер Н.А. - Интернет-университет информационных технологий - ИНТУИТ.ру, 2005. -176 с.

16. Ногл, М. TCP/IP. Иллюстрированный учебник М.: изд-во ДМК Пресс, 2001 — 480 с.

17. Фейт, С. TCP/IP Архитектура, протоколы, реализация (включая IP версии 6 и IP Security) - Изд.: Лори, 2000 - 424

18. Берлин, А.Н. Основные протоколы Интернет - Изд.: Бином, 2013 - 504

19. Семенов, Ю.А. /Алгоритмы телекоммуникационных сетей. Часть 1, 2 и 3. - изд.: Национальный Открытый Университет "ИНТУИТ" 2016 - 832

20. Герасименко Сети и телекоммуникации. Учебное пособие / Б. В. Соболь, А. А. Манин - изд.: Феникс, 2015 г. - 191

21. Хант К. TCP/IP. Сетевое администрирование - Изд.: Символ-Плюс, 2007 - 816

22. Средства информационного взаимодействия в современных распределенных гетерогенных системах / Р.Э. Асратян, В. Н. Лебедев; Изд.: Ленанд, 2009 - 130 стр.

23. IPv6. Администрирование сетей / Н. Р. Мэрфи, Д. Мэлоун Изд.: Кудиц-образ, 2007 год, 320 с.

24. Иртегов, Д.В. Введение в сетевые технологии СПб.: БХВ-Петербург, 2004 - 560 с.

25. Общее описание RFC 1883, 1995

26. Общее описание RFC 5006, 2007

27. Общее описание RFC 6106, 2010

28. IPv6 используется уже в 10% сетевых устройств мира [Электронный ресурс]/ www.overclockers.ru - информационных сайт

29. https://www.overclockers.ru/so^news/73277/ipv6-ispolzuetsya-uzhe-v-10-setevyh-ustrojstv-mira.html (дата обращения 20.04.2016)

29. Cisco: к 2015 г. количество сетевых устройств может превысить 15 млрд [Электронный ресурс]/ www.cisco.com - официальный сайт компании Cisco http://www.cisco.com/web/RU/news/releases/txt/2011/060111b.html

30. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение Изд. 2-е, испр. : Пер. с англ. М. : Издательский дом "Вильяме", 2003. — 1104 с. : ил.

31. Тимофеев, А.В. Адаптивное управление и интеллектуальный анализ информационных потоков в компьютерных сетях. - СПб.: Анатолия, 2012, 280 с Смелянский, Р. Л. Компьютерные сети. В 2 томах. Том 2. Сети ЭВМ:Р. Л. Издательство: Академия ISBN: 978-5-7695-7153-4.978-5-7695-7152-7, 2011 - 240 стр.

32. . TCP/IP. Для профессионалов / Т. Паркер, К. Сиян; 3-е изд. СПб.: Питер, 2004. - 859 с.: ил.

33. Дилип, Н. Стандарты и протоколы Интернета - Изд.: Русская Редакция, 2000 - 384 с.

34. Анализ сетевых протоколов: Лабораторный практикум по курсу «Сети ЭВМ и телекоммуникации»/ Н. Н. Коннов, В. Б. Механов. - Пенза: Изд-во ПГУ, 2010 - Ч. 1. - 68 с.

35. Web-протоколы. Теория и практика / Кришнамурти Б., Дж. Рекс-форд; изд.: Бином, 2010 - 592 с.

36. Кульгин, М. В. Компьютерные сети. Практика построения, 2-е изд. — СПб.: Питер, 2003. — 416 с.

37. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Б. Синклер; Изд.: БХВ-Петербург 2004 - 752

38. Моделирование и синтез оптимальной структуры сети Ethernet / Благодаров А. В., Пылькин А. Н., Скуднев Д. М. и др.; Изд.: Горячая линия-Телеком, 2014 - 112 с.

39. Таненбаум, Э. Компьютерные сети, Учебное пособие по компьютерным сетям. 5-е изд. - СПб.: Питер, 2012. — 960 с.

40. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей - Москва: Техносфера, 2003. - 512с.

41. Семенов, Ю.А. Телекоммуникационные технологии // book.itep.ru: сервер по телекоммуникационным технологиям. 2014. URL: http://book.itep.riP4/41/eth_4111.htm (дата обращения: 11.06.2014).

42. Битнер, В. И. Михайлова, Ц. Ц. Сети нового поколения - NGN -М.: Горячая линия - Телеком, 2011 - 227 стр.

43. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети - М.: НОУ "Интуит", 2016г.- 395с.

44. Гулиян, Г. Б. Распределенные сети: современные технологии и основы проектирования - Изд.: НОЧ «МФПУ «Синергия» 2007 - 22 с.

45. Построение коммутируемых компьютерных сетей / Смирнова Е. В., Баскаков И. В., Пролетарский А. В. и др.; изд.: НОУ "Интуит"2016 - 202

46. Смирнова, Е.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных - изд.: БХВ-Петербург, 2012 - 272

47. Поляк-Брагинский, А.В. Локальные сети. Модернизация и поиск неисправностей - СПб.: БХВ-Петербург, 2006— 640 с.

48. Епанешников, А. М. Локальные вычислительные сети - изд.: Диалог-МИФИ, 2005 - 224 с.

49. Чекмарев, Ю.В. Локальные вычислительные сети - М.: ДМК Пресс, 2009 - 200 с.

50. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : Учеб.пособие для вузов / С.В. Никифоров .- М. : Финансы и статистика , 2003 - 223 с.

51. Сети и телекоммуникации: учеб. пособие для вузов / Пескова С. А., Кузин А. В. и др. 3-е изд., стер. .- М. : Академия, 2008 .- 350 с.

52. Семенов, А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов. - М.: ДМК Пресс; М.: Компания АйТи, 2003. - 416 с.

53. Кузьменко, Н. Г. Компьютерные сети и сетевые технологии - изд.: Наука и техника, 2013 - 368 с.

54. Основы локальных сетей / Новиков Ю.В., Кондратенко С.В. - М.: Интернет-Университет Информационных Технологий, 2005. — 360 с.

55. Вычислительная техника, сети и телекоммуникации. Учебное пособие для ВУЗов / Гребешков А.Ю., Попова Н.А. - М.: Гор. линия-Телеком, 2015 - 190 с.

56. Телекоммуникационные системы и сети: Учебное пособие. В 3-х томах под. ред. профессора В.П.Шувалова. - Изд.3-е,испр. и доп.- М.: Горячая линия-Телеком, 2003 - 647 с.: ил.

57. Вычислительные системы, сети и телекоммуникации / Пятибратов А. П., Гудыно Л. П., Кириченко А. А. М.: Финансы и статистика, 2004. — 512 с.: ил.

58. Тарасов, В.Н. Проектирование и моделирование сетей ЭВМ в системе OPNET Modeler: лабораторный практикум / В.Н. Тарасов, Н.Ф. Бахарева, А.Л. Коннов, Ю.А. Ушаков. - Оренбург: 2012. - 258 с.

59. Описание программного продукта Riverbed Modeler [Электронный ресурс]/ www.riverbed.com - официальный сайт компании Riverbed http://www.riverbed.com/gb/products/steelcentral/steelcentral-riverbed-modeler.html

60. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Б. Синклер - «БХВ-Петербург», 2004 - 740

61. Гулевич Д. С. Сети связи следующего поколения: Учеб. пособие / Д.С. Гулевич - Интернет-университет информационных технологий - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2007. - 184 с.

62. Величко, В.В. Телекоммуникационные системы и сети: Учеб. пособие В 3 томах. Том 3. Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.В. Шувалов, А.Ф; под ред. В.П. Шувалова. - М.: Горячая линия - Телеком, 2005. - 592 с.

63. Ершов, В.А. Мультисервисные телекоммуникационные сети: Учеб. пособие / В.А. Ершов, Кузнецов Н.А. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. - 432 с.: ил.

Додаток А

Копія тези конференції

Досвід використання нової форми підтвердив простоту та інтерактивність взаємодії студента зі змістом online. На думку самих студентів така форма навчання дає свободу вибору, комунікацій та планування свого часу. Сьогодні в університеті вирішили зробити керованою і самостійну роботу студентів.

Перелік джерел посилання.

1. Коротун О. В. Методологічні засади змішаного навчання в умовах вищої освіти //Інформаційні технології в освіті. – 2016. – №. 3 (28). – С. 117-129.

2. Кривонос О.М., Коротун О.В. Змішане навчання як основа формування ІКТ-компетентності вчителя / О.М. Кривонос, О.В. Коротун // *Наукові записки. – Випуск 8. – Серія: Проблеми методики фізико-математичної і технологічної освіти.* Частина 2. – Кіровоград: РВВ КДПУ ім. В. Винниченка, 2015 – 180 с.

3. Moebs, S. & Weibelzahl, S. (2006). Towards a good mix in blended learning for small and medium sized enterprises – Outline of a Delphi Study. Proceedings of the Workshop on Blended Learning and SMEs held in conjuction with the 1stEuropean Conference on Technology Enhancing Learning Crete, Greece, pp. 1-6.

4. Collis B. Flexible learning in a digital world: experiences and expectations / Betty Collis, Jef Moonen. – London : Kogan Page Limited, 2001. – 231 p.

5. Триус Ю. В., Герасименко І. В. Комбіноване навчання як інноваційна освітня технологія у вищій школі //Theory and methods of e-learning. – 2012. – Т. 3. – С. 299-308.

УДК 004.7:004.94

Николин О.І., *студент 6 курсу спеціальності «Телекомунікації та радіотехніка»*
Яськів В.І., *к.т.н., доцент кафедри радіотехнічних систем*

ОЦІНЮВАННЯ ПРОДУКТИВНОСТІ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Тернопільський національний технічний університет імені Івана Пулюя

Організація великих мереж не можлива без процедури об'єднання великого числа мережевих засобів в окремі мережеві сегменти, що призводить до виникнення великого об’єму службового трафіку, що зумовлює затримки трафіку та збільшення інтервалу часу пересування пакетів в мережі. Оператори зв'язку прагнуть до збільшення продуктивності роботи мультисервісних мереж шляхом оптимізації мережевих параметрів пропускної здатності, завантаженості серверів, часу затримок пакетів у мережі та швидкодії мережевих засобів. На практиці цю задача вирішують шляхом використання сучасних технологій, зокрема організовують мережі VLAN у поєднанні із протоколом IPv6 [1]. Таке використання забезпечує збільшення продуктивності роботи мережі. Проте більшість підходів можуть не завжди бути ефективними у різних випадках їх використання. Для визначення продуктивності мережі із застосуванням тої чи іншої технології в мережах інфокомунікаційного характеру застосовують методи імітаційного моделювання, яке забезпечує процедуру раннього проєктування/дослідження мережі. Тому здійснення процедури оцінювання продуктивності мультисервісної мережі зв'язку зі сторони параметрів часових затримок пакетів, завантаження мережеві, пропускної здатності із використанням методів і засобів імітаційного моделювання при проєктуванні/дослідженні мережі є актуальною задачею. Для дослідження продуктивності мережі розроблено імітаційну модель мережі комп’ютерними засобами Riverbed Modeler Academic Edition, а результати її роботи зображено на рис.1.

(а) (б) (в)

Рис.1. Параметри мережі для протоколів IPv4 та IPv6: а) кількість оброблених пакетів; б) кількість байт, які обробив сервер; в) завантаження процесора маршрутизатора

На рис.1,а-б видно, що в деякі проміжки часу мережа із протоколом IPv4 працює швидше, а ніж з IPv6. Маршрутизатор забезпечує обробку пакетів без затрати значного часу на затримку пакетів через тримання їх у своїй пам'яті. Проте на рис.1,в видно, що завантаженість процесора маршрутизатора на обробку і передавання послуг із використання протоколу IPv6 більша за загальною кількості оброблених бітів даних, на відміну від IPv4.

Перелік джерел посилання.

1. Олифер В. Г.. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. СПб.:Питер, 2010. 944 с.

УДК 330.341.1

***Олійник Н.М.*[1]**, *к.т.н., доцент кафедри економіки, підприємництва та економічної безпеки*
***Макаренко С.М.*[2]**, *к.е.н., доцент кафедри економіки, менеджменту та адміністрування*
***Камінчук В.Б.*[1]**, *студентка 6 курсу спеціальності «Економіка» ОПП «Економіка підприємства»*

РОЛЬ ІННОВАЦІЙ В РЕАЛІЗАЦІЇ СТАЛОГО СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ ПІДПРИЄМСТВА

[1]Херсонський національний технічний університет
[2]Херсонський державний університет

Постановка проблеми в загальному вигляді і її зв'язок з важливими науковими і практичними задачами. Актуальність теми дослідження пов’язана з тим, що в сучасних умовах розвитку ринкової економіки, що характеризуються стрімким підвищенням рівня конкуренції на внутрішньому та зовнішніх ринках постачання сировини й збуту кінцевої продукції, зростанням вимогливості покупців до споживчих характеристик товарів, робіт, послуг, втримати наявні позиції та забезпечити економічне зростання може лише те підприємство, яке володіє конкурентними перевагами в усіх сферах господарської діяльності. Зокрема, у сферах економії часу, зниження витрат, покращення якості, забезпечення гнучкості, впровадження інновацій, розвитку знань тощо [1]