МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Юглічек Олександр Васильович

Засоби захисту комп'ютерної мережі з використанням обладнання Cisco/ Computer network security tools based on Cisco mains

напрям підготовки: 123 Комп’ютерна інженерія
фахове спрямування - Комп’ютерна інженерія
Бакалаврська робота

Виконав студент групи КСМ-43/2
Олександр Васильович Юглічек

Науковий керівник:
Вербовий С.О.

Тернопіль - 2018

РЕЗЮМЕ

Дипломний проект містить 73 сторінок пояснюючої записки, 14 рисунків, 12 таблиць та 2 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою проекту є впровадження засобів захисту комп'ютерної мережі з використанням обладнання Cisco.

Проаналізовано основні загрози комп’ютерних мереж. Проаналізовано основні способи забезпечення надійності комп’ютерних мереж.

Здійснено вибір апаратного забезпечення.

Здійснено розробку структури мережі. В результаті було створено логічну структуру мережі підприємства, а також змодельовано мережу на основі технології IP.

Забезпечено захист даних на комутаторі та захист безпровідної мережі.

Проведено моделювання комп’ютерної мережі в сережовищі Cisco Packet Tracer. Перевірено роботу робочих станцій за допомогою консольної утиліти “ping”: зв'язок між ними в межах однієї підмережі, зв'язок із ПК з іншої підмережі, зв'язок між ПК та ноутбуками. Таким чином перевірялись і правильність налаштування портів маршрутизаторів та комутаторів. Останнім етапом тестування зроблено перевірку коректної роботи

Ключові слова: МЕРЕЖА, IPv4, IP, ПРОТОКОЛ, ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ.

RESUME

The diploma project contains 73 pages of explanatory note, 14 figures, 12 tables and 2 appendices. Volume of graphic material 2 sheets of A3 format.

The aim of the project is to implement computer network security tools using Cisco equipment.

The main threats of computer networks are analyzed. The main ways to ensure the reliability of computer networks are analyzed.

Hardware selection made.

The network structure has been developed. As a result, a logical structure of the enterprise network was created, as well as a network based on IP technology was modeled.

Data protection on the switch and protection of the wireless network are provided.

Computer network simulation in Cisco Packet Tracer was performed. Workstations have been tested using the ping console utility: communication between them within one subnet, communication with a PC from another subnet, communication between a PC and laptops. In this way, the correctness of the routers and switches ports was checked. The last stage of testing is to check the correct operation

Keywords: NETWORK, IPv4, IP, PROTOCOL, SECURITY.

ЗМІСТ

					ДП.КСМ. 07262/16.00.00.000 ПЗ		
Змн.	Лист	№ докум.	Підпис	Дата			
Розробив		Юглічек.О.В			ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ CISCO	Літ.	Арк. 8 / Акрушів 60
Перевір.		Вербовий С.О.					
Консульт.		Паздрій І.Р.				ТНЕУ. ФКІТ. КСМ-43/2	
Н. Контр.		Гураль І.В.					
Затвердив		Березький О.М					

ВСТУП

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють наступні рівні:

1) фізичний;

2) програмно-технічний;

3) управлінський;

4) технологічний;

5) рівень користувача;

6) мережевий;

7) процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Для виконання дипломного проекту необхідно вирішити наступні завдання:

– Проаналізувати основні загрози комп’ютерних мереж.

– Проаналізувати основні способи забезпечення надійності комп’ютерних мереж.

– Здійснити вибір апаратного забезпечення.

– Забезпечити захист даних на комутаторі та захист безпровідної мережі.

– Провести моделювання комп’ютерної мережі в сережовищі Cisco Packet Tracer.

1 АНАЛІЗ КОРПОРАТИВНИХ МЕРЕЖ

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам. Залежно від масштабу підприємства, а також від складності і різноманіття вирішуваних завдань розрізняють мережі відділу, мережі кампусу і корпоративні мережі (термін «корпоративні» в даній класифікації набуває вузького значення — мережу великого підприємства).

Користувачем корпоративної мережі повинен бути тільки співробітник компанії. На відміну від транспортних мереж, мереж компанії зазвичай не доступні для інших користувачів або груп.

Концепція корпоративної мережі.

Будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи зв'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес процесу, а також інформаційно, обмінюючись документами, факсами, письмовими і усними розпорядженнями і так далі крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і так далі.

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації.

Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також

сервісні застосування, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення і звукозаписи), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються “Службами Інтернету” незалежно від того, де вони використовуються (у Інтернеті або корпоративній мережі).

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи і інші структури, що знаходяться на значному віддаленні один від одного. Принципи, по яких будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні.

Процес створення корпоративної інформаційної системи.

Можна виділити основні етапи процесу створення корпоративної інформаційної системи:

– провести інформаційне обстеження організації;

– за результатами обстеження вибрати архітектуру системи і апаратно-програмні засоби її реалізації;

– за результатами обстеження вибрати і/або розробити ключові компоненти інформаційної системи.

Для корпоративних систем рекомендується архітектура клієнт/сервер. Архітектура клієнт/сервер надає технологію доступу кінцевого користувача до інформації в масштабах підприємства. Таким чином, архітектура клієнт/сервер дозволяє створити єдиний інформаційний простір, в якому кінцевий користувач має своєчасний і безперешкодний (але санкціонований) доступ до корпоративної інформації.

Вибір СУБД. Вибір системи управління для корпоративної бази даних - один з ключових моментів в розробці інформаційної системи. На Російському ринку присутні практично всі СУБД, що належать до елітного класу - Oracle, Informix, Sybase, Ingres. Питання, яку СУБД використовувати, можна вирішити тільки за результатами попереднього обстеження і отримання інформаційних моделей діяльності.

1.1 Мережі відділів

Мережі відділів це мережі, які використовуються порівняно невеликою групою співробітників, працюючих в одному відділі підприємства. Ці співробітники вирішують деякі загальні задачі, наприклад ведуть бухгалтерський облік або займаються маркетингом. Вважається, що відділ може нараховувати до 100-150 співробітників. Головною метою мережі відділу є розділення локальних ресурсів, таких як додатки, дані, принтери і модеми. Звичайно мережі відділів мають один або два файлових сервери і не більш тридцять користувачів (рисунок 1.1). Мережі відділів звичайно не розділяються на підмережі. У цих мережах локалізується велика частина трафіка підприємства. Мережі відділів звичайно створюються на основі якої-небудь однієї мережевої технології Ethernet, Token Ring. Для такої мережі характерний один або, максимум, два типи операційних систем. Частіше за все це мережа з виділеним сервером, наприклад NetWare, хоч невелика кількість користувачів робить можливою використання однорангових мережевих ОС.

Задачі управління мережею на рівні відділу відносно прості: включення нових користувачів, усунення простих відмов, інсталяція нових вузлів і установка нових версій програмного забезпечення. Такою мережею може управляти співробітник, що присвячує обов'язкам адміністратора тільки частину свого часу. Частіше за все адміністратор мережі відділу не має спеціальної підготовки, але є тією людиною у відділі, який краще за всіх

розбирається в комп'ютерах, і само собою виходить так, що він займається адмініструванням мережі.

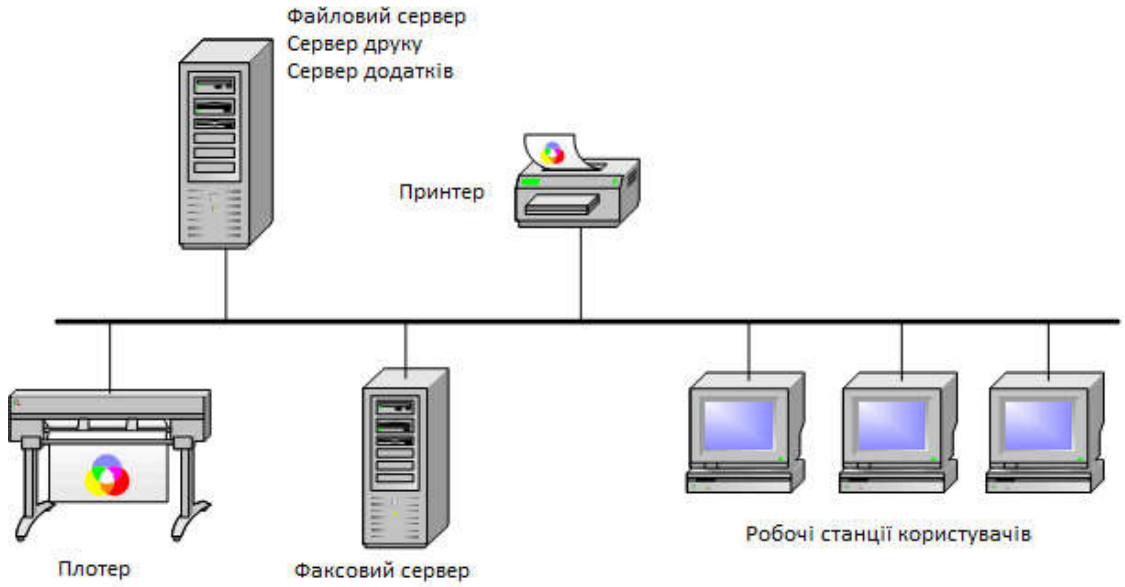


Рисунок 1.1 - Приклад мережі масштабу відділу

Існує і інший тип мереж, близький до мереж відділів, мережі робочих груп. До таких мереж відносять зовсім невеликі мережі, що включають до 10-20 комп'ютерів. Характеристики мереж робочих груп практично не відрізняються від описаних вище характеристик мереж відділів. Такі властивості, як простота мережі і однорідність, тут виявляються в найбільшій мірі, в той час як мережі відділів можуть наближатися в деяких випадках до наступного за масштабом типу мереж мережам кампусів.

1.2 Мережі кампусів

Мережі кампусів отримали свою назву від англійського слова campus студентське містечко. Саме на території університетських містечок часто виникала необхідність об'єднання декількох дрібних мереж в одну велику

мережу. Зараз цю назву не зв'язують зі студентськими містечками, а використовують для позначення мереж будь-яких підприємств і організацій.

Основні особливостімереж кампусів представлені на рисунку 1.2. Мережі цього типу об'єднують безліч мереж різних відділів одного підприємства в межах окремої будівлі або в межах однієї території, що покриває площу в декілька квадратних кілометрів.

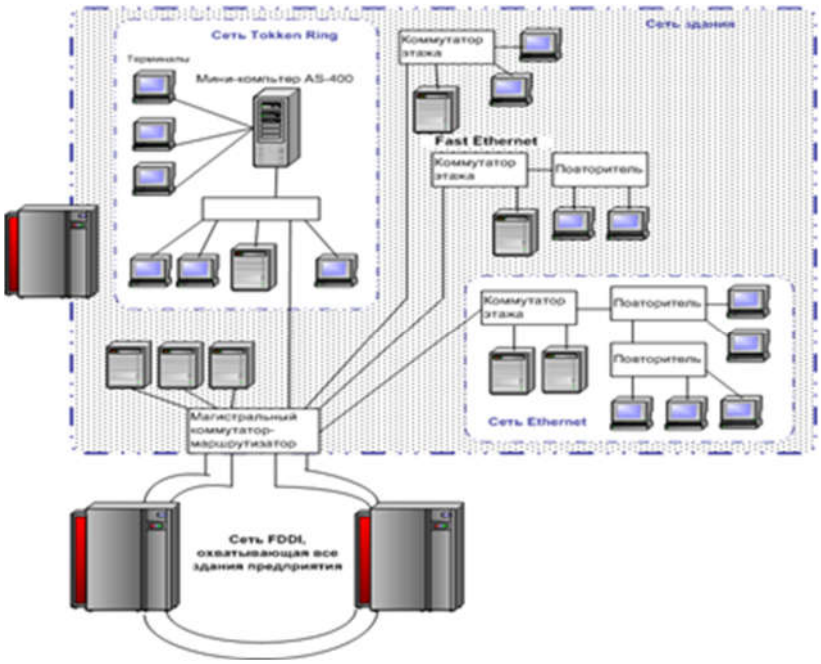


Рисунок 1.2 - Приклад мережі масштабу кампусу

При цьому глобальні з'єднання в мережах кампусів не використовуються. Служби такої мережі включають взаємодію між мережами відділів, доступ до загальних баз даних підприємства, доступ до загальних факсу-серверів, високошвидкісних модемів і високошвидкісних принтерів. У результаті співробітники кожного відділу підприємства отримують доступ до деяких файлів і ресурсів мереж інших відділів. Важливою службою, що надається мережами кампусів, став доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів вони розташовуються.

Саме на рівні мережі кампуса виникають проблеми інтеграції неоднорідного апаратного і програмного забезпечення. Типи комп'ютерів, мережевих операційних систем, мережевого апаратного забезпечення можуть

відрізнятися в кожному відділі. Звідси витікають складності управління мережами кампусів. Адміністратори повинні бути в цьому випадку більш кваліфікованими, а засоби оперативного управління мережею більш довершеними.

1.3 Основні поняття і аналіз загроз

Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям “інформація”. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям:

Інформація – нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення.

Інформація – це відомості, які є об’єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп’ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Відповідно до різноманітності поняття інформації, словосполучення “інформаційна безпека” в різних контекстах може мати різний сенс. Так, у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що

використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону “Про інформацію, інформатизацію і захист інформації”, що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

– інформації та інформаційних систем;

– суб’єктів – учасників інформаційних процесів;

– правовідносин виробників – споживачів інформаційної продукції;

– власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб’єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури.

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб’єктів інформаційних відносин та інтересів цих суб'єктів, пов’язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій.

Тут необхідно зауважити, що трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно різнитися. Для ілюстрації досить зіставити режимні державні організації і навчальні заклади. У першому випадку “хай краще все зламається, ніж ворог дізнається хоч один секретний біт”, у другому – “немає у нас жодних секретів, аби все працювало”. Отже, інформаційна безпека не зводиться виключно до

захисту від несанкціонованого доступу до інформації, це поняття принципово ширше.

Суб’єкт інформаційних відносин може постраждати (зазнати збитки та/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій власне захист від несанкціонованого доступу до інформації стоїть за важливістю зовсім не на першому місці.

1.4 Загрози уразливості корпоративних і безпровідних мереж

Загроза — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза — це будь-який потенційно можливий несприятливий вплив.

Некоректна реалізація комп'ютерною інформаційною системою функцій, запланованих її автором чи власником, часто призводить до збитків і трагедій. Прикладами є втрата зонду NASA "Марінер-1" у 1962році через помилку у коді [5], написаному на мові Фортран, чи смертельні випадки серед пацієнтів через вади програмного забезпечення апаратів для радіотерапії Therac-25 у 80-х роках.

Із появою модемного зв'язку, глобальних мереж й Інтернету загрозу почала становити несанкціонована взаємодія із системою третіх осіб, хоча при цьому система може функціонувати у відповідності до намірів та очікувань її авторів та власників. Сценарії, що можуть призвести до несанкціонованого використання системи, можна класифікувати за їхнім походженням.

До можливих загроз безпеці інформації відносять:

– стихійні лиха й аварії;

– збої та відмови устаткування;

– наслідки помилок проектування і розроблення компонентів автоматизованих систем (надалі АС);

– помилки персоналу під час експлуатації;

– навмисні дії зловмисників і порушників.

Помилки реалізації. До цієї групи належать технічні помилки, яких програмісти припускаються через свою недостатню обізнаність або неуважність. Прикладом є недостатня перевірка параметрів або результатів системних викликів, що може призвести до таких вразливостей, як переповнення буфера, невміле застосування функції *printf() чи цілочисельне переповнення. Поширеним результатом помилок реалізації є можливість одержання повного контролю над процесом особою, що не має відповідних прав, чи можливість безпосередньої взаємодії з операційною системою.

Класифікацію загроз за ознаками наведено в таблиці 1.1.

Таблиця 1.1 — Класифікація загроз за ознаками

Ознака класифікації	Причини, спрямованість, характеристики загроз
Природа виникнення	Природні загрози (виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (викликані діяльністю людини)
Принцип несанкціонованого доступу (НСД)	Фізичний доступ: – подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; – розкрадання документів і носіїв інформації; – візуальне перехоплення інформації, виведеної на екрани моніторів і принтери; – підслуховування; – перехоплення електромагнітних випромінювань. Логічний доступ (доступ із використанням засобів комп'ютерної системи)

Продовження таблиці 1.1

Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні).
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження).
Режим НСД	За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ.
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки — санкціонований користувач. Міжсегментне: – несанкціоноване вторгнення з відкритої мережі в закриту; – порушення обмежень доступу з одного сегмента закритої мережі в інший.
Наявність зворотнього зв'язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив). Без зворотного зв'язку (атакуючий не отримує відповіді).

Для кращого розуміння методів захисту комп'ютерної системи слід спочатку ознайомитися з типами атак, які можуть бути здійснені проти неї. Такі небезпеки зазвичай можна віднести до однієї з наступних категорій.

– Чорний хід (бекдор).

Чорний хід, або бекдор у комп'ютерній системі, криптосистемі чи алгоритмі — це метод обходу звичайного процесу аутентифікації, забезпечення

віддаленого доступу до комп'ютера, одержання доступу до незашифрованої інформації тощо.

Бекдори можуть відбуватися у формі встановлення програми (наприклад, Back Orifice) або змін у роботі існуючої програми чи фізичного пристрою.

– DoS-атака.

На відміну від інших атак, DoS-атаки застосовуються не для одержання несанкціонованого доступу чи керування системою, а для того, щоб унеможливити роботу останньої. В результаті атаки акаунт окремої жертви може виявитися заблокованим унаслідок умисного багаторазового введення невірного пароля, або ж унаслідок перевантаження мережі буде заблоковано усіх її користувачів. На практиці цьому виду атак дуже складно перешкодити, оскільки для цього необхідно проаналізувати поведінку цілих мереж, а не лише поведінку невеличкої частини коду.

1.5 Способи забезпечення інформаційної безпеки

При побудові бездротових мереж однією з найбільш гострих проблем є забезпечення їх безпеки. Якщо в звичайних мережах інформація передається по дротах, то радіохвилі, які використовуються для бездротових рішень, досить легко перехопити при наявності відповідного обладнання. Принцип дії бездротової мережі призводить до виникнення великої кількості можливих вразливостей для атак і проникнень.

Обладнання бездротових локальних мереж WLAN (Wireless Local Area Network) включає в себе точки бездротового доступу і робочі станції для кожного абонента.

Точки доступу AP (Access Point) виконують роль концентраторів, які забезпечують зв'язок між абонентами і між собою, а також функцію мостів, які здійснюють зв'язок з кабельною локальною мережею і з Інтернетом. Кожна точка доступу може обслуговувати кілька абонентів. Кілька близько

розташованих точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, забезпечені бездротовими адаптерами, отримують доступ до мережі. Такі зони доступу створюються в місцях масового скупчення людей: в аеропортах, студентських містечках, бібліотеках, магазинах, бізнес-центрах і т. д.

У точки доступу є ідентифікатор набору сервісів SSID (Service Network Idetnifier). SSID - це 32-бітна рядок, що використовується в якості імені бездротової мережі, з якої асоціюються всі вузли. Ідентифікатор SSID необхідний для підключення робочої станції до мережі. Щоб зв'язати робочу станцію з точкою доступу, обидві системи повинні мати один і той же SSID. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися з точкою доступу і з’єднався з мережею.

Головна відмінність між провідними і бездротовими мережами пов'язано з наявністю неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротових структур, виробляти цілий ряд нападів, які неможливі в дротовому світі.

При використанні бездротового доступу до локальної мережі загрози безпеки істотно зростають. Перелічимо основні вразливості і загрози бездротових мереж.

Мовлення радіомаяка. Точка доступу включає з певною частотою широкомовний "радіомаяк", щоб оповіщати навколишні бездротові вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку бездротового доступу, включаючи, як правило, SSID, і запрошують зареєструватися бездротові вузли в даній області. Будь-яка робоча станція, що знаходиться в режимі очікування, може отримати SSID і додати себе в відповідну мережу. Мовлення радіомаяка є вродженою патологією бездротових мереж. Багато моделей дозволяють відключати SSID частину цього мовлення, щоб запобігти бездротове підслуховування, але SSID посилається при підключенні, тому все одно існує невелике вікно уразливості.

Виявлення WLAN. Для виявлення бездротових мереж WLAN

використовується, наприклад, утиліта NetStumber спільно з супутниковим навігатором глобальної системи позиціонування GPS. Дана утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері уможливлює виявлення мереж WLAN під час обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером в руках.

Підслуховування. Підслуховування ведуть для збору інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Обладнання, що використовується для підслуховування в мережі, може бути не складніше того, яке застосовується для звичайного доступу до цієї мережі. Бездротові мережі за своєю природою дозволяють з'єднуватись з фізичної мережею комп'ютерів, які знаходилися безпосередньо в мережі. Це дозволяє підключиться до бездротової мережі, розташованій в будівлі, людині, що сидить в машині на стоянці поруч з ним. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Помилкові точки доступу в мережу. Досвідчений атакуючий може організувати неправдиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад аутентифікаційну інформацію. Цей тип атак іноді застосовують в поєднанні з прямим глушінням, щоб заглушити справжню точку доступу в мережу.

Відмова в обслуговуванні. Повну паралізацію мережі може викликати атака типу "відмова в обслуговуванні" (Dos). Мета будь-якої DoS-атаки полягає в створенні перешкоди при доступі користувача до мережевих ресурсів. Бездротові системи особливо сприйнятливі до таких атак. Фізичний рівень в бездротової мережі - абстрактний простір навколо точки доступу. Зловмисник може включити пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком, - таке завдання не викликає особливих труднощів. Сам факт проведення DoS-атаки на фізичному рівні в бездротової

мережі важко довести.

Атаки типу "людина-в-середині". Атаки типу "людина-в-середині" виконуються на бездротових мережах набагато простіше, ніж на провідних, так як до провідної мережі потрібно реалізувати певний вид доступу. Зазвичай атаки "людина-в-середині" використовуються для порушення конфіденційності і цілісності сеансу зв'язку. Атаки "людина-в-середині" більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Зловмисник використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад спуфінгу IP-адрес, зміни MAC-адреси для імітування іншого хоста і т.д.

Анонімний доступ в Інтернет. Незахищені бездротові ЛОМ (локальні обчислювальні мережі) забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використовувати незахищену мережу WLAN організації для виходу через неї в Інтернет, де вони будуть здійснювати протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною ЛОМ формально стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяну шкоду жертві атаки хакерів.

Атаки, які використовуються хакерами для злому безпровідних мереж, не обмежуються описаними вище.

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз,

так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють наступні рівні:

1) фізичний;

2) програмно-технічний;

3) управлінський;

4) технологічний;

5) рівень користувача;

6) мережевий;

7) процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

На жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління інформаційною безпекою, не на достатньому рівні проводиться підготовка відповідних фахівців для системи управління НБ.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Для пошуку рішень проблем інформаційної безпеки при роботі у мережі Інтернет був створений незалежний консорціум ISTF (Internet Security Task Force) – громадська організація, що складається з представників і експертів компаній-постачальників засобів інформаційної безпеки, електронного бізнесу і провайдерів інтернет- інфраструктури. Ціль цього консорціуму – розробка технічних, організаційних і операційних посібників з безпеки діяльності в Інтернеті.

Консорціум ISTF виділив дванадцять областей інформаційної безпеки, на яких в першу чергу повинні сконцентрувати свою увагу творці електронного бізнесу, щоб забезпечити його працездатність. Цей список, зокрема, включає

наступні пункти: автентифікація (механізм об’єктивного підтвердження ідентифікуючої інформації), право на приватну, персональну інформацію (забезпечення конфіденційності інформації), визначення подій безпеки (Security Events), захист корпоративного периметру, визначення атак, контроль за потенційно небезпечним вмістом (Malicious Content), контроль доступу, адміністрування, реакція на події.

Рекомендації ISTF призначені для існуючих або знову утворених компаній електронної комерції та електронного бізнесу. Ці рекомендації допомагають визначити потенційні проломи в їх комп'ютерних мережах, які, якщо не звернути на них належної уваги, можуть використовуватися хакерами. Це може привести до атак на систему електронної комерції, збитків і навіть до краху електронного бізнесу. Консорціум ISTF настійно рекомендував скористатися його напрацюваннями ще до початку організації компанії, має намір зайнятися електронною комерцією і бізнесом.

Реалізація рекомендацій консорціуму ISTF означає, що захист інформації в системі електронного бізнесу повинна бути комплексною.

Згідно з рекомендаціями ISTF і класифікації «рубіжів захисту» Hurwitz Group першим і найважливішим етапом розробки системи інформаційної безпеки електронного бізнесу є механізми управління доступом до мереж загального користування та з них, а також механізми безпечних комунікацій, реалізовані між мережевими екранами і продуктами приватних захищених віртуальних мереж (VPN).

Супроводжуючи їх засобами інтеграції і управління всією ключовий інформацією системи захисту (PKI - інфраструктура відкритих ключів), можна отримати цілісну, централізовано керовану систему інформаційної безпеки.

Наступний рубіж включає в себе інтегровані в загальну структуру засоби контролю доступу користувачів в систему разом з системою одноразового входу і авторизації (Single Sign-On).

Антивірусний захист, засоби аудиту та запобігання атак, по суті, завершують створення інтегрованої цілісної системи безпеки, якщо мова не йде про роботу з конфіденційними даними.

Застосування комплексу засобів захисту на всіх рівнях корпоративної системи дозволяє побудувати ефективну і надійну систему забезпечення інформаційної безпеки.

1.6 Постановка задачі

Для виконання дипломного проекту необхідно вирішити наступні завдання:

- Проаналізувати основні загрози комп’ютерних мереж.
- Проаналізувати основні способи забезпечення надійності комп’ютерних мереж.
- Здійснити вибір апаратного забезпечення.
- Забезпечити захист даних на комутаторі та захист безпровідної мережі.
- Провести моделювання комп’ютерної мережі в сережовищі Cisco Packet Tracer.

2 ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Вибір апаратного забезпечення

CISCO 2811 — маршрутизатор для потреб невеликих підприємств, офісів і філіалів (до 36 робочих місць).

В таблиці 2.1 показані технічні характеристики маршрутизатора Cisco 2811.

Таблиця 2.1 — Технічні характеристики маршрутизатора Cisco 2811

Характеристики	Опис
Загальне	
Тип приладу	Маршрутизатор
Форм-фактор	Зовнішній - modular - 1U
Ширина	43.82 cm
Глибина	41.66 cm
Висота	4.45 cm
Вага	6.4 kg
Пам'ять	
RAM	256 MB (встановлено) / 760 MB (максимально) - DDR SDRAM
Флеш-пам'ять	64 MB (встановлено) / 256 MB (максимально)
Параметри мережі	
Технологія підключення	Wired
Канальний протокол	Ethernet, Fast Ethernet
Мережевий/ Транспортний протокол	IPSec
Протокол віддаленого адміністрування	SNMP 3
Індикатори стану	Link activity, живлення
Характеристики	Modular design, firewall protection, 128-bit кодування, апаратне кодування, підтримка VPN, підтримка MPLS, фільтрація URL, 256-bit кодування

Продовження таблиці 2.1

Підтримувані стандарти	IEEE 802.3af
Сокети розширення / Інтерфейси звязку	
Сокети розширення Сокетів всього (Вільно)	4 (4) x HWIC ¦ 2 (2) x AIM ¦ 1 (1) x NME ¦ 2 (2) x PVDM - SIMM 80-PIN ¦ 2 memory ¦ 1 CompactFlash Card
Інтерфейси	2 x network - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 2 x USB ¦ 1 x management - console - RJ-45 ¦ 1 x network - auxiliary - RJ-45

На рисунку 2.3 зображено зовнішній вигляд маршрутизатора CISCO 2811.

Рисунок 2.3 — Маршрутизатор CISCO 2811

Комутатори Cisco Catalyst серії 2960-X (рисунок 2.4) це стекові комутатори фіксованої конфігурації, призначені для використання в якості комутаторів рівня доступу при побудові офісних мереж підприємства та їх філій.

Рисунок 2.4 — Комутатор Cisco Catalyst серії 2960-X

Традиційно серія 2960-х отримала збільшення апаратної потужності в два рази і при цьому підвищила своє енергозбереження.

Нова лінійка комутаторів отримала:

– 24 або 48 порти 10/100/1000 Ethernet.

– SFP SFP або + висхідного порти.

– Стекування за технологією FlexStack-Plus.

– PoE + з бюджетом до 740 Вт.

– Низький рівень споживання енергії та розширені функції керування електроживленням.

– USB-Ethernet порти управління.

– Вбудовані функції NetFlow-Lite.

– LAN Base і для ПО LAN Lite IOS Cicso 2960-x.

– Cisco IOS IP-Lite з підтримкою динамічної маршрутизації і функціями рівня 3 для XR-2960.

– Покращена обмежений термін служби обладнання.

– Висока відмовостійкість, що забезпечується наявністю резервного джерела живлення в моделях 2960-XR.

Міжмережевий екран CISCO ASA5510 (рисунок 2.5).

Рисунок 2.5 — Міжмережевий екран CISCO ASA5510

Таблиця 2.2 - Технічні характеристики міжмережевого екрану CISCO ASA5510

Фізичні характеристики	
Розміри (ширина x глибина x висота), см:	20.04 x 36.20 x 4.45
Вага, кг:	9.07

Продовження таблиці 2.2

Тип установки, особливості конструкції:	– Форм-фактор: 1 RU, установка в 19" стійку – Установка в стійку: так – Настінний монтаж: ні – Сокет для замка безпеки (для фіз. безпеки): ні
Параметри живлення:	– Вхідна напргуа: 100 - 240 В AC, 3.0 A, 43 / 67 Гц – Вихідна потужність: в стійкому стані- 150 Вт, максимальна - 190 Вт
Характеристики пам’яті	
Пам’ять:	256 МБ
Мінімальний об’єм системної флеш-пам’яті:	64 МБ
Мережеві особливості	
Тип ліцензії:	Ліцензія Data Encryption Standard (3DES)
Шифрування:	Data Encryption Standard (DES)
Користувацькі вузли:	Необмежена кількість
Пропускна здатність міжмережевого екрана:	До 300 Мбит/с
Максимальна пропускна здатність міжмережевого екрана и IPS:	– До 150 Мбит/с при використанні AIP SSM-10 – До 300 Мбит/с при використанні AIP SSM-20
Пропускна здатність 3DES/AES VPN:	До 170 Мбит/с
Користувачі IPsec VPN:	250
Користувачі SSL VPN:	– Включено: 2 – Максимум: 250
Одночасні сесії:	– Включено: 50,000 – Максимум: 130,000

Опис: Продуктивність: 300 Мбіт / с, 3DES / AES VPN 170 Мбіт / с, від 50000 одночасних сесій, Користувачі: 250 IPsec VPN, 2 SSL VPN. Шифрування: DES, 5 портів 10 / 100BaseT 2 порти 10/100 / 1000BaseT, 3 x USB 2.0.

2.2 Захист на комутаторі

Мережевий комутатор (англ. network switch) або світч (від англ. switch — «перемикач») — пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

На відміну від концентратора, що поширює трафік від одного під'єднаного пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Комутатор працює на канальному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Для з'єднання декількох мереж на основі мережного рівня служать маршрутизатори.

Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

Є декілька видів загроз для мережевих комутаторів: DoS-атаки, ARP атаки, мережеві шторми, відстеження DHCP, несанкціонований доступ через порти.

– Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service

attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється:

a) примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;

b) заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.

– У галузі комп'ютерних мереж, ARP spoofing (ARP cache poisoning або ARP poison routing) — мережева атака, при якій зловмисник надсилає підроблені повідомлення протоколу ARP (Address Resolution Protocol) в локальну мережу.. За допомогою ARP spoofing зловмисник посилає підробленє ARP повідомлення на локальну мережу. Зазвичай мета полягає в тому, щоб зв'язати MAC-адресузловмисника з IP-адресою хоста на який здійснюється атака, зазвичай це основний шлюз, щоб трафік замість цієї IP-адреси, був надісланий зловмиснику.

ARP spoofing може дозволити зловмиснику перехоплювати пакети даних в мережі, змінювати трафік, або зупинити весь трафік. Часто ця атака є підготовкою для інших атак, таких як DoS-атака, атака «людина посередині», TCP hijacking.

Атака може бути використана тільки в мережах, що працюють на основі Address Resolution Protocol.

Оскільки в більшості мереж клієнти отримують IP адреси за допомогою DHCP, а не ручного налаштування, стає можливою захист від такої атаки за

допомогою DHCP Snooping і Dynamic ARP Inspection на рівні комутаторів. Перша функція реалізує прив'язку MAC-адреси до отриманого через DHCP IP-адресою. Друга перевіряє відповідність MAC-адреси відправника і змісту ARP-відповіді; в разі їх розбіжності кадр з ARP-відповіддю відкидається.

– Широкомовний шторм (мережевий шторм) — накопичення великих об'ємів broadcast та multicast трафіку в комп'ютерній мережі. Широкомовний шторм може спожити доступні ресурси мережі і не дати їй можливості транспортувати корисний трафік. Мережевий пакет що спричиняє такий шторм часом називаються «чорнобильським пакетом» (англ. Chernobyl packet).

Комутатори для своєї роботи постійно використовують таблицю MAC адрес, яка також називається бруківці таблицею. Це поліпшення в порівнянні з функціонуванням концентраторів дозволяє знизити обсяг широкомовного трафіку в мережі. Однак бруківка таблиця не є нескінченною. Один з видів атак спрямований на переповнення таблиці MAC-адрес, що призводить до зниження швидкості передачі користувальницького трафіку аж до повної непрацездатності мережі.

Стандартним рішенням цієї проблеми є обмеження кількості оброблюваних MAC-адрес для кожного порту комутатора. Розподіл фізичної мережі на кілька віртуальних зменшує масштаб проблеми і полегшує її діагностику, а також дозволяє більш оперативно відновити функціональність мережі.

Класичний протокол остовного дерева використовує ряд таймерів для забезпечення своєї роботи, що призводить до деякої затримки (близько 40 сек) почала передачі користувальницького трафіку. Оскільки побудована топологія є деревом, в ній існує кореневої комутатор, через який проходить весь трафік. Все разом є вузьким місцем не тільки в сенсі швидкого і правильного функціонування мережі, але також і з точки зору її безпеки.

Нехай спочатку в мережі було два комутатора: Root, кореневої, і Switch1. Потім зловмисник підключив контрольований ним комутатор Rogue, налаштований так, щоб стати кореневим вузлом дерева STP.

Тепер весь легітимний трафік може бути перехоплений атакуючим, що є

реалізацією атаки «людина посередині».

З'явилася можливість вивести всю мережу з ладу, періодично ставлячи / знімаючи Rogue комутатор. З точки зору його сусідів буде відбуватися зміна топології, тобто виникне необхідність у запуску STP, хоча ніякого «реального» зміни мережі не відбувається. Внаслідок інерційності протоколу, мережа стане недоступною для користувача трафіку на деякий час, що означає успішність атаки на порушення правильної роботи.

Рішенням проблеми з кореневим комутатором є правильне проектування мережі, а саме зміна пріоритету «цільового» кореневого комутатора на максимально можливе. Також деякі пристрої дозволяють ігнорувати повідомлення STP на певних портах, що дозволяє запобігти обидві розглянуті атаки.

Підміна MAC-адрес є однією з найпростіших атак. Крім реалізації «людина посередині», вона дозволяє також вивести з ладу мережу за допомогою порушення зв'язності, що може привести до відмови в обслуговуванні для ряду клієнтів.

Варіантів розв'язання проблеми кілька. Просте, але погано масштабується - вручну або статично прив'язати адреси до порту. Незважаючи на недоліки даного рішення, воно активно застосовується внаслідок передбачуваності поведінки пристроїв і рідкісного зміни фізичної топології мережі. Інший підхід передбачає використання протоколів аутентифікації з виділеними серверами перевірки автентичності, наприклад, протокол 802.1X.

Незважаючи на те, що DHCP є протоколом прикладного рівня моделі OSI, основна його робота зосереджена на канальному рівні. Це означає, що виникнення проблем з його функціонуванням буде мати наслідки на одному з найбільш базових рівнів мережі.

Перше повідомлення DHCP Discover від клієнта Host є широкомовною, тобто його отримають всі користувачі мережі, в тому числі сервер DHCP_server і зловмисник Rogue. Вони відправлять свої відповіді DHCP Offer клієнту, з яких він повинен вибрати те, що його «влаштує». За замовчуванням в більшості систем клієнт вибирає перше що прийшло пропозицію, ігноруючи інші. Таким

чином, відкривається пролом: якщо відповідь від Rogue прийде раніше, атака виявиться успішною. Сервер може бути фізично більш віддалений від клієнта, ніж зловмисник, а також бути менш швидким, тому ймовірність успішної реалізації атаки досить висока.

Наслідки:

Зловмисник може в своїй відповіді клієнту вказати неправильні дані про мережі, що призведе до неможливості його подальшої роботи, тобто буде реалізований відмову в обслуговуванні.

У більшості випадків протокол DHCP надає клієнту інформацію про шлюзі за замовчуванням. Таким чином, зловмисник має можливість вказати себе в якості шлюзу, що є реалізацією атаки «людина посередині» на мережевому рівні.

Одне з рішень - функція комутатора, звана DHCP Snooping, яка полягає в наступному:

– всі порти комутатора діляться на довірені (trusted), до яких підключені DHCP сервера, і ненадійні (untrusted);

– повідомлення, відправлені DHCP серверами (DHCP Offer, Ack, Nack, LeaseQuery) і приходять на ненадійні порти, відкидаються;

– повідомлення DHCP, що приходять на ненадійні порти, які містять MAC-адресу, неспівпадаючий з MAC-адреса відправника, відкидаються;

– повідомлення DHCP, що приходять на ненадійний порт і містять опцію 82, відкидаються;

– повідомлення DHCP Discover розсилаються тільки по довірених портам.

2.3 Мережевий екран

Міжмережевий екран, мережевий екран, брандмауер, фаєрво́л, файрво́л англ. Firewall, буквально «вогняна стіна» — пристрій або набір пристроїв,

сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв.

Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютерчи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку (функція редиректу).

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

– stateless (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;

– stateful (фільтрація з урахуванням контексту), з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Для того щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

– Фаєрвол мережного рівня представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

– Фаєрвол прикладного рівня також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп'ютери.

– Фаєрвол рівня з'єднання схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів.

МЕ можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP—адресам (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з’єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь—яких типів файлів: рекламної інформації або виконуваних програмних модулів).

МЕ розділяють на три види:

– пакетні фільтри (packet filter);

– сервера прикладного рівня (application gateways);

– сервера рівня з’єднання (circuit gateways).

МЕ з пакетними фільтрами приймають рішення про те чи пропускати пакет, чи відкинути, переглядаючи IP—адреси, прапорці або номери TCP портів в заголовку цього пакета. IP—адреса та номер порту – це інформація мережевого і транспортного рівнів. Водночас, пакетні фільтри використовують також інформацію прикладного рівня, тобто всі стандартні сервіси в TCP/IP асоціюються з певним номером порту.

Переваги пакетних фільтрів: відносно невисока вартість; гнучкість у визначенні правил фільтрації; невелика затримка при проходженні пакетів.

Недоліки: локальна мережа стає видима з мережі Internet; правила фільтрації пакетів важкі в описі, потрібні дуже хороші знання технологій TCP і UDP; при порушенні працездатності МЕ всі комп’ютери стають повністю незахищеними або недоступними; аутентифікацію з використанням IP—адреси можна обдурити використанням IP—спуфінга (атакуюча система видає себе за іншу, використовуючи її IP—адресу); відсутня аутентифікація на рівні користувача.

2.4 Захист безпровідної мережі

Безпровідна мережа — тип комп'ютерної мережі, яка використовує бездротове з'єднання для передачі даних й підключення до мережевих вузлів.

Залежно від використовуваної технології безпровідні мережі можна розділити на три типи:

- локальні обчислювальні мережі;
- розширені локальні обчислювальні мережі;
- мобільні мережі (переносні комп'ютери).

Основні відмінності між цими типами мереж — параметри передачі. Локальні і розширені локальні обчислювальні мережі використовують передавачі і приймачі, що належать тій організації, в якій функціонує мережа. Для переносних комп'ютерів середовищем передачі служать загальнодоступні мережі, наприклад телефонна мережа або Інтернет.

Трансивер, який ще й іноді називають точкою доступу (англ. access point), забезпечує обмін сигналами між комп'ютерами з безпровідним підключенням і кабельною мережею. У безпровідних ЛОМ використовуються невеликі настінні трансивери. Вони встановлюють радіоконтакт з переносними пристроями. Наявність цих трансиверів і не дозволяє назвати таку мережу строго

безповідною.

Стандарт Wi-Fi розроблений на основі IEEE 802.11. З точки зору безпеки, слід враховувати середовище передачі сигналу, в безпровідних мережах отримати доступ до переданої інформації набагато простіше, ніж у провідних мережах. Досить помістити антену в зоні дії.

Існує два основних варіанти устрою безповідної мережі:

– Ad-hoc - передача безпосередньо між пристроями;

– Hot-spot - передача здійснюється через точку доступу.

В Hot-spot мережах присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але й доступ до зовнішніх мереж. З погляду захисту інформації Hot-spot має більше значення, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених у цій безповідній мережі.

Цей спосіб не входить до стандарту IEEE 802.11. Фільтрацію можна здійснювати такими трьома способами:

– Точка доступу дозволяє отримати доступ станціям з будь-якою MAC-адресою.

– Точка доступу дозволяє отримати доступ тільки станціям, чиї MAC-адреси є в довіреному списку.

– Точка доступу забороняє доступ станціям, чиї MAC-адреси є в "чорному списку".

Найнадійнішим з погляду безпеки є другий спосіб, хоча він не розрахований на підміну MAC-адреси, що легко здійснити зловмисникові.

Для свого виявлення точка доступу розсилає кадри-маячки (англ. beacon frames). Кожен такий кадр містить службову інформацію для підключення і, зокрема, присутній SSID (ідентифікатор безповідної мережі). У разі прихованого SSID це поле порожнє, тобто виявлення безповідної мережі є неможливим і не можна до неї підключитися, не знаючи значення SSID. Але всі станції в мережі, які підключені до точки доступу, знають SSID і під час підключення, коли розсилають Probe Request запити, вказують ідентифікатори мереж, наявні в їх профілях підключень. Прослуховуючи робочий трафік, з

легкістю можна отримати значення SSID, необхідне для підключення до бажаної точки доступу.

Аутентифікація - видача певних прав доступу абоненту на основі наявного в нього ідентифікатора.

IEEE 802.11 передбачає два методи аутентифікації:

– Відкрита аутентифікація (англ. Open Authentication):

Робоча станція робить запит аутентифікації, у якому присутня тільки MAC-адреса клієнта. Точка доступу відповідає або відмовою, або підтвердженням аутентифікації. Рішення ухвалює на основі MAC-фільтрації, тобто це захист на основі обмеження доступу, що не є безпечним.

– Аутентифікація із загальним ключем (англ. Shared Key Authentication):

Необхідно налаштувати статичний ключ шифрування алгоритму WEP (англ. Wired Equivalent Privacy). Клієнт робить запит у точки доступу на аутентифікацію, на що отримує підтвердження, яке містить 128 байт випадкової інформації. Станція шифрує отримані дані алгоритмом WEP (виконується побітове додавання з модулем 2 даних повідомлення з послідовністю ключа) і надсилає зашифрований текст разом із запитом на асоціацію. Точка доступу розшифровує текст і порівнює з початковими даними. У разі збігу надсилає підтвердження асоціації, і клієнт вважається підключеним до мережі. Схема аутентифікації із загальним ключем вразлива до атак «Man in the middle». Алгоритм шифрування WEP — це проста XOR-послідовність з корисною інформацією, отже, прослухавши трафік між станцією і точкою доступу, можна відновити частину ключа. IEEE почав розробки нового стандарту IEEE 802.11i, але через труднощі затвердження, організація WECA (англ. Wi-Fi Alliance) спільно з IEEE анонсували стандарт WPA (англ. Wi-Fi Protected Access). У WPA використовується TKIP (англ. Temporal Key Integrity Protocol, протокол перевірки цілісності ключа), який використовує вдосконалений спосіб керування ключами та покадрову зміну ключа.

WPA також використовує два способи аутентифікації:

– Аутентифікація за допомогою наданого ключа WPA-PSK (англ. Pre-Shared Key) (Enterprise Autentification).

– Аутентифікація за допомогою RADIUS-сервера (англ. Remote Access Dial-in User Service).

Методи шифрування.

– WEP-шифрування (англ. Wired Equivalent Privacy):

Аналог шифрування трафіку в провідних мережах. Використовується симетричний потоковий шифр RC4 (англ. Rivest Cipher 4), який досить швидко функціонує. На сьогоднішній день WEP і RC4 не вважаються криптостійкими.

Є два основних протоколи WEP:

40-бітний WEP (довжина ключа 64 біта, 24 з яких — це вектор ініціалізації, який передається відкритим текстом); 104-бітний WEP (довжина ключа 128 біт, 24 з яких — це теж вектор ініціалізації); вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності алгоритму.

– TKIP-шифрування (англ. Temporal Key Integrity Protocol):

Використовується той же симетричний потоковий шифр RC4, але є більш криптостійким. Вектор ініціалізації становить 48 біт. Враховані основні атаки на WEP. Використовується протокол Message Integrity Check для перевірки цілісності повідомлень, який блокує станцію на 60 секунд, якщо послані протягом 60 секунд два повідомлення не пройшли перевірку цілісності. З урахуванням всіх доопрацювань і удосконалень TKIP все одно не вважається криптостійким.

– CKIP-шифрування (англ. Cisco Key Integrity Protocol):

Має подібності з протоколом TKIP. Створений компанією Cisco. Використовується протокол CMIC (англ. Cisco Message Integrity Check) для перевірки цілісності повідомлень.

– WPA-шифрування:

Замість уразливого RC4, використовується криптостійкий алгоритм шифрування AES (англ. Advanced Encryption Standard). Можливе використання EAP (англ. Extensible Authentication Protocol, розширюваний протокол

автентифікації).

Є два режими:

Pre-Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі;

– Enterprise - перевірка здійснюється серверами RADIUS;

– WPA2-шифрування (IEEE 802.11i):

Прийнятий у 2004 році, з 2006 року WPA2 повинна підтримувати все вироблене Wi-Fi обладнання. В даному протоколі застосовується RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Спочатку в WPA2 використовувався протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника). Основою є алгоритм AES. Для сумісності зі старим обладнанням є підтримка TKIP і EAP (англ. Extensible Authentication Protocol) з деякими його доповненнями. Як і в WPA є два режими роботи: Pre-Shared Key і Enterprise.

Перш ніж перейти розробки мережі, потрібно її спроектувати. Для цього було вибрано програму-симулятор "CISCO Packet Tracer 7". На рисунку 3.1, зображено побудову локальної мережі згідно логічної топології.

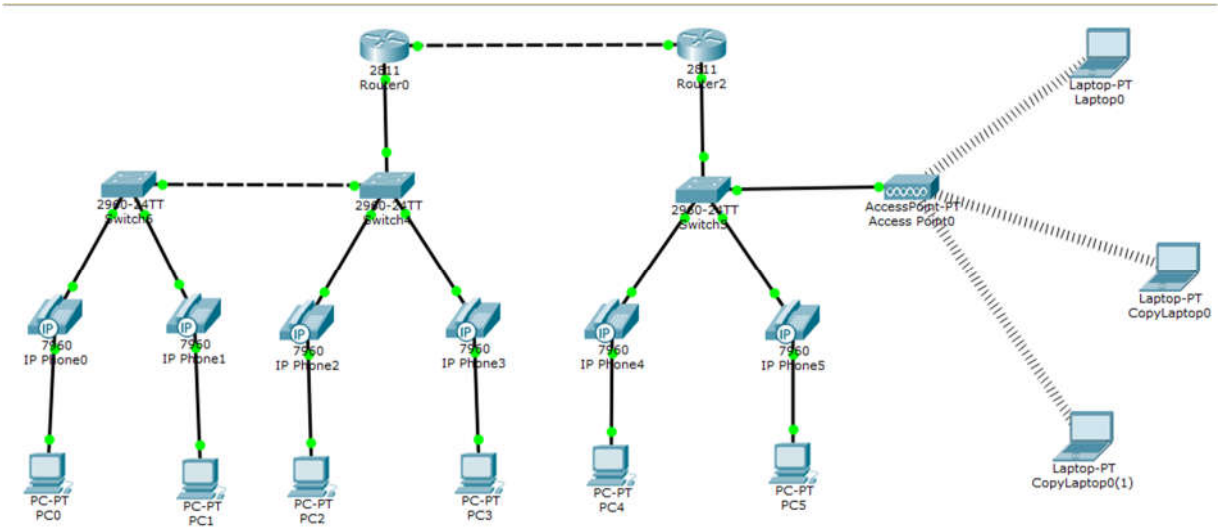


Рисунок 3.1 — Загальний вигляд локальної мережі

Як видно з рисунку 3.1 комп'ютерна мережа складається із 6 робочих станцій, 3 ноутбуків, 3 концетраторів, 2 комутаторів та однієї безпровідної точки доступу.

3.1 Налаштування комутаторів

Наступним етапом після побудови локальної мережі є налаштування обладнання. Цей процес починається із налаштування комутаторів та VLAN.

Для початку потрібно використати команди для задання IP-адреси підмережі:

Switch 6

Switch(config)#interface vlan 1

Switch(config-if)#ip address 10.3.0.100 255.255.255.0

Switch(config-if)#no shutdown

Результат зображено на рисунках 3.2 – 3.4.

```
GigabitEthernet0/1   Down    1       --                  00E0.F93C.C119
GigabitEthernet0/2   Down    1       --                  00E0.F93C.C11A
Vlan1                Up      1       10.3.0.100/24       0001.4284.5D18
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.2 — Задання IP-адреси для підмережі

Switch 4

Switch(config)#interface vlan 1

Switch(config-if)#ip address 10.3.0.0 255.0.0.0

Switch(config-if)#no shutdown

```
GigabitEthernet0/1   Down    1       --                  0001.6372.4919
GigabitEthernet0/2   Down    1       --                  0001.6372.491A
Vlan1                Up      1       10.3.0.0/8          0001.C750.29C2
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.3 — Задання IP-адреси для підмережі

Switch 5

Switch(config)#interface vlan 1

Switch(config-if)#ip address 20.4.0.0 255.0.0.0

Switch(config-if)#no shutdown

```
GigabitEthernet0/1   Down    1       --                  00D0.58B3.BB19
GigabitEthernet0/2   Down    1       --                  00D0.58B3.BB1A
Vlan1                Up      1       20.4.0.0/8          00D0.9731.BAC0
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.4 — Задання ip-адреси для підмережі

Наступним кроком є налаштування голосових портів, оскільки мережа передбачає використання IP-телефонів.

IP-телефонія - це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відео зображень та факсів у режимі реального часу.

При відправленні або отриманні електронної пошти відбувається передача «пакета» інформації через мережу Інтернет. Аналогічним чином працює й IP-телефонія. Створення «пакетів» — перетворення аналогових (зокрема, звукових) сигналів у цифрові, їх стискання, передачу мережею Internet і зворотне перетворення в аналогові відбувається завдяки існуванню протоколу передачі даних через Інтернет (IP — Internet Protocol), звідси і назва «IP-телефонія».

Перелік використаних команд наведено нижче, а результат їх виконання представлено на рисунку 3.5.

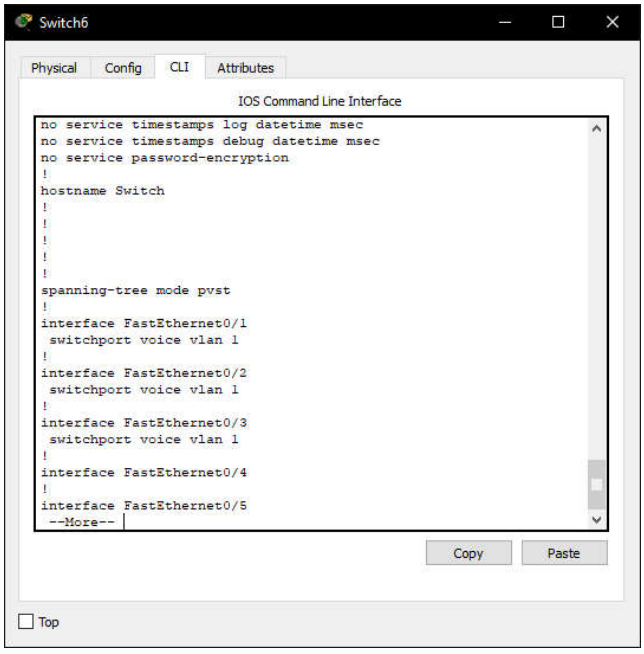


Рисунок 3.5 — Налаштування голосових портів комутатора 6

Switch>enable

Switch#conf te

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface fa 0/1

Switch(config-if)#switchport voice vlan 1
Switch(config-if)#exit

Switch(config)#interface fa 0/2
Switch(config-if)#switchport voice vlan 1
Switch(config-if)#exit

Switch(config)#interface fa 0/3
Switch(config-if)#switchport voice vlan 1
Switch(config-if)#exit

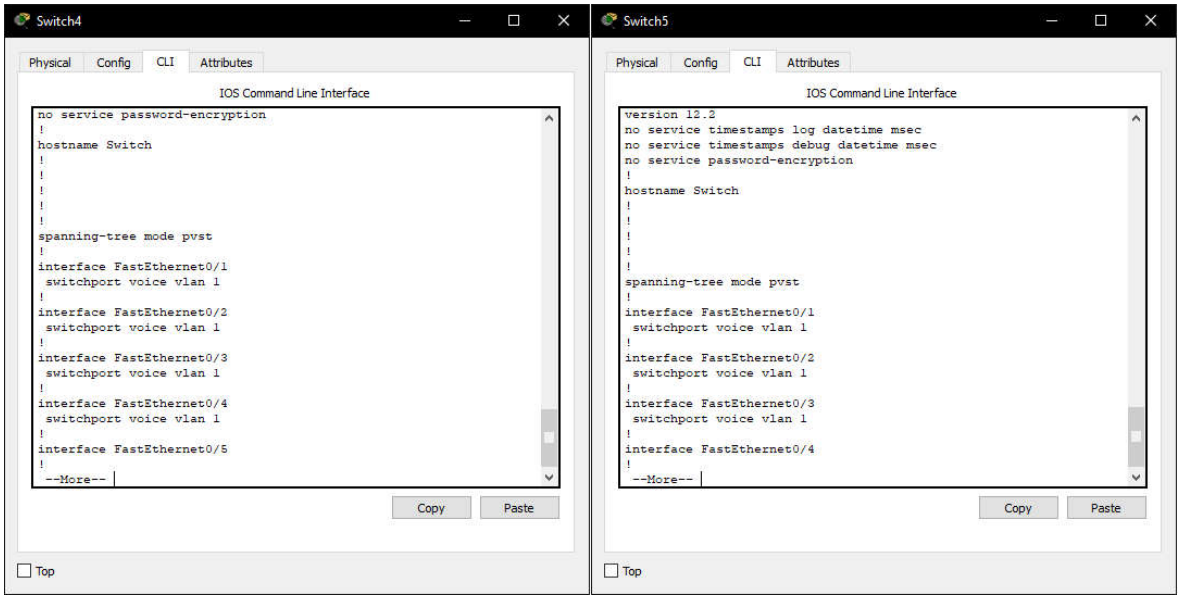


Рисунок 3.6 — Налаштування голосових портів комутаторів 4 і 5

Аналогічні дії було повторено на комутаторах 4 та 5 (рисунок 3.6).

3.2 Налаштування маршрутизаторів

Наступним кроком після налаштування комутаторів є налаштування маршрутизаторів. Для початку, по аналогії з комутаторами, портам передачі

даних присвоювались їх IP-адреси. Для цього було використано наступні команди:

```
Router>enable
Router#conf te
Router(config)#interface fa 0/0
Router(config-if)#ip address 10.3.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa 0/1
Router(config-if)#ip address 30.10.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Результат виконання зображено на рисунках 3.7 - 3.8.

```
Port            Link   VLAN   IP Address        IPv6 Address                          MAC Address
FastEthernet0/0 Up     --     10.3.0.1/24       <not set>                             0060.3E23.2401
FastEthernet0/1 Up     --     30.10.1.1/24      <not set>                             0060.3E23.2402
Vlan1           Down   1      <not set>         <not set>                             00E0.F9BE.5D74
Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.7 — Налаштування IP-адрес маршрутизатора Router0

```
Router>enable
Router#conf te
Router(config)#interface fa 0/0
Router(config-if)#ip address 20.4.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa 0/1
Router(config-if)#ip address 30.10.1.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

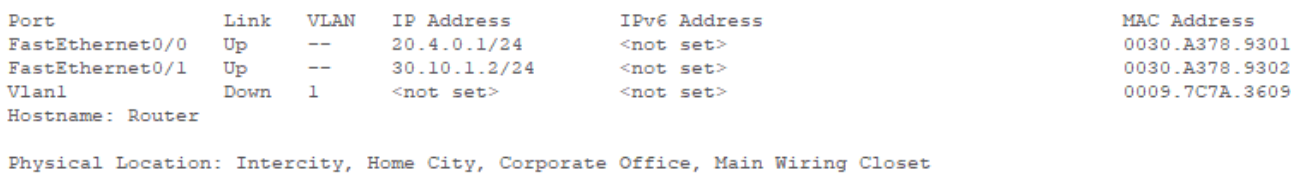


Рисунок 3.8 — Налаштування IP-адрес маршрутизатора Router2

В даній мережі маршрутизатори також будуть виконувати роль TFTP-серверів.

TFTP (англ. Trivial File Transfer Protocol — тривіальний протокол передачі файлів) — простий, покроково синхронізований протокол передачі файлів, який дозволяє клієнтам зчитувати або записувати файли сервера. Одним із основних використань протоколу є первинне завантаження бездискових робочих станцій у локальній мережі. Найчастіше TFTP використовується саме через простоту його реалізації. Протокол працює поверх протоколу UDP.

Тобто, з TFTP-сервера IP-телефони в даній мережі будуть отримувати свою прошивку (програмне забезпечення) при завантаженні.

Router0 Router2

Router(config)#ip dhcp excluded-address 10.3.0.1 / 20.4.0.1

Router(config)#ip dhcp pool Phones

Router(dhcp-config)#network 10.3.0.0 255.255.255.0 / 20.4.0.0 255.255.255.0

Router(dhcp-config)#default-router 10.3.0.1 / 20.4.0.1

Router(dhcp-config)#option 150 ip 10.3.0.1 / 20.4.0.1

Router(dhcp-config)#exit

Дані команди виконують наступні функції: резервують IP-адреси портів для того, щоб IP-телефони не могли присвоїти собі їх адресу, створюють пул IP-адрес для телефонів, встановлюють стандартну точку входу/виходу даних у вигляді порта маршрутизатора. Результат зображено на рисунках 3.9 – 3.10.

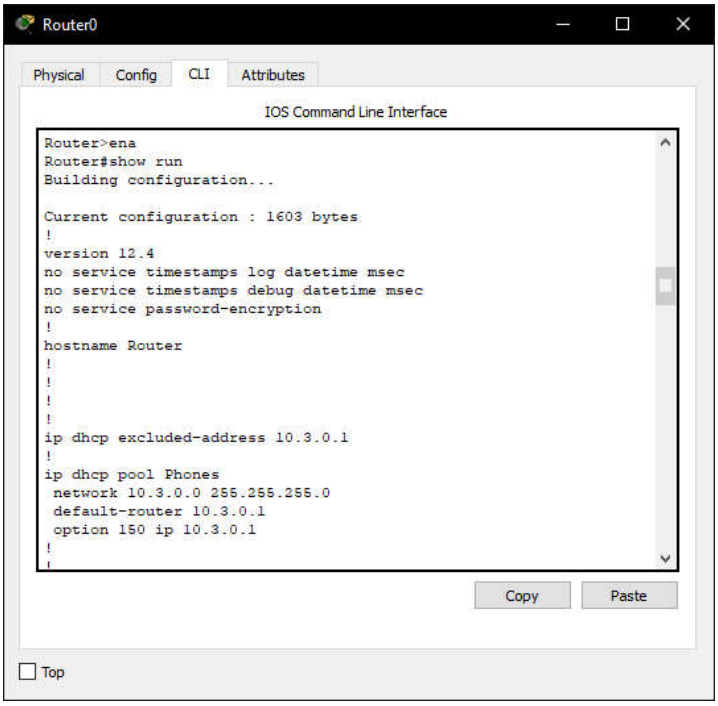


Рисунок 3.9 — Створення пулу IP-адрес IP-телефонів в мережі Router0

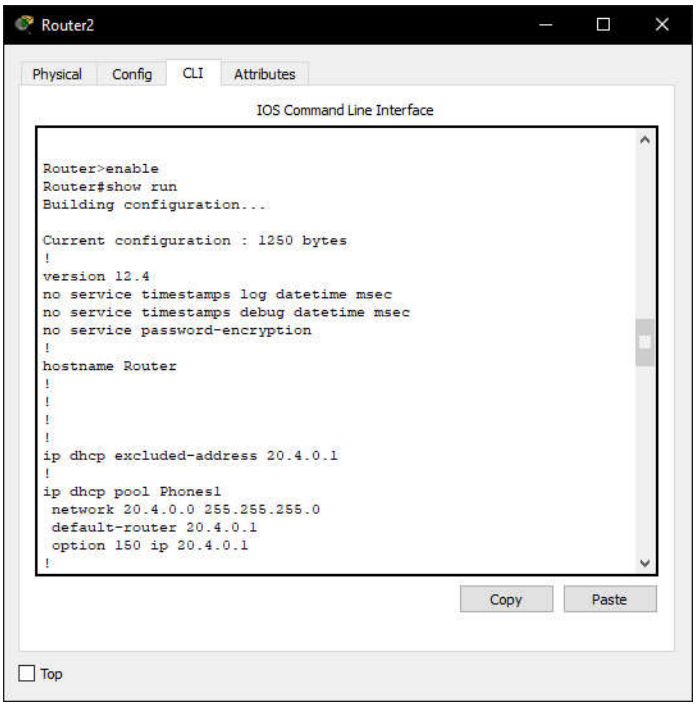


Рисунок 3.10 — Створення пулу IP-адрес IP-телефонів в мережі Router2

Наступним кроком було налаштування телефонії. Нижче наведено перелік команд які визначають максимальну кількість телефонів в мережі, максимальну кількість визначених телефонних номерів, джерело їх видачі у вигляді маршрутизатора, автоматичне розподілення номерів між телефонами.

Результат виконання зображено на рисунку 3.11.

Router(config)#telephony-service

Router(config-telephony)#max-ephones 6

Router(config-telephony)#max-dn 6

Router(config-telephony)#ip source-address 10.3.0.1 port 2000 / 20.4.0.1 port2000

Router(config-telephony)#auto assign 1 to 6

Router(config-telephony)#exit

Router(config)#ephone-dn 1

Router(config-ephone-dn)#number 101

Router(config-ephone-dn)#exit

Router(config)#ephone-dn 2

Router(config-ephone-dn)#number 102

Router(config-ephone-dn)#exit

Router(config)#ephone-dn 3

Router(config-ephone-dn)#number 103

Router(config-ephone-dn)#exit

Router(config)#ephone-dn 4

Router(config-ephone-dn)#number 104

Router(config-ephone-dn)#exit

Router(config)#ephone-dn 5

Router(config-ephone-dn)#number 105

Router(config-ephone-dn)#exit

Router(config)#ephone-dn 6

Router(config-ephone-dn)#number 106

Router(config-ephone-dn)#exit

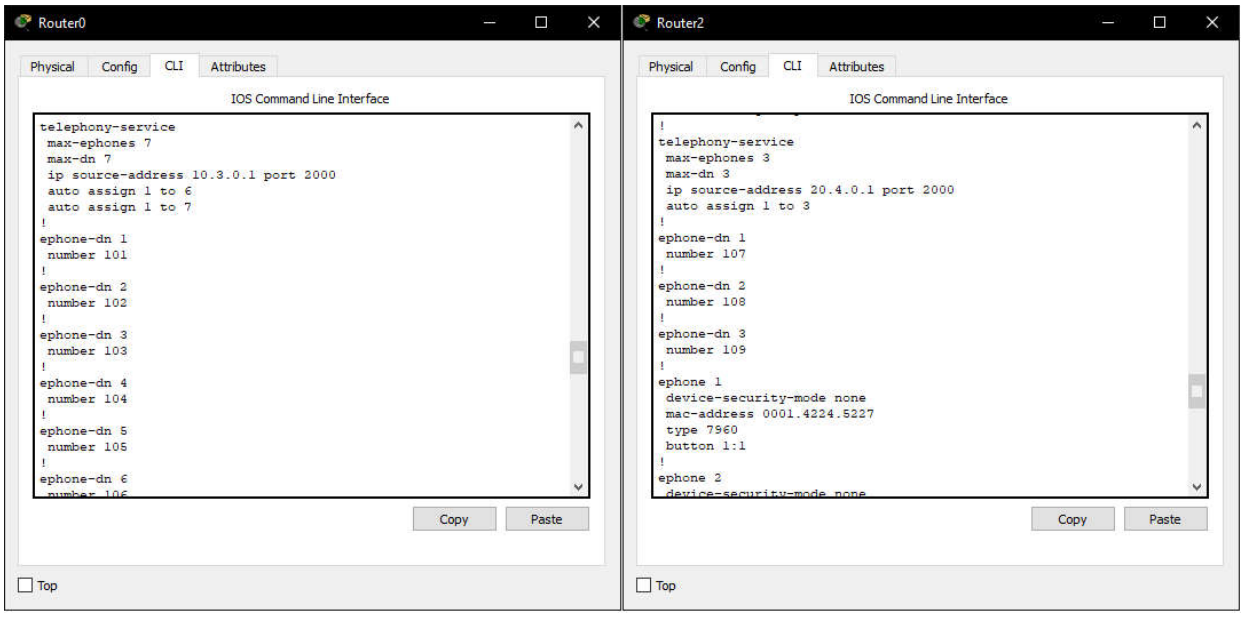


Рисунок 3.11 — Налаштування телефонії Router0 та Router2

Останнім кроком в налаштуванні маршрутизаторів було встановлення мостів між ними, налаштування вихідної точки виклику POTS, вказання

шаблону номерів, який повинен набрати користувач, щоб здійснити виклик, який включає префікс і номер призначення, призначення адресу певної мережі для отримання дзвінків від точки виклику VoIP. Нижче наведено перелік команд використаних для даних цілей, а результат роботи зображено на рисунку 3.12.

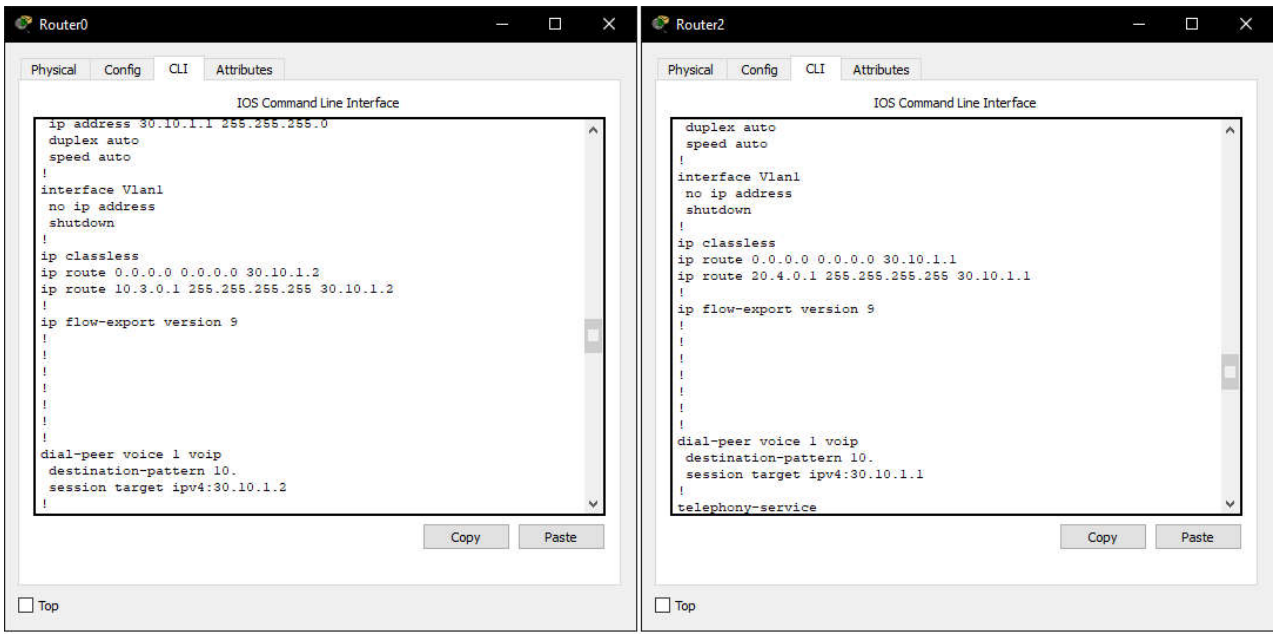


Рисунок 3.12 — Налаштування адресації на Router0 та Router2

Router 0

Router(config)#ip route 0.0.0.0 0.0.0.0 30.10.1.2

Router(config)#ip route 10.3.0.1 255.255.255.255 30.10.1.2

Router(config)#dial-peer voice 1 voip

Router(config-dial-peer)#destination-pattern 10.

Router(config-dial-peer)#session target ipv4:30.10.1.2

Router 2

Router(config)#ip route 0.0.0.0 0.0.0.0 30.10.1.1

Router(config)#ip route 20.4.0.1 255.255.255.255 30.10.1.1

Router(config)#dial-peer voice 1 voip

Router(config-dial-peer)#destination-pattern 10.

Router(config-dial-peer)#session target ipv4:30.10.1.1

3.3 Налаштування робочих станцій

Налаштування персональних комп'ютерів не потребує особливих затрат часу та зусиль. Все, що було потрібно – задати їм власні IP-адреси та маску згідно до їх підмережі, та вказати для них відповідний шлюз по замовчуванню, зображено на рисунку 3.13.

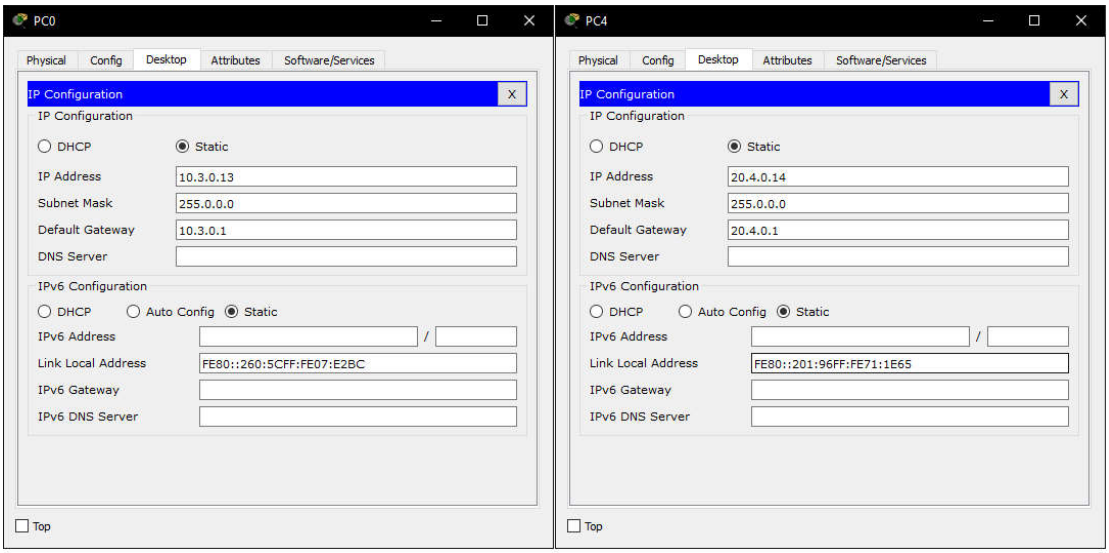
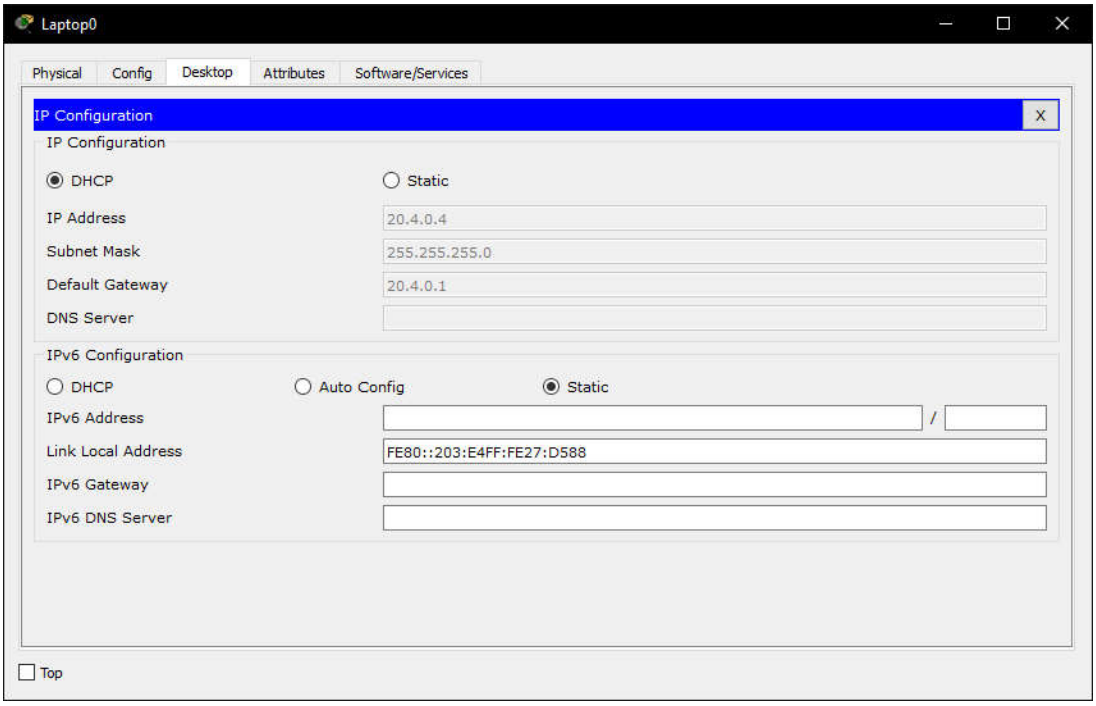


Рисунок 3.13 — Налаштування IP-адрес ПК



Риснок 3.14 — Налаштування динамічної роздачі IP-адрес для ноутбуків

Для ноутбуків було вибрано автоматичний вибір IP-адрес, в зв'язку з постійною зміною їх чисельності всередині офісу (рисуноку 3.14).

3.4 Організація безпеки комутаторів та маршрутизаторів

Останнім кроком є налаштування безпеки на комутаторах та маршрутизаторах. Для цього було використано функцію Port Security. Port Security - це функція канального рівня, яка створена для запобігання несанкціонованої зміни MAC адреси мережевого підключення. Також, дана функція захищає комутатор від атак, які можуть бути спрямовані на переповнення таблиці MAC адрес. Нижче приведено перелік команд для задання захисту на трьох портах комутатора Switch6, а результат виконання цих команд на Switch6, Switch4, Switch5 зображено на рисунку 3.15.

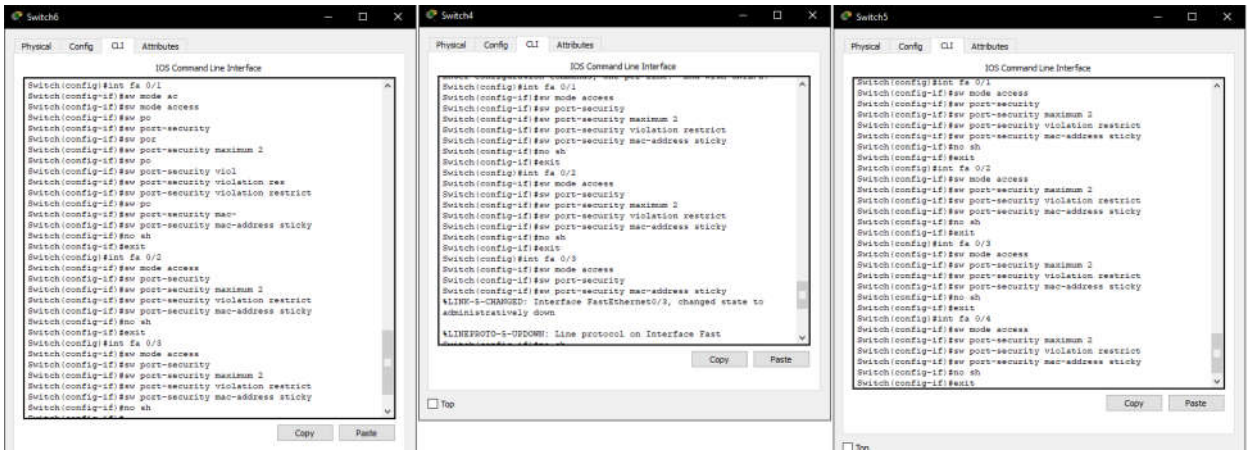


Рисунок 3.15 — Налаштування захисту на комутаторах

Switch(config)#int fa 0/1

Switch(config-if)#sw mode access

Switch(config-if)#sw port-security

Switch(config-if)#sw port-security maximum 2

Switch(config-if)#sw port-security violation restrict

Switch(config-if)#sw port-security mac-address sticky

```
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#int fa 0/2
Switch(config-if)#sw mode access
Switch(config-if)#sw port-security
Switch(config-if)#sw port-security maximum 2
Switch(config-if)#sw port-security violation restrict
Switch(config-if)#sw port-security mac-address sticky
Switch(config-if)#no sh
Switch(config-if)#exit

Switch(config)#int fa 0/3
Switch(config-if)#sw mode access
Switch(config-if)#sw port-security
Switch(config-if)#sw port-security maximum 2
Switch(config-if)#sw port-security violation restrict
Switch(config-if)#sw port-security mac-address sticky
Switch(config-if)#no sh
Switch(config-if)#exit
```

Далі на кожному з комутаторів було створено користувача з рівнем доступу до 15 та задано пароль для telnet з використанням функції VTY. VTY - VirtualTeletYpe, віртуальний інтерфейс, який забезпечує віддалений доступ до пристрою.

Telnet (англ. TErminaL NETwork)— мережевий протокол для реалізації текстового інтерфейсу по мережі (у сучасній формі — за допомогою транспорту TCP). Назву «telnet» мають також деякі утиліти, що реалізують клієнтську частину протоколу.

Нижче наведено перелік використаних команд, а результат їх виконання зображено на рисунках 3.16 – 3.18.

Switch6

Switch>en

Switch#conf te

Switch(config)#username sw6 secret sw6

Switch(config)#line vty 0 15

Switch(config-line)#privilege level 15

Switch(config-line)#exit

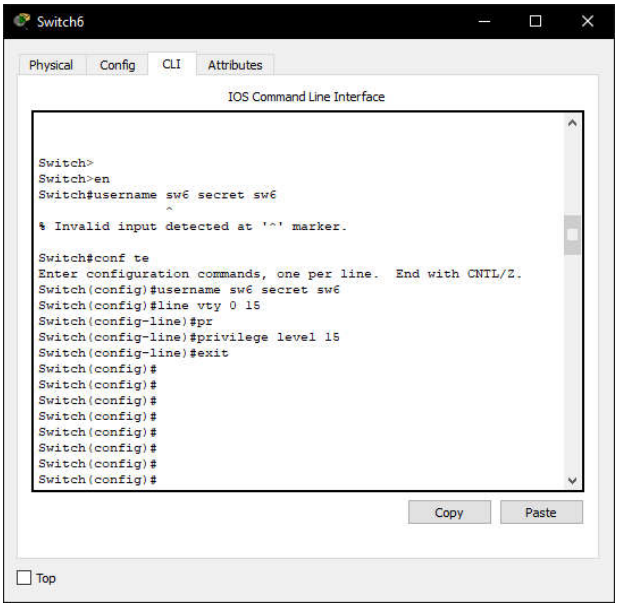


Рисунок 3.16 — Задання рівня доступу для користувача до 15 і пароль для Telnet на Switch6

Switch4

Switch>en

Switch#conf te

Switch(config)#username sw4 secret sw4

Switch(config)#line vty 0 15

Switch(config-line)#privilege level 15

Switch(config-line)#exit

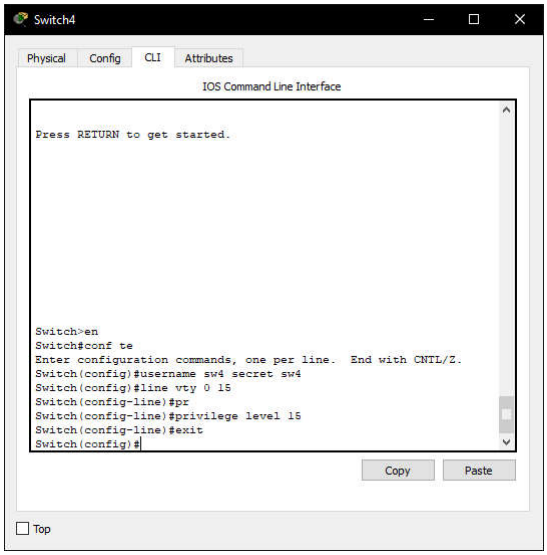


Рисунок 3.17 — Задання рівня доступу для користувача до 15 і пароль для Telnet на Switch4

Switch5

Switch>en

Switch#conf te

Switch(config)#username sw5 secret sw5

Switch(config)#line vty 0 15

Switch(config-line)#privilege level 15

Switch(config-line)#exit

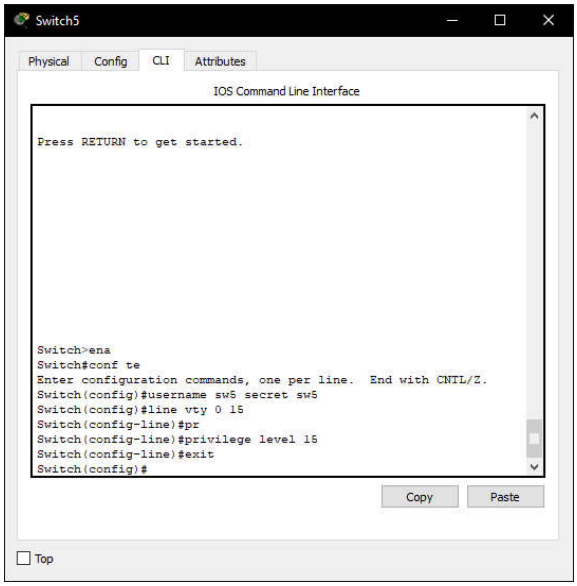


Рисунок 3.18 — Задання рівня доступу для користувача до 15 і пароль для Telnet на Switch5

Далі по аналогії проводилось налаштування маршрутизаторів, тільки тепер з використанням протоколу AAA, зображено на рисунках 3.19 та 3.20.

AAA (від англ. Authentication, Authorization, Accounting) - використовується для опису процесу надання доступу і контролю над ним.

Authentication (аутентифікація) - зіставлення персони (запиту) існуючої облікового запису в системі безпеки. Здійснюється за логіном, паролем, сертифікату, смарт-карти і т. д.

Authorization (авторизація, перевірка повноважень, перевірка рівня доступу) - зіставлення облікового запису в системі (і персони, що пройшла аутентифікацію) і певних повноважень (або заборони на доступ). У загальному випадку авторизація може бути «негативною» (користувачеві А заборонений доступ до серверів компанії).

Accounting (облік) - стеження за споживанням ресурсів (переважно мережевих) користувачем. У accounting включається так само і запис фактів отримання доступу до системи (англ. Access logs).

```
Router0
Router(config)#aaa new-model
Router(config)#username r0 secret r0
Router(config)#line vty 0 15
Router(config-line)#privilege level 15
Router(config-line)#exit
```

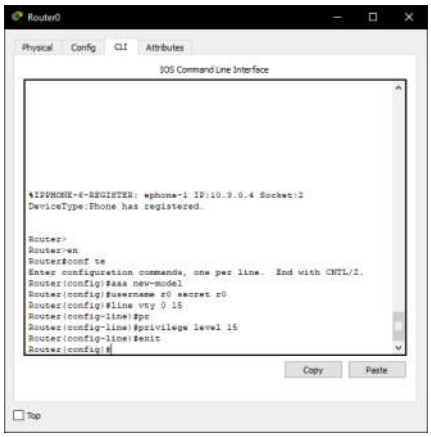


Рисунок 3.19 — Задання рівня доступу для користувача до 15 і пароль для Telnet на Router0

Router2

Router(config)#aaa new-model

Router(config)#username r0 secret r0

Router(config)#line vty 0 15

Router(config-line)#privilege level 15

Router(config-line)#exit

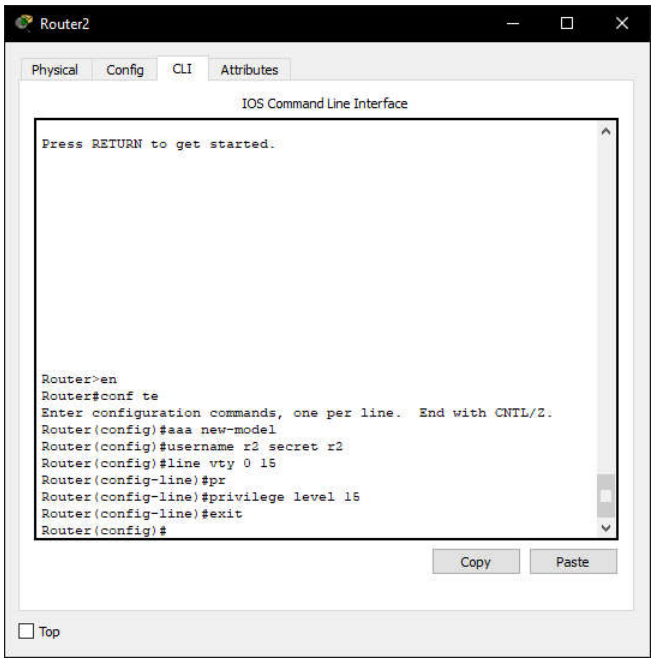


Рисунок 3.20 — Задання рівня доступу для користувача до 15 і пароль для Telnet на Router2

На цьому налаштування роботи та безпеки комутаторів та маршрутизаторів було закінчено наступним кроком є перевірка працездатності розробленої мережі.

3.5 Перевірка працездатності мережі

Останнім етапом розробки мережі є перевірка роботи усіх вузлів та усунення можливих помилок. Для початку було перевірено роботу робочих

станцій за допомогою консольної утиліти “ping”: зв'язок між ними в межах однієї підмережі, зв'язок із ПК з іншої підмережі, зв'язок між ПК та ноутбуками. Таким чином перевірялись і правильність налаштування портів маршрутизаторів та комутаторів, зображено на рисунках 3.21 – 3.23.

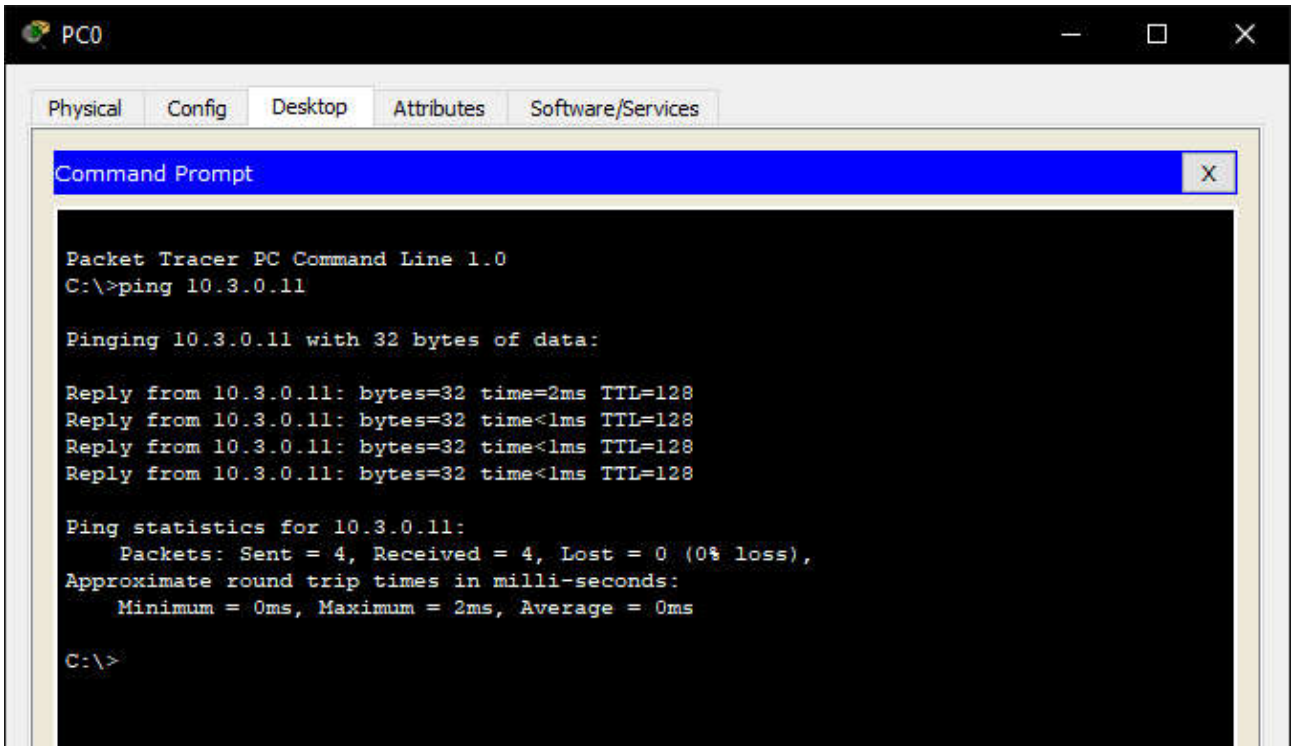


Рисунок 3.21 —Перевірка зв’язку між ПК однієї підмережі

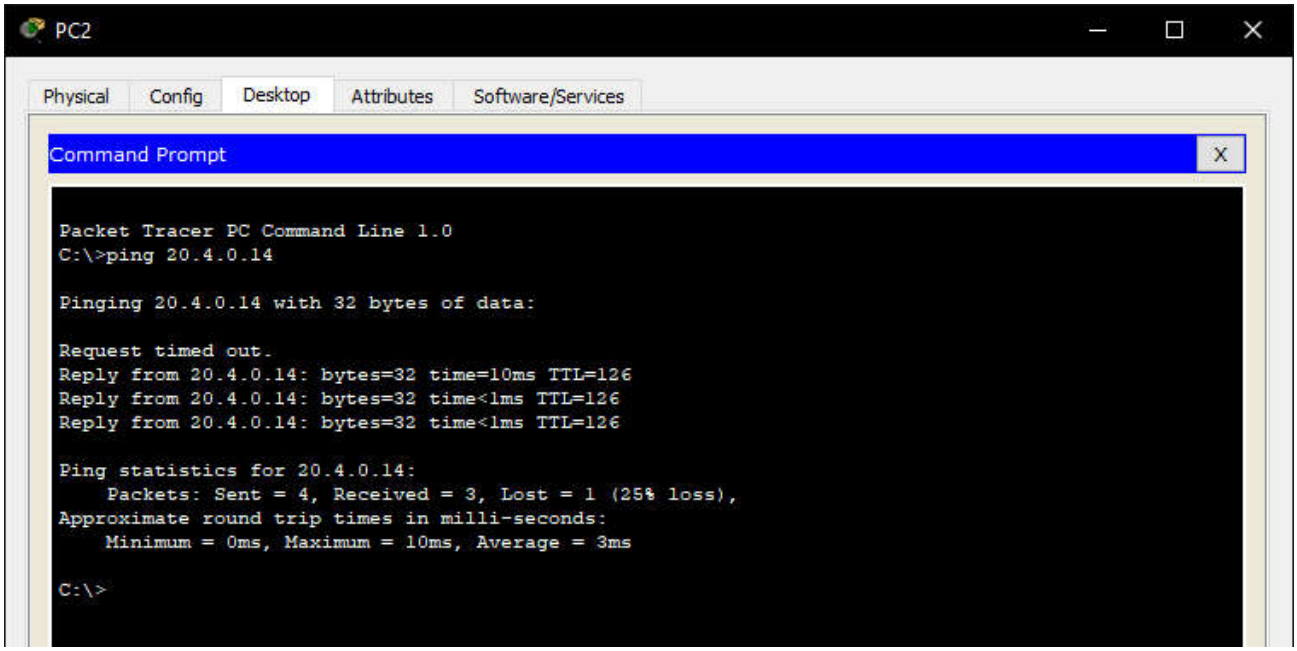


Рисунок 3.22 —Перевірка зв’язку між ПК різних підмереж

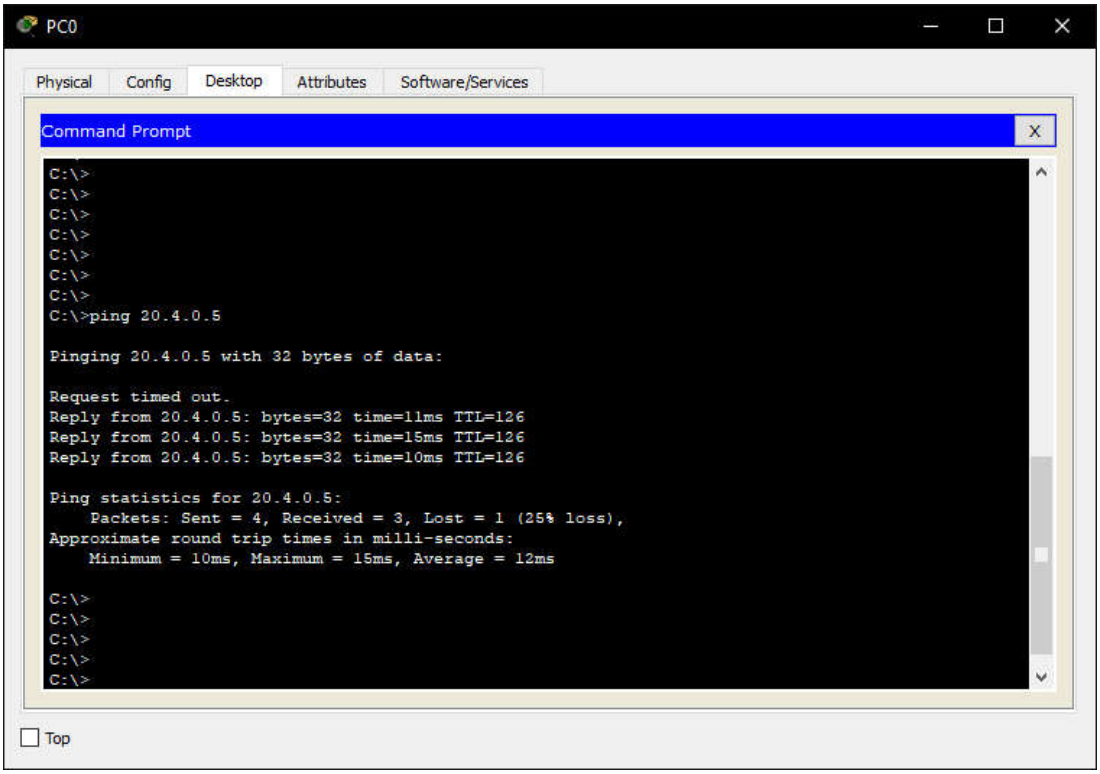


Рисунок 3.23 —Перевірка зв’язку між ПК та ноутбуком

З інформації отриманої за допомогою утиліти “ping” було визначено, що ПК, ноутбуки, комутатори та маршрутизатори було налаштовано правильно і зв'язок налагоджено.

Останнім етапом тестування є перевірка коректної роботи IP-телефонів. Для цього було використано режим симуляції дзвінка. Спочатку було перевірено зв'язок між IP-телефонами однієї підмережі, зображено на рисунках 3.24 та 3.25.

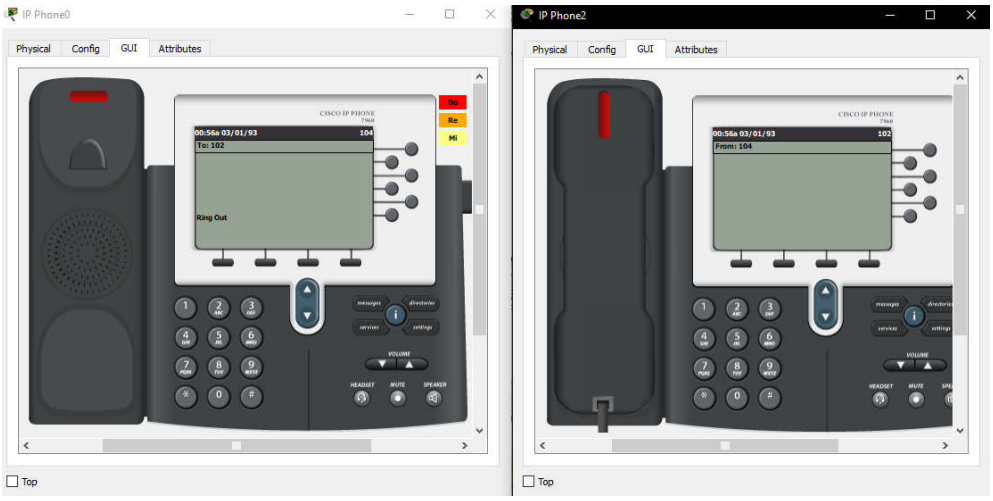


Рисунок 3.24 —Перевірка виклику між IP-телефонами однієї підмережі

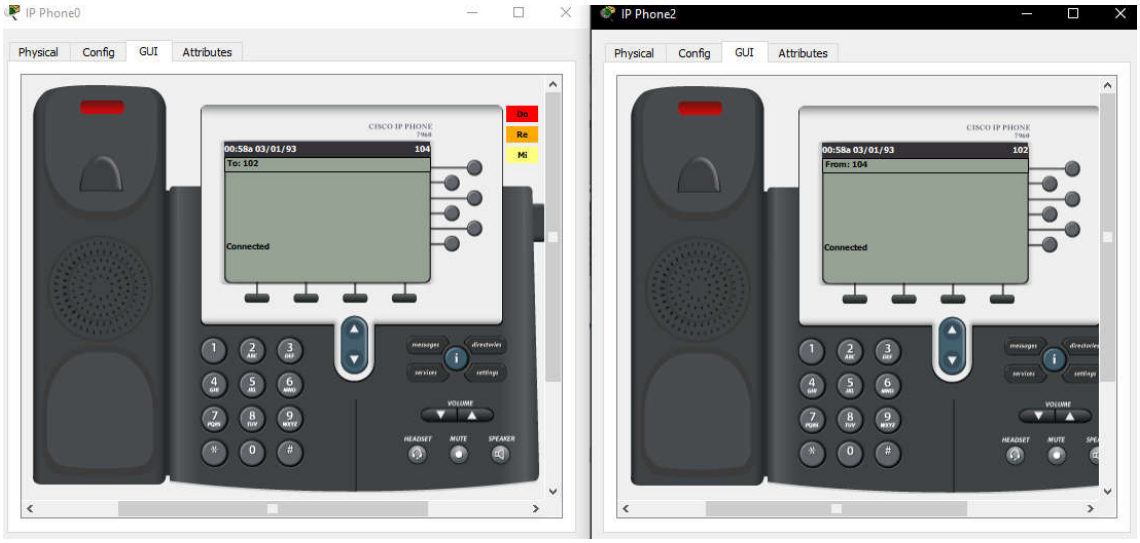


Рисунок 3.25 —Перевірка зв’язку між IP-телефонами однієї підмережі

Рисунок 3.24 свідчить про те, що виклик було здійснено IP-телефоном з номером 102 до IP-телефону з номером 104, а рисунок 3.25 підтверджує прямий зв'язок між ними, про що свідчить напис “Connected” (з’єднано) на екрані обох IP-телефонів. Далі було перевірено зв'язок між IP-телефонами різних підмереж аналогічним способом, зображено на рисунках 3.26 та 3.27.

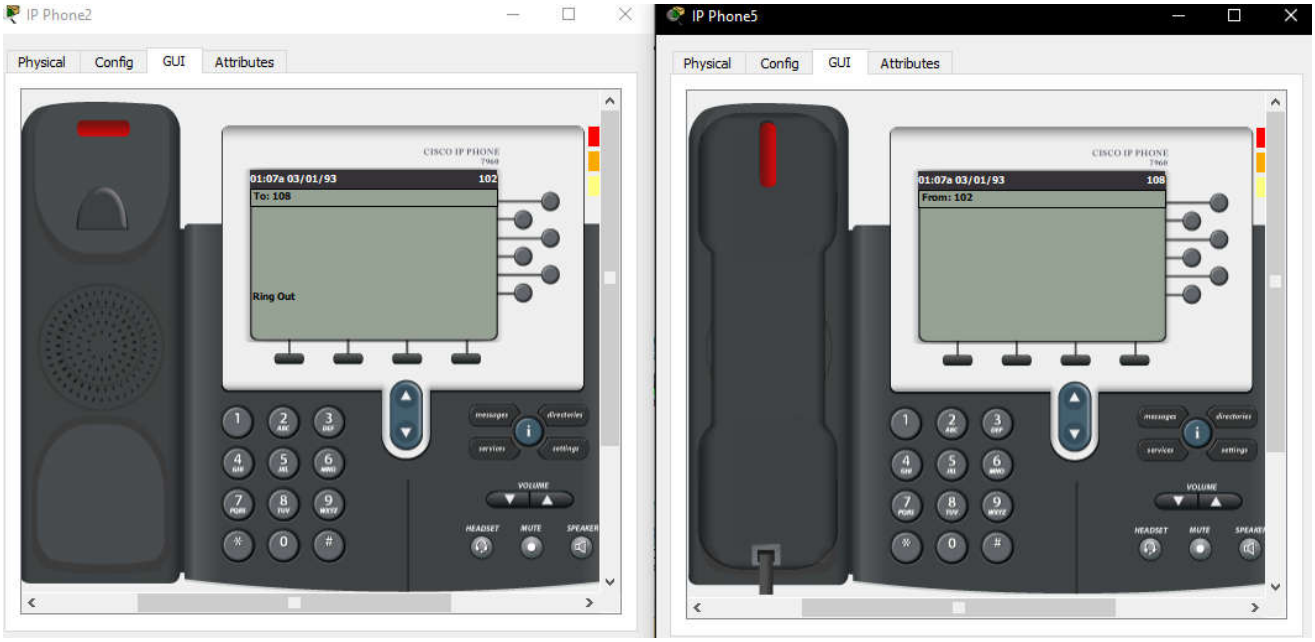


Рисунок 3.26 —Перевірка виклику між IP-телефонами різних підмереж

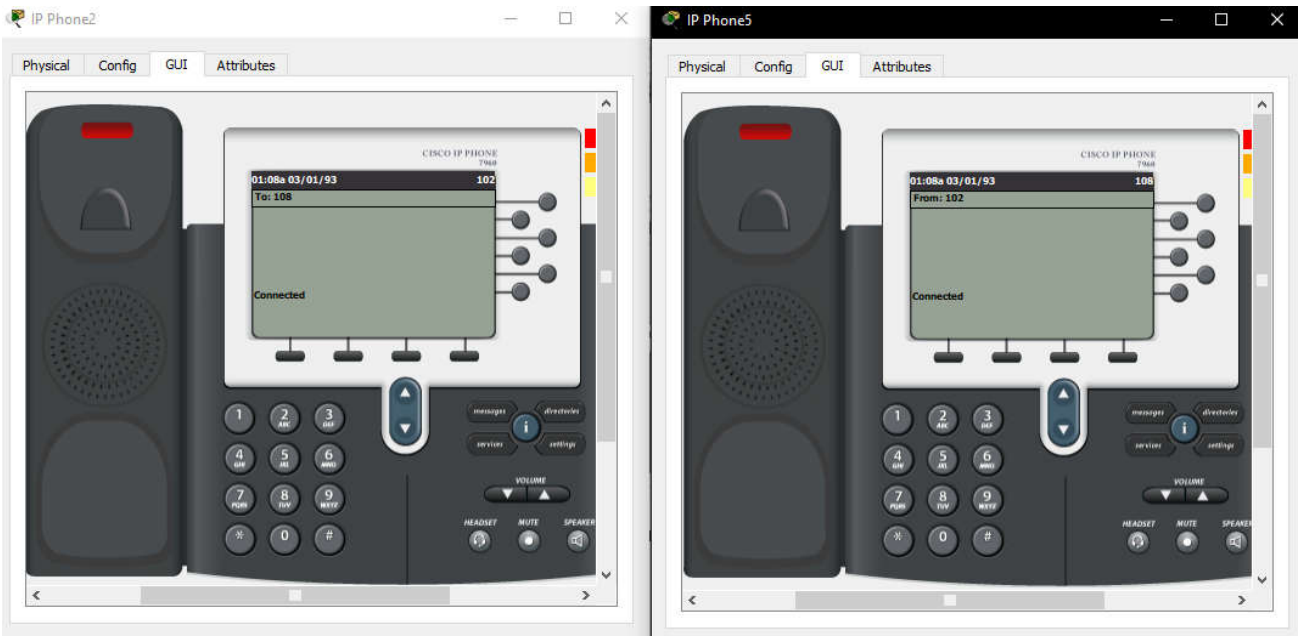


Рисунок 3.27 —Перевірка зв’язку між IP-телефонами різних підмереж

На обох рисунках результати аналогічні попереднім, а це означає, що IP-телефони та прохідні порти на комутаторах і маршрутизаторах було налаштовано вірно.

4 Техніко-економічний розділ

Метою техніко-економічного розділу є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту мережі для підприємства і прийняття рішення про його подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для визначення загальної тривалості проведення НДР дані витрат часу з окремих операцій доцільно звести у таблицю 4.1.

4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломник; консультант техніко-економічного розділу (таблиця 4.1).

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

Посада виконавців	Місячний оклад (стипендія), грн.
Керівник ДП, викладач	4916,00
Консультант техніко-економічного розділу, доцент	6026,00
Студент	1300,00

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} , \quad (4.1)$$

де n_{ij} – чисельність розробників *i*-ої спеціальності *j*-го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником *i*-ої спеціальності *j*-го тарифного розряду, год;

C_{ij} – годинна ставка працівника *i*-ої спеціальності *j*-го тарифного розряду, грн.

Середньогодинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_i}, \quad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника *i*-ої спеціальності *j*-го тарифного розряду, грн;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ - місячний фонд робочого часу працівника *i*-ої спеціальності *j*-го тарифного розряду, год. (приймаємо 168 год).

Коефіцієнт *h*, який визначає розмір додаткової заробітної плати, для керівника та консультанта техніко-економічного розділу дорівнює 1,47.

Середньогодинна ставка керівника ДП дорівнює:

$$C_{ij} = \frac{4916 \cdot (1+1{,}47)}{168} = 72{,}28 \text{ грн/год.}$$

Середньогодинна ставка консультанта техніко-економічного розділу ДП дорівнює:

$$C_{ij} = \frac{6026 \cdot (1 + 1{,}47)}{168} = 88{,}60 \text{ грн/год.}$$

Середньогодинна оплата студента дорівнює:

$$C_{ij} = \frac{1300}{168} = 7{,}73 \text{ грн/год.}$$

Звідси, загальні витрати на оплату праці ($B_{ОП}$) дорівнюють:

$$B_{ОП} = 16 \cdot 72{,}28 + 144 \cdot 7{,}73 + 2 \cdot 88{,}60 = 2446{,}80 \text{ грн.}$$

Дані для розрахунку витрат на оплату праці наведено в таблиці 4.2

Таблиця 4.2 - Середній час виконання НДР та стадії (операції) технологічного процесу

Назва операції (стадії)	Середній час виконання операції, год.	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн.
Керівник ДП, викладач	16	72,28	1156,48
Консультант ТЕР, доцент	2	88,60	177,20
Розробка проекту мережі, студент	144	7,73	1113,12
Разом			2446,80

Крім того, слід визначити відрахування на соціальні заходи. Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

$$B_{Ф} = 0{,}205 \cdot B_{\text{ОП}},$$

$$B_Ф = \frac{20,5}{100} \cdot 2446,80 = 501,59 \text{ грн.}$$

Загальна сума витрат на матеріальні ресурси (B_M) визначається за формулою:

$$B_M = \sum_{i=1}^{n} K_i \cdot Ц_i, \qquad (4.3)$$

де K_i - витрата і-го типу матеріалу, натуральні одиниці вимірювання;

$Ц_i$ - ціна за одиницю *i*-го типу матеріалу, грн;

i - тип матеріального ресурсу;

n - кількість типів матеріальних ресурсів.

Звідси, витрати на матеріальні ресурси дорівнюватимуть:

B_M =48000,00+24000,00+2530,00+20890,00+450,00+1100,00=96970,00 грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна за одиницю, грн.	Загальна сума, грн.
Маршрутизатор Cisco 2811	шт.	3	16000,00	48000,00
Комутатор 2950-24	шт.	2	12000,00	24000,00
Безпровідний маршрутизатор 300N	шт.	1	2530,00	2530,00
Server PT	шт.	1	20890,00	20890,00
Перехресний кабель	м.	25	18,00	450,00
Прямий кабель	м.	100	11,00	1100,00
Разом		9		96970,00

Загальна сума витрат на електроенергію розраховується за формулою:

$$B_E = \sum_{i=1}^{n} P_i \cdot k_i \cdot T_i \cdot Ц \,, \qquad (4.4)$$

де P_i - паспортна потужність *i*-го електрообладнання, кВт;

k_i - коефіцієнт використання потужності *i*-го електрообладнання (приймається 0,7¸ 0,9);

T_i - час роботи і-го обладнання за весь період розробки, год;

Ц - ціна електроенергії, грн / кВт·год;

i - тип електрообладнання;

n - кількість електрообладнання.

Для розробки проекту даної комп'ютерної мережі використовується один ПК потужністю P = 0,22 кВт з монітором потужністю P = 0,013 кВт, який за весь період розробки працює 25 годин, та друкуючий пристрій потужністю P = 0,37 кВт, який працює 3 години.

$$B_E = 0{,}9 \cdot (0{,}22 + 0{,}013) \cdot 25 \cdot 0{,}9 + 0{,}9 \cdot 0{,}37 \cdot 3 \cdot 0{,}9 = 5{,}61 \text{ грн.}$$

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосуємо метод прямолінійного списання. Загальна сума амортизаційних відрахувань (B_{AM}) визначається за формулою:

$$B_{AM} = \sum_{i=1}^{n} \frac{B_i \cdot H_i}{100}, \qquad (4.5)$$

де B_i - вартість *i*-го обладнання на початок звітного періоду, грн;

H_i - річна норма амортизації *i*-го обладнання, %;

i - тип обладнання;

n - кількість обладнання.

Для проектування даної комп'ютерної мережі використовуються один ноутбук вартістю 7300 грн., та принтер вартістю 4150 грн.

Тоді:

$$B_{AM} = \frac{7300 \cdot 10}{100} + \frac{4150 \cdot 20}{100} = 1560{,}00 \text{грн.}$$

Транспортні витрати слід прогнозувати у розмірі 8–12 % від загальної суми матеріальних витрат.

$$B_T = 0.08 \cdot B_M \,, \tag{4.6}$$

де B_T – транспортні витрати.

$$B_T = 0{,}08 \cdot 96970\,{,}00 = 7757\,{,}60 \text{ грн.}$$

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створенням необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати становлять 150 % від суми основної та додаткової заробітної плати працівників.

$$H_B = 1{,}5 \cdot B_{ОП} \,, \tag{4.7}$$

де H_B – накладні витрати.

$$H_B = 1{,}5 \cdot 2446{,}80 = 3670{,}20 \text{ грн.}$$

Загальні витрати (B_{KC}) розрахуємо за формулою:

$$B_{КС} = B_{ОП} + B_{Ф} + B_{М} + B_{Е} + B_{АМ} + B_{Т} + H_{В} \quad (4.8)$$

Результати проведених розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат

Зміст витрат	Сума, грн.
Витрати на оплату праці (осн. і дод. ЗП)	2446,80
Відрахування на соціальні заходи	501,59
Матеріальні витрати	96970,00
Витрати на електроенергію	5,61
Амортизаційні відрахування	1560,00
Транспортні витрати	7757,60
Накладні витрати	3670,20
РАЗОМ по кошторису	112911,80

4.2 Розрахунок ціни проекту

Договірна ціна ($Ц_Д$) для проектних рішень розраховується за формулою:

$$Ц_Д = B_{КС} \cdot \left(1 + \frac{p}{100}\right), \quad (4.9)$$

де $B_{КС}$ – кошторисна вартість, грн;

p - середній рівень рентабельності, % (приймаємо 26% за погодженням з керівником).

$$Ц_Д = 112911{,}80 \cdot (1+0{,}26) = 142268{,}86 \text{ грн.}$$

4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень

Економічна ефективність (E_P) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_P = \frac{П}{B_{КС}}\ , \qquad (4.10)$$

де $П$ – прибуток, грн;

$B_{КС}$ – кошторисна вартість, грн.

$$E_P = 30016{,}81 / 112911{,}80 = 0{,}26$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_P):

$$T_P = \frac{1}{E_P} \qquad (4.11)$$

Тобто:

$$T_P = 1/0{,}26 = 3{,}8 \text{ р.}$$

Прийнятним вважається термін окупності близький до 7 років.

Розраховані економічні показники проекту занесемо до таблиці 4.5.

Таблиця 4.5 - Економічні показники розробки

Показник	Значення
Собівартість, грн.	112911,80
Плановий прибуток, грн.	30016,81
Ціна, грн.	142268,86
Економічна ефективність	0,26
Термін окупності, рік	3,8

Враховуючи основі економічні показники з таблиці 4.5, можна зробити висновок, що при економічній ефективності 0,26 та терміні окупності – 3,8 роки проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним. Як можна побачити із розрахунків, основними є матеріальні витрати. Тому, з метою зниження вартості мережі, варто було б здійснювати закупівлю обладнання у офіційних дилерів вказаних марок обладнання.

ВИСНОВКИ

У даній дипломній роботі були вирішені поставлені завдання, такі як:

1. Проаналізовано основні загрози комп’ютерних мереж.

2. Проаналізовано основні способи забезпечення надійності комп’ютерних мереж.

3. Здійснено вибір апаратного забезпечення.

4. Здійснено розробку структури мережі. В результаті було створено логічну структуру мережі підприємства, а також змодельовано мережу на основі технології IP.

5. Забезпечено захист даних на комутаторі та захист безпровідної мережі.

6. Проведено моделювання комп’ютерної мережі в сережовищі Cisco Packet Tracer. Перевірено роботу робочих станцій за допомогою консольної утиліти “ping”: зв'язок між ними в межах однієї підмережі, зв'язок із ПК з іншої підмережі, зв'язок між ПК та ноутбуками. Таким чином перевірялись і правильність налаштування портів маршрутизаторів та комутаторів. Останнім етапом тестування зроблено перевірку коректної роботи IP-телефонів. Для цього було використано режим симуляції дзвінка. Було перевірено зв'язок між IP-телефонами однієї підмережі і поазано, що IP-телефони та прохідні порти на комутаторах і маршрутизаторах було налаштовано вірно.

7. Зроблено розрахунок економічної ефективності проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Смирнов И.Г. Структурированные кабельные системы - проектирование, монтаж и сертификация./ И.Г. Смирнов – СПб.: Экон-Информ, 2005.- 131 с.

2. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей. функции, выбор, разработка./ Ю.В. Новиков., Д.Г. Карпенко – Москва: 1998.- 110 с.

3. Платонов В.В. Программно-аппаратные средства защиты информации./ В.В. Платонов – Москва: Информационная безопасность, 2013 . – 69 с.

4. Одом У. Компьютерные сети. Первый шаг./ У. Одом – СПб.: «Вильямс», 2006 . – 240 с.

5. Сайт: методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” 2011р [Електронний ресурс] – Режим доступу: http://buklib.net/books/23878/

6. Купер Д. Архитектура корпоративных сетей/ Д. Купер – Москва: МПРЕСС, 2014 – 94 с.

7. Гамаюн І. П. Оцінювання міри схожості між об’єктам, що характеризуються кількісними і номінальними ознаками / І.П. Гамаюн, О.П. Безменова – Харків : НТУ «ХПІ», 2013. – 9 с.

8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. / Б. Скляр - Москва: Информатика. Компьютеры, 2003. – 1106 с.

9. Сапаров В.Е. Руководящий документ. Выпускные квалификационные работы. Общие требования по оформлению пояснительной записки / В.Е. Сапаров - Самара: ПГУТИ, 2009. - 28 с.

10. Кулаков Ю.А. Локальні мережі. Навчальний посібник. / Ю.А. Кулаков, Г.М. Луцький - Київ: Юніор, 1998. – 45 с.

11. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире./ Б.Шнайер – СПб.: «Питер», 2003. – 368 с.

12. Портнов, Э.Л. Оптические кабели связи [Текст] / Э.Л. Портнов– М. «Информсвязь», 2000 – 112 с.

13. Руководство по Cisco IOS [Текст]. - СПб.: Питер, М.: Издательство «Русская Редакция», 2008. -784 с

14. Официальный сайт произвоизводителя оборудования Cisco Systems [Электронный ресурс] / Режим доступа – http://www.cisco.com.

15. Транспортные сети и системы электросвязи. Системы мультиплексирования: Учебник для студентов ВУЗов по специальности «Телекоммуникации» [Текст] / Под ред. В.К. Стеклова. – К.; 2003 – 352 с.

16. Дональд, Дж. Стерлинг. Техническое руководство по волоконной оптике [Текст] / Дональд Дж. Стерлинг., пер. Московченко А. – Издательство «ЛОРИ» – 1998.

17. Официальный сайт компании D-Link. Техническое описание медиаконвертора DMC-920 [Электронный ресурс] / Режим доступа – http://ftp.dlink.ru/pub/transciever_mediaconverter/DMC-920/Data_sh.

18. Основы организации сетей Cisco, том 2 [Текст].: Пер. с англ. - М.: Издательский дом «Вильямс», 2005. - 215 с.

19. Слепов Н.Н. Оптоволоконные системы дальней связи. Перспективы развития [Текст] // Н.Н. Слепов. - Электроника: НТБ – 2004. – 109 с.

20. Кульгин М. Технологии корпоративных сетей. / М. Кульгин. - Изд. «Питер», 1999. – 154 с.

21. Виткев О. Основы сетей Cisco, том 1. / Виткев О. М.: Издательский дом "Вильяме", 2005. – 231 с.

22. Перминов С. Построение розничных и дистрибьюторских сетей. / С. Перминов. - СПБ.: Информатика. Компьютеры, 2014. - 55с.

23. Олексюк В., Балик Н., Балик А. Організація комп’ютерної локальної мережі. / В. Олексюк, Н. Балик, А. Балик. – Тернопіль: Підручники та посібники, 2006. – 41 с.

24. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та мережі» / О.М. Березький, Л.О. Дубчак, Р.Б Трембач, Г.М. Мельник,

Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2016.–65 с.

25. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп'ютерна інженерія/ І.Р. Паздрій – Тернопіль: ТНЕУ, 2014. – 37 с.