МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних технологій та комп'ютерної інженерії

В.Ю. Каштан, Я.В. Панферова, В.С. Зарічний

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
спеціальності 126 Інформаційні системи та технології

Дніпро
НТУ «ДП»
2024

Комп’ютерні мережі [Електронний ресурс]: методичні рекомендації до виконання лабораторних робіт для здобувачів ступеня бакалавра спеціальності 126 Інформаційні системи та технології / уклад.: В.Ю. Каштан, Я.В. Панферова, В.С. Зарічний ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2024. – 86 с.

Укладачі:
В.Ю. Каштан, канд. техн. наук, доц.;
Я.В. Панферова, асист.;
В.С. Зарічний, асист.

Затверджено науково-методичною комісією спеціальності 126 Інформаційні системи та технології (протокол № 10 від 14.10.2024) за поданням кафедри інформаційних технологій та комп’ютерної інженерії (протокол № 4 від 30.09.2024).

Методичні рекомендації містять опис методики виконання лабораторних робіт з дисципліни «Комп’ютерні мережі» студентами спеціальності 126 Інформаційні системи та технології.

Орієнтовано на активізацію навчальної діяльності бакалаврів та закріплення практичних навичок з даної дисципліни.

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп’ютерної інженерії, д-р техн. наук, проф. В.В. Гнатушенко.

ЗМІСТ

ВСТУП

Методичні рекомендації призначені для студентів спеціальності 126 Інформаційні системи та технології, що вивчають дисципліну «Комп'ютерні мережі».

Методичні рекомендації включають низку частково взаємопов'язаних робіт, під час виконання яких студенти мають можливість отримати досвід роботи з мережним аналізатором Wireshark, командами операційної системи Windows, протоколами Ethernet, ARP, IP, TCP, UDP, HTTP, DHCP, DNS та FTP. Визначати типи IP-адрес та навчитися організовувати підмережі за допомогою маски змінної довжини. Налаштовувати маршрутизацію, налаштовувати захищений доступ до проміжних пристроїв та захищену Wi-Fi мережу.

Перед виконанням лабораторної роботи студенти повинні:

– ознайомитися з методичними рекомендаціями;

– повторити лекційний матеріал, пов'язаний з лабораторною роботою;

– підготовити відповіді на питання, які наведені у методичних рекомендаціях наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп'ютері або в зошиті, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

Загальні вимоги до виконання лабораторної роботи, що мають забезпечити максимальну оцінку:

– повна відповідність звіту про виконання лабораторної роботи методичним рекомендаціям;

– володіння теоретичним матеріалом про предмет досліджень;

– загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу;

– відповідність оформлення звіту чинним стандартам.

КРИТЕРІЇ ОЦІНЮВАННЯ ЛАБОРАТОРНИХ РОБІТ

Лабораторні роботи є важливою частиною навчального процесу, оскільки дають здобувачам можливість на практиці застосовувати теоретичні знання та набувати навичок у виконанні завдань, аналізі отриманих результатів і вирішенні практичних задач. Основною метою лабораторних робіт є формування у здобувачів навичок самостійного виконання завдань із використанням сучасних інструментів і методів, а також розвиток здатності аналізувати результати, робити висновки та обґрунтовувати свої дії.

Кожна лабораторна робота має свої мету, структуру виконання та вимоги до змісту звіту і питань для захисту роботи. Оцінювання виконання робіт спрямоване на перевірку рівня знань і практичних навичок студента, його вміння використовувати різноманітні методи, інструменти та підходи для вирішення поставлених завдань. При цьому оцінка формується з урахуванням якості оформлення звіту, правильності виконаних завдань і відповідей під час захисту роботи.

Система оцінювання розроблена для того, щоб забезпечити об’єктивність і чіткість у визначенні рівня знань студентів. Загальний результат за лабораторні роботи є складовою підсумкової оцінки за дисципліну, сприяючи підвищенню мотивації студентів до опанування практичних навичок та глибшого розуміння теоретичних основ.

Лабораторна робота	Критерії	Макс. бал	Роз’яснення
Лабораторна робота №1	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	3 бали	3 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: статичні дані захопленого мережного трафіку; скріншоти програми Wireshark в ході виконання роботи з описом дій; файл захоплених пакетів в Wireshark; фільтр відображення по варіанту згідно таблиці 1.1 2 бали – Завдання виконано правильно,

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за роботу №1	*Лабораторну*	*7 балів*	
Лабораторна робота №2	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	2 бали	– 2 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: лістинг командного рядку в ході виконання лабораторної роботи; розрахунок та графік залежності

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
Лабораторна робота №2			пропускної здатності мережі; 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №2		*6 балів*	
Лабораторна робота №3	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	4 бали	4 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: – скрін вікна Endpoints з MAC-адресами з визначенням їх типу; перелік IP-адрес призначення при фільтрації за широкомовним трафіком; перелік IP-адрес призначення при фільтрації багатоадресної розсилки; розрахунок та

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			графік затримки передачі файлу; розрахунок та графік залежності пропускної здатності мережі 3 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 2 бали – Є неточності в розрахунках та побудові графіку залежності пропускної здатності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №3	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №3		*8 балів*	
Лабораторна робота №4	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			оформлення.
Лабораторна робота №4	Виконане завдання	4 бали	4 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: скріншот топології мережі та таблиця адресація вузлів згідно варіанту; опис значущих виконуваних кроків (з вказівкою їх суті); проект мережі з назвою за правилом Surname_Group_lab04.pkt. – розрахунок та графік залежності пропускної здатності мережі 3 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 2 бал – Завдання виконано частково або з певними помилками. 1 бал – Проект налаштовано частково. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №4	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за роботу №4	*Лабораторну*	*8 балів*	

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
Лабораторна робота №5	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
Лабораторна робота №5	Виконане завдання	5 балів	5 балів – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: лістинг командного рядка в ході виконання першої частини роботи; структура заголовків ARP-запиту та відповідна йому ARP-відповідь, захоплених в Wireshark; дамп захоплених пакетів в Wireshark надати разом зі звітом; таблиця 4.1 зі значеннями MAC-адрес задіяних інтерфейсів всіх пристроїв в мережі, побудованій в Cisco Packet Tracer; вміст ARP-таблиці на PC0 після виконання другої частини роботи; вміст MAC-таблиці комутатора Switch0; вміст ARP-таблиці на маршрутизаторі R1. 4 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 3 бали – Завдання виконано правильно, але є неточності вмісту MAC-таблиці комутатора Switch0 або вміст ARP-таблиці на маршрутизаторі R1. 2 бали – Не наведено лістингу програми; структура заголовків ARP-запиту та відповідна йому ARP-відповідь має неточності.

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №5	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №5		*9 балів*	
Лабораторна робота №6	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	2 бали	2 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: відповіді на поставленні запитанні в ході виконання роботи. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності.

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №6	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за роботу №6	*Лабораторну*	*6 балів*	
Лабораторна робота №7	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	2 бали	2 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: заповненні відповідями таблиці 7.2-7.5 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист	3 бали	3 бали – Здобувач надав чітку,

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
	роботи		правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №7		*6 балів*	
Всього за 3 семестр		**50 балів**	
Лабораторна робота №8	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	2 бали	2 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: визначити найбільшу підмережу та маску для неї; потім визначити наступну за розмірами підмережу та маску для неї та присвоїти їй наступну комбінацію на звільнених бітах; продовжувати поділ підмереж відповідного розміру на підмережі до тих пір, поки не буде досягнута потрібна кількість вузлів у кожній підмережі 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №8		*6 балів*	
	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	4 бали	4 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: скріншот побудованої мережі в Packet Tracer; таблиці призначень IP-адрес (табл. 9.1 і 9.2); таблиця 9.3 з результатами перевірки досяжності мереж; застосовані команди з налаштувань та їх опис; проект мережі з назвою за правилом Surname_Group_lab09.pkt. 3 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
Лабораторна робота №9			оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 2 бали – Завдання виконано частково або з певними помилками. 1 бал – Проект налаштовано частково. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №9	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №9		*8 балів*	
Лабораторна робота №10	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	3 бали	3 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: – опис застосованих сервісів та їх параметри налаштувань; проект мережі в Packet Tracer з назвою за правилом

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			Surname_Group_lab10.pkt 2 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №10		*7 балів*	
Лабораторна робота №11	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	3 бали	3 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: проект мережі з назвою за правилом

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			Surname_Group_Meraki.pkt 2 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №11		*7 балів*	
Лабораторна робота №12	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	3 бали	3 бали – Завдання виконано повністю, відповіді точні, детальні й

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			правильні, усі вимоги до завдання дотримані: схему логічної топології мережі; команди налаштування маршрутів на кожному кроці з поясненнями; перевірки досяжності мереж у вигляді табл. 7.1 після виконання кроків 1-3; таблиці маршрутизації на кожному маршрутизаторі після кожного кроку виконання лабораторної роботи; – проект мережі з назвою за правилом Surname_Group_lab12.pkt 2 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №12		*7 балів*	
Лабораторна робота №13	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та висновки. Немає орфографічних або

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	4 бали	4 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: статистика роботи кожного типу NAT з відповідями на запитання; – звіт та проект мережі з назвою за правилом Surname_Group_NAT.pkt 3 бали – Завдання виконано правильно, але є незначні недоліки в деталізації або оформленні. Відповіді в основному правильні, але можуть містити дрібні неточності. 2 бали – Завдання виконано частково або з певними помилками. 1 бал – Проект налаштовано частково. Відповіді є, але вони неповні або мають суттєві неточності.
Лабораторна робота №13	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №13		*8 балів*	
Лабораторна робота №14	Оформлений звіт	1 бал	1 бал – Звіт повний, чіткий, структурований відповідно до вимог: містить мету, хід роботи, результати та

Лабораторна робота	Критерії	Макс. бал	Роз'яснення
			висновки. Немає орфографічних або структурних помилок. 0,5 балів – Звіт оформлений, але є незначні недоліки у структурі, деталізації або описі результатів. 0 балів – Звіт відсутній або не відповідає базовим вимогам щодо оформлення.
	Виконане завдання	3 бали	3 бали – Завдання виконано повністю, відповіді точні, детальні й правильні, усі вимоги до завдання дотримані: план впровадження безпеки портів і його реалізація; перевірка роботи функції безпеки портів з поясненнями; проект мережі з назвою за правилом Surname_Group_PortSec.pkt 2 бали – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 1 бал – Завдання виконано частково або з певними помилками. Відповіді є, але вони неповні або мають суттєві неточності. 0 балів – Завдання виконане неправильно або зовсім не виконане.
Лабораторна робота №14	Захист роботи	3 бали	3 бали – Здобувач надав чітку, правильну й повну відповідь на три питання щодо роботи, продемонструвавши глибоке розуміння матеріалу. 2 бали – Відповідь надана правильно, але є неповнота або незначні помилки в поясненні. 1 бал – Відповідь правильна, але містить суттєві неточності або неповну інформацію, що демонструє поверхневе розуміння матеріалу. 0 балів – Відповідь неправильна або взагалі відсутня.
Всього за Лабораторну роботу №14		*7 балів*	
Всього за 4 семестр		**50 балів**	

1 ЛАБОРАТОРНА РОБОТА №1
ВИВЧЕННЯ ІНТЕРФЕЙСУ ПРОГРАМИ WIRESHARK

1.1 Мета лабораторної роботи

Ознайомитись з програмою Wireshark для аналізу мережних протоколів. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички з написання фільтрів. Вивчити стек TCP/IP та взаємодію протоколів.

1.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

– робота з командним рядком операційної системи Windows 10;
– діагностичні команди та засоби Windows 10 для роботи в мережі;
– модель OSI та взаємодія протоколів;
– стек протоколів TCP/IP;
– функціональні можливості програми Wireshark;
– правила написання фільтрів для аналізаторів мережних протоколів.

Далі виконати такі дії:

– запустити програму Wireshark;
– відкрити вікно конфігурації захвату (рис. 1.1). Для цього потрібно перейти в меню *Capture->Options* або по комбінації клавіш CTRL+K;
– обрати інтерфейс, на якому буде виконуватися захоплення пакетів, та почати захоплення пакетів;

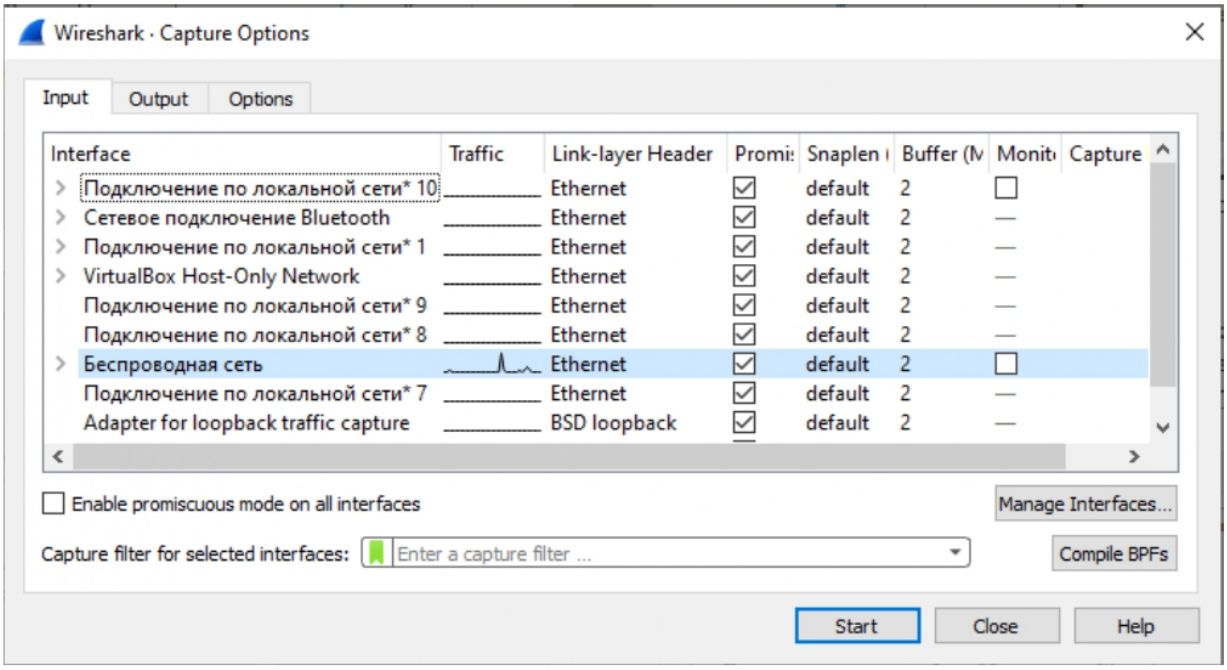

Рисунок 1.1 – Вікно опцій захвату

– відкрити командний рядок (*Пуск->Стандартні->Командний рядок* або на панелі пошуку в Windows ввести *cmd* (рис. 1.2);

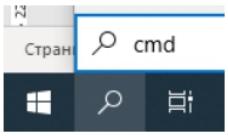

Рисунок 1.2 – Запуск командного рядка у вікні пошуку

– переглянути в командному рядку список доступних сусідніх вузлів;

```
C:\Users\Пользователь>net view
```

– відправити ехо-запити на IP-адреси сусідніх вузлів а за їх відсутності на адресу шлюза;

```
C:\Users\Пользователь>ping 192.168.1.1
```

Щоб дізнатися адресу шлюзу, в командному рядку ввести команду «ipconfig» і знайти параметр «Основной шлюз» мережевої карти, на якій ведеться передача даних (рис.1.3);

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::682c:b909:cc7d:deab%4
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.149
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.1.1
```

Рисунок 1.3 – Мережні налаштування мережного адаптера

– згенерувати додатковий трафік, відкривши в браузері будь-яку сторінку;

– зупинити захват пакетів в Wireshark (на панелі інструментів  або через меню *Capture->Stop* (Ctrl+E)) та використовуючи пункти меню *Statistics* визначити характеристики отриманого мережного трафіку, а саме:

1) які протоколи використовувались в мережі;
2) відсоткове співвідношення трафіку різних протоколів в мережі;
3) середню швидкість трафіку (кадрів/с, байт/с);
4) IPv4-адреси и порти TCP та UDP, між якими велася передача даних.

– відфільтувати поток з найбільшою затримкою в мережі;

– візуалізувати графік отриманих даних за допомогою пункту меню Statistics->Io Graphs;

– візуалізувати інформаційні потоки за допомогою пункту меню Statistics->Flow Graph;

– обрати будь-який з захоплених пакетів і перелічити його заголовки;

– визначити IP та MAC-адреси в трафіку через меню Statistics->Endpoints;

– налаштувати фільтр на відображення пакетів ARP та ICMP (рис. 1.4);

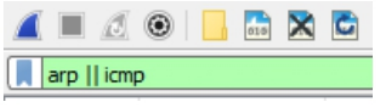

Рисунок 1.4 – Поле фільтру для захвату пакетів ARP та ICMP

– зберегти захоплені пакеті в файл *File->Save as…* та разом зі звітом надати викладачу;

– відкрити в Wireshark файл с захопленими пакетами під час підключення до маршрутизатора по telnet на ПК (надається викладачем). Визначити IP-адреси цих

пристроїв. Визначити пароль, який передавався під час встановлення сеансу до маршрутизатора. Для цього на будь-якому пакеті, в якому велася передача даних по telnet, натиснути правою кнопкою і вибрати *Follow ->TCP Stream* або на панелі меню *Analyze-> Follow ->TCP Stream* (рис.1.5);

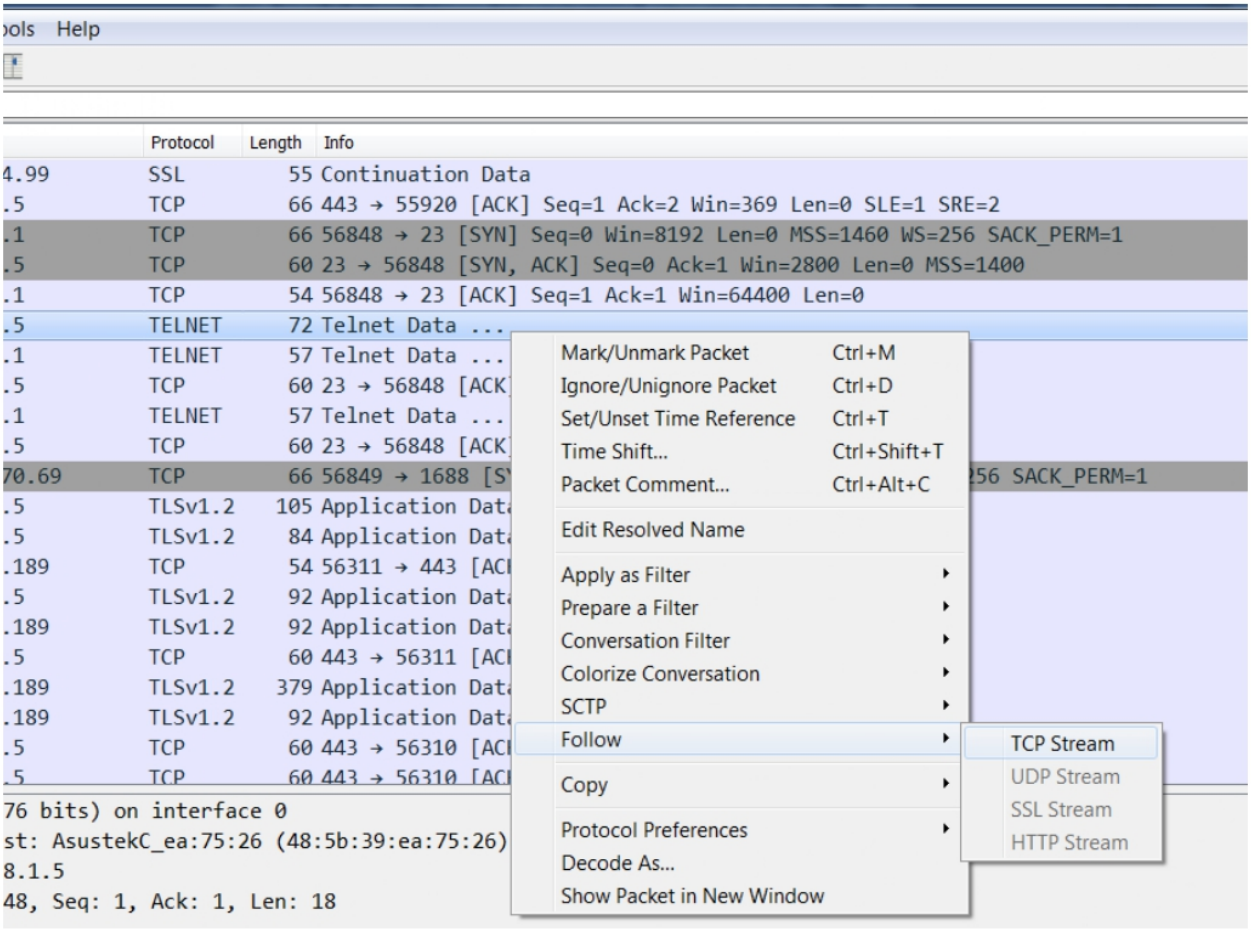

Рисунок 1.5 – Відстеження всього потоку TCP для обраного пакету

– привести приклад написання фільтру відображення по варіанту згідно таблиці 1.1.

Таблиця 1.1 – Варіанти фільтрів відображення

№	Фільтр відображення
1.	Тільки трафік від вузлів з MAC-адресами виробника TP-LINK, які починаються з f4:f2:6d.
2.	Тільки трафік icmp, виключаючи echo-запити (type=8) та echo-відповіді (type=0).
3.	IP-пакети від вузла 192.168.0.5 довжиною більше 1450 байт.
4.	Тільки трафік між машинами в локальній підмережі 192.168.30.0/24.
5.	IP-пакети з встановленим прапором фрагментації (mf) від вузла 10.0.0.5.
6.	TCP-пакети з встановленим прапором зняття з'єднання (res) на порт 23.

Продовження табл. 1.1

7.	TCP-пакети з вузла 192.168.10.5 з встановленим прапором встановлення з'єднання (syn).
8.	Весь вхідний трафік, виключаючи трафік SSH (TCP порт 22) генерований вузлом 192.168.5.101.
9.	Тільки трафік від вузла з MAC-адресом f4:f2:6d:54:a0:78, які включали в себе DNS-запити.
10.	Широкомовний трафік без ARP-запитів.
11.	Всі HTTP-запити типу GET на адрес 91.198.36.14 .
12.	IGMP-звіти приналежності (Membership Query Message) до групи 224.0.0.113.
13.	Тільки ARP-запити від вузла 192.168.0.10.
14.	Тільки DHCP-запити від вузла з MAC-адресом 6c:f0:49:70:ba:8b.
15.	Тільки DHCP-відповіді від вузла 192.168.0.1 MAC-адрес 6c:f0:49:70:ba:8b.
16.	Тільки пакети з широкомовними адресами 255.255.255.255 на порт призначення 68 протоколу UDP.
17.	IP-пакети між машинами в локальній підмережі 180.15.30.0/24 з довжиною пакету більше 1400 байт.
18.	FTP-пакети с запитами від клієнта 185.15.1.10.
19.	DNS-пакети від вузла 192.168.15.26
20.	Всі ARP-відповіді крім вузла 192168.0.10.
21.	Всі telnet-пакети з командою «End of File» від вузла 195.15.2.3.
22.	Всі DHCP-пакети від вузла 192.168.0.5.
23.	Тільки broadcast і multicast-пакети мережі 172.16.0.0/16.
24.	Тільки ARP-відповіді від вузла 192.168.0.10
25.	Тільки пакети http, які містили javascript в полі content_type.

1.2 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– статичні дані захопленого мережного трафіку;
– скріншоти програми Wireshark в ході виконання роботи з описом дій;
– файл захоплених пакетів в Wireshark;
– фільтр відображення по варіанту згідно таблиці 1.1.

1.3 Питання для підготовки до захисту лабораторної роботи

1. У якому випадку вузол може бачити всі пакети в сегменті Ethernet?
2. Який протокол канального рівня підтримує мережа учбового класу?
3. Які типи адрес необхідні для взаємодії вузлів в локальній мережі?
4. Дайте визначення терміну "інкапсуляція", використовуючи як приклад будь-який захоплений пакет.
5. До якого рівню моделі OSI відноситься протокол IP?

2 ЛАБОРАТОРНА РОБОТА №2
ОТРИМАННЯ ВІДОМОСТЕЙ ПРО MAC-АДРЕСИ І МЕРЕЖНІ НАЛАШТУВАННЯ TCP/IP

2.1 Мета лабораторної роботи

Вивчити команди командного рядка для отримання відомостей про MAC-адреси вузла і поточні мережні налаштування TCP/IP. Отримувати відомості про клієнтські сервіси DHCP і DNS і оновлювати їх. Вивчити інформацію, яка міститься в таблиці маршрутизації ПК.

2.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– мережні та діагностичні команди Windows (Додаток А);

– синтаксис діагностичних команд «getmac», «ipconfig», «nbtstat» та «route».

Далі виконати такі дії:

– запустити командний рядок;

– відобразити довідку по використанню команди «ipconfig»;

– вивести повну конфігурацію TCP/IP для всіх адаптерів;

– вивести на екран вміст кешу служби розпізнавання імен DNS;

– оновити мережні налаштування, отримані від DHCP-сервера тільки для адаптера локальної мережі;

– відобразити довідку по використанню команди «getmac»;

– отримати детальну інформацію про MAC-адреси всіх існуючих на локальному комп'ютері мережних адаптерів;

– відобразити довідку по використанню команди «route»;

– відобразити таблицю маршрутизації вузла та проаналізувати її записи;

– відобразити довідку по використанню команди «nbtstat»;

– відобразити таблицю NetBIOS-імен на локальному комп'ютері;

– відобразити розв'язання NetBIOS-імен та статистику реєстрації.

2.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– лістинг командного рядку в ході виконання лабораторної роботи.

2.4 Питання для підготовки до захисту лабораторної роботи

1. Як можна з'ясувати MAC-адресу комп'ютера?
2. Як можна з'ясувати IP-адресу комп'ютера?
3. Як можна з'ясувати MAC-адресу комп'ютера в локальній мережі?
4. Як оновити IP-адрес комп'ютера?
5. Як з'ясувати кеш служби розпізнавання імен DNS?

3 ЛАБОРАТОРНА РОБОТА №3
ДОСЛІДЖЕННЯ КАДРУ ПРОТОКОЛУ ETHERNET ТА ПРОПУСКНОЇ ЗДАТНОСТІ FAST ETHERNET

3.1 Мета лабораторної роботи

Вивчення формату кадру Ethernet, призначень його полів та адресування в локальних мережах. Дослідження залежності пропускної здатності мережі Fast Ethernet від розміру кадру.

3.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– функції протоколу Ethernet;

– адресація в Ethernet;

– структура заголовку кадру Ethernet;

– часові параметри Fast Ethernet;

– розрахунок пропускної здатності та часу передачі кадру в мережі Fast Ethernet (Додаток Б).

Виконання лабораторної роботи складається з двох частин. В першій частині необхідно дослідити заголовок кадру Ethernet, перехоплюючи і досліджуючи мережний трафік в Wireshark. В другій частині необхідно дослідити залежність часу передачі файлу завданим розміром та пропускної здатності мережі Fast Ethernet від розміру кадру Ethernet.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Вивчення формату кадру Ethernet, призначень його полів та адресування в локальних мережах

Далі виконати такі дії:

– запустити на ПК командний рядок;

– визначити MAC-адрес мережної плати комп'ютера;

```
>ipconfig /all
```

– відкрити програму Wireshark і запустити захват пакетів тривалістю в кілька хвилин;

– в командному рядку виконати «ping» на сусідні вузли та шлюз;

– для збільшення інтенсивності генерації кадрів відкрити будь-який сайт в браузері;

– зупинити захват пакетів та отримати відомості про MAC-адреси в заголовках кадрів Ethernet, які були захоплені Wireshark, на відповідній вкладці вікна *Endpoints* (рис.3.1) через меню *Statistics->Endpoints*;

– проаналізувати та законспектувати зі вкладки Ethernet (рис. 3.1), які типи MAC-адрес були захоплені Wireshark;

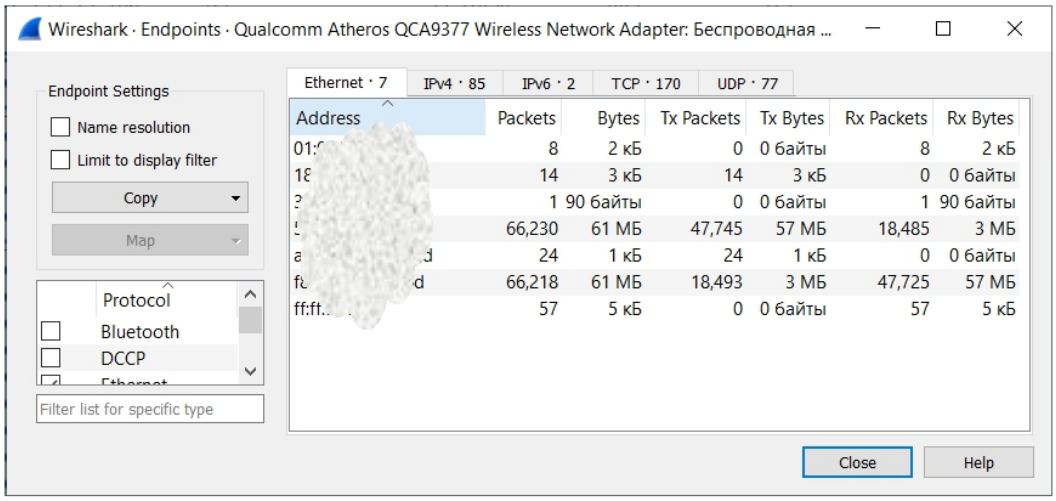

Рисунок 3.1 – Вікно Endpoints

– відфільтрувати MAC-адреси широкомовної розсилки, крім ARP (eth.addr==ff:ff:ff:ff:ff:ff && !arp), проаналізувати та законспектувати всі IP-адреси призначення (рис.3.2);

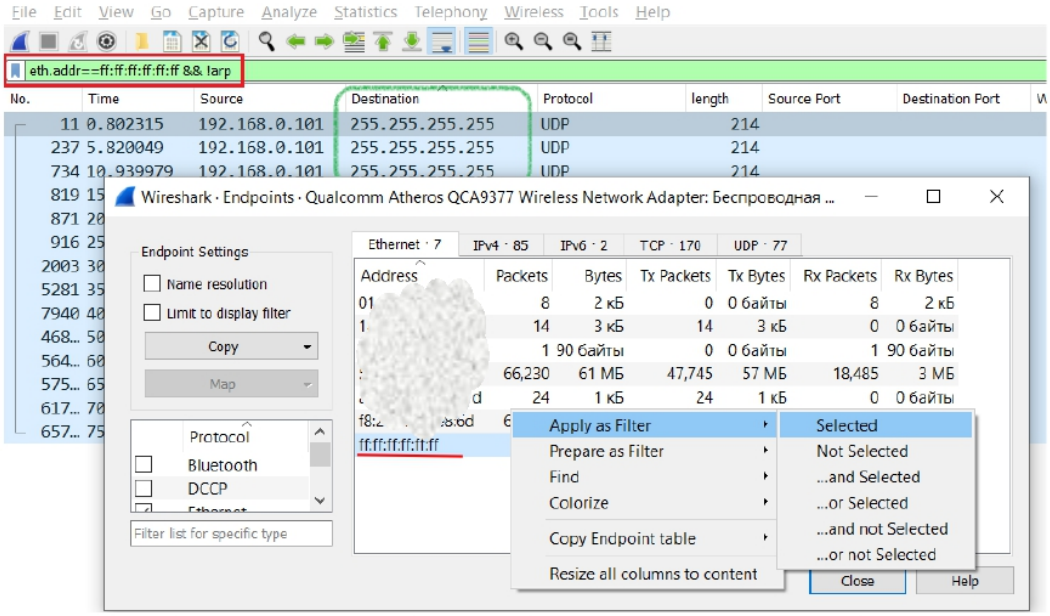

Рисунок 3.2 – Фільтрація широкомовних кадрів

– у вікні захоплених пакетів вибрати будь-який широкомовний пакет і розглянути значення основних полів його заголовку Ethernet II (рис. 3.3). Визначити адреси, на які надходять дані кадри і пакети, для канального (MAC-адреси) і мережного (IP-адреси) рівня та представити у вигляді таблиці 3.1.

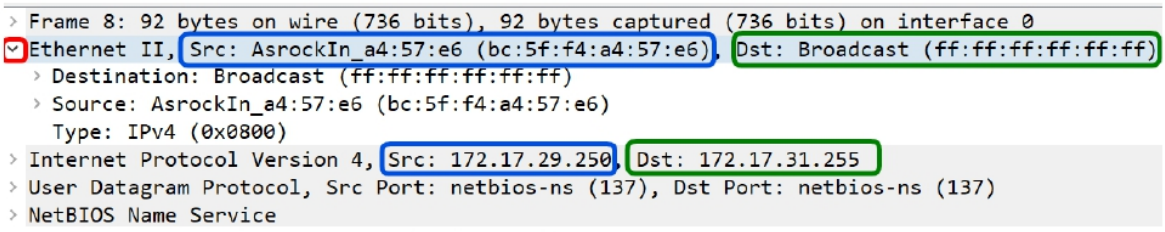

Рисунок 3.3 – Ієрархічна структура заголовків

Таблиця 3.1 – Канальні та мережні адреси в пакеті

MAC Source	
IP Source	
MAC Destination	
IP Destination	

– відфільтрувати MAC-адреси багатоадресної розсилки, якщо вони були захоплені Wireshark. Вибрати будь-який пакет і розглянути значення основних полів його заголовку Ethernet II. Визначити адреси, на які надходять дані кадри і пакети, для канального і мережного рівня у вигляді табл. 3.1.

ЧАСТИНА 2. Дослідження залежності часу передачі файлу та пропускної здатності мережі Fast Ethernet від розміру кадру Ethernet

В цій частині вам необхідно дослідити, як довжина кадру Ethernet впливає на час передачі файлу та на пропускну здатність мережі Fast Ethernet. Використовуючи відомості в Додатку Б необхідно виконати розрахунки для різного значення довжини поля корисних даних кадру Ethernet та побудувати графіки залежності.

Далі виконати такі дії:

– використовуючи відомості в Додатку Б побудувати графік затримки передачі файлу розміром *10*№* Мбайт (№ - номер за списком в групі) в одному сегменті мережі Fast Ethernet, якщо довжина поля корисних даних кадру N_d буде мати наступні значення: 128, 512, 1000, 1500 та 4096 байт;

– побудувати графік залежності пропускної здатності мережі Fast Ethernet від довжини поля корисних даних кадру N_d, якщо N_d буде мати наступні значення: 128, 512, 1000, 1500 та 4096 байт.

Примітка. Зверніть увагу, що в Додатку Б наведено розрахунок часу передачі для одного кадру довжиною 46 та 1500 байт поля даних, а не всього файлу.

3.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– скрін вікна Endpoints з MAC-адресами з визначенням їх типу;
– перелік IP-адрес призначення при фільтрації за широкомовним трафіком;
– перелік IP-адрес призначення при фільтрації багатоадресної розсилки;
– розрахунок та графік затримки передачі файлу;
– розрахунок та графік залежності пропускної здатності мережі.

3.4 Питання для підготовки до захисту лабораторної роботи

1. Чому дорівнюють максимальний та мінімальний розміри кадру Ethernet?
2. Яка частина в MAC-адресі відображає виробника мережної карти?
3. Які типи кадрів Ethernet бувають, в чому їх відмінності?
4. Яка довжина заголовку Fast Ethernet?
5. Як записується широкомовний MAC-адрес Ethernet?

4 ЛАБОРАТОРНА РОБОТА №4
МЕРЕЖНІ ПРИСТРОЇ І ЗАСОБИ КОМУНІКАЦІЙ. СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ CISCO PACKET TRACER

4.1 Мета лабораторної роботи

Ознайомитися з основними мережними пристроями та засобами передачі даних комп'ютерних мереж з використанням середовища моделювання Cisco Packet Tracer, навчитися додавати у симуляторі нові пристрої, створювати з'єднання, налаштовувати вузли та перевіряти підключення.

4.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– кінцеві та проміжні пристрої;
– середовище передачі даних;
– топології мереж;
– інтерфейс програми Cisco Packet Tracer.

У цій лабораторній роботі, застосовуючи різні пристрої, ви побудуєте в Packet Tracer модель домашньої мережі (рис.4.1), безпечний бездротовий зв'язок, доступ до Internet та налаштуєте пристрої відповідно до таблиці адресації (табл. 4.1). Перевірите створену конфігурацію, протестувавши наскрізне з'єднання шляхом звернення до веб-сервера і маршрутизатора провайдера.

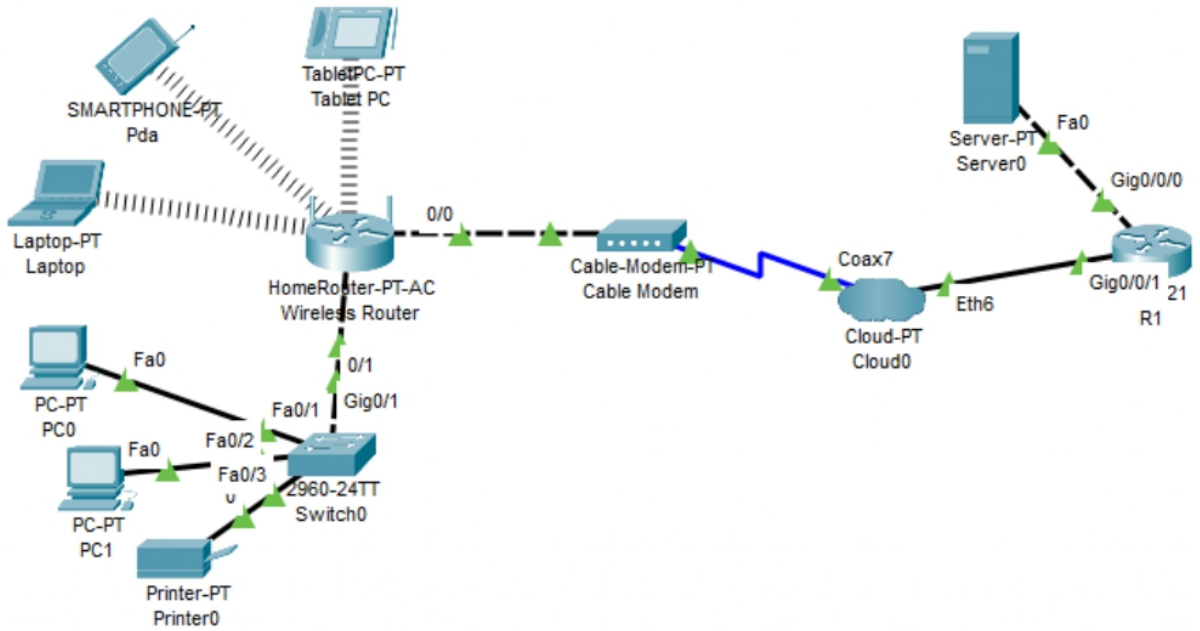

Рисунок 4.1 – Модель мережі

Таблиця 4.1 – Адресація пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	DNS
Wireless Router	LAN	№*10.№.0.1	255.255.255.0	N/A	209.165.201.30
	Internet	209.165.200.226	255.255.255.224	209.165.200.225	
R1	G0/0/1	209.165.200.225	255.255.255.224	N/A	
	G0/0/0	209.165.201.1	255.255.255.224	N/A	
Server0	fe0	209.165.201.30	255.255.255.224	209.165.201.1	
Laptop, Pda, Tablet PC	Wireless0	DHCP		№*10.№.0.1	
PC0	fe0	№*10.№.0.3	255.255.255.0	№*10.№.0.1	
PC1	fe0	№*10.№.0.4	255.255.255.0	№*10.№.0.1	
Printer0	fe0	№*10.№.0.10	255.255.255.0	№*10.№.0.1	

де № – номер студента за списком в групі.

Далі виконати такі кроки.

Крок 1. Вибір пристроїв і побудова мережі

1. Запустити програму Packet Tracer.

2. Додати в робочу область пристрої та з'єднати їх між собою, як показано на рис. 4.1. Наприклад, щоб побудувати нижній сегмент мережі, що складається з комутатора, двох ПК та принтера, для цього необхідно додати в робочу область один комутатор серії 2960-24TT з групи елементів Switches панелі вибору типових пристроїв і зв'язків (рис.4.2), два комп'ютери PC-PT та принтер Printer-PT з групи *End Devise*.

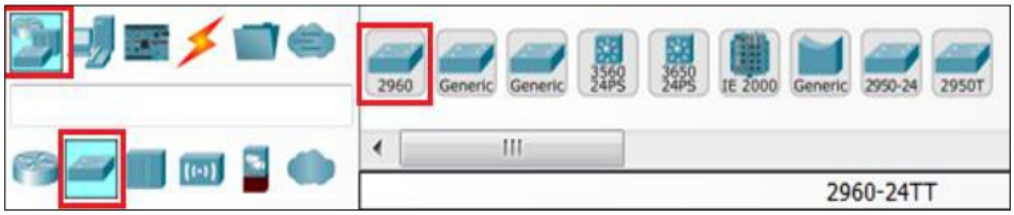

Рисунок 4.2 – Панель вибору типових пристроїв і зв'язків

3. Клацніть значок *Connections* (у вигляді блискавки) на панелі вибору пристроїв і зв'язків та виберіть прямий кабель (*Copper Straight-Through*), клацнувши по ньому (рис.3.3). Курсор прийме вид роз'єму з кінцем кабелю, що звисає.

Рисунок 4.3 – Панель вибору з'єднань

4. Клацніть PC0. У вікні виберіть варіант для підключення FastEthernet0. Перетягніть інший кінець підключення до комутатора Switch0 і клацніть на ньому, щоб відкрити список підключень. Виберіть *FastEthernet0/1*, щоб завершити підключення.

5. Аналогічно зробіть підключення другого PC та Printer-PT до комутатора, підключивши до порту *FastEthernet0/2* та *FastEthernet0/3* комутатора Switch0 відповідно.

Примітка. Якщо ви хочете помістити кілька пристроїв одного і того ж типу на робочий простір, натискання і перетягування може стати дуже виснажливим. Щоб уникнути цього, ви можете утримувати клавішу CTRL при натисканні на пристрій в панелі вибору пристроїв.

Крок 2. Налаштування Wireless Router та базових функцій безпеки бездротової мережі

Примітка. В методичних рекомендаціях далі всі приклади будуть наведені для 25-го варіанту.

1. Відкрийте властивості пристрою Wireless Router, натиснувши на його зображення, та перейдіть на вкладку GUI.

2. Налаштуйте параметри інтерфейсу, підключеного до Інтернету. Для параметра *Internet Connection Type* виберіть значення *Static IP* в списку. Потім введіть дані, згідно табл. 4.1 (рис. 4.4).

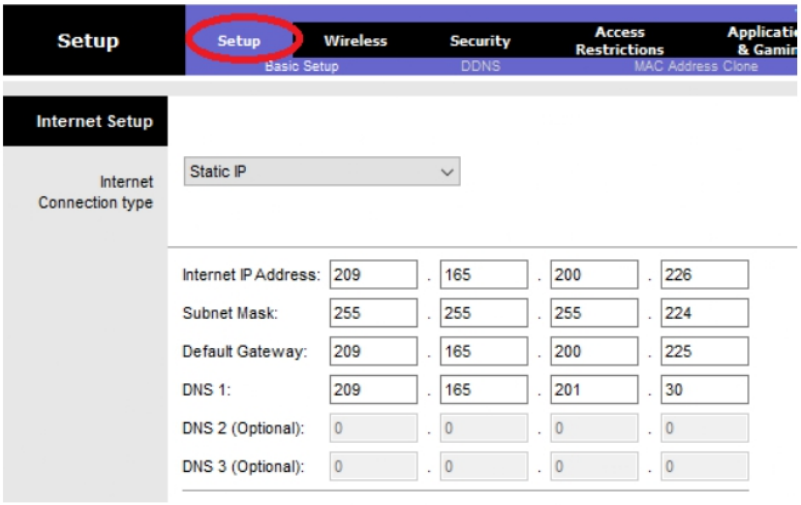

Рисунок 4.4 – IP-налаштування інтерфейсу, підключеного до Інтернету

3. Налаштуйте параметри внутрішньої мережі. Прокрутіть сторінку вниз до розділу *Network Setup* і налаштуйте наступні параметри:

– IP-адреса: №*10.№.0.1, де № – номер студента за списком в групі. Наприклад, для варіанту 25 (№=25) маємо IP-адресу 250.25.0.1;

– маска підмережі: 255.255.255.0;

– початкова IP-адреса: для останнього октету введіть значення 11;

– максимальна кількість користувачів: 25.

Примітка. Зміни в діапазоні IP-адрес пулу DHCP будуть показані тільки після того, як ви натиснете кнопку *Save Settings*.

4. Налаштуйте бездротову мережу для бездротових пристроїв. Відкрийте параметри *Basic Wireless Settings* на вкладці *Wireless*. Встановіть режим мережі *Auto*. Змініть SSID на *MyHome* (рис. 4.5).

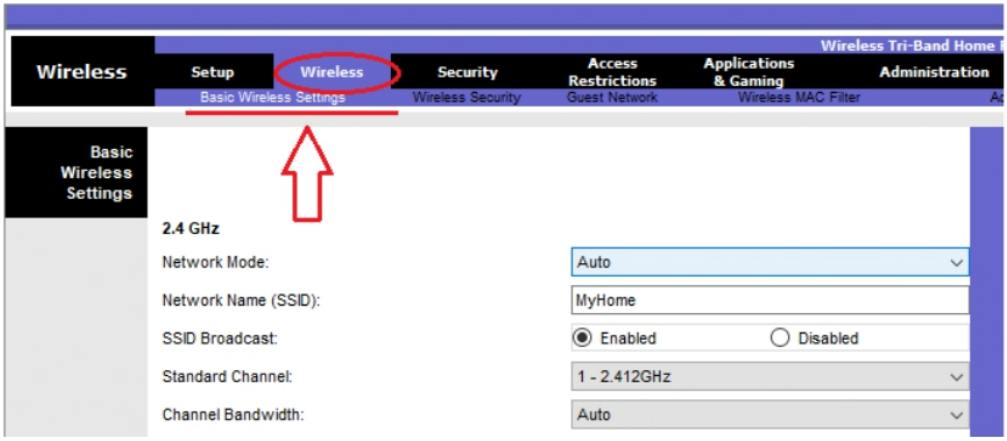

Рисунок 4.5 – Налаштування бездротової мережі для бездротових пристроїв

5. Налаштуйте базові функції безпеки бездротової мережі в параметрах *Wireless Security* на вкладці *Wireless*. В даний момент режим безпеки вимкнений. Змініть режим безпеки на *WPA2 Personal*. В полі *Passphrase* введіть 123Cisco (рис.4.6).

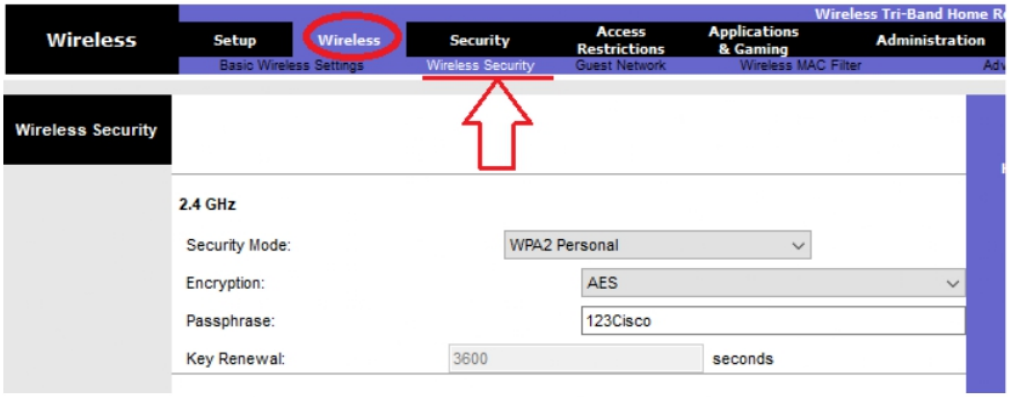

Рисунок 4.6 – Налаштування функції безпеки бездротової мережі

6. Опустіться до низу сторінки і клацніть Save Settings.

Крок 3. Налаштування Cloud0

1. Клацніть на Cloud0 та виберіть на вкладці *Config* інтерфейс *Ethernet6*. Оберіть тип *Cable* для *Provider Network*.

2. На вкладці *Config* в розділі *Connections* для *Cable* додайте з'єднання *Coaxial7-Ethernet6*. (рис. 4.7).

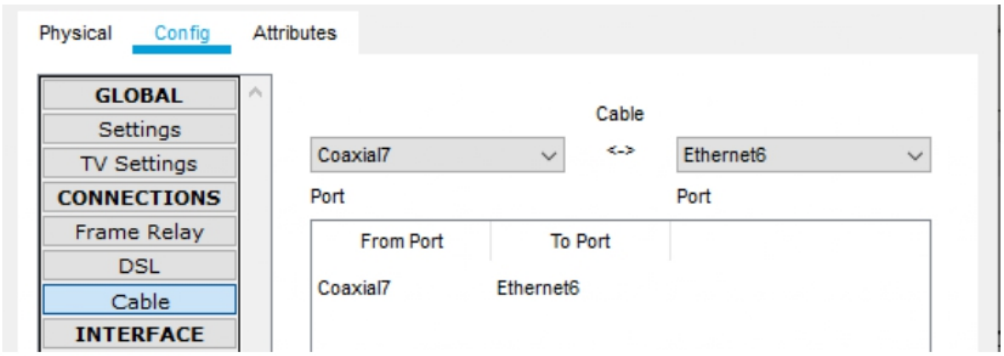

Рисунок 4.7 – Налаштування з'єднання для Cloud

Крок 4. Налаштування маршрутизатора R1

1. Клацніть R1 та оберіть вкладку *Config*.
2. Налаштуйте IP-адреси інтерфейсів відповідно до таблиці43.1.
3. Включіть інтерфейси, поставивши галочку навпроти *Port Status* (рис. 4.8).

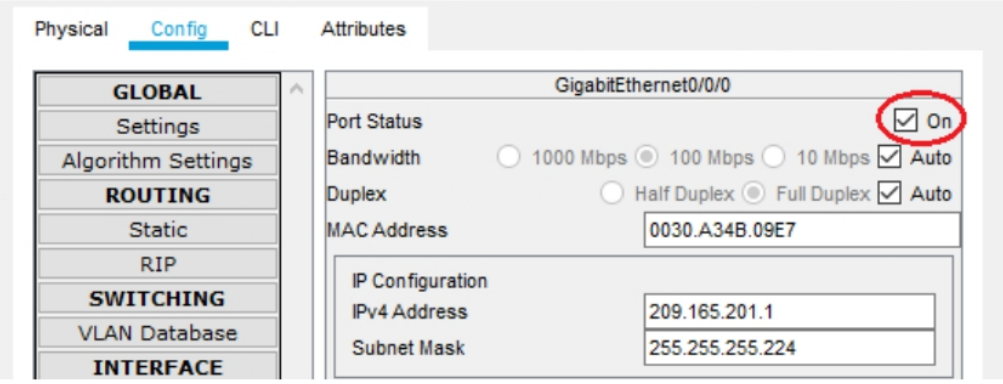

Рисунок 4.8 – Налаштування інтерфейсів на R1

Крок 5. Налаштування бездротових клієнтів для доступу до бездротової мережі

1. Для Laptop необхідно замінити дротову мережну карту на бездротову. Для цього на вкладці *Physical* знайдіть кнопку на пристрої та вимкніть його. Клацніть на мережній карті на ноутбуці та перемістіть її в зону модулів зліва. Оберіть модуль *WPC300N* та перемістіть в звільнений слот на ноутбуці. Включіть ноутбук.
2. Клацніть Laptop і виберіть *Desktop>PC Wireless*. Відкриється вікно графічного користувальницького інтерфейсу Linksys для клієнта.
3. Відкрийте вкладку *Connect* і натисніть кнопку *Refresh*, якщо необхідно. Ви повинні побачити *MyHome* в полі *Wireless Network Name*.
4. Клацніть *MyHome* і виберіть команду *Connect*.
5. *Pre-shared Key* – пароль, налаштований на кроці 2, пункті 5. Введіть пароль і натисніть кнопку *Connect*.
6. Закрийте інтерфейс користувача і клацніть *Command Prompt*. Виконайте команду «ipconfig», щоб переконатися, що Laptop отримав IP-адресу.
7. Для налаштування смартфона та планшета оберіть вкладку *Config* та інтерфейсі *Wireless0* зробіть налаштування відповідно до налаштувань бездротової мережі.

Крок 6. Налаштування PC0, PC1 та принтера

1. Клацніть PC0. У вікні управління відкрийте вкладку *Desktop*.
2. Оберіть додаток *IP Configuration* і введіть дані з таблиці 4.1 для PC0.
3. Повторіть налаштування IP-адреси для PC1 та принтера.

Крок 7. Налаштування Server0

1. Налаштуйте IP-адресу сервера відповідно до таблиці 4.1.
2. Відкрийте вкладку *Services* і виберіть розділ *HTTP*.
3. Виберіть варіант *On*, щоб включити HTTP і HTTP Secure (HTTPS).
4. Необов'язковий крок. Змінити HTML-код.

5. Відкрийте вкладку *Services* і виберіть розділ *DNS*.
6. Виберіть варіант *On*, щоб включити сервіс DNS.
7. Додати запис у відповідних полях:
   а) Name: labkm.com;
   б) Address: 209.165.201.30 (IP-адреса Server0).
8. Натиснути кнопку *Add* щоб додати запис.

Крок 8. Перевірка підключення до мережі

Підключення до мережі можна перевірити за допомогою команди «ping». Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вживати відповідні заходи щодо усунення неполадок.

1. Клацніть PC0. На вкладці *Desktop* виберіть додаток *Command Prompt*.
2. Надішліть echo-запит на IP-адресу комп'ютера PC1, наприклад:
   `C:\> ping 250.25.0.4`
3. Надішліть echo-запит на IP-адресу Wireless Router, наприклад:
   `C:\> ping 250.25.0.1`
4. З командного рядка надішліть echo-запит на IP-адресу Server0.
   `C:\> ping 209.165.201.30`

Крок 9. Перевірка працездатності веб-серверу

1. На будь-якому вузлі відкрити вкладку *Desktop* та додаток *Web Browser*.
2. В полі URL ввести IP-адресу Server0 і натиснути кнопку *Go*. Відкриється веб-сайт Server0.

Крок 10. Перевірка сервісу DNS

1. На будь-якому вузлі відкрити вкладку *Desktop* та вибрати додаток *Command Prompt.*
2. Виконати команду «ping» на IP-адресу Server0, щоб перевірити з'єднання.
3. Виконати команду «nslookup labkm.com», щоб перевірити роботу DNS. Повинні отримати IP-адресу для імені labkm.com.
4. Закрити додаток *Command Prompt* та відкрити *Web Browser*.
5. В полі URL ввести labkm.com і натиснути кнопку *Go*. Відкриється веб-сайт Server0.

4.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис завдання з початковими умовами та даними;

– скріншот топології мережі та таблиця адресація вузлів згідно варіанту;

– опис значущих виконуваних кроків (з вказівкою їх суті);

– проект мережі з назвою за правилом Surname_Group_lab04.pkt (наприклад, Ivanov_126-24-1_lab04.pkt) разом зі звітом надати на перевірку в системі Moodle або на корпоративну поштову скриню викладача.

4.4 Питання для підготовки до захисту лабораторної роботи

1. Які типи мережевого середовища ви знаєте?
2. Які є типи витої пари?
3. Як перевірити зв'язок між пристроями?
4. Які типи мережевих з'єднань в Packet Tracer ви знаєте?
5. Яка різниця між комутатором та маршрутизатором, та коли їх слід застосовувати?

5 ЛАБОРАТОРНА РОБОТА №5
ВИВЧЕННЯ ПРОТОКОЛУ ARP

5.1 Мета лабораторної роботи

Вивчити роботу протоколу ARP, отримати практичні навички по роботі з командою ARP в командному рядку Windows.

5.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– функції та робота протоколу ARP;
– синтаксис команди «arp»;
– структура заголовку протоколу ARP.

Виконання лабораторної роботи складається з двох частин. В першій частині необхідно дослідити роботу протоколу ARP в локальній мережі. В другій частині виконується вивчення роботи протоколу ARP в побудованій мережі в Packet Tracer з лабораторної роботи №4.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Вивчення роботи протоколу ARP в локальній мережі

Роботу слід проводити парами з використанням двох комп'ютерів, підключених до одного сегмента локальної мережі та IP-адресами, які належать одній IP-мережі. ПК повинні мати вихід в Інтернет. В разі неможливості наявності в мережі другого ПК, можна використовувати IP-адреси інших пристроїв, наприклад ТВ, ноутбука, принтера або шлюза (роутера).

Далі виконати такі дії:

– відкрити вікно командного рядка на ПК і відобразити довідкову інформацію по команді «arp»;

```
>arp /?
```

– відобразити ARP-таблицю;

```
>arp -a
```

– запустити програму Wireshark та почати захоплення пакетів;

– в командному рядку очистити ARP-таблицю;

– відобразити ARP-таблицю та переконатися в тому, що вона очищена або має менше записів;

– надіслати echo-запит за допомогою команди «ping» зі свого ПК на інший ПК в мережі (або інший пристрій, наприклад шлюз) для динамічного додавання запису в ARP-таблицю;

– після відправки echo-запиту зупинити захоплення пакетів в Wireshark;

– налаштувати в Wireshark фільтр на відображення тільки пакетів ARP та ICMP;

– на підставі отриманих даних визначити і задокументувати в звіт заголовок ARP-запиту і ARP-відповіді та звернути увагу на інкапсуляцію ARP-повідомлень;

– відобразити ARP-таблицю та визначити MAC-адрес сусіднього ПК (або шлюзу), перевірити це значення на сусідньому ПК;

– зберегти в файл дамп захоплених пакетів в Wireshark для відправлення зі звітом викладачу;

– почати нове захоплення даних програмою Wireshark;

– надіслати echo-запит за допомогою команди «ping» на кілька IP-адрес в Інтернет;

– визначити, на який MAC-адрес призначення відправлялись echo-запити та якому пристрою він належить.

ЧАСТИНА 2. Вивчення роботи протоколу ARP в Packet Tracer

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №4. Перед початком виконання перевірте працездатність мережі, виконавши «ping» з PC до Server0. Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вжити відповідні заходи щодо усунення неполадок.

Примітка. Якщо команда «ping» видає повідомлення «Reply from x.y.z.w: Destination host unreachable», збережіть налаштування на Wireless Router, натиснувши кнопку *Save Settings* на вкладці GUI.

Далі виконати такі дії:

– визначити MAC-адреси інтерфейсів маршрутизаторів Wireless Router та R1 та заповнити отриманими відомостями табл. 5.1. Для цього на Wireless Router необхідно зайти в GUI на вкладці *Status* на відповідній мережі, а на R1 на вкладці CLI ввести команду show interface *interface,* наприклад

```
> show interfaces g0/0/0
```

або іструментом лупа «  » обрати опцію *Port Status Summary Table*;

– визначити MAC-адреси всіх PC та бездротових пристроїв та заповнити таблицю 5.1 ;

– перейдіть з режиму реального часу *Realtime* до режиму моделювання *Simulation* в правому нижньому кутку програми;

Таблиця 5.1 – IP та MAC-адреси пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	MAC-адреса
Wireless Router	LAN	№*10.№.0.1	
	Internet	209.165.200.226	
R1	G0/0/1	209.165.200.225	
	G0/0/0	209.165.201.1	
Server0	fe0	209.165.201.30	
Laptop	Wireless0	DHCP	
Pda	Wireless0	DHCP	
Tablet PC	Wireless0	DHCP	
PC0	fe0	№*10.№.0.3	
PC1	fe0	№*10.№.0.4	
Printer0	fe0	№*10.№.0.10	

Примітка. У нижньому правому куті інтерфейсу Packet Tracer розміщені кнопки перемикання між режимами *Realtime* і *Simulation*. Packet Tracer завжди запускається у режимі *Realtime*, у якому мережні протоколи оперують у реальних часових проміжках. Проте, можливості Packet Tracer дозволяють користувачеві "зупинити час" за допомогою перемикання до режиму моделювання *Simulation*. У цьому режимі пакети відображаються у вигляді конвертів, час керується подіями, а користувач може покроково проходити по мережних подіях.

– налаштуйте *Event List Filters* лише на відображення повідомлень протоколів ARP та ICMP (рис. 5.1);

Рисунок 5.1 – Налаштування Event List Filters

– на PC0 на вкладці *Decstop* відкрити додаток *Command Promt* та відправити echo-запити на PC1. Дослідити роботу протоколу ARP, використовуючи інструменти режиму симуляції (рис.5.2);

Рисунок 5.2 – Інструменти симуляції

– для заповнення відомостями ARP-таблиці з командного рядка PC0 відправити echo-запити на принтер та всі бездротові пристрої;

– відобразити ARP-таблицю на PC0 та проаналізувати її;

– з командного рядка PC0 відправити echo-запит на Server0 та визначити, на який MAC-адрес призначення відправлялись echo-запити та якому пристрою в мережі він належить;

– відобразити MAC-таблицю на комутаторі Switch0 та проаналізувати її;

```
>show mac address-table
```

або іструментом лупа «  » ->MAC Table

– відобразити ARP-таблицю на маршрутизаторі R1 та проаналізувати її;

```
>show arp
```

або іструментом лупа «  » ->ARP Table

Примітка. Інструменту для відображення ARP-таблиці на Wireless Router не розроблено.

5.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– лістинг командного рядка в ході виконання першої частини роботи;

– структура заголовків ARP-запиту та відповідна йому ARP-відповідь, захоплених в Wireshark;

– дамп захоплених пакетів в Wireshark надати разом зі звітом;

– таблиця 4.1 зі значеннями MAC-адрес задіяних інтерфейсів всіх пристроїв в мережі, побудованій в Cisco Packet Tracer;

– вміст ARP-таблиці на PC0 після виконання другої частини роботи;

– вміст MAC-таблиці комутатора Switch0;

– вміст ARP-таблиці на маршрутизаторі R1.

5.4 Питання для підготовки до захисту лабораторної роботи

1. Як і коли видаляються статичні записи в ARP-таблиці?
2. Навіщо додавати статичні записи ARP-таблицю?
3. При виконанні команди «ping» на IP-адреси в Інтернет, який IP-адрес призначення був в ARP-запиті і чому?
4. При виконанні команди «ping» на IP-адреси в Інтернет, на який MAC-адрес призначення відправлялись echo-запити і чому?
5. Коли в мережі виникають широкомовні ARP-запити?

6 ЛАБОРАТОРНА РОБОТА №6
ДОСЛІДЖЕННЯ МОДЕЛЕЙ TCP/IP І OSI

6.1 Мета лабораторної роботи

Сформувати засади для розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI.

6.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– мережні протоколи та їх взаємодія;

– функції рівнів моделі OSI;

– порівняння моделей TCP/IP та OSI.

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №4 «Мережні пристрої і засоби комунікацій».

В лабораторній роботі буде досліджено процес запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК. Не зважаючи на те, що більшість поданої інформації детально розглядатиметься пізніше, це завдання дає можливість вивчити функціональність Packet Tracer і відтворити процес інкапсуляції.

Далі виконати такі кроки.

Крок 1. Перевірка працездатності мережі

Перед початком виконання перевірте працездатність мережі, виконавши «ping» з PC0 до Server0. Якщо команда «ping» видає повідомлення «Reply from x.y.z.w: Destination host unreachable», збережіть налаштування на Wireless Router, натиснувши кнопку *Save Settings* на вкладці GUI.

Крок 2. Перехід з режиму реального часу (Realtime) до режиму моделювання (Simulation mode)

1. Перейдіть з режиму реального часу *Realtime* до режиму моделювання *Simulation* в правому нижньому кутку програми.

2. Налаштуйте *Event List Filters* лише на відображення повідомлень HTTP.

Крок 3. Створення HTTP-трафіку

На початку моделювання панель *Simulation Panel* порожня. Вгорі на панелі у списку подій вказані п'ять стовпців. У міру того, як трафік генерується і поступово просувається, у списку з'являтимуться події.

1. Натисніть на PC0, потім вкладку *Desktop* і відкрийте веб-браузер, обравши додаток *Web Browser*.

2. У полі URL введіть labkm.com і натисніть *Go*.

3. Оскільки час у режимі моделювання залежить від подій, потрібно використовувати кнопку *Capture/Forward* для відображення подій у мережі. Натискайте кнопку *Capture/Forward,* поки відповідь з сервера не надійде до PC0. Погляньте на сторінку веб-браузера на PC0. Чи відбулися якісь зміни?

Крок 4. Дослідження вмісту протокольного блоку даних HTTP

1. Натисніть на першому кольоровому квадратному полі у списку подій: *Event List* > колонка *Type*. Можливо знадобиться розгорнути *Simulation Panel* або використати смугу прокрутки безпосередньо під *Event List*.

Відобразиться вікно *PDU Information at Device: PC0*. Оскільки це початок передавання, у вікні є лише дві вкладки: *OSI Model* і *Outbound PDU Details*. При появі більшої кількості подій, з'явиться ще третя вкладка *Inbound PDU Details*.

2. Переконайтесь, що обрано вкладку *OSI Model*. Під колонкою *Out Layers* натисніть на *Layer 7*.

Яка інформація наведена за допомогою пронумерованих записів нижче полів *In Layers* та *Out Layers* для *Layer* 7 в першому і останньому подіях?

Яке значення для *Dst Port* для *Layer* 4 міститься у колонці *Out Layers*

Яке значення має *Dest IP* для *Layer 3* у колонці *Out Layers*?

Яка інформація показана на *Layer 2* у колонці *Out Layers*?

3. Натисніть на вкладці *Outbound PDU Details*. Інформація, наведена під *PDU Formats* відповідає рівням моделі TCP/IP.

Яка інформація традиційно міститься у розділі *IP PDU Details*, у порівнянні з інформацією з вкладки *OSI Model*? З яким рівнем вона пов'язана?

Яка інформація традиційно міститься у розділі *TCP PDU Details*, порівняно з інформацією на вкладці *OSI Model*, і з яким рівнем вона пов'язана?

Який *Host* вказаний у розділі *HTTP* деталей PDU?

З яким рівнем пов'язана ця інформація у вкладці *OSI Model*?

4. Натисніть на наступному кольоровому квадраті у *Event List*. Активний лише рівень 1 (незабарвлений). Пристрій переміщує кадрі з буфера до мережі.

5. Перейдіть до 8-ої події HTTP у *Event List*, коли пакет досягає Server0 від R1, і натисніть на кольоровому квадраті. Це вікно містить як вхідні рівні *In Layers* так і вихідні рівні *Out Layers*. Зверніть увагу на напрямок стрілки безпосередньо у колонці *In Layers*, вона вказує вгору, у напрямку передавання даних. Перейдіть по цих рівнях, зважаючи на попередньо розглянуті елементи. Зверху колонки стрілка вказує праворуч. Це означає, що зараз сервер надсилає інформацію назад до клієнта.

Які основні відмінності можна побачити при порівнянні даних, зображених у колонці *In Layers* з даними колонки *Out Layers*?

6. Перейдіть до вкладки *Inbound* та *Outbound PDU Details*. Перегляньте деталі PDU.

7. Натисніть на останній події HTTP у *Event List*. Скільки вкладок відображається для цієї події? Чому?

Крок 5. Перегляд додаткових подій

1. Закрийте усі відкриті вікна з інформацією про PDU.

2. У розділі *Event List Filters > Visible Events*, натисніть на *Show All/None,* щоб відобразити події всіх протоколів.

Які додаткові типи подій *Event Types* відображаються?

Примітка: Ці додаткові записи відіграють різні ролі протоколів у TCP/IP. Протокол ARP надсилає запити про MAC-адреси для вузлів отримувачів. DNS відповідає за визначення IP-адреси для відповідних доменних імен. Додаткові події TCP відповідають за встановлення з'єднання, узгодження параметрів передачі даних і закриття з'єднання (сеансів зв'язку) між пристроями.

3. Натисніть на першій події DNS у вікні *Event List*. Розгляньте вкладки *OSI Model* і *PDU Detail* та зверніть увагу на процес інкапсуляції. Якщо поглянути на вкладку *OSI Model*, виділивши *Layer* 7, опис того, що відбувається, буде розміщений безпосередньо нижче *In Layers* і *Out Layers* (“1. The DNS client sends a DNS query to the DNS server.”). Це дуже важливі дані, які допомагають зрозуміти процеси, які мають місце при передачі даних.

4. Натисніть на вкладці *Outbound PDU Details*. Яка інформація міститься у полі *NAME*: у розділі запиту *DNS QUERY*?

5. Натисніть на останньому кольоровому квадраті DNS у списку подій.

На якому пристрої було захоплено PDU?

Яке значення вказане поряд з *ADDRESS*: у частині *DNS Answer* на вкладці *Inbound PDU Details*?

6. Налаштуйте *Event List Filters* на відображення подій HTTP та TCP.

7. Знайдіть другу подію TCP у переліку *Event List,* коли пакет надходить з R1 до Server0. Оберіть *Layer 4* на вкладці *OSI Model*.

Яка інформація відображається у пункті 4 і 5 пронумерованого списку, що міститься безпосередньо під *In Layers* і *Out Layers*?

Окрім інших важливих функцій, TCP керує підключенням і відключенням каналу передавання даних. Саме ця подія відображає, що канал зв'язку налаштовано (ESTABLISHED).

8. Натисніть на останній події TCP. Оберіть *Layer 4* у вкладці *OSI Model*. Ознайомтесь з записами, наведеними безпосередньо нижче *In Layers* і *Out Layers*.

Яке призначення цієї події, виходячи з інформації в останньому записі списку?

6.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– відповіді на поставленні запитанні в ході виконання роботи.

6.4 Питання для підготовки до захисту лабораторної роботи

1. Які переваги використання багаторівневої мережної моделі?
2. Для чого необхідні протоколи при передаванні даних?
3. Які схожості та відмінності між моделлю OSI та моделлю TCP/IP?
4. Які ключові протоколи пов'язані з кожним рівнем моделі TCP/IP?
5. Які організації розробляють стандарти для моделі OSI та TCP/IP?

7 ЛАБОРАТОРНА РОБОТА №7
ВИЗНАЧЕННЯ IPV4-АДРЕС

7.1 Мета лабораторної роботи

Навчитися визначати структуру IPv4-адреси, в тому числі мережну частину, частину вузла і маску підмережі. Визначати різні типи IPv4-адрес та їх використання.

7.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

– правила переходу з двійкової системи числення в десяткову та навпаки;

– структура IPv4-адреси;
– використання операції «І» для визначення мережної частини;
– одноадресна, широкомовна і багатоадресна розсилка IPv4;
– типи IPv4-адрес.

Далі виконати такі дії:
– використати операцію «|» для визначення мережної частини в IP-адресах вузлів, завданих в табл. 7.1;

Таблиця 7.1 – Варіанти завдань

№ вар.	Завдання1		Завдання2	
	IP-адреса вузла	Маска	IP-адреса вузла	Префікс
6.	72.60.124.23	255.255.224.0	13.165.140.153	/10
7.	238.78.57.116	255.248.0.0	59.3.115.89	/11
8.	60.255.110.21	255.255.192.0	112.231.164.30	/12
9.	12.211.92.185	255.128.0.0	126.210.206.234	/13
10.	165.114.253.9	255.255.252.0	220.24.105.100	/14
11.	253.171.224.98	255.255.240.0	3.174.130.238	/15
12.	225.194.116.5	255.240.0.0	79.80.159.149	/20
13.	92.159.7.53	255.255.252.0	112.37.195.31	/17
14.	43.117.230.183	255.255.192.0	98.107.124.156	/18
15.	146.247.87.2	255.255.240.0	55.160.113.10	/19
16.	188.233.122.101	255.255.224.0	56.211.33.164	/21
17.	192.19.3.8	255.255.254.0	53.119.203.221	/22
18.	84.6.223.106	255.255.252.0	67.200.116.39	/23
19.	216.45.42.190	255.255.248.0	243.162.237.152	/22
20.	138.46.140.94	255.248.0.0	4.82.38.2	/21
21.	152.205.232.105	255.255.192.0	144.112.213.91	/20
22.	107.214.175.68	255.255.224.0	210.254.11.42	/19
23.	57.198.77.193	255.255.240.0	11.104.213.125	/18
24.	122.227.157.232	255.255.128.0	201.24.249.88	/17
25.	228.219.147.134	255.255.252.0	17.124.16.162	/18

– заповнити таблицю 7.2 відомостями для визначених мереж з табл.7.1;

Таблиця 7.2 – Відомості про мережі

IP-адрес мережі	Маска або префікс	Адреса першого вузла	Адреса останнього вузла	Широкомовна адреса	Кількість вузлів

– проаналізувати таблицю 7.3 та визначити тип адреси: адрес вузла, адрес мережі, багатоадресна або широкомовна розсилка;

Таблиця 7.3 – Адрес вузла, адрес мережі, багатоадресна або широкомовна розсилка

IP-адрес	Маска	Тип адреси
10.1.1.1	255.255.255.252	
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

– проаналізувати таблицю 7.4 і визначити тип адреси: загальний або приватний;

– проаналізувати таблицю 7.5 і визначити, чи є пара IP-адрес/префікс допустимою адресою вузла;

Таблиця 7.4 – Загальний/приватний

IP-адрес/префікс	Загальний/приватний
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Таблиця 7.5 – Допустима/недопустима адреса вузла

IP-адрес/префікс	Допустима/недопустима адреса	Причина
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

7.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– заповненні відповідями таблиці 7.2-7.5.

7.4 Питання для підготовки до захисту лабораторної роботи

1. До якого класу належить IP-адрес комп'ютера учбового класу?
2. До якої IP-мережі належить IP-адрес комп'ютера учбового класу?
3. Чому при визначенні мережної адреси важлива маска мережі?
4. Яким пристроям зазвичай присвоюються статичні IP-адреси?
5. При налаштування двох ПК в одній мережі ПК-А присвоєно IP-адресу 192.168.1.18, а ПК-Б IP-адресу 192.168.1.33. Маска мережі обох комп'ютерів: 255.255.255.240. Чи зможуть ці ПК взаємодіяти один з одним безпосередньо?

8 ЛАБОРАТОРНА РОБОТА №8
РОЗРАХУНОК ПІДМЕРЕЖ МЕТОДОМ VLSM

8.1 Мета лабораторної роботи

Навчитися розбивати мережу на підмережі методом VLSM, визначати адреси підмереж, а також діапазон IP-адрес вузлів для підмереж.

8.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– правила переходу з двійкової системи числення в десяткову та навпаки;

– сегментація мереж;

– використання масок в IP-адресації;

– використання в IP-адресації масок змінної довжини.

У цьому завданні ви є мережним фахівцем, який здійснює налаштування мережі нової компанії (рис.8.1). Вам потрібно створити декілька підмереж згідно організаційної структури компанії та розподілити адресний простір.

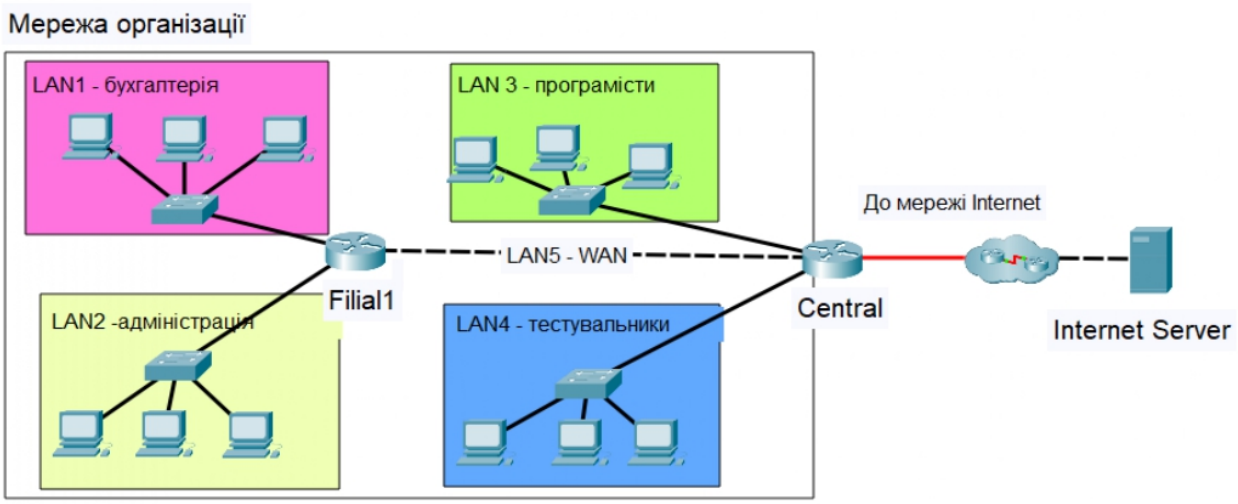

Рисунок 8.1 – Топологія мережі

Обрана адреса організації 10.№.0.0, де № – номер згідно з варіантом. Префікс мережі та кількість вузлів в відділах LAN1-LAN4 завдано по таблиці 8.1 згідно з варіантом. Через маршрутизатор Central забезпечується доступ до мережі Internet.

Таблиця 8.1 – Варіанти завдань

№ вар.	Префікс	LAN1	LAN2	LAN3	LAN4
1.	/19	20	24	128	66
2.	/20	15	20	120	90
3.	/20	60	41	80	120
4.	/19	40	10	130	80
5.	/18	5	13	80	100
6.	/17	5	8	20	28
7.	/16	12	6	400	380
8.	/20	14	10	110	80
9.	/19	18	11	600	450
10.	/18	50	16	700	395
11.	/18	9	15	450	381
12.	/17	6	9	451	365
13.	/19	7	19	560	680
14.	/20	26	11	260	300
15.	/17	22	24	720	615
16.	/16	18	50	800	1000
17.	/18	40	18	789	980
18.	/17	15	8	502	362
19.	/19	21	25	262	368
20.	/20	9	16	52	40
21.	/18	8	20	262	359
22.	/19	15	5	53	50
23.	/18	16	6	177	152
24.	/17	8	17	400	350
25.	/19	23	7	300	260

Необхідно поділили адресний простір організації на необхідну кількість підмереж відповідно до рис. 8.1. При розподілі адресного простору необхідно врахувати кількість вузлів у кожній підмережі (табл. 8.1) та інші аспекти, наприклад, майбутнє розширення вузлів і підмереж в компанії.

Методом VLSM для кожної підмережі маска обчислюється окремо, дозволяючи використовувати більш точну кількість хостів у кожній підмережі. Застосування при розділені на підмережі масок змінної довжини забезпечує заощадливіше використання адресного простору.

Необхідно розробити схему IP-адресації поділу мережі організації на підмережі, використовуючи маски змінної довжини.

Далі виконати такі дії.

1. Визначити найбільшу підмережу та маску для неї. На звільнених бітах перша допустима комбінація присвоюється цій підмережі. Занести у таблицю 8.2 відповідні дані.

2. Потім визначити наступну за розмірами підмережу та маску для неї та присвоїти їй наступну комбінацію на звільнених бітах. Занести у таблицю 8.2 відповідні дані.

3. Продовжувати поділ підмереж відповідного розміру на підмережі до тих пір, поки не буде досягнута потрібна кількість вузлів у кожній підмережі. Відповідні результати необхідно надати у вигляді таблиці 8.2.

Таблиця 8.2 – Підмережі організації

Назва підмережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Маска у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів

4. Дати відповіді на наступні питання:

– кількість необхідних IP-адрес (N);

– кількість IP-адрес, необхідних для каналу LAN5 між маршрутизаторами;

– кількість IP-адрес, доступних у вихідній мережі ($N_{поч}$);

– кількість IP-адрес, доступних в розбитій мережі ($N_{роз}$);

– який відсоток адресного простору використовується в вихідній мережі ($N/N_{поч} *100$);

– який відсоток адресного простору використовується в розрахованій мережі ($N/N_{роз} *100$).

8.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;

– опис завдання з початковими умовами і даними;

– відповіді на зазначені питання;

– розрахунок адресації мережі у вигляді таблиці 8.2;

– схему розподілу адресного простору у вигляді логічної топології (рис 8.2).

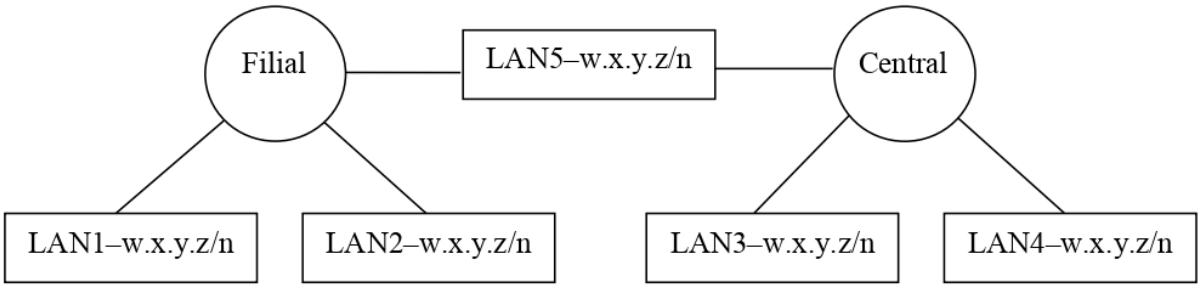

Рисунок 8.2 – Логічна топологія методом маски постійної довжини

8.4 Питання для підготовки до захисту лабораторної роботи

1. Який є запас на випадок появи додаткових мереж?
2. Який є запас на випадок збільшення числа вузлів?
3. Який основний мотив розбиття IP-мереж на підмережі?
4. Який недолік розрахунку мереж за допомогою маски постійної довжини?
5. Чому маска підмережі так важлива при аналізі IPv4-адреси?

9 ЛАБОРАТОРНА РОБОТА №7 ПОБУДОВА МЕРЕЖІ В CISCO PACKET TRACER І БАЗОВЕ НАЛАШТУВАННЯ ТА ЗАХИСТ ПРОМІЖНИХ ПРИСТРОЇВ

9.1 Мета лабораторної роботи

В програмі Packet Tracer побудувати мережу з лабораторної роботи № 6 та отримати практичні навички з базового налаштування проміжних пристроїв.

9.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– робота з командним рядком (CLI) операційної системи Cisco IOS (Internetwork Operating System);

– робота з контекстною довідкою в CLI;

– базове налаштування пристроїв Cisco.

Виконання лабораторної роботи складається з п’яти частин. В першій частині необхідно побудувати мережу в програмі Packet Tracer, задокументувати схему адресації та налаштувати ПК. В другій частині вивчається робота з довідковою системою Cisco IOS. В третій частині виконується налаштування базових параметрів комутаторів. В четвертій частині налаштування маршрутизаторів. В п’ятій частині виконується перевірка підключень до мережі.

Послідовність виконання окремих частин наведена нижче.

ЧАСТИНА 1. Побудова мережі в Packet Tracer та документація схеми адресації

Крок 1. Побудова мережі в Packet Tracer

1. Запустити програму Packet Tracer та побудувати мережу організації з лабораторної роботи №8 (рис. 8.1). Кожну підмережу (LAN1 – LAN4) представити мінімум трьома ПК. Для об'єднання ПК в одну мережу використовувати комутатори серії Cisco Catalyst 2960. Для об'єднання мереж використовувати маршрутизатори серії Cisco 4331.

2. Між маршрутизаторами Filial та Central використовувати послідовний кабель. Для підключення через даний кабель, необхідно додати в вільний слот інтерфейсну панель NIM-2T на вкладці *Physical* (рис.9.1).

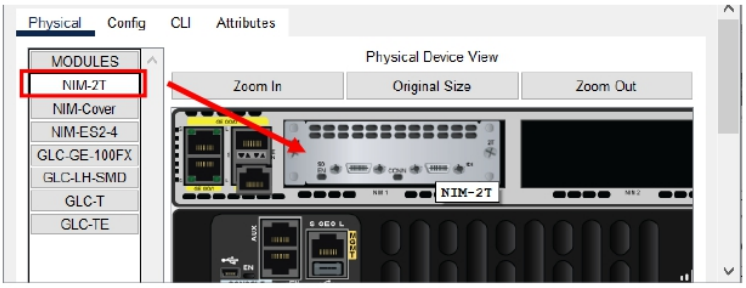

Рисунок 9.1 – Вкладка *Physical* маршрутизатора

3. Доступ до мережі Інтернет змоделювати маршрутизатором постачальника Інтернет-послуг ISP (рис. 9.2). На рис. 9.2 задана адресація постачальника послуг та IP-адреса Інтернет-сервера. Обрати модель Cisco 4331.

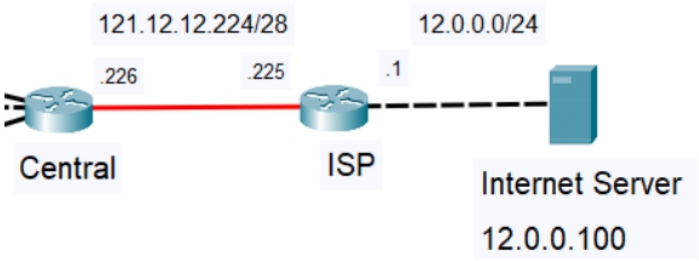

Рисунок 9.2 – Мережа Internet

Примітка. Якщо ви хочете помістити кілька пристроїв одного і того ж типу на робочий простір, натискання і перетягування може стати дуже виснажливим. Щоб уникнути цього, ви можете утримувати клавішу CTRL при натисканні на пристрій в панелі вибору пристроїв.

Крок 2. Документація схеми адресації

1. Для IP-адресації мережі використовувати розрахунки з лабораторній роботі №6. Задокументувати схему IP-адресації і підключень пристроїв у вигляді таблиці 9.1 з урахуванням таких вимог:

– перші допустимі IP-адреси призначаються інтерфейсам маршрутизаторів в локальних мережах;

– другі з допустимих IP-адрес призначаються комутаторам;

– останні з використовуваних IP-адрес призначаються ПК;

– ISP та Internet Server задати інтерфейсам IP-адреси відповідно до рис.9.1.

2. Кожному ПК задати статичну IP-адресу, маску і шлюз за замовчуванням. Заповнити таблицю 9.2 відповідними даними для кожної робочої станції.

Таблиця 9.1 – Адресація пристроїв і їх підключення

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Шлюз
Filial	Gig0/0/0			–
	Gig0/0/1			–
	S0/1/_			–
Central	Gig0/0/0			–
	Gig0/0/1			–
	S0/1/_			–
	Gig0/0/2	122.12.12.226	255.255.255.240	–
ISP	Gig0/0/2	122.12.12.225	255.255.255.240	–
	Gig0/0/0	12.0.0.1	255.255.255.0	–
Switch_LAN1	VLAN1			
Switch_LAN2	VLAN1			
Switch_LAN3	VLAN1			
Switch_LAN4	VLAN1			

Таблиця 9.2 – IP-адресація ПК

Мережа	IP-адрес PC1	IP-адрес PC2	IP-адрес PC3	Маска	Шлюз
LAN1					
LAN2					
LAN3					
LAN4					

Крок 3. Налаштування IP-адресації на ПК

1. Послідовно клацніть на кожному ПК та у вікні управління відкрийте вкладку *Desktop*.

2. Оберіть додаток *IP Configuration* і введіть дані з таблиці 9.2.

Приклад побудованої мережі в Packet Tracer наведено на рис.9.3. В цьому прикладі застосовувався адресний простір 10.160.0.0/17 для розділення мережі на 5 підмереж методом VLSM з кількістю користувачів:

– LAN1 – 18;
– LAN2 – 50;
– LAN3 – 300;
– LAN4 – 400;
– WAN – 2.

Для зручності на робочу область винесено відомості про адресацію в підмережах та задіяні інтерфейси маршрутизаторів.

Примітка. Всі подальші приклади в цій і наступній лабораторних роботах будуть наведені для цього прикладу.

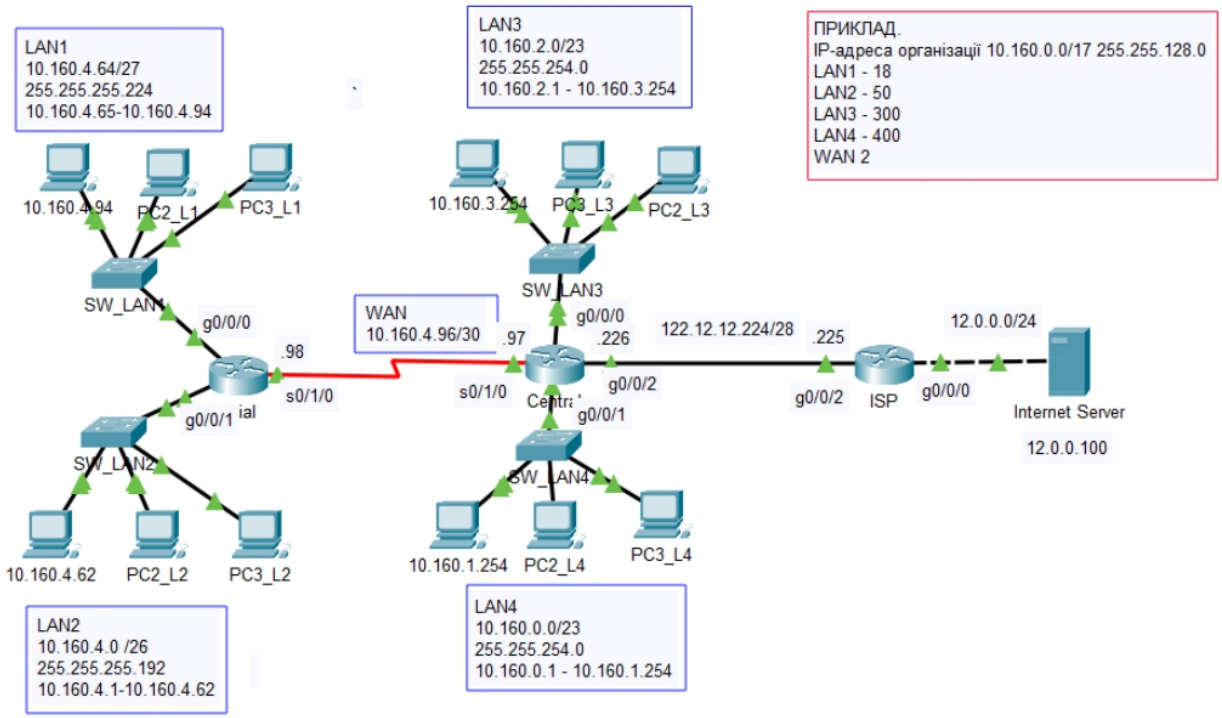

Рисунок 9.3 – Приклад побудованої мережі в Packet Tracer

ЧАСТИНА 2. Використання довідкової системи Cisco IOS

Крок 1. Консольне підключення до комутатора в LAN1

1. У групі *Connections* виберіть світло-блакитний консольний кабель (Console).

2. Клацніть будь-який ПК в LAN1. Виберіть варіант для підключення RS-232.

3. Перетягніть інший кінець консольного підключення до комутатора в LAN1 і клацніть на ньому, щоб відкрити список підключень. Виберіть консольний порт (Console), щоб завершити підключення.

Крок 2. Встановлення сеансу термінального зв'язку з комутатором Switch_LAN1

1. Клацніть на ПК з консольним підключенням і відкрийте вкладку *Desktop*.

2. Клацніть значок програми *Terminal*. Перевірте правильність параметрів за замовчуванням, встановлених для порту: 9600, 8, None, 1, None. Натисніть *OK*.

3. У вікні може бути показано кілька повідомлень. У будь-якої частини вікна має з'явитися повідомлення «Press RETURN to get started!». Натисніть клавішу *Enter*.

Що означає символ після імені комутатора?

Крок 3. Вивчення довідки по Cisco IOS

В IOS доступна довідка по командам. В даний момент відображається запрошення, зване режимом користувача, і пристрій очікує введення команд.

Найпростіший спосіб викликати довідку, це ввести знак питання (?) в будь-якому місці командного рядка.

1. Відкрийте список всіх допустимих команд в режимі користувача.

```
Switch>?
```

Яка команда починається з букви «s»?

2. У командному рядку введіть «t» зі знаком питання в кінці (?).

```
Switch> t?
```

Які відображаються команди?

3. У командному рядку введіть «te» зі знаком питання в кінці (?).

```
Switch> te?
```

Які відображаються команди?

Крок 4. Вхід в привілейований режим

1. Наберіть «en» і натисніть клавішу Tab.

```
Switch> en<Tab>
```

Що відображається після натискання клавіші Tab?

2. Введіть команду «enable» і натисніть клавішу *Enter*. Як змінився вигляд командного рядка комутатора і що це означає?

3. У привілейованому режимі введіть знак питання «?».

```
Switch #?
```

4. На екрані повинен з'явитися список команд. У нижній частині екрана з'явиться рядок «-more-». Для того щоб продовжити виведення списку команд натисніть або клавішу *Enter* (вивід на екран лінію за лінією), або *Space* (вивід посторінково). Щоб вийти з перегляду списку команд, натисніть «q».

5. Перерахуйте десять доступних команд в привілейованому режимі.

Крок 5. Список команд «show»

Виведіть всі команди show, ввівши «show ?» в привілейованому режимі.

```
Switch# show ?
```

Чи доступна команда «running-config» в даному режимі?

Крок 6. Використання довідкової системи при установці дати і часу

1. Введіть «show clock» в привілейованому режимі.

```
Switch# show clock
```

Яка відображається інформація та рік?

2. Використовуйте контекстну довідку і команду «clock», щоб встановити поточний час на комутаторі. Введіть команду «clock» і натисніть клавішу *Enter*.

```
Switch# clock <ENTER>
```

Яка інформація відображається?

3. IOS видала повідомлення «% Incomplete command», яке означає, що команду введено не повністю. У довідці можна отримати додаткові відомості про час, якщо ввести після команди пробіл і знак питання (?).

4. Введіть з клавіатури «clock ?» І потім натисніть *Enter*. Відзначте відмінності в реакції комутатора на ваші дії при введенні цих команд.

```
Switch# clock ?
```

5. Встановіть поточний час та день на комутаторі шляхом введення з клавіатури «clock ?» І дотримуйтесь далі опису команди з екрану допомоги:

```
Switch# clock ?
Switch# clock set ?
Switch# clock set 10:30:30 ?
Switch# clock set 10:30:30 17 April ?
Switch# clock set 10:30:30 17 April 2024
```

6. Поверніться в привілейований режим, натиснувши Ctrl+Z. Введіть «show clock» щоб переглянути поточні час і дату на комутаторі.

Крок 7. Редагування команд в Cisco IOS

1. У привілейованому режимі введіть «show history» та не натискайте клавішу *Enter*.

2. Натисніть «Ctrl+A». Дана команда встановить курсор на початок рядка.

3. Натисніть «Ctrl+E». Дана команда встановить курсор в кінець рядка.

4. Натисніть «Ctrl+A», а потім «Ctrl+F». Дана команда встановлює курсор на один символ вперед.

5. Натисніть «Ctrl+B». Дана команда встановлює курсор на один символ назад.

6. Натисніть *Enter*, а після цього «Ctrl+P». Дана послідовність повторює останню введену команду. Натисніть кнопку «Вгору». Це також повторить останню введену команду.

7. Використовуйте інші гарячі клавіші в консолі за необхідності:

«Ctrl+W» – стерти попереднє слово;

«Ctrl+U» – стерти всю лінію;

«Ctrl+C» – вихід з режиму конфігурації;

«Ctrl+Z» – застосувати поточну команду і вийти з режиму конфігурації;

«Ctrl+Shift+6» – зупинка тривалих процесів (так званий escape sequence).

ЧАСТИНА 3. Налаштування базових параметрів комутатора

Крок 1. Перегляд поточної конфігурації комутатора

1. Виконайте команду «show running-config».

```
Switch# show running-config
```

Скільки у комутатора інтерфейсів FastEthernet?

Скільки у комутатора інтерфейсів Gigabit Ethernet?

Який діапазон значень, що відображаються в vty-лініях?

2. Відкрийте вміст NVRAM «show startup-config».

Чому комутатор відповідає повідомленням «startup-config is not present»?

Крок 2. Вхід в режим глобальної конфігурації

1. Наберіть «config» в привілейованому режимі. При введенні команди «config» IOS просить вказати той її варіант, який буде використовуватися:

```
Switch # config
```

```
Configuring from terminal, memory, or network [terminal]?
```

2. Натисніть *Enter*, щоб прийняти параметр за замовчуванням, вказаний в квадратних дужках.

Як змінився вигляд командного рядка і що це означає?

Крок 3. Заборона небажаних пошуків в DNS

Вимкніть пошук в DNS, щоб запобігти спробам комутатора перетворювати введені невірні команди таким чином, як ніби вони є іменами вузлів.

```
Switch (config) # no ip domain-lookup
```

Крок 4. Налаштування імені комутатора

Встановіть для комутатора ім'я по табл. 7.1 командою «hostname».

```
Switch(config)#hostname Switch_LAN1
```

Крок 5. Налаштування пароля привілейованого режиму

1. Встановіть зашифрований пароль *class* на вхід в привілейований режим.

```
Switch_LAN1(config) #enable secret class
```

2. Здійсніть вихід з режиму глобальної конфігурації через «Control+Z», а потім з привілейованого режиму командою «disable». Спробуйте тепер знову здійснити вхід в привілейований режим. Зверніть увагу, що при введенні паролю на екрані символи не відображаються.

3. Покажіть поточну конфігурацію комутатора.

```
Switch_LAN1# show running-config
```

4. Знайдіть в поточній конфігурації пароль на вхід в привілейований режим. Чому пароль enable secret відображається не так, як його ввели?

Крок 6. Налаштування доступу до консолі

1. Введіть «line ?» в режимі глобальної конфігурації.

```
Switch_LAN1(config)# line ?
```

2. Встановіть пароль *cisco* на консоль:

```
Switch_LAN1(config)#line console 0
Switch_LAN1(config-line)#password cisco
Switch_LAN1(config-line)#login
Switch_LAN1(config-line)#exit
```

3. Закрийте сеанс консолі, ввівши команду «exit» в привілейованому режимі.

```
Switch_LAN1# exit
```

4. Переконайтеся, що доступ до консолі захищений паролем. Для цього натисніть клавішу *Enter*, щоб увійти в режим користувача.

Крок 7. Налаштування доступу до vty по протоколу SSH

Лінії VTY (Virtual Terminal Line) потрібні для віддаленого адміністрування пристроєм по Telnet або SSH. Використання Telnet небезпечно, так як дані передаються по мережі в незашифрованому вигляді. Тому рекомендується по можливості використовувати протокол SSH. Для налаштування по SSH необхідно

змінити параметри за замовчуванням: «domain-name», «hostname”, та задати протокол шифрування.

1. Привласніть домену ім'я за правилом *Surname.Group.com*, наприклад:

```
Switch_LAN1(config)# ip domain-name Ivanov.126-24-1.com
```

2. Для шифрування даних створіть ключ RSA довжиною 1024 біт.

```
Switch_LAN1(config)# crypto key generate rsa
Після запиту введіть 1024.
```

3. Створіть користувача-адміністратора *admin* з паролем *cisco123*.

```
Switch_LAN1(config)# username admin password cisco123
```

4. Налаштуйте лінії VTY для перевірки реєстраційних даних в локальних базах даних імен користувачів, а також для дозволу віддаленого доступу лише по протоколу SSH.

```
Switch_LAN1(config-line)# login local
Switch_LAN1(config-line)# transport input ssh
```

Крок 8. Перевірка конфігурацій

1. Перегляньте поточну конфігурацію комутатора за допомогою команди привілейованого режиму «show running-config».

```
Switch_LAN1(config)#do show running-config
```

Примітка. Приставка «do» дозволяє виконувати команди «show» в будь-якому режимі, не виходячи в привілейований.

2. Знайдіть налаштовані паролі і команди. Зверніть увагу, що паролі на консольні та термінальні лінії відображаються у відкритому вигляді.

Крок 9. Шифрування паролів

1. Зашифруйте всі поточні і наступні паролі.

```
Switch_LAN1(config)# service password-encryption
```

2. Перегляньте поточну конфігурацію.

3. Знайдіть налаштовані паролі і команди. Зверніть увагу, що паролі на консольні та термінальні лінії відображаються в зашифрованому вигляді.

Крок 10. Встановлення банера MOTD

Налаштуйте повідомлення, яке буде відображатися всім, хто входить в систему на комутаторі. Це повідомлення називається щоденним банером (MOTD). Текст банера можна укласти в подвійні лапки або використовувати будь-який символ, відмінний від символу в рядку MOTD.

```
Switch_LAN1(config)#banner motd #Building power will be off from
7:00 AM until 9:00 AM this coming Tuesday#
```

Крок 11. Налаштування інтерфейсу керування комутатором

Через віртуальний інтерфейс комутатора (SVI) можна отримати віддалений доступ по Telnet або SSH з метою відображення і налаштування його параметрів. На SVI-інтерфейсі можна сконфігурувати IP-адресу, яку зазвичай називають адресою керування. За замовчуванням через VLAN 1 забезпечується керування

комутатором по мережі. Налаштуйте IP-адресу на комутаторі Switch_LAN1 по даним з табл. 7.1, наприклад:

```
Switch_LAN1 (config)# interface vlan 1
Switch_LAN1(config-if)# ip address 10.160.4.66 255.255.255.224
Switch_LAN1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN:Line protocol on Interface Vlan1, changed
state to up
```

Для доступу до комутатора з віддалених мереж необхідно вказати IP-адресу шлюзу, наприклад:

```
Switch_LAN1(config)# ip default-gateway 10.160.4.65
```

Крок 12. Перевірка налаштування інтерфейсу керування комутатором.

Команда «show ip interface brief» в привілейованому режимі інформує про IP-адресу, а також про стан всіх портів і інтерфейсів комутатора. Стан інтерфейсу VLAN 1 повинен бути up/up (працює/працює), а інтерфейсу призначена IP-адреса.

```
Switch_LAN1# show ip interface brief
```

Крок 13. Перевірка віддаленого підключення по протоколу SSH

На даному етапі, поки не налаштована маршрутизація, до комутатора Switch_LAN1 можна підключатися тільки з ПК, які знаходяться в тому ж сегменті мережі, що і комутатор. Після виконання лабораторної роботи №9 до комутатора можна буде підключатися з будь-якого віддаленого ПК.

1. На будь-якому ПК в LAN1 відкрийте командний рядок *Command Prompt* на кладці *Desktop*.

2. Введіть «ssh» і натисніть Enter, не додаючи будь-яких параметрів, щоб відобразити інструкції використання команди. Параметр *-l* — це літера «L».

3. Спробуйте увійти до комутатора за його IP-адресою через створеного локального користувача *admin* з паролем *cisco123*. Наприклад:

```
> ssh -l admin 10.160.4.66
```

4. Після успішного входу перейдіть в режим привілейованого доступу і збережіть конфігурацію, виконавши наступний крок.

Крок 14. Збереження конфігурації комутатора в NVRAM

Щоб внесені зміни не загубилися після перезавантаження системи і відключення живлення необхідно створити резервні копії файлу конфігурації в NVRAM.

```
Switch_LAN1# copy running-config startup-config
```

Яка найкоротша версія команди «copy running-config startup-config»?

Крок 15. Налаштування комутаторів в інших сегментах

1. По табл.7.1 виконайте базові налаштування на інших комутаторах, задавши назву пристрою, паролі до ліній, доступ по SSH, пароль до привілейованого режиму, IP-адресу та шлюз. Змініть наведений скріпт

відповідними даними, скопіюйте та вставте в командному рядку комутатора в режимі користувача.

```
enable
configure terminal
no ip domain-lookup
hostname SW_LAN2
enable secret class
service password-encryption
line console 0
password cisco
login
username admin secret cisco123
ip domain-name Ivanov.126-24-1.com
crypto key generate rsa
1024
line vty 0 4
login local
transport input ssh
interface vlan1
ip address 10.160.4.2 255.255.255.192
no shutdown
ip default-gateway 10.160.4.1
do copy run st
```

ЧАСТИНА 4. Налаштування маршрутизаторів

Крок 1. Базове налаштування маршрутизаторів

1. На кожному маршрутизаторі виконайте базові налаштування, змінивши наведений скріпт відповідними даними.

```
enable
configure terminal
no ip domain-lookup
hostname Filial
enable secret class
service password-encryption
line console 0
password cisco
login
username admin secret cisco123
ip domain-name Ivanov.126-24-1.com
crypto key generate rsa
1024
line vty 0 4
login local
transport input ssh
do copy run start
```

Використовуйте відомості в таблиці адресації табл. 9.1 та активуйте задіяні інтерфейси. Вважається хорошою практикою налаштовувати опис на кожному інтерфейсі, це допомагає документувати її. Приклад налаштування для g0/0/0:

```
Filial(config)# interface gigabitethernet 0/0/0
Filial(config-if)# ip address 10.160.4.65 255.255.255.224
Filial(config-if)# no shutdown
Filial(config-if)# description Connection to LAN1
```

2. Збережіть налаштування на кожному маршрутизаторі.

```
Filial# copy running-config startup-config
```

ЧАСТИНА 5. Перевірка підключень до мережі

Крок 1. Перевірка підключення до мережі

1. Для перевірки правильного налаштування ПК і доступності локальних інтерфейсів маршрутизаторів виконайте команду «ping» з командного рядка кожного ПК на його шлюз. Echo-запити повинні бути успішними. При невдалому виконанні echo-запитів виконайте пошук і усунення несправностей.

2. Перевірте досяжність мереж, відправивши echo-запити по табл. 9.3, та дайте пояснення.

Примітка. На даний момент ПК не можуть відправляти echo-запити на ПК в віддалених мережах.

Таблиця 9.3 – Результат перевірки досяжності мереж командою «ping»

ping		Так/ні	Пояснення
Від	До		
LAN1	LAN2		
LAN1	LAN3		
LAN3	LAN4		
LAN1	Central-Se0/1/0		
LAN1	Central-g0/0/2 (122.12.12.226)		
LAN1	Internet Server (12.0.0.100)		

9.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;
– опис завдання з початковими умовами та даними;
– скріншот побудованої мережі в Packet Tracer;
– таблиці призначень IP-адрес (табл. 9.1 і 9.2);
– таблиця 9.3 з результатами перевірки досяжності мереж;
– застосовані команди з налаштувань та їх опис;
– проект мережі з назвою за правилом *Surname_Group_lab09.pkt*.

9.4 Питання для підготовки до захисту лабораторної роботи

1. Чому на комутаторі порти знаходяться в відключеному стані?
2. Чому не виконується ping до вузлів в віддалених мережах?
3. Для чого потрібна команда «login» при налаштуванні доступу до ліній vty та консолі?
4. Який слід використовувати кабель при підключенні двох ПК між собою?
5. На якому рівні моделі OSI працює комутатор?

10 ЛАБОРАТОРНА РОБОТА №10
ВПРОВАДЖЕННЯ І НАЛАШТУВАННЯ СЕРВІСІВ ВЕБ-СЕРВЕРУ, СЕРВЕРУ ЕЛЕКТРОННОЇ ПОШТИ, DHCP, DNS ТА FTP

10.1 Мета лабораторної роботи

Вивчити призначення та особливості сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP, їх налаштування та перевірку в програмі Packet Tracer.

10.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– використання портів сервісами веб-серверу, серверу електронної пошти, DHCP, DNS та FTP;

– функції протоколів HTTP, SMTP, POP3, DHCP, DNS та FTP.

Вихідними даними є мережа в Packet Tracer з лабораторної роботи №9 «Побудова мережі в Cisco Packet Tracer і базове налаштування та захист проміжних пристроїв».

Виконання лабораторної роботи складається з п’ятьох частин. В першій частині необхідно налаштувати веб-сервіс. В другій частині налаштування серверу електронної пошти. В третій частині виконується налаштування записів на DNS-сервері. В четвертій частині налаштування серверу DHCP та перевірка сервісів DHCP та DNS. В п‘ятій частині налаштування FTP-сервісу.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Налаштування та перевірка веб-серверу

Крок 1. Налаштування веб-серверу

1. Додати в мережу LAN1 сервер *Server-PT* з групи *End Devise*, дати йому назву *MultiServer* та привласнити п’яту IP-адресу з діапазону допустимих IP-адрес цієї підмережі.

2. На MultiServer відкрити вкладку *Services* і вибрати розділ *HTTP*.

3. Вибрати варіант *On*, щоб включити HTTP і HTTP Secure (HTTPS).

4. Змінити HTML-код, щоб на головній сторінці сайту відображались відомості про автора роботи.

Крок 2. Перевірка працездатності веб-серверу

1. На будь-якому вузлі в мережі LAN1 відкрити вкладку *Desktop* та вибрати додаток *Web Browser*.

2. В полі URL ввести IP-адресу MultiServer і натиснути кнопку *Go*. Відкриється веб-сайт MultiServer.

3. Перевірити працездатність веб-серверу з вузлів в підмережах LAN1 або LAN2 через його IP-адресу.

ЧАСТИНА 2. Налаштування та перевірка серверу електронної пошти

Крок 1. Налаштування MultiServer для відправки (SMTP) і отримання (POP3) повідомлень електронної пошти

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *EMAIL*.
2. Вибрати варіант *On*, щоб включити SMTP і POP3.
3. Призначте ім'я домену surname.pt і натиснути кнопку *Set*, де *surname* – прізвище розробника проекту, наприклад ivanov.pt.
4. Створити користувачів з ім'ям user1 та user2 і паролем cisco. Натиснути + для додавання користувачів.

Крок 2. Налаштування та перевірка ПК для використання сервісу електронної пошти

1. На будь-якому вузлі в мережі LAN1 відкрити вкладку *Desktop* та вибрати додаток *Email*.
2. Ввести відповідні значення у відповідних полях:
   а) Your Name: User1;
   б) Email Address: user1@*surname*.pt;
   в) Incoming Mail Server: IP-адреса MultiServer;
   г) Outgoing Mail Server: IP-адреса MultiServer;
   д) User Name: user1;
   е) Password: cisco;
3. Натиснути кнопку *Save*. З'явиться вікно поштового оглядача.
4. Натиснути кнопку *Receive*. Якщо всі налаштування клієнта і сервера виконані правильно, у вікні поштового оглядача з'явиться повідомлення про підтвердження «Receive Mail Success».
5. Вибрати інший ПК в цій мережі, відкрити вкладку *Desktop* та вибрати додаток *Email*.
6. Виконати відповідні налаштування email для user2.

Крок 3. Відправка електронної пошти від user1 до user2

1. У вікні *Mail Browser* на user1 натиснути кнопку *Compose*.
2. Ввести наступні значення у відповідних полях:
   а) To: user2@*surname*.pt;
   б) Subject: вкажіть тему повідомлення;
   в) Email Body: введіть текст листа.
3. Натиснути *Send*.
4. Натиснути кнопку *Receive* на user2 і переконатися, що він отримав повідомлення електронної пошти. Двічі клацнути повідомлення електронної пошти.
5. Натиснути кнопку *Reply*, ввести відповідь і натиснути кнопку *Send*.
6. Переконатися, що user1 отримав відповідь.

ЧАСТИНА 3. Налаштування записів на DNS-сервері

Крок 1. Налаштування записів на DNS-сервері

1. Додати в мережу LAN2 сервер *Server-PT* з групи *End Devise*, дати йому назву ServerDNS та привласнити п'яту IP-адресу з діапазону допустимих IP-адрес цієї підмережі.
2. На ServerDNS відкрити вкладку *Services* і вибрати розділ *DNS*.
3. Вибрати варіант *On*, щоб включити сервіс DNS.
4. Додати запис для MultiServer у відповідних полях:
    а) Name: labkm.com;
    б) Address: IP-адреса MultiServer.
5. Натиснути кнопку *Add* щоб додати запис.

ЧАСТИНА 4. Налаштування серверу DHCP та перевірка сервісів DHCP та DNS

Крок 1. Налаштування серверу DHCP

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *DHCP*.
2. Вибрати варіант *On*, щоб включити сервіс DHCP.
3. Ввести відповідні значення у відповідних полях:
    а) Default Gateway: IP-адреса шлюза;
    б) DNS Server: IP-адреса ServerDNS;
    в) Start IP Address: виключити перші 10 адрес;
    г) Subnet Mask: маска мережі LAN1;
4. Натиснути кнопку *Add* щоб додати запис.

Крок 2. Перевірка сервісу DHCP для вузлів в LAN1

1. На кожному вузлі LAN1 відкрити вкладку *Desktop* і вибрати розділ *IP Configuration*.
2. Вибрати варіант *DHCP* і дочекатися виконання запиту DHCP.

Крок 3. Перевірка сервісу DNS

1. На MultiServer відкрити вкладку *Desktop* і в розділі *IP Configuration* в полі DNS Server вказати IP-адресу ServerDNS.
2. На будь-якому вузлі в мережі LAN1 відкрити вкладку *Desktop* та вибрати додаток *Command Prompt.*
3. Виконати «ping» на IP-адресу ServerDNS, щоб протестувати з'єднання.
4. Виконати команду «nslookup labkm.com», щоб перевірити роботу ServerDNS. Повинні отримати IP-адрес для імені labkm.com.
5. Закрити додаток *Command Prompt* та відкрити *Web Browser.*
6. В полі URL ввести labkm.com і натиснути кнопку *Go*. Відкриється веб-сайт MultiServer.
7. Перевірити працездатність веб-серверу з вузлів в інших підмережах, додавши в налаштуваннях IP-адресу ServerDNS.

ЧАСТИНА 5. Налаштування FTP-сервісу на MultiServer

Крок 1. Налаштування FTP-сервісу на MultiServer

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *FTP*.

2. Вибрати варіант *On*, щоб включити сервіс FTP.

3. У розділі *User Setup* створити облікові записи користувачів (табл.10.1). Натиснути *Add* для додавання облікового запису.

Таблиця 10.1 – Облікові записи на сервері FTP

Ім'я користувача	Пароль	Дозволи
anonymous	anonymous	Read List
administrator	cisco	full permission

Крок 2. Відправка конфігураційного файлу на FTP-сервер

1. На будь-якому вузлі в мережі FTP-сервера відкрити вкладку *Desktop* і вибрати додаток *Text Editor*.

2. Набрати текст в текстовому редакторі та при його закритті зберегти під назвою README.txt.

3. На вкладці *Desktop* відкрити вікно *cmd* і виконати наступні дії.

   а) Введіть «ftp *IP-адреса MultiServer*». Зачекайте кілька секунд, поки клієнт підключиться.

   б) Сервер виведе запит для введення імені користувача і пароля. Використати облікові дані для облікового запису administrator.

   в) Рядок зміниться на ftp>. Ввести команду «dir» для перегляду вмісту каталогу. З'явиться каталог файлів на MultiServer.

   г) Для перенесення файлу README.txt в рядку ftp> ввести «put README.txt». Файл README.txt буде переданий з вузла на MultiServer.

   д) Ввести команду «dir», щоб упевнитися, що файл був переданий. Файл README.txt тепер є в списку файлів каталогу.

   е) Закрити FTP-клієнт, ввівши команду «quit». Командний рядок набуде вигляду PC>.

10.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– опис застосованих сервісів та їх параметри налаштувань;

– проект мережі в Packet Tracer з назвою за правилом *Surname_Group_lab10.pkt* разом зі звітом відправити на перевірку в систему Moodle або на корпоративну поштову скриню викладача.

10.4 Питання для підготовки до захисту лабораторної роботи

1. Який протокол перетворює ім'я labkm.com в IP-адресу?
2. Який протокол транспортного рівня використовується для передачі DNS?
3. Які переваги використання DHCP?
4. У чому полягає основне призначення DNS?
5. У чому недолік доступу до FTP з командного рядка?

11 ЛАБОРАТОРНА РОБОТА №11
НАЛАШТУВАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ MERAKI

11.1 Мета роботи

Ознайомитися з міжмережевим екраном Meraki Security Appliance та доступом до налаштувань через хмарний веб-сервіс.

11.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій, методичні вказівки до даної роботи і довідку в Packet Tracer (*Help->Content->Configuring Devices->Meraki Devices*), наступні питання:

– мережні пристрої Meraki;

– налаштування пристроїв Meraki в Packet Tracer;

– нова архітектура мереж Cisco SD-WAN.

У цій лабораторній роботі ви додасте до підмереж LAN3 та LAN4 міжмережевий екран Meraki Security Appliance (SA) та налаштуєте бездротове підключення для користувачів через хмарний веб-сервер Meraki.

Cisco Meraki − це набір керованих через Інтернет мережевих рішень, що забезпечують єдине джерело управління місцями розташування, інфраструктурою і пристроями.

Meraki SA − це керовані з хмари пристрої Unified Threat Management (UTM) з підтримкою програмно-конфігурованих глобальних мереж (Software Defined Wide Area Networking - SD-WAN) і бездротовими можливостями.

Cisco Packet Tracer версії 7.2 і вище підтримує спрощену версію Meraki SA модель MX65W та хмарний веб-сервер Meraki.

Далі виконати такі дії.

Крок 1. Додавання пристроїв Meraki і побудова мережі

1. Додайте в мережу LAN4 з блоку *Wireless Devises* пристрій Meraki-MX65W. З'єднайте через кабель Straight-Throuhg порт Internet 1 на Meraki SA з вільним портом на комутаторі (рис. 11.1).

2. Додайте в топологію нового користувача та під'єднайте до GigabitEthernet3 на Meraki SA (рис. 11.1).

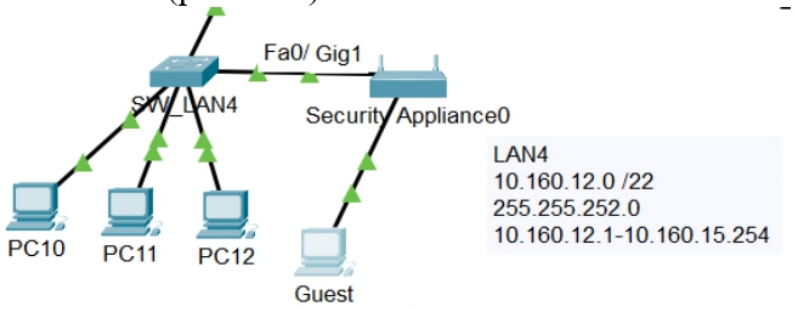

Рисунок 11.1 – Побудова мережі з Meraki-MX65W

3. На вкладці *Physical* Meraki SA під'єднайте до нього блок живлення.

4. Для демонстрації керування Meraki SA з будь-якої точки локації, додайте до ISP мережу з веб-сервером Meraki та ПК для керування через веб-сервер (рис. 11.2). В табл. 11.1 наведені відомості для адресації пристроїв в цій мережі. На ISP локальному інтерфейсу в цій мережі надайте першу IP-адресу.

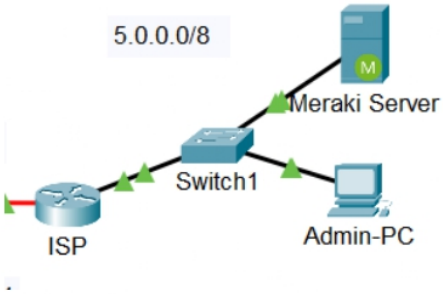

Рисунок 11.2 – Мережа з веб-сервером Meraki

Таблиця 11.1 – IP-адресація пристроїв в мережі з веб-сервером Meraki

Пристрій	Мережа	IPv4 Address	Default Gaeway	DNS Server
Meraki Server	5.0.0.0/8	5.5.5.5/8	5.5.5.1	
Admin-PC		5.5.5.10/8	5.5.5.1	5.5.5.5
ISP		5.5.5.1/8		

Крок 2. Налаштування базових початкових параметрів Meraki SA

1. Перед HTTP-сеансом надайте доданому ПК в LAN4 або статичну IP-адресу з мережі 192.168.0.0/24 (не забудьте вказати адресу DNS-сервера в організації).

2. **ВАЖЛИВО**! Налаштуйте маршрутизатор Central в якості DHCP-сервера, щоб Meraki SA отримав адресу на інтерфейсі Internet 1 динамічно. На Central в командному рядку CLI виконайте налаштування сервісу DHCP з відповідними до вашого варіанту параметрами. Наприклад, для мережі 10.160.12.0/22:

#виключемо з роздачі перші 10 адрес з діапазону допустимих адрес

```
Central(config)# ip dhcp excluded-address 10.160.12.1 10.160.12.10
```

#створимо пул DHCP з назвою LAN4

```
Central(dhcp-config)# ip dhcp pool LAN4
```

#оголосимо адресу мережі LAN4, з якої будуть роздаватися IP-адреси

```
Central(dhcp-config)#network 10.160.12.0 255.255.252.0
```

#адреса Default Gateway в LAN4

```
Central(dhcp-config)#default-router 10.160.12.1
```

адреса ServerDNS

```
Central(dhcp-config)# dns-server 10.160.4.10
```

#зберігаємо налаштування

```
Central(dhcp-config)#do copy run start
```

Примітка: при статичному налаштуванні IP-адреси взаємодії між сервером та SA не має (баг програми).

3. Увімкнений Meraki SA можна налаштувати через HTTP-сеанс від ПК до SA з URL-адресою http://setup.meraki.com або http://192.168.0.1. Ім'я користувача - це серійний номер Meraki SA без пароля (рис. 11.3).

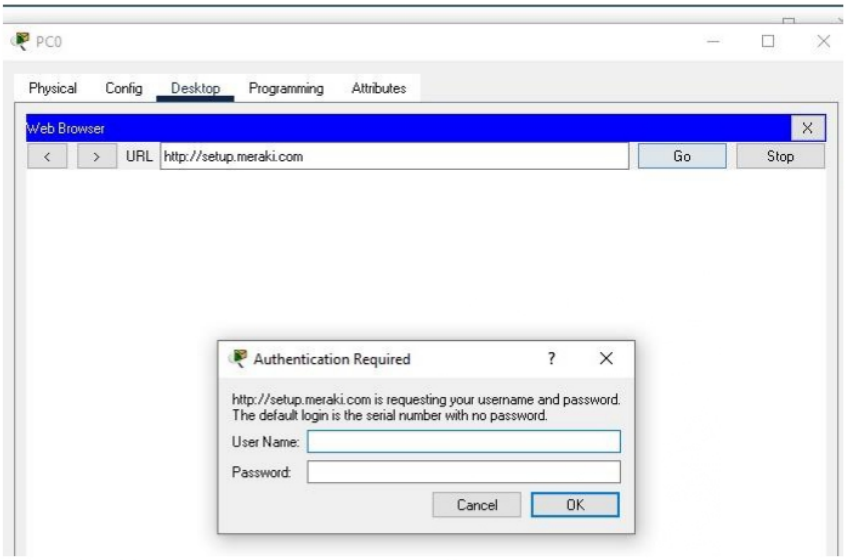

Рисунок 11.3 – Встановлення HTTP-сеансу від ПК до Meraki SA

Серійний номер можна знайти на вкладці *Config* в розділі *Settings* пристрою Meraki SA (рис. 11.4). Задокументуйте його для подальшого використання.

Рисунок 11.4 – Серійний номер SA Meraki SA

4. Після входу відображатиметься поточний статус Meraki SA.

5. На вкладці *Configure* в розділі *Internet 1* налаштуйте:

– Connection type: Direct;

– IP assignment: DHCP.

6. Збережіть налаштування на Meraki SA. Він повинен отримати адресу на інтерфейсі *Internet 1* динамічно.

7. На вкладці *Connection* в розділі *Security Appliance details* задокументуйте MAC-адресу пристрою для подальшого використання.

Крок 3. Налаштування DNS-сервера для доступу до сервера Meraki за URL-адресою

Базова мережева конфігурація Meraki SA може бути досягнута через HTTP-сеанс з ПК, безпосередньо підключеного до пристрою безпеки за URL-адресою http://setup.meraki.com або http://192.168.0.1. Однак функції бездротового зв'язку і безпеки повинні бути налаштовані через хмарний сервер Meraki за URL-адресою

https://dashboard.meraki.com після підключення пристрою безпеки до сервера Meraki.

1. Внесіть в розділ *DNS* на ServerDNS організації адресу хмарного сервера Meraki (рис. 11.5).

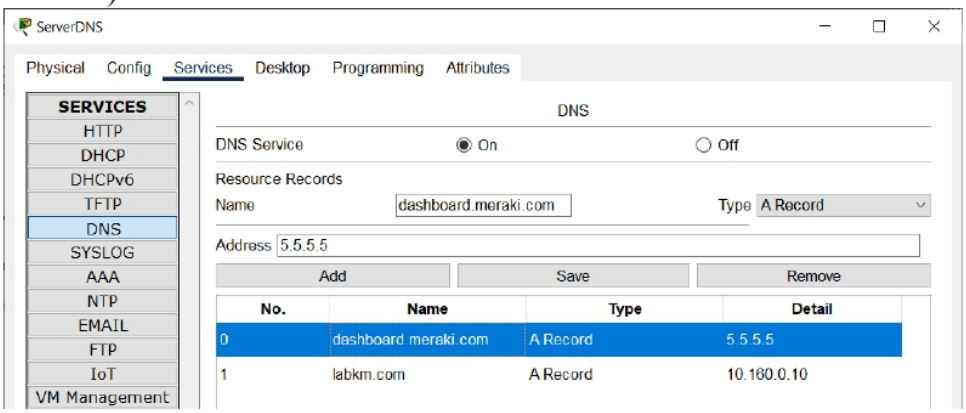

Рисунок 11.5 – DNS-запис URL-адреси сервера Meraki

2. На Admin-PC підключиться до веб-сервера Meraki для налаштування вашої організації і Meraki SA (https://dashboard.meraki.com*)*. Зверніть увагу, що підключення тільки по протоколу HTTPS.

3. Створіть нового користувача (рис. 11.6):

– email: meraki_admin@cisco.com;

– password: 12345678.

4. Використовуйте зареєстровану адресу електронної пошти та пароль для входу в панель керування.

5. Якщо це перший вхід в систему або в обліковий запис не додано ніякі мережі або пристрої, панель управління і навігація зліва обмежені. Якщо додані мережі і пристрої, на панелі керування з'явиться список мереж і пристроїв, а на лівій панелі навігації буде більше параметрів.

6. Використовуйте зареєстровану адресу електронної пошти та пароль для входу в панель керування.

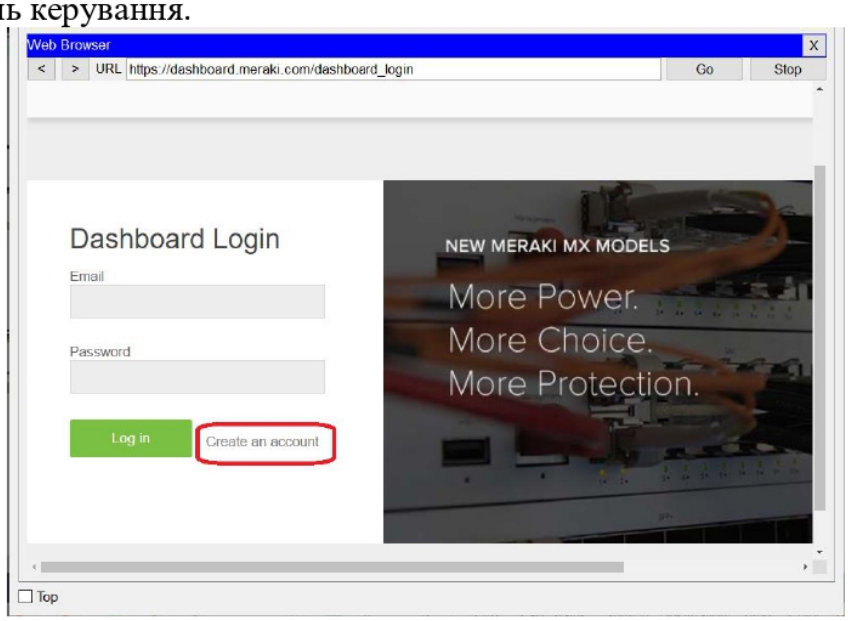

Рисунок 11.6 – Додавання нового користувача до веб-сервера Meraki

7. Якщо це перший вхід в систему або в обліковий запис не додано ніякі мережі або пристрої, панель управління і навігація зліва обмежені. Якщо додані мережі і пристрої, на панелі керування з'явиться список мереж і пристроїв, а на лівій панелі навігації буде більше параметрів.

Крок 4. Створення мереж та реєстрація пристроїв

В Meraki Dashboard доступ до сторінки створення мереж та реєстрації пристроїв можна отримати, натиснувши посилання *Create a network* на лівій навігаційній панелі або в меню *Organization* > *Create a network.*

1. Створіть нову мережу LAN4 (рис. 11.7).

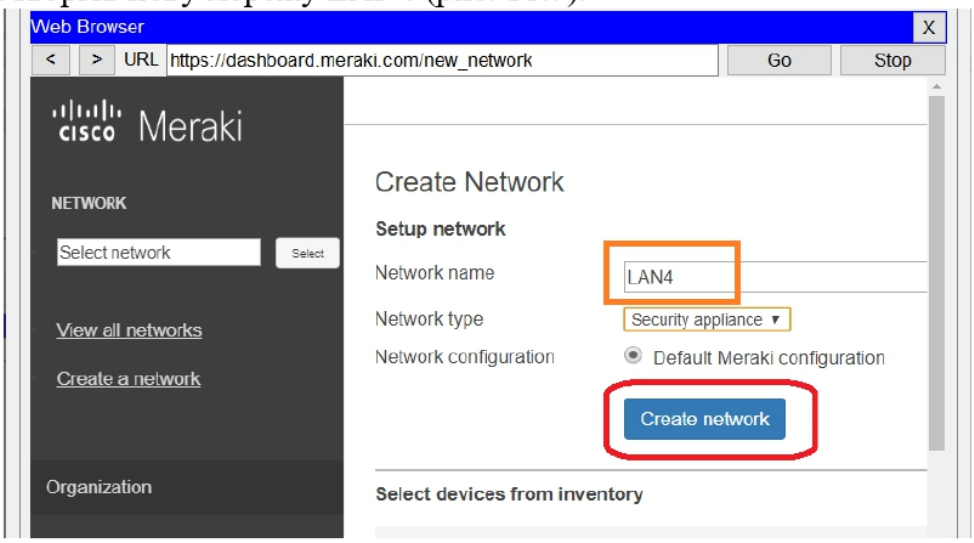

Рисунок 11.7 – Додавання нової мережі в Meraki Dashboard

2. Додайте в мережу LAN4 пристрій Meraki-MX65W з задокументованими його параметрами (рис. 11.8).

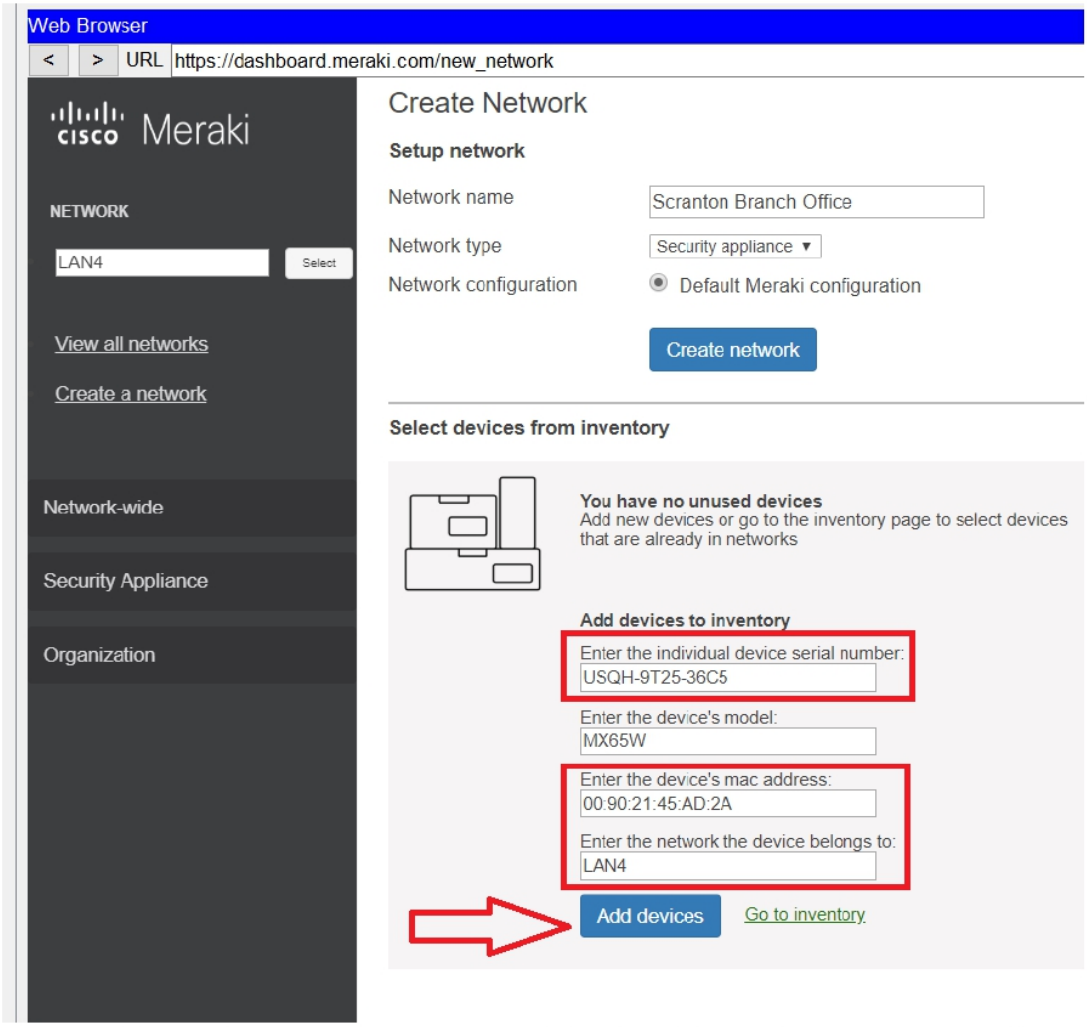

Рисунок 11.8 – Додавання пристрою Meraki-MX65W до Meraki Dashboard

3. Якщо пристрій буде успішно додано, но сторінці *Security Appliance* > *Appliance Status* відображатимуться поточні дані про стан портів (рис.11.9). Посилання Uplink показуватиме конфігурацію WAN Інтернет-порту..

Примітка. Якщо по повторному відкриті проекту не буде відображатися актуальний стан портів, збережіть налаштування на веб-сторінці цього пристрою (http://setup.meraki.com), натиснувши кнопку *Save* на вкладці *Configure,* та почекайте, поки оновиться інформація.

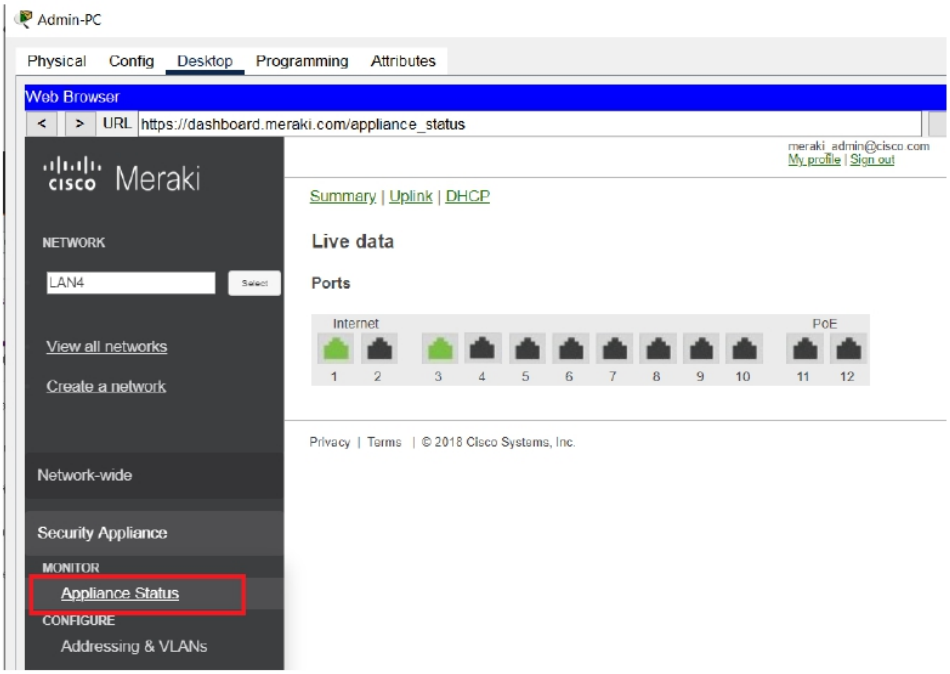

Рисунок 11.9 – Стан портів пристрою

4. На сторінці *Security Appliance->Wireless Settings* налаштуйте параметри Wi-Fi мережі для бездротового під'єднання користувачів згідно рис. 11.10.

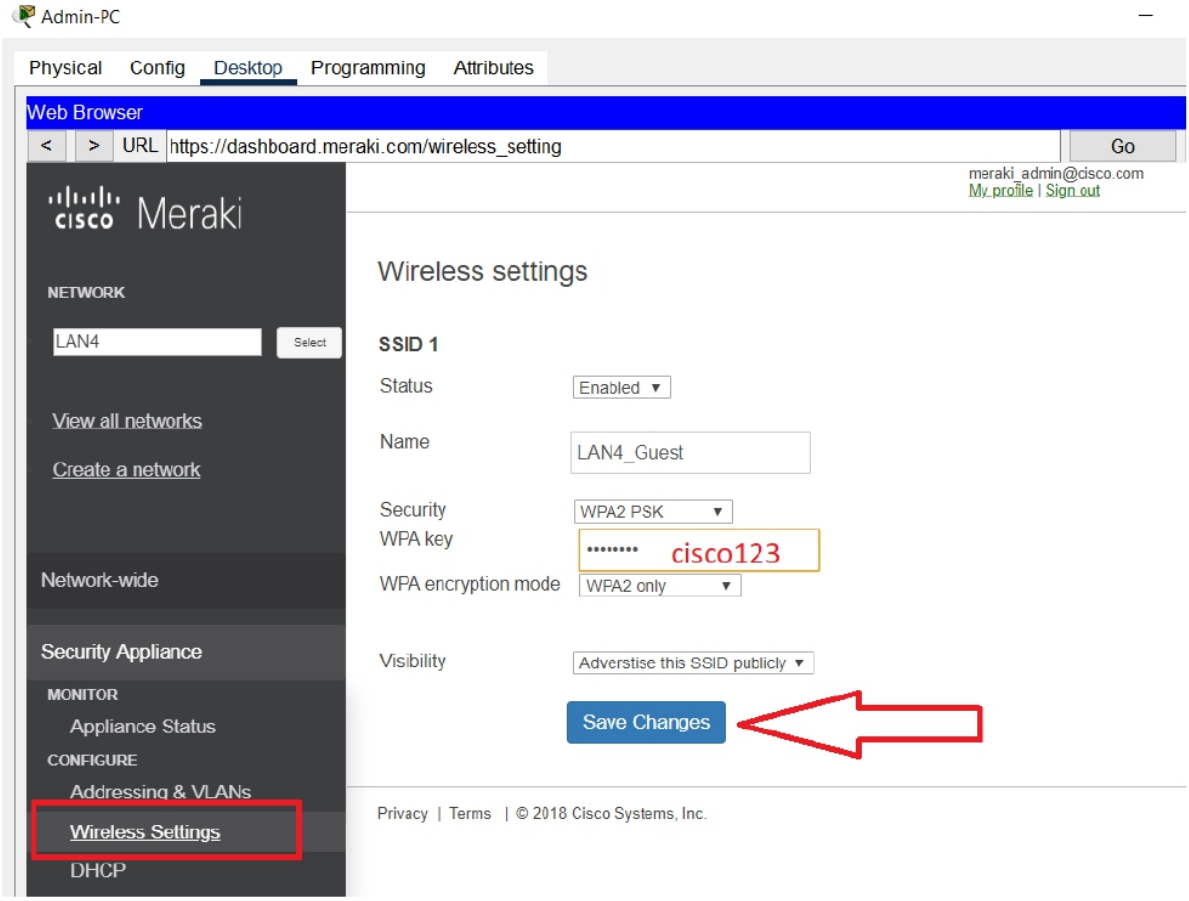

Рисунок 11.10 – Налаштування параметрів мережі Wi-Fi

5. Додайте в LAN4 бездротових клієнтів (наприклад ноутбук з доданим бездротовим інтерфейсом WPC300N) та зробіть на них налаштування відповідно до налаштувань бездротової мережі.

Крок 5. Додавання до підмережі LAN3 Meraki SA та налаштування бездротового підключення для користувачів.

6. Аналогічним чином додайте до підмережі LAN3 міжмережевий екран Meraki SA та налаштуєте відповідне бездротове підключення для користувачів через хмарний веб-сервер Meraki.

11.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– проект мережі з назвою за правилом *Surname_Group_Meraki.pkt* відправити в систему Moodle або на корпоративну поштову скриню викладача.

11.4 Питання для підготовки до захисту лабораторної роботи

1. Що включає в себе рішення Cisco Meraki?
2. Які переваги має використання Cisco Meraki для підприємств?
3. Яка роль Meraki SA (Security Appliance) у розгалуженій мережі?
4. Які основні функції і можливості Meraki SA?
5. Як Meraki сприяє забезпеченню безпеки мережі в офісних приміщеннях та віддалених робочих місцях?

12 ЛАБОРАТОРНА РОБОТА №12
НАЛАШТУВАННЯ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ І МАРШРУТІВ ЗА ЗАМОВЧАННЯМ ДЛЯ IPV4

12.1 Мета лабораторної роботи

Налаштування динамічної маршрутизації і маршрутів за замовчанням на маршрутизаторах мережі організації з метою забезпечення взаємодії між всіма ПК.

12.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– порядок роботи дистанційно-векторного протоколу динамічної маршрутизації EIGRP;

– налаштування EIGRP на маршрутизаторах Cisco;

– принцип дії та конфігурація маршрутів за замовчанням;

– перевірка маршрутної інформації.

Вихідні дані: налаштована мережа з лабораторної з лабораторної роботи №11.

Для обміну даними між підмережами організації та для забезпечення доступу в Інтернет внутрішнім користувачам, потрібно визначити маршрути для їх

досягнення і внести їх в таблиці маршрутизації. Для цього було прийнято рішення застосувати протокол динамічної маршрутизації EIGRP. При такому рішенні маршрути обчислюються автоматично.

Налаштуйте протокол EIGRP на маршрутизаторах Filial та Central. Також врахуйте, що:

– маршрутизатори Filial та Central повинні анонсувати лише мережі організації;

– номер автономної системи EIGRP = № варіанта;

– на маршрутизаторі Central повинен бути прописаний маршрут за замовчуванням до маршрутизатора ISP (в Інтернет);

– Central повинен поширити маршрут за замовчуванням на інші маршрутизатори EIGRP, щоб вузли могли отримати доступ до сервера в Інтернеті;

– на ISP оголосити статичний маршрут до IP-адреси мережі організації.

У разі успішного налаштування відповідно до вимог, всі вузли повинні мати можливість пінгувати один одного та Internet Server.

Далі виконати наведені кроки.

Крок 1. Перевірка конфігурацій

1. Перевірте досяжність мереж, відправивши echo-запити по табл. 9.3 з лабораторної роботи №9, та дайте пояснення.

2. Використовуйте команду «show ip route» щоб переглянути таблицю маршрутизації на кожному маршрутизаторі. На даному кроці кожен маршрутизатор покаже тільки свої мережі, з'єднані безпосередньо з ним. Занотуйте їх у звіт з лабораторної роботи.

Крок 2. Налаштування та перевірка EIGRP

Примітка. В прикладах для налаштування використовується номер автономної системи 100 до топології на рис. 9.3.

1. На маршрутизаторі Filial увімкніть маршрутизацію EIGRP, наприклад

```
Filial(config)# router eigrp 100
```

2. Оголосіть напряму підключені мережі на маршрутизаторі Filial (LAN1, LAN2, WAN), використовуючи інверсну маску мережі, наприклад:

```
Filial(config-router)#network 10.160.4.64 0.0.0.31
Filial(config-router)#network 10.160.4.0 0.0.0.63
Filial(config-router)#network 10.160.4.96 0.0.0.3
```

3. Вимкніть на Filial поширення оновлень на всі локальні мережі, наприклад:

```
Filial(config-router)#passive-interface g0/0/0
Filial(config-router)#passive-interface g0/0/1
```

4. Виконайте аналогічні налаштування на Central, оголосивши безпосередньо підключені його мережі (LAN3, LAN4, WAN) та вимкнувши поширення в локальні мережі, наприклад:

```
Central(config)# router eigrp 100
Central(config-router)# network 10.160.2.0 0.0.1.255
Central(config-router)#network 10.160.0.0 0.0.1.255
Central(config-router)#network 10.160.4.96 0.0.0.3
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.160.4.98
(Serial0/1/0) is up: new adjacency
Central(config-router)#passive-interface g0/0/0
Central(config-router)#passive-interface g0/0/1
```

Після додавання інтерфейсів у процес маршрутизації EIGRP з'являться повідомлення відносин суміжності із сусідніми пристроями.

5. Перевірте досяжність мереж, відправивши echo-запити по табл. 9.3. Обґрунтуйте зміни в новій таблиці. Якщо EIGRP налаштований правильно, echo-запити між усіма пристроями в підмережах організації мають бути успішними, але без доступа в Інтернет.

6. Відобразіть таблиці маршрутизації на даному кроці на кожному маршрутизаторі та занотуйте їх у звіт.

Крок 3. Налаштування та перевірка доступу до Інтернет

У таблицях маршрутизації не може бути маршрутів для всіх можливих вузлів мережі Інтернет. В корпоративних середовищах маршрути за замовчуванням виводять Інтернет-трафік з мережі до ISP.

Маршрут за замовчуванням, вказує який шлюз використовувати, якщо в таблиці маршрутизації немає шляху до адреси призначення. Маршрути за замовчуванням вказують наступний маршрутизатор на шляху до ISP. У команді використовується або IP-адреса наступного переходу, або вихідний інтерфейс.

Синтаксис команд налаштування маршруту за замовчуванням:

```
ip route 0.0.0.0 0.0.0.0 { ip-address | exit-intf }
```

1. Виберіть маршрутизатор Central. Оголосіть маршрут за замовчуванням з відповідною IP-адресою наступного переходу (за топологією на рис. 9.3 це інтерфейс G0/0/2 маршрутизатора ISP з IP-адресою 122.12.12.225). Це викличе трафік до будь-якого невідомого адресу призначення до ISP, що імітує доступ в Інтернет.

```
Central(config)#ip route 0.0.0.0 0.0.0.0 122.12.12.225
```

2. Маршрутизатор Central оголосить цей маршрут іншим маршрутизаторам в домені, якщо додати команду «redistribute static» в конфігурацію EIGRP.

```
Central(config-router)# redistribute static
```

3. Подивіться таблицю маршрутизації на Filial. Як забезпечується магістраль для Інтернет-трафіку в його таблиці маршрутизації?

4. Перевірте досяжність мереж, відправивши echo-запити по табл. 9.3. Обґрунтуйте зміни в новій таблиці.

5. Оголосіть на маршрутизаторі ISP маршрут до загальної IP-адреси мережі організації.

Синтаксис команд налаштування статичного маршруту:

```
ip route [IP_company summary_mask ip-address]
```

– *IP_company summary_mask* – це IP-адреса та маска мережі організації до її поділу на підмережі (за топологією на рис. 9.3 це 10.160.0.0 255.255.128.0);

– *ip-address* – це IP-адреса інтерфейсу маршрутизатора, на який буде відправлятися трафік (за топологією на рис. 9.3 це інтерфейс маршрутизатора Central G0/0/2 з IP-адресою 122.12.12.226).

ISP(config) # ip route 10.160.0.0 255.255.128.0 122.12.12.226

6. Перевірте досяжність мереж, відправивши echo-запити по табл. 9.3. Обґрунтуйте зміни в новій таблиці.

7. Виберіть кожен маршрутизатор і перегляньте таблицю маршрутизації. Переконайтеся, що таблиці маршрутизації мають відомості про всі мережі та занотуйте їх у звіт.

Крок 4. Перевірка налаштувань EIGRP

1. Проаналізуйте таблицю IP-маршрутизації EIGRP. Команда «show ip route eigrp» (рис. 12.1). Виконує виведення таблиці маршрутизації протоколу EIGRP.

```
Filial#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 8 subnets, 5 masks
D       10.160.0.0/23 [90/2172416] via 10.160.4.97, 00:09:58, Serial0/1/0
D       10.160.2.0/23 [90/2172416] via 10.160.4.97, 00:09:58, Serial0/1/0
D*EX 0.0.0.0/0 [170/2172416] via 10.160.4.97, 00:09:58, Serial0/1/0
```

Рисунок 12.1 – Приклад таблиці маршрутизації EIGRP на Filial

2. На одному з маршрутизаторів введіть команди і вивчіть їх результати.

```
Router#show ip eigrp {interfaces | topology | neighbors | traffic}
```

Команда «show ip eigrp topology» (рис. 12.2) виводить таблицю сусідніх пристроїв EIGRP.

```
Filial#show ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(10.160.4.98)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 0.0.0.0/0, 1 successors, FD is 2172416
         via Rstatic (2172416/5120)
P 10.160.0.0/23, 1 successors, FD is 2172416
         via 10.160.4.97 (2172416/5120), Serial0/1/0
P 10.160.2.0/23, 1 successors, FD is 2172416
         via 10.160.4.97 (2172416/5120), Serial0/1/0
P 10.160.4.0/26, 1 successors, FD is 5120
         via Connected, GigabitEthernet0/0/1
P 10.160.4.64/27, 1 successors, FD is 5120
         via Connected, GigabitEthernet0/0/0
P 10.160.4.96/30, 1 successors, FD is 2169856
         via Connected, Serial0/1/0
```

Рисунок 12.2 – Приклад таблиці сусідніх пристроїв EIGRP на Filial

Команда «show ip eigrp neighbors» (рис. 12.3) виводить відносини суміжності, встановлених із сусідніми маршрутизаторами, які беруть участь у роботі протоколу EIGRP.

```
Filial#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt  Num
0   10.160.4.97     Se0/1/0        11   00:16:50  40     1000  0   20
```

Рисунок 12.3 – Приклад таблиці суміжності пристроїв EIGRP

Команда «show ip eigrp interfaces» (рис. 12.4) надає інформацію про інтерфейси, які беруть участь у роботі протоколу EIGRP та параметри їх взаємодії.

```
Filial#show ip eigrp interfaces
IP-EIGRP interfaces for process 100

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/1/0            1        0/0      1236       0/10          0           0
```

Рисунок 12.4 – Приклад інформації про інтерфейси EIGRP

3. Командою «show ip protocols» (рис. 12.5) перевірте інформацію про активовані протоколи маршрутизації та параметри їх функціонування та оголошені мережі.

```
Filial#show ip protocols

Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.160.4.64/27
    10.160.4.0/26
    10.160.4.96/30
  Passive Interface(s):
    GigabitEthernet0/0/0
    GigabitEthernet0/0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.160.4.97     90            152869429
  Distance: internal 90 external 170
```

Рисунок 12.5 – Приклад параметрів маршрутизації EIGRP та оголошених мереж

12.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– схему логічної топології мережі;

– команди налаштування маршрутів на кожному кроці з поясненнями;

– перевірки досяжності мереж у вигляді табл. 7.1 після виконання кроків 1-3;

– таблиці маршрутизації на кожному маршрутизаторі після кожного кроку виконання лабораторної роботи;

– проект мережі з назвою за правилом *Surname_Group_lab12.pkt* разом зі звітом відправити на перевірку в систему Moodle або на корпоративну поштову скриню викладача.

12.4 Питання для підготовки до захисту лабораторної роботи

1. Яке значення адміністративної дистанції має статичний маршрут?

2. У чому різниця між кодами C, D, S і S*, зазначеними поруч з маршрутами в таблиці маршрутизації?

3. Поясніть термін «шлюз за замовчуванням».

4. Поясніть термін «інверсна маска».

5. Чим динамічна маршрутизація відрізняється від статичної маршрутизації?

13 ЛАБОРАТОРНА РОБОТА №13
НАЛАШТУВАННЯ СТАТИЧНОГО, ДИНАМІЧНОГО NAT ТА PAT

1.4 Мета роботи

Налаштування, застосування та перевірка різних типів перетворення мережних адрес (NAT) на граничному маршрутизаторі мережі організації з внутрішніх IP-адрес в зовнішні публічні адреси.

1.5 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

– типи NAT;
– принцип роботи статичного NAT;
– принцип роботи динамічного NAT;
– налаштування NAT на маршрутизаторах Cisco.

Вихідними даними є побудована мережа в Packet Tracert з лабораторної роботи №12.

Далі виконати наведені кроки.

Крок 1. Розробка NAT відповідно сценарію

Постачальник послуг Інтернету ISP виділив для організації діапазон публічних IP-адрес 209.165.202.128/27. Цей діапазон надає організації 30 публічних IP-адрес. IT-відділ надав наступну інформацію для перетворення наданих IP-адрес (табл. 13.1):

Таблиця 13.1 – Вихідні дані для NAT

Inside local	Inside global	Тип NAT
MultiServer	209.165.202.129	статичний
ServerDNS	209.165.202.130	статичний
LAN1	209.165.202.131-209.165.202.157	NAT
LAN2-LAN4	209.165.202.158	PAT

Крок 2. Налаштування статичної маршрутизації

Статичний маршрут використовується на ділянці від ISP до Central, тоді як маршрут за замовчуванням використовується на ділянці від Central до ISP. Підключення інтернет-провайдера до Інтернету змодельоване loopback-адресом (lo0) маршрутизатора ISP.

1. Видаліть статичний маршрут на ISP до мережі організації, яка приналежить приватній мережі.

2. Створіть статичний маршрут на маршрутизаторі ISP до діапазону виділених публічних IP-адрес 209.165.202.128/27 організації.

```
ISP(config) # ip route 209.165.202.128 255.255.255.224 {IP_Cental
|| out_interface}
```

Крок 3. Налаштування статичного NAT

Статичний NAT задає однозначну відповідність однієї адреси іншій. Іншими словами, при проходженні через маршрутизатор, адреса(и) змінюються на строго задану адресу, один-до-одного. Запис такої трансляції зберігається необмежено довго, поки є рядок в конфігурації.

Згідно табл. 13.1 виконайте статичне перетворення, завдяки чому користувачі зможуть отримати доступ до серверів з Інтернету.

1. Виберіть граничний маршрутизатор Central. Введіть

```
Central(config)#ip nat inside source static IP_MultiServer 209.165.202.129
Central(config)#ip nat inside source static IP_ServerDNS 209.165.202.130
```

2. Налаштуйте всі інтерфейси, підключені до підмереж організації, як внутрішні інтерфейси NAT. Наприклад:

```
Central (config-if)#ip nat inside
```

3. Налаштуйте інтерфейс підключення до ISP як зовнішній інтерфейс NAT.

```
Central(config-if)#ip nat outside
```

Крок 4. Перевірка роботи статичного NAT

1. Відобразіть таблицю статичних перетворень NAT за допомогою команди «show ip nat translations» за заповніть ними табл. 13.2.

Таблиця 13.2 – Перетворення NAT на Central

Protocol	Inside global	Inside local	Outside local	Outside global	Пояснення

2. З командного рядка MultiServer відправте exo-запит на lo0-адрес ISP.

3. Перегляньте таблицю NAT та додайте результат в табл. 13.2.

4. Оскільки статичний NAT налаштований для MultiServer, переконайтеся в успішному проходженні exo-запиту від Admin-PC до серверу через публічну адресу 209.165.202.130.

```
> ping 209.165.202.130
```

5. Перегляньте таблицю NAT та додайте результат в табл. 13.2.

6. Переконайтеся в успішному проходженні exo-запиту від Admin-PC до ServerDNS через публічну адресу 209.165.202.129.

```
ISP > ping 209.165.202.129
```

7. Спробуйте exo-запити від Admin-PC до ServerDNS та MultiServer через внутрішню IP-адресу. Чи успішно виконані запити і чому?

8. Спробуйте exo-запити з командного рядка ПК в мережі LAN1 та інших ПК в підмережах організації на lo0-адрес ISP. Чи успішно виконані запити і чому?

9. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 5. Налаштування динамічного NAT

В динамічному NAT при проходженні через маршрутизатор нова адреса вибирається динамічно з деякого пулу адрес. Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік по цій трансляції відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається.

Налаштуємо трансляцію внутрішніх адрес вузлів в підмережі LAN1 в зовнішні при проходженні трафіку через маршрутизатор Central.

1. Очистіть дані NAT перед додаванням динамічних перетворень.

```
Central# clear ip nat translation *
Central# clear ip nat statistics
```

2. Створіть іменований стандартний список контролю доступом ACL назвою ACL_LAN1, який дозволяє весь трафік від мережі LAN1.

Примітка. ACL керують трафіком, порівнюючи адресу джерела IP-пакетів з адресами, заданими в списку. Маски, використовувані для списків доступу, є зворотними (wildcard-mask) (наприклад, зворотна маска для 255.255.255.0 буде 0.0.0.255).

```
Central(config)# ip access-list standard ACL_LAN1
Central(config-std-nacl)# permit LAN1 wildcard-mask
Central(config-std-nacl)# exit
```

3. Створіть пул з назвою NAT_LAN1 з адрес, вказавши стартову і кінцеву придатних до використання публічних IP-адрес.

```
Central(config)#  ip  nat  pool  NAT_LAN1  209.165.202.131
209.165.202.157 netmask 255.255.255.224
```

4. Створіть трансляцію NAT, зіставши ACL-список ACL_ LAN1 зі пулом зовнішніх адрес NAT_LAN1.

```
Central (config)#ip nat inside source list ACL_LAN1 pool NAT_LAN1
```

Крок 6. Перевірка роботи динамічного NAT

1. З командного рядка **всіх** ПК в мережі LAN1 відправте ехо-запити на lo0-адрес ISP. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet. Відобразіть перетворення NAT на маршрутизаторі Central за допомогою команди «show ip nat translations». Додайте результати в табл. 13.2.

2. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 7. Налаштування NAT з перевантаженням (PAT)

Динамічний NAT з перевантаженням (PAT) працює майже також, як динамічний NAT, але при цьому відбувається трансляція багато-в-один, задіюючи при цьому можливості транспортного рівня.

1. Очистіть дані NAT перед додаванням динамічних перетворень.

```
Central# clear ip nat translation *
Central# clear ip nat statistics (в PT не підтримується)
```

2. Створіть іменований ACL-список назвою ACL_PAT, відповідний IP-адресам мереж LAN2-LAN4.

```
Central(config)# ip access-list standard ACL_PAT
Central(config-std-nacl)# permit LAN2 wildcard-mask
Central(config-std-nacl)# permit LAN3 wildcard-mask
Central(config-std-nacl)# permit LAN4 wildcard-mask
```

3. Визначте пул PUBLIC_PAT придатних до використання публічних IP-адрес.

```
Central(config)# ip nat pool PUBLIC_PAT 209.165.202.158
209.165.202.158 netmask 255.255.255.224
```

4. Створіть трансляцію NAT, зіставши ACL-список ACL_PAT з пулом зовнішніх адрес PUBLIC_PAT з параметром overload.

```
Central (config)#ip nat inside source list ACL_PAT pool
PUBLIC_PAT overload
```

Крок 8. Перевірка роботи PAT

1. З командного рядка ПК в кожній із мереж LAN2-LAN4 відправте ехо-запити на lo0-адрес ISP. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet. Відобразіть перетворення NAT на маршрутизаторі Central за допомогою команди «show ip nat translations». Додайте результати в табл. 13.2.

2. Перевірте статистику PAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

13.2 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– табл. 13.1 з вихідними даними для NAT;

– табл. 13.2 з перетвореннями NAT та поясненнями;

– статистика роботи кожного типу NAT з відповідями на запитання;

– звіт та проект мережі з назвою за правилом *Surname_Group_NAT.pkt* відправити разом зі звітом в систему Moodle або на корпоративну поштову скриню викладача.

1.6 Питання для підготовки до захисту лабораторної роботи

1. У чому полягає перевага статичного NAT?

2. Навіщо потрібно використовувати NAT в мережі?

3. Які обмеження динамічного NAT?

4. Коли вузол повертає зовнішній глобальний адрес назад в пул для використання іншим вузлом?

5. У чому полягає перевага PAT?

2 ЛАБОРАТОРНА РОБОТА № 14
НАЛАШТУВАННЯ НА КОМУТАТОРАХ ФУНКЦІЇ SWITCH PORT SECURITY

2.1 Мета лабораторної роботи

Налаштувати і перевірити роботу функції безпеки порту, спрямовану на блокування будь-якого пристрою з MAC-адресом, який невідомий комутатору.

2.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

– технологія Switchport Port Security на комутаторах Cisco.

Вихідними даними є побудована мережа в Packet Tracert з лабораторної роботи №13.

Далі виконати наведені кроки.

Крок 1. Планування впровадження Port Security

Розробіть функцію безпеки портів на комутаторах в мережі LAN1 відповідно до наступного плану:

а) на порту, до якого приєднаний MultiServer:
   – кількість дозволених MAC-адрес: 1;
   – призначення MAC-адрес: статично;
   – режим реагування при порушенні безпеки: restrict.

б) на портах, до яких приєднані користувачі:
   – кількість дозволених MAC-адрес: 1;
   – призначення MAC-адрес: динамічно;
   – режим реагування при порушенні безпеки: shutdown.

в) всі невикористовувані порти відключити.

Крок 2. Налаштування функції безпеки портів

Функція безпеки порту дозволяє обмежити вхідний трафік порту за рахунок обмеження числа MAC-адрес, які можуть використовуватися для відправки трафіку через цей порт.

1. Налаштуйте всі порти в режим доступу.

```
Switch(config)# interface range інтерфейси
Switch(config-if-range)# switchport mode access
```

2. Перейдіть в командний рядок комутатора в мережі LAN1 і ввімкніть функцію безпеки на порту, до якого приєднаний MultiServer.

```
Switch(config)# interface інтерфейс
Switch(config-if)# switchport port-security
```

3. Вкажіть лише один пристрій як максимум для доступу до цього порту.

```
Switch(config-if)# switchport port-security maximum 1
```

4. Призначте MAC-адрес MultiServer статично.

```
Switch(config-if)# switchport port-security mac-address MAC-адрес
```

5. Налаштуйте рівень порушення безпеки так, щоб в разі атаки порт залишався включеними, а пакети, що поступають від невідомих джерел, відкидалися.

```
Switch(config-ifя# switchport port-security violation restrict
```

6. На портах, до яких під'єднанні користувачі, виконати відповідні налаштування функції безпеки портів.

7. Відключити всі невикористовувані порти.

Крок 3. Перевірка функції безпеки портів

1. Виконайте ехо-запити між вузлами в мережі LAN1 та MultiServer.

2. Перевірте, чи включена функція безпеки портів, і чи були додані MAC-адреси вузлів в поточну конфігурацію.

3. Підключить комп'ютер зловмисника (наприклад, Laptop) до будь-якого невикористовуваного порту комутатора і зверніть увагу на індикатори стану каналу.

4. Включить порт і переконайтесь, що стороннє підключення може відправляти ехо-запити на вузли в локальній мережі. Після перевірки вимкніть порт, використовуваний стороннім підключенням.

5. Відключить будь-який ПК і підключить стороннє підключення до порту цього ПК.

8. Надішліть ехо-запити від стороннього підключення на вузли в локальній мережі і переконайтесь, що порт відключився.

6. Відобразіть порушення безпеки заблокованого порту.

```
Switch # show port-security interface інтерфейс
```

9. Відключить стороннє підключення, знову підключить ПК і включіть заблокований порт. Тепер ПК може відправляти ехо-запити на вузли в локальній мережі.

10. Відключить MultiServer і підключить стороннє підключення до порту сервера. Переконайтесь, що стороннє підключення не може відправляти ехо-запити на вузли в мережі.

6. Відобразіть порушення безпеки порту, підключеного до стороннього підключення.

11. Відключить стороннє підключення і знову підключить MultiServer. Тепер MultiServer може відправляти ехо-запити на вузли в локальній мережі.

13.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– план впровадження безпеки портів і його реалізація;

– перевірка роботи функції безпеки портів з поясненнями;

– проект мережі з назвою за правилом *Surname_Group_PortSec.pkt* відправити разом зі звітом в систему Moodle або на корпоративну поштову скриню викладача.

2.3 Питання для підготовки до захисту лабораторної роботи

12. Чому вузли можуть відправляти ехо-запити один одному, а стороннє підключення ні?
13. Які режими реагування можуть бути налаштовані на порушення безпеки?
14. Які налаштування за замовчуванням для функції Port Security?
15. Як очистити таблицю MAC-адрес, для підключення інших пристроїв?
16. З якими функціями комутатора несумісна функція Port Security?

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Cisco Networking Academy: Learn Cybersecurity, Python & More. *Networking Academy*. URL: https://www.netacad.com (date of access: 15.01.2024).

2. Комп'ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. – Вінниця : ВНТУ, 2020. – 378 с.

3. Жураковський Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36615.

4. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36641

5. Wireshark · Go Deep. *Wireshark*. URL: https://www.wireshark.org/ (date of access: 15.01.2024).

6. CIDR/VLSM Calculator - subnettingpractice.com. *subnettingpractice.com*. URL: https://subnettingpractice.com/vlsm.html (date of access: 15.01.2024).

ДОДАТОК А

Мережні та діагностичні команди Windows

Команда	Опис
arp	Вивід і редагування таблиці трансляції IP-адрес в фізичні з використанням протоколу дозволу адрес (ARP).
getmac	Вивід MAC-адрес мережних адаптерів комп'ютера. Команда «getmac» може використовуватися для отримання інформації про MAC-адреси віддаленого комп'ютера в мережі, проте необхідно щоб користувач мав право доступу.
ftp	Обмін файлами з комп'ютером, на якому запущена служба сервера FTP.
hostname	Вивід мережної назви комп'ютера. Ця команда доступна тільки після установки підтримки протоколу TCP/IP.
ipconfig	Вивід всіх поточних налаштувань TCP/IP на комп'ютері і поновлення параметрів DHCP і DNS. При виклику команди «ipconfig» без параметрів виводяться IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера.
nbtstat	Засіб діагностики розпізнавання імен NetBIOS. Вивід статистики протоколу і поточних підключень TCP/IP за допомогою NBT (NetBIOS через TCP/IP).
netstat	Вивід стану TCP-з'єднань та портів, що прослуховуються комп'ютером. Крім цього виводить статистику Ethernet, таблиці маршрутизації, статистику IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP через IPv6 і UDP через IPv6).
nslookup	Діагностична команда для виведення відомостей в базі даних DNS-сервера, які відносяться до вузла або домену.
netsh	Найбільш повна і функціональна команда для керування конфігурацією різних мережних служб на локальному або віддалених комп'ютерах з використанням командного рядка. Можливості «netsh» настільки великі, що важко знайти мережне завдання, яке неможливо було б вирішити за допомогою цієї команди.
ping	Перевірка з'єднань в мережах на основі TCP/IP та служби перетворення імен DNS.
Tracer	Діагностична команда, призначена для визначення маршруту IP-пакетів до точки призначення за допомогою echo-повідомлень протоколу ICMP (Internet Control Message Protocol) та повідомляє час, необхідний для досягнення кожного вузла по шляху до заданого вузла.
pathping	Засіб визначення маршруту, що поєднує функції команд «ping» і «Tracer». Ця команда показує ступінь втрати пакетів на будь-якому маршрутизаторі або каналі та дозволяє визначити, які маршрутизатори або канали викликають неполадки в роботі мережі.
route	Вивід та зміна таблиці маршрутизації на комп'ютері.
net	Управління налаштуваннями мережі в командному рядку Windows. Синтаксис наведено в Додатку В.

ДОДАТОК Б

Розрахунок пропускної здатності мережі Fast Ethernet

Виконаємо розрахунки пропускної здатності мережі Fast Ethernet для кадру з мінімально (N_{dmin}=46 байт) та максимальною довжиною (N_{dmax}=1500 байт) поля даних в кадрі.

Розмір кадру в байтах визначають за формулою:

$$N_k = N_s + N_d$$

де N_s – службова інформація кадру Fast Ethernet разом з преамбулою, байт; N_s = 26 байт;

N_d– розмір поля даних кадру.

Розмір мінімального і максимального кадру в байтах:

$$N_{kmin} = 26 + 46 = 72 \text{ (байт)}$$
$$N_{kmax} = 1500+26 = 1526 \text{ (байт)}$$

Так як один байт дорівнює восьми бітам, мінімальний і максимальний розмір кадру в бітах:

$$N_{kmin} = 72*8 = 576 \text{ (біт)}$$
$$N_{kmax} = 1526*8 = 12208 \text{ (біт)}$$

Пропускну здатність Fast Ethernet визначають за формулою:

$$N_{ps} = N_1 * N_2 * K \text{ (біт)}$$

де N_1 - кількість біт в одному кілобіті; N_1 = 1024;

N_2 - кількість кілобіт в одному мегабіті; N_2= 1024;

K - коефіцієнт швидкості передачі даних; K = 100.

$$N_{ps} = 1024 * 1024 * 100 = 104857600 \text{ (біт)}$$

Якщо врахувати міжкадровий інтервал, то отримаємо довжину проходження кадрів:

$$L_k = N_{mi} + N_k$$

де N_{mi} – міжкадровий інтервал; N_{mi} = 96 біт;

N_k – розмір кадру разом з службовою інформацією.

Тоді період проходження кадрів мінімальної і максимальної довжини:

$$L_{kmin} = 576 + 96 = 672 \text{ (біт)}$$
$$L_{kmax} = 12208 + 96 = 12604 \text{ (біт)}$$

Тоді час проходження кадрів можна визначити за формулою:

$$T = \frac{L_k}{N_{ps}} * K_{mks}$$

де L_k – довжину проходження кадрів, біт;

N_{ps} – пропускна здатність Fast Ethernet, біт;

K_{mks} – кількість мікросекунд в одній секунді; $K_{mks} = 10^6$;

Час проходження мінімального і максимального кадрів:

$$T_{min} = \frac{672}{104857600} * 10^6 = 6{,}4 \text{(мкс)}$$
$$T_{max} = \frac{12604}{104857600} * 10^6 = 117{,}6 \text{(мкс)}$$

Частоту слідування кадрів, тобто кількість кадрів, що проходять по мережі за 1 секунду можна визначити за формулою:

$$F = \frac{N_{ps}}{L_k}, \text{ (кадр/с)}$$

Отримуємо частоту слідування кадрів при мінімальному і максимальному розмірі кадру:

$$F_{min} = \frac{104857600}{672} = 156038 \text{ (кадр/с)}$$

$$F_{max} = \frac{104857600}{12604} = 8522 \text{ (кадр/с)}$$

Знаючи частоту проходження кадрів F і розмір поля даних кадру N_d в байтах можна розрахувати корисну пропускну здатність мережі:

$$P = F * N_d * 8, \text{ (біт/с)}$$

$$P_{min} = F_{min} * L_{kmin} * 8 = 156038 * 46 * 8 = 57421984, \text{ (біт/с)}$$

$$P_{max} = F_{max} * L_{kmax} * 8 = 8522 * 1500 * 8 = 102264000, \text{ (біт/с)}$$

Або в Мбіт/с:

$$P = \frac{P}{N_1 * N_2} \text{ (Мбіт/с)}$$

де N_1 - кількість біт в одному кілобіті; N_1 = 1024;

N_2 - кількість кілобіт в одному мегабіті; N_2= 1024;

$$P_{min} = \frac{57421984}{1024*1024} = 54.76 \text{ (Мбіт/с)}$$

$$P_{max} = \frac{102264000}{1024*1024} = 97.52 \text{ (Мбіт/с)}$$

Навчальне видання

Каштан Віта Юріївна
Панферова Яна Володимирівна
Зарічний Володимир Сергійович

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
спеціальності 126 Інформаційні системи та технології

Видано в авторській редакції.

Електронний ресурс.
Підписано до видання 12.11.2024. Авт. арк. 6,2.

Національний технічний університет «Дніпровська політехніка».
49005, м. Дніпро, просп. Дмитра Яворницького, 19.