ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента (ки) **Забродського А.В**
(прізвище та ініціали)
представлену на здобуття освітнього ступеня «бакалавр»
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему Захищена комп'ютерна мережа організації на базі протоколу OSPF

2. Актуальність. В умовах сьогодення однією з характерних рис розвитку суспільства безперервний розвиток комп'ютерних технологій. Основним елементом сучасних технологій комп'ютер, який використовується в усіх сферах людського життя: в побуті, на підприємствах, банках,в системах зв'язку і управління транспортом, сфері розваг тощо. Сучасне суспільство характеризується проникненням бізнесу у всі сфери людського життя. При цьому в діловому світі можна спостерігати дві незаперечні тенденції - до укрупнення бізнесу і до збільшення ролі, яку ньому відіграють сучасні системи комунікації. Насправді, керування великим підприємством може бути успішним лише в разі узгодженості дій її ключових структурних підрозділів.

(зазначити, які питання теоретичного і практичного характеру визначають актуальність роботи)

3. Основний зміст роботи викладено на 76 сторінках тексту, містить 3 таблиці та 41 ілюстрацію Список використаних літературних джерел налічує 28 найменувань.

4. Зміст розділів роботи *(зазначити за кожним розділом, які питання досліджені та з якою метою)*

Розділ 1. Теоретичні відомості за наданим технічним завданням. У даному розділі виконано постановку задачі, наведені теоретичні відомості про компанію Cisco та досліджено протокол маршрутизації OSPF, описано загальні відомості про міжмережеву операційну систему, а також наведені теоретичні відомості про списки доступа (ACL).

Розділ 2. Розробка та проектування топології комп'ютерної мережі. У розділі здійснено вибір мережевої топології та обладнання для організації роботи мережі, розроблено схему адресації пристроїв.

Розділ 3. Налагодження обладнання. Описано процеси налагодження пристроїв мережі, захисту мережі, та здійснено перевірку працездатності мережі.

5. Висновки обгрунтовані, повністю відповідають поставленим завданням, мають теоретичне та практичне значення. Практичне значення отриманих результатів полягає у проектуванні та розробці захищеної комп'ютерної мережі підприємства на базі протоколу OSPF та симуляції її використання на базі програмного забезпечення Graphical Network Simulator-3.

(обґрунтованість, теоретичне і практичне значення)

6. Список використаних літературних джерел. Джерела опрацьовані у повному обсязі відповідають змісту роботи.

(обсяг і повнота опрацювання за змістом роботи)

7. Додатки _____

(перелік додатків та повнота їх опрацювання за змістом роботи)

8. Таблиці та ілюстрації Ілюстрації носять інформаційний характер, є доповненням до змісту роботи. _____

(призначення таблиць та їх використання для підтвердження досліджень в роботі)

9. Якість оформлення роботи на достатньому рівні _____

10. Ставлення студента (ки) до виконання випускної кваліфікаційної роботи відповідально

11. Висновок

В цілому при написанні випускної кваліфікаційної роботи студент (ка) **Забродський А.В.**

(*прізвище та ініціали)*

вміння /невміння/ підібрати необхідну літературу, інформаційну базу, проаналізувати їх, зробити відповідні висновки і оформити свої дослідження у випускній кваліфікаційній роботі.

Випускна кваліфікаційна робота студента (ки) **Забродського А.В.**

(*прізвище та ініціали)*

написана на достатньо /недостатньо/ високому рівні та може /не може/ бути допущена до захисту в Екзаменаційній комісії.

Науковий керівник д. п.н., доцент, професор кафедри інженерії програмного забезпечення

(*вчений ступінь, звання, посада)*

(*підпис)* Вакалюк Т.А.

(*прізвище та ініціали)*

«17» 06 2020 р.

РЕЦЕНЗІЯ

на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Забродського Андрія Віталійовича
на тему: „Проект захищеної комп'ютерної мережі організації
на базі протоколу OSPF"

Кваліфікаційну роботу студента Забродського А. В. "Проект захищеної комп'ютерної мережі організації на базі протоколу OSPF" присвячено актуальній тематиці – розробленню захищеної мережі підприємства на базі протоколу OSPF.

Робота містить проект мережі на основі обладнання Cisco, виконаний у середовищі GNS3. До складу пояснювальної записки входить вступ, три розділи основного тексту, висновки, список використаної літератури, два додатки.

У першому розділі пояснювальної записки здійснено аналіз теоретичних відомостей про досліджувані технології. Зокрема, розглянуто операційну систему Cisco IOS, протокол динамічної маршрутизації OSPF та списки керування доступом (ACL).

У другому розділі пояснювальної записки виконано проектування мережевої топології, сформовано таблиці параметрів та адресації підмереж, обрано мережеве обладнання та описано його основні можливості, розроблено базову політику безпеки системи.

У третьому розділі пояснювальної записки описано базові налаштування пристроїв мережі, зокрема адресація (статична та динамічна), маршрутизація (статична та за протоколом OSPF). Налагоджено NAT та списки доступу. Протестовано функціонування мережі. Проаналізовано результати тестування, сформовано висновки щодо перспектив поліпшення роботи мережі.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на належному рівні. Тему роботи розкрито досить повно. Студентом продемонстровано ґрунтовні теоретичні знання та практичні фахові навички. Пояснювальну записку сформовано загалом логічно, науково й технічно грамотно. Функціонал проекту мережі відповідає заявленому.

Позитивний бік роботи полягає у тому, що одержані результати може бути застосовано для налаштування реального обладнання мережі та для дослідження різноманітних атак на подібні мережі. Водночас, робота має низку недоліків, серед яких: некоректне формулювання предмету дослідження, помилкові використання деяких термінів, значні відмінності між україномовним та англомовним варіантом реферату, деякі відхилення від вимог щодо оформлення пояснювальної записки (наприклад, відсутність номеру в заголовку підрозділу 2.3), недостатня кількість посилань на літературні джерела. Вказані недоліки у цілому не знижують досить високу якість і актуальність роботи.

У цілому кваліфікаційна робота студента Забродського А. В. „Проект захищеної комп'ютерної мережі організації на базі протоколу OSPF" відповідає вимогам рівня вищої освіти "бакалавр" спеціальності 123 "Комп'ютерна інженерія" і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – "добре".

Рецензент,
доцент кафедри
КІ та КБ, к.пед.н.
19 червня 2020 р.



О. С. Головня

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

Пояснювальна записка

до випускної кваліфікаційної роботи бакалавра

на тему:

«Захищена комп’ютерна мережа організації на базі протоколу OSPF»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Забродський А.В
Керівник, професор кафедри ІПЗ, д. пед. н.,
доцент_____ Вакалюк Т.А.
Рецензент, доцент кафедри КІ та КБ к.пед.н.,
_____ Головня О.С.

Житомир – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студента **Забродського Андрія Віталійович**
Тема роботи: **Захищена комп'ютерна мережа організації на базі протоколу OSPF**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Графічний симулятор мереж GNS3
3. Маршрутизатори Cisco 3660
4. Комутатори Cisco 2960
5. Операційні системи Cisco IOS, Windows XP.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Вакалюк Т.А.	06.04.2020	06.04.2020
2	Вакалюк Т.А.	20.04.2020	20.04.2020
3	Вакалюк Т.А.	11.05.2020	11.05.2020

Керівник _____ Вакалюк Т.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 7 квітня 2020	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації периметрового захисту для сучасних мереж	8 квітня 2020 – 11 квітня 2020	Виконано
3	Аналіз технологій периметрового захисту на основі міжмережного екранування	12 квітня 2020 – 16 квітня 2020	Виконано
4	Аналіз можливостей мережного обладнання Cisco для організації периметрового захисту	17 квітня 2020 – 19 квітня 2020	Виконано
5	Розробка загального проекту мережі організації	20 квітня 2020 – 24 квітня 2020	Виконано
6	Проектування підсистеми периметрового захисту та вибір обладнання для її реалізації	25 квітня 2020 – 30 квітня 2020	Виконано
7	Розробка політики безпеки периметрового захисту	1 травня 2020 – 4 травня 2020	Виконано
8	Проектування та створення сценаріїв тестування функціоналу підсистеми	5 травня 2020 – 9 травня 2020	Виконано
9	Базове налагодження пристроїв мережі	10 травня 2020 – 13 травня 2020	Виконано
10	Налагодження підсистеми периметрового захисту	14 травня 2020 – 18 травня 2020	Виконано
11	Тестування роботи підсистеми периметрового захисту	19 травня 2020 – 22 травня 2020	Виконано
12	Аналіз результатів тестування	23 травня 2020 – 24 травня 2020	Виконано
13	Написання пояснювальної записки	25 травня 2020 – 29 травня 2020	Виконано
14	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 8 червня 2020	Виконано
16	Захист	13 червня 2020	Виконано

Студент _____Забродський А.В

Керівник _____Вакалюк Т.А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми периметрового захисту мережі та пояснювальної записки до нього. Пояснювальна записка до роботи містить 76 сторінок, 41 ілюстрацію та 3 таблиці.

Метою роботи є розробка захищеної комп'ютерної мережа організації на базі протоколу OSPF за допомогою обладнання Cisco.

В роботі визначено основні завдання на розробку підсистеми, яка забезпечить захист від зовнішніх втручань. Також в роботі проаналізовані різні види захисту мереж на базі обладнання Cisco, обґрунтовано актуальність даної системи захисту, обґрунтований вибір виробника обладнання – Cisco. Розроблені, сформовані та налагоджені загальний проект мережі та проект підсистеми захисту. Наведено загальна топологія мережі був проведений опис конкретних серій обладнання, що будуть використані при побудові даного проекту захисту, опис політики інформаційної безпеки та тестування проекту. Також наводяться результати тестування системи. Наглядно розглянуто налаштування DHCP і NAT.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, OSPF, МЕРЕЖА, NAT, CISCO, DHCP.

ABSTRACT

The bachelor's thesis consists of a program complex based on the program Graphical Network Simulator-3 for modeling the performance of the computer network of the enterprise based on the OSPF protocol. The documentation for the bachelor's thesis contains 76 pages, 41 illustrations and 3 tables.

The purpose of the thesis is to develop a computer network using GNS, which simulates the process of network operation based on the OSPF protocol, which includes interaction with the main elements of its protection against interference.

The work also contains the main taskspromising development of the system, analyzed analogues of the developed system. The test results of the system are also present in the thesis.

KEYWORDS: PROTECTION, OSPF, NETWORK, NAT, CISCO, DHCP.

ЗМІСТ

РЕФЕРАТ **6**

ABSTRACT **3**

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ **5**

ВСТУП **7**

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ЗА НАДАНИМ ТЕХНІЧНИМ ЗАВДАННЯМ **9**

1.1 Постановка задачі 9

1.2 Теоретичні відомості про компанію Cisco 10

1.3 Теоретичні відомості про протокол маршрутизації OSPF 15

1.4 Загальні відомості про міжмережеву операційну систему 21

1.5 Теоретичні відомості про списки доступу (ACL) 23

Висновки до розділу 1 27

РОЗДІЛ 2. РОЗРОБКА ТА ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМПЮТЕРНОЇ МЕРЕЖІ **28**

2.1 Вибір мережевої топології 28

2.2 Вибір обладнання для організації роботи мережі 32

Розробка схеми адресації пристроїв 39

Висновки до розділу 2 42

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ **43**

3.1 Налагодження пристроїв мережі 43

3.2 Налагодження захисту мережі 46

3.3 Перевірка працездатності мережі 50

Висновки до розділу 3 57

ВИСНОВКИ **58**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **60**

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN– (Virtual Private Network) – віртуальна приватна мережа.

MPLS – (Multiprotocol Label Switching) – багатопротокольна комутація по міткам.

NGN – (Next Generation Network) – мережі нового покоління.

IP – (Internet Protocol) – міжмережевий протокол.

BGP – (Border Gateway Protocol) – протокол граничного шлюзу.

VR – (Virtual Reality) – віртуальна реальність.

VPLS – (Virtual Private Local Area Network Service) – віртуальна приватна локальна мережа).

WAN – (Wide Area Network) – глобальна мережа.

Frame Relay – ретрансляція кадрів.

ATM – (Asynchronous Transfer Mode) – асинхронний спосіб передачі даних.

L2 VPN – Layer 2 VPN.

L3 VPN – Layer 3 VPN.

POP – (Point of precense) – точка присутності.

ПК – персональний комп’ютер.

ПЗ – програмне забезпечення.

PPTP – (Point-to-Point Tunneling Protocol) – тунельний протокол точка-точка.

PPPoE – (Point-to-point protocol over Ethernet) – протокол передачі кадрів PPP через Ethernet.

IPSec – (IPSecurity) – протокол захисту даних, що передається через IP.

ЛОМ – локальна обчислювальна мережа.

TCP – (TransmissionControlProtocol) – протокол керування передачею даних.

CER – (Customer Enge Router) – граничний маршрутизатор клієнта.

PER – (Provider Enge Router) – граничний маршрутизатор мережі провайдера.

MAC – (Media Access Control) – фізична адеса пристрою.

LSP – (Label Switch Path) – тунель, шлях в MPLS.

EIGRP – (Enhanced Interior Gateway Routing Protocol) – протокол маршрутизації.

OSPF – (Open Shortest Path First) – протокол динамічної маршрутизації.

VRF – (Virtual Routing and Forwarding) – технологія, що дозволяє реалізовувати на базі одного фізичного маршрутизатора мати декілька віртуальних.

CEF – (Cisco Express Forwarding) – технологія високошвидкісної маршрутизації.

STP – (Spanning Tree Protocol) – протокол покривного дерева.

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

LAN – (Local Area Network) – локальна мережа.

ВСТУП

В умовах сьогодення однією з характерних рис розвитку суспільства є безперервний розвиток комп’ютерних технологій. Основним елементом сучасних технологій є комп'ютер, який використовується в усіх сферах людського життя: в побуті, на підприємствах, в банках,в системах зв'язку і управління транспортом, сфері розваг тощо.

Сучасне суспільство характеризується проникненням бізнесу у всі сфери людського життя. При цьому в діловому світі можна спостерігати дві незаперечні тенденції - до укрупнення бізнесу і до збільшення ролі, яку в ньому відіграють сучасні системи комунікації.

Насправді, керування великим підприємством може бути успішним лише в разі узгодженості дій її ключових структурних підрозділів. І все ж таки, потрібно розуміти, що глобальна мережа Інтернет протягом багатьох років перестала бути тільки мережею передачі даних і навіть її цінність, як джерело інформації, з точки зору ділового співтовариства, також відходить на задній план. Інтернет сьогодні - це одночасно: активний споживчий ринок, товарна і валютна біржа, щодня на просторах світової «павутини» відбуваються угоди на астрономічні суми. Але сучасні послуги Інтернету необхідні не тільки діловим замовникам - мережа все частіше використовується рядовими користувачами: вона стає доступом до популярних розваг, елементом престижу, засобом заробітку тощо. По мірі розвитку і ускладнення послуг, вони ,зазвичай, стають більш вимогливі до ресурсів мережі зв'язку на базі якої надаються. Внаслідок цього термін «сучасні послуги зв'язку» часто нероздільний з поняттям «широкосмуговий доступ».

Попит на такі послуги призвів до революційної зміни сучасних телекомунікаційних мереж і завданням будь-якого оператора і провайдера послуг стає знаходження оптимального способу їх надання з найбільшою вигодою для себе і з найкращою якістю для замовника. Однією з технологій, що сприяли згаданій революції є технологія OSPF. Незважаючи на свій досить

поважний вік, вона вже протягом десятиліть являється досить популярною технологією.

Протокол був розроблений у зв'язку з необхідністю в інтернет-співтоваристві впровадити непатентований внутрішній протокол шлюзу (IGP) з високою функціональністю для сімейства протоколів TCP / IP. OSPF це динамічний, ієрархічний протокол стану зв'язку, який використовується для маршрутизації всередині автономних систем.

Метою дипломної роботи є проектування та розробка захищеної комп'ютерної мережі підприємства на базі протоколу OSPF та симуляції її використання на базі програмного забезпечення Graphical Network Simulator-3.

Встановлена мета обумовлює наступні **завдання**:

- проведення аналізу задач симуляції мережі підприємства;
- визначення архітектури та узагальненої структури системи;
- обґрунтування та вибір засобів реалізації системи;
- розробка інформаційного та математичного забезпечення системи;
- проектування структурних складових та алгоритмів роботи системи.

Об’єктом дослідження є захищена комп’ютерна мережа організації.

Предметом дослідження є засоби розробки симуляції комп'ютерної мережі.

Розроблена система може бути використана для прикладного створення комп'ютерної мережі підприємства.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ЗА НАДАНИМ ТЕХНІЧНИМ ЗАВДАННЯМ

1.1 Постановка задачі

На сьогоднішній день у світі існує понад 130 мільйонів комп'ютерів і більше 80% з них об'єднані в різноманітні інформаційно-обчислювальні мережі (від малих локальних мереж в офісах - до глобальних мереж типу Internet).

Всесвітня тенденція до об'єднання комп'ютерів у мережу обумовлена переліком важливих причин, таких як потреба в прискоренні передачі даних, можливість швидкого обміну інформацією між користувачами, одержання і передача (факсів, E-mail листів і іншого) не відходячи від робочого місця.

В дипломній роботі необхідно розробити комп'ютерну мережу підприємства, що найбільше наблизить процес використання мережі до реалістичного. Для реалізації поставленого завдання, основними етапами є:

1. Планування мережі:

1.1. Створення загальної концепції мережі.

1.2. Визначення, для вирішення яких прикладних задач буде використовуватися мережа.

1.3. Необхідність підключення до глобальних або до інших локальних мереж.

1.4. Вимоги до програмних засобів за допустимим розміром мережі, швидкістю, гнучкістю, розмежуванням прав доступу, вартості, за можливостями контролю обміну інформацією тощо.

1.5. Технічні характеристики обладнання і його вартість.

1.6. Основні напрями та інтенсивність інформаційних потоків у мережі.

1.7. Характер інформації (дані, відео, аудіо, зображення), що передається мережею, бо це безпосередньо позначається на необхідній швидкості передачі.

1.8. Контроль її працездатності та безпеки.

1.9. Розмір мережі.

2. Побудова комп'ютерної моделі з використанням додатку Graphical Network Simulator-3:

2.1. Можливості монтажу кабельної системи у приміщеннях і між ними, а також заходи по забезпеченню цілісності кабелю.

2.2. Структуру, ієрархію і основні частини мережі (по підрозділах підприємства, а також по приміщеннях, поверхах і будівлях підприємства).

2.3. Вибір мережевого апаратного забезпечення.

3. Проведення комп'ютерного експерименту:

3.1. Комп’ютерне моделювання.

3.2. Цикл комп'ютерного експерименту.

4. Аналіз отриманих результатів:

4.1. Доцільність використання

Результатом реалізації поставленого завдання є створення комп'ютерної мережі на базі протоколу OSPF.

1.2 Теоретичні відомості про компанію Cisco

Cisco Systems, Inc. - один зі світових лідерів в області постачання товарів, в тому числі програмного забезпечення, а також послуг у сфері створення і забезпечення роботи комп'ютерних мереж. Виробнича лінія компанії включає маршрутизатори, комутатори, пристрої віддаленого доступу, перетворювачі протоколу, пристрої інтернет-сервісів і організації мережі, програмне забезпечення управління мережею, які об'єднують географічно роззосереджені локальні мережі (LAN), глобальні мережі (WAN) та сам Інтернет [13].

Cisco обслуговує три головних сегменти ринку:

1. Великі організації, включаючи корпорації, рядові підприємства, інженерні мережі та навчальні заклади, що потребують складних мережевих рішень, які, як правило, пов'язують різні місця розташування.

2. Постачальників послуг, включаючи інтернет-провайдерів, телефонні і кабельні компанії, і провайдерів бездротового зв'язку.

3. Дрібні і середні підприємства, потреби яких включають підключення до Інтернету або зв'язок з бізнес-партнерами.

Компанія все більше розвиває експертні знання в області організації оптоволоконних мереж, а також супутніх експертних знань про роботу багатофункціональних мереж, які пропонують аудіо та відео можливості мережі на додаток до традиційних.

Cisco Systems була заснована в грудні 1984 року в Менло-Парку, Каліфорнія, співробітниками Стенфордського університету, сімейною парою - Леонардом Бозек і Сандрою Лернер. Бозек був менеджером лабораторії кафедри інформатики, а Лернер здійснювала контроль роботи комп'ютерів у вищій школі бізнесу. У Стенфорді Бозек створив спосіб об'єднання двох локальних мереж у відділах, де працювали він і його дружина, простягнувши для цього 500 ярдів кабелю по кампусу.

Спочатку Лернер і Бозек спробували продати міжмережеву технологію, яку розробив Бозек, існуючим комп'ютерним фірмам, але вони не зуміли нікого зацікавити новими можливостями. Тоді вони вирішили почати свою власну справу, Cisco Systems, засноване на цій технології. Між іншим, назва походить від скороченої форми назви міста Сан-Франциско. До Бозек і Лернер приєдналися в якості співзасновників колеги Грег Сец, Білл Вестфілд і Кірк Лоід. Стенфордський університет пізніше спробував отримати 11 мільйонів доларів в якості ліцензійної винагороди від нової компанії, тому що Бозек розробив технологію в період роботи в університеті, але, в кінцевому рахунку, університет погодився на компенсацію 150000 доларів, безкоштовні маршрутизатори, і службу підтримки.

У момент заснування компанія мала вкрай обмежений бюджет. Фактично, Бозек і Лернер довелося закласти їх будинок, збільшити заборгованість по кредитній карті і відстрочити виплату зарплат друзям, які працювали на них, щоб успішно запустити підприємство. І навіть після двох

років ведення бізнесу Лернер продовжувала працювати додатково, щоб отримати достатній рівень доходу для себе і своєї сім'ї.

Основним продуктом Cisco з самого початку був міжмережевий маршрутизатор, а також апаратні засоби злиття з програмним забезпеченням, які автоматично вибирають найефективніший маршрут для передачі даних між мережами.

Компанія ввела підтримку множинних протоколів (стандартів передачі даних) і тому могли об'єднувати різні види мереж з різною архітектурою, засновані на різних апаратних засобах, таких як персональні комп'ютери сумісні з IBM, комп'ютери Apple Macintosh, автоматизовані робочі місця UNIX та універсальні ЕОМ IBM.

Так, в 1986 році після того, як Cisco представила свій перший продукт - маршрутизатор для пакета протоколу TCP / IP (протокол TCP / інтернет-Протокол), вона стала першою компанією постачальником маршрутизаторів мультипротокол на комерційній основі. Рік по тому Cisco продавала маршрутизатори на загальну суму 250 000 доларів в місяць. Продажі в кінці бюджетного року - липні 1987 року становили 1.5 мільйони доларів, при цьому в компанії працювало лише 8 співробітників. Спочатку Cisco продавала свої маршрутизатори університетам, науково-дослідним центрам, авіакосмічній промисловості та урядовим організаціям, зв'язуючись з програмістами і інженерами через ARPANET, попередником того, що пізніше стало відомо, як Інтернет.

У 1988 році компанія налаштувалася на продаж своїх міжмережевих маршрутизаторів провідним корпораціям з географічно розосередженими підрозділами, які використовували різні мережі. З цією метою Cisco розробила маршрутизатори, що підтримують ще більшу кількість комунікаційних протоколів, в результаті чого стала лідером в своєму сегменті, так як маршрутизатори Cisco змогли підтримувати більше протоколів, ніж аналоги інших виробників.

До кінця 1980-х років, коли почав розвиватися комерційний ринок мережевого обміну, високоефективні маршрутизатори Cisco за помірною ціною мали конкретні переваги перед конкурентами.

Хоча у Cisco був високий показник зростання обсягу продажів, молода компанія все ще потребувала інвесторів; в 1988 Бозек і Лернер були змушені звернутися за підтримкою до венчурного капіталіста Дональду Т. Валентайн, з Sequoia Capital. Валентайн, однак, зажадав, щоб власники здали йому контрольний пакет акцій компанії. Таким чином, Валентайн став головою, а потім найняв Джона Моргріджа в якості нового президента компанії і генерального директора.

Моргрідж, який мав ступінь MBA Стенфордського університету, був виконавчим директором в компанії-виробнику ноутбуків GRiD Systems Corp., і до цього пропрацював шість років віце-президентом продажів і маркетингу в Stratus Computer. Моргрідж замінив кілька менеджерів Cisco, які були друзями Бозек і Лернер, на більш компетентних і досвідчених керівників. У лютому 1990 року Cisco стала акціонерним товариством, після чого Бозек і Лернер почали продавати їх акції. Продажі в закінченні бюджетного року - в липні 1990 р. становили 69,8 мільйонів доларів, чистий дохід становив 13.9 мільйонів доларів, а в компанії працювало 254 співробітника. При Моргрідж Бозек дали посаду керівника дослідницьких робіт, а Лернер зробили главою служби по роботі з клієнтами. Однак Лернер, як відомо, не була в добрих стосунках з Моргрідж і, в серпні 1990 року, вона була звільнена, після чого Бозек також пішов.

Коли Бозек і Лернер покинули компанію, вони продали залишок їх акцій за 100 мільйонів доларів. Пара згодом віддала більшу частину прибутку в їх улюблені благодійні установи. У вересні 1993 року Cisco за 95 мільйонів доларів придбала Crescendo Communications, в результаті чого з'явилися принципово нові продукти під назвою Copper Distributed Data Interface (CDDI).

Розвиток ATM технологій Crescendo стало основною причиною того, що компанія Cisco придбала цю фірму. Згодом Crescendo Communications було

перейменовано в Workgroup Business Unit, і розроблені ними технології комутації були пізніше включені в маршрутизатори Cisco. Друге велике придбання Cisco зробила в серпні 1994 року. Це була компанія Newport Systems Solutions, яка була куплена за 93 мільйони доларів в еквіваленті акцій. Newport Systems Solutions продали виробничу лінію LAN2LAN, а також програмне забезпечення, що використовується в з'єднанні локальних мереж. Цей програмний продукт став першим новим найменуванням продукції Workgroup Businesses Unit, починаючи з придбання Crescendo.

У початку 1994 року Cisco оголосила про створення нової мережевої архітектури, CiscoFusion, яка допоможе забезпечити клієнтам поступовий перехід від маршрутизаторів до нових комутаторів мережевих технологій перемикання LAN і ATM. CiscoFusion дозволив користувачам використовувати і спрямовувати комутаційні методи з максимальною зручністю. Кілька нових комутаційних продуктів були введені в березні 1994 року, як частина цієї архітектури, включаючи інтерфейсний процесор ATM і комутатор Catalyst FDDI-to-Ethernet LAN. У цей період Cisco перемістила свій головний офіс з одного кінця Силіконової Долини в інший, з Менло-Парку в недавно побудований комплекс офісної будівлі в Сан-Хосе, Каліфорнія. Зростаючий розмір компанії вимагав офісу більших розмірів. Трудові ресурси компанії виросли з 1 451 у липні 1993 року до 2 262 в липні 1994 року. В цьому році Cisco активно наймала талановиті кадри з менших, які перебувають в жахливому стані компаній, які змушені були звільняти персонал.

У 1994 фінансовому році Cisco отримала 1 мільярд доларів від продажу, закінчивши рік 31 липня 1994 року, з 1.24 мільярдами доларів в чистій сумі продажів, 92-відсотковим збільшенням обороту за попередній рік, і 314.9 мільйонами доларів чистого доходу, що на 83% більше, ніж в 1993 фінансовому році. Пізніше в жовтні 1994 року, Cisco завершила ще два придбання компаній, залучених в комутаційний сектор. Вона витратила 240 мільйонів доларів на Kalpana, Inc., виробника комутаційних продуктів Ethernet; і 120 мільйонів

доларів на LightStream Corp., який займався комутацією ATM і Ethernet, а також маршрутизацією.

1.3 Теоретичні відомості про протокол маршрутизації OSPF

Протокол OSPF (Open Shortest Path First) – це протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), який використовує для знаходження найкоротшого шляху алгоритм Дейкстри. Протокол OSPF являє собою протокол внутрішнього шлюзу (Interior Gateway Protocol — IGP). Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи [1].

Протокол був розроблений IETF в 1988 році. Остання версія протоколу представлена в RFC 2328 в 1998 році.

Серед властивостей протоколу OSPF слід виокремити такі:

– Висока швидкість збіжності;
– Підтримка мережних масок змінної довжини VLSM;
– Відсутність обмежень досяжності;
– Оптимальне використання пропускної здатності мережі;
– Оптимальний вибір шляху маршрутизації.

Згідно з RFC 2328 даний протокол є незапатентований тобто відкритий для громадськості, таким же, як є протокол RIP. Але OSPF на відміну від RIP, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), не має обмеження на довжину шляху 15-ма переходами, а також протокол враховує пропускну здатність мережі при виборі маршруту. Все це робить OSPF потужним, масштабованим протоколом маршрутизації.

Протокол OSPF є складним протоколом, який розроблений з урахуванням особливостей функціонування мереж, які відрізняються за типами, розмірами, структурою та іншими параметрами. Відповідно у протоколі наявна велика кількість функціональних можливостей з підтримки таких мереж. Зрозуміло, що при налагодженні функціонування протоколу слід враховувати: особливості типу мережі, її структури, розмір, інформаційні потоки, які

проходять через неї, зв’язки з іншими мережами тощо. Очевидно, що у різних випадках деякі етапи налагодження протоколу є обов’язковими або, принаймні, рекомендованими, деякі – непотрібними.

Початок роботи протоколу OSPF може виконуватися як у цілому на маршрутизаторі, так і на окремих його інтерфейсах. Зазвичай, коли використовується перший підхід, то на маршрутизаторі запускається лише один загальний локальний процес маршрутизації OSPF. У випадку другого підходу запускається кілька окремих процесів. Частина параметрів функціонування протоколу налагоджується глобально на весь пристрій, решта параметрів налагоджується на інтерфейсах маршрутизатора, які беруть участь у роботі протоколу для певних канальних сегментів мереж [2].

Існує три основні типи мережі:

– точка-точка (Point-to-Point);

– широкомовна мережа з множинним доступом (BMA, Broadcast Multiple Access);

– нешироковмовна мережа з множинним доступом (NBMA, Non-Broadcast Multiple Access).

Як правило, тип мережі визначається автоматично у відповідності до типу інтерфейсу. У цьому випадку і алгоритм функціонування OSPF обирається автоматично. У деяких випадках можлива (і є доцільною) зміна типу мережі на інтерфейсі з метою пришвидшення роботи та зменшення об’єму службового трафіка протоколу OSPF. Наприклад, двоточкове Ethernet-з’єднання між маршрутизаторами автоматично функціонуватиме як широкомовна мережа, хоча доцільніше його було б налагодити саме як двоточкове з’єднання.

За замовчуванням метрика маршруту у протоколі OSPF розраховується за стандартною формулою, яка використовує пропускні здатності окремих ділянок (інтерфейсів, канальних сегментів), з яких складається маршрут:

$$M = \sum_{i=1}^{N} \left\lceil \frac{RefBW}{BW_i} \right\rceil \qquad (1)$$

Формула (1) застосовується для розрахунку метрики, де M – метрика певного маршруту; N – кількість ділянок маршруту; RefBW (Reference BandWidth) – еталонна пропускна здатність, максимальне значення пропускної здатності для розрахунку метрик у протоколі OSPF, біт/с; за замовчуванням на момент прийняття стандарту встановлена як 108 біт/с.RefBW може змінюватися адміністративно; BWi (BandWidthi) – значення пропускної здатності і-ї ділянки (канального сегменту) маршруту, біт/с; за замовчуванням дорівнює фізичній пропускній здатності інтерфейсу; BWi може змінюватися адміністративно.

Необхідно зазначити, що метрика маршруту протоколу OSPF є величиною безрозмірною.

Стандартні значення метрик інтерфейсів за умови використання стандартного значення RefBW для найбільш поширених технологій наведені у табл. 1.1.

У мережах з множинним доступом відносини сусідства встановлюються між всіма маршрутизаторами. Якби всі маршрутизатори в стані сусідства обмінювалися топологічною інформацією, це призвело б до розсилання великої кількість копій оголошень про стан каналів (link-state advertisement, LSA). Якщо, приміром, кількість маршрутизаторів в мережі з множинним доступом рівне n, то буде встановлено n•(n-1)/2 стосунків сусідства. Кожен маршрутизатор буде розсилати n-1 LSA своїм сусідам, плюс одне LSA для мережі, в результаті мережа згенерує n^2 LSA. Для запобігання проблеми розсилки копій LSA в мережах з множинним доступом вибирається виділений маршрутизатор (DR) і запасний виділений маршрутизатор (BDR).

Таблиця 1.1

Стандартні значення метрик інтерфейсів (каналів) протоколу OSPF

Технологія	Serial T1	Serial E1	Ethernet	Fast Ethernet	Gigabit Ethernet
Пропускна здатність, Мбіт/с	1,544	2,048	10	100	1000
Метрика інтерфейсу	64	48	10	1	1

Виділений маршрутизатор (designated router, DR) – керує процесом розсилки LSA в мережі. Кожен маршрутизатор мережі встановлює відносини суміжності з DR. Інформація про зміни в мережі відправляється маршрутизатором, який виявив ці зміни, на виділений маршрутизатор, а той, в свою чергу, відповідає за те, щоб ця інформація була відправлена іншим маршрутизаторам мережі. Недоліком в схемі роботи з DR маршрутизатором є те, що при виході його з ладу повинен бути вибраний новий DR. Нові відносини сусідства повинні бути сформовані і, поки бази даних маршрутизаторів не синхронізуються з базою даних нового DR, мережа буде недоступна для пересилки пакетів. Для усунення цього недоліку вибирається резервний виділений маршрутизатор.

Резервний виділений маршрутизатор (backup designated router, BDR). Кожен маршрутизатор мережі встановлює відносини сусідства не тільки з DR, але і BDR. DR і BDR також встановлюють відносини сусідства і між собою. При виході з ладу DR, BDR стає DR і виконує всі його функції. Так як маршрутизатори мережі встановили відносини сусідства з BDR, час недоступності мережі мінімізується. Маршрутизатор, обраний DR або BDR в одній приєднаній до нього мережі з множинним доступом, може не бути DR (BDR) в іншій приєднаній мережі. Роль DR (BDR) є властивістю інтерфейсу, а не властивістю всього маршрутизатора. Іншими словами, в кожному сегменті множинного доступу (наприклад, комутаційному сегменті Ethernet), в якому спілкуються два і більше OSPF-маршрутизатора, процес вибору і розподілу

ролей DR/BDR відбувається незалежно від інших сегментів множинного доступу.

Для обміну інформацією використовуються LSA-повідомлення, між відправкою яких встановлюються таймери протоколу:

HelloInterval – інтервал часу в секундах після закінчення якого маршрутизатор відправляє наступний hello-пакет з інтерфейсу. Для широкомовних мереж і мереж точка-точка значення за замовчуванням, як правило, 10 секунд. Для неширокомовних мереж з множинним доступом значення за замовчуванням 30 секунд;

RouterDeadInterval – інтервал часу в секундах після закінчення якого сусід буде вважатися «мертвим». Цей інтервал повинен бути кратним значенню HelloInterval. Як правило, RouterDeadInterval дорівнює 4 інтервалам відправки hello-пакетів, тобто за замовчуванням – 40 секунд;

Wait Timer – інтервал часу в секундах після закінчення якого маршрутизатор обере DR в мережі. Його значення дорівнює значенню інтервалу RouterDeadInterval;

RxmtInterval – інтервал часу в секундах після закінчення якого маршрутизатор повторно відправить пакет на який не отримав підтвердження про отримання (наприклад, Database Description пакет або Link State Request пакети). Цей інтервал називається також Retransmit interval. Значення інтервалу 5 секунд.

При поділі автономної системи на зони, маршрутизаторам приналежним до однієї зони не відома інформація про детальну топології інших зон.

У OSPF-мережах розрізняють 4 типи маршрутизаторів:

Внутрішній маршрутизатор (internal router) — маршрутизатор, усі інтерфейси якого належать одній зоні, має лише одну базу даних стану каналів;

Граничний маршрутизатор (area border router, ABR) — з’єднує одну або більше зон з магістральною зоною і виконує функції шлюзу для міжзонального трафіку, завжди має бути хоча б один інтерфейс який належить магістральній зоні, для кожної приєднаної зони підтримує окрему базу даних стану каналів;

Магістральний маршрутизатор (backbone router) — маршрутизатор у якого завжди хоча б один інтерфейс належить магістральній зоні, не завжди є граничним; внутрішній маршрутизатор, інтерфейси якого належать нульовій зоні, також є магістральним;

Граничний маршрутизатор автономної системи (AS boundary router, ASBR) — це маршрутизатор, один з портів якого знаходиться в домені OSPF протоколу, а другий в домені будь-якого іншого з внутрішніх шлюзових протоколів (наприклад RIP або EIGRP), може знаходитись в будь-якому місці автономної системи, окрім тупикової зони. Виняток з цього правила - ABR може бути і ASBR.

Для обміну інформації між маршрутизаторами щодо каналів маршрутизатора, всіх інтерфейсів та стану каналів використовуються LSA-повідомлення.

Алгоритм роботи протоколу OSPF:

Маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF. Маршрутизатори, що розділяють загальний канал передачі даних, стають сусідами, коли вони приходять до домовленості при певних параметрах, зазначених в їх hello-пакетах.

На наступному етапі роботи протоколу маршрутизатори будуть намагатися перейти в стан суміжності зі своїми сусідами. Перехід у стан суміжності визначається типом маршрутизаторів, які обмінюються hello-пакетами, і типом мережі, по якій передаються hello-пакети. OSPF визначає кілька типів мереж і кілька типів маршрутизаторів. Пара маршрутизаторів, що знаходяться в стані суміжності, синхронізує між собою базу даних стану каналів.

Кожен маршрутизатор посилає оголошення про стан каналу маршрутизаторам, з якими він знаходиться в стані суміжності.

Кожен маршрутизатор, який отримав оголошення від суміжного маршрутизатора, записує передану в ньому інформацію в базу даних стану

каналів маршрутизатора і розсилає копію оголошення всім іншим суміжним з ним маршрутизаторам.

Розсилаючи оголошення всередині однієї OSPF-зони, всі маршрутизатори будують ідентичну базу даних стану каналів маршрутизатора.

Коли база даних побудована, кожен маршрутизатор використовує алгоритм «найкоротший шлях першим» для обчислення графа без петель, який буде описувати найкоротший шлях до кожного відомого пункту призначення із собою як кореня. Цей граф - дерево найкоротших шляхів.

Кожен маршрутизатор будує таблицю маршрутизації зі свого дерева найкоротших шляхів.

1.4 Загальні відомості про міжмережеву операційну систему

Міжмережева операційна система Cisco (IOS) - це сімейство мережевих операційних систем, що використовуються на багатьох маршрутизаторах Cisco Systems і існуючих мережевих комутаторах Cisco. Раніше комутатори Cisco запускали CatOS. IOS це пакет функцій маршрутизації, комутації, міжмережевої взаємодії і телекомунікацій, інтегрованих в багатофункціональну операційну систему. Хоча база коду IOS включає в себе спільне багатозадачне ядро, більшість функцій IOS перенесено на інші ядра, такі як QNX і Linux, для використання в продуктах Cisco.

Не всі продукти Cisco працюють під управлінням IOS. Помітні виключення включають продукти безпеки ASA, які працюють під управлінням операційної системи Linux, маршрутизатори-носії, на яких працює IOS-XR, і продукти Cisco Nexus для комутаторів і FC, які працюють під управлінням Cisco NX-OS.

Мережева операційна система IOS була розроблена в 1980-х роках для маршрутизаторів, які мали тільки 256 КБ пам'яті і низьку обчислювальну потужність процесора. Завдяки модульним розширенням IOS був адаптований до розширення можливостей обладнання і нових мережевих протоколів. При розробці IOS основний лінійкою продуктів Cisco Systems були

маршрутизатори. Компанія придбала ряд молодих компаній, що спеціалізуються на мережевих комутаторах, таких як винахідник першого комутатора Ethernet Kalpana, і в результаті комутатори Cisco не працювали з IOS. Серія Cisco Catalyst протягом деякого часу буде працювати під управлінням CatOS. У ранніх модульних мережевих комутаторах шасі від Cisco модулі з функціями маршрутизації рівня 3 були окремими пристроями, що працюють під управлінням IOS, в той час як модулі комутатора рівня 2 працювали з CatOS. В кінцевому підсумку Cisco представила власний режим для шасі, так що вони працюють тільки з однієї операційною системою. Для комутаторів Nexus Cisco розробила NX-OS, яка аналогічна IOS, за винятком того, що вона заснована на Linux.

Cisco IOS має монолітну архітектуру через обмежені апаратних ресурсів маршрутизаторів і комутаторів в 1980-х роках. Це означає, що всі процеси мають прямий апаратний доступ для економії часу процесора. Між процесами немає захисту пам'яті, а IOS має планувальник виконання до завершення, що означає, що ядро не перешкоджає виконанню процесу. Замість цього процес повинен виконати виклик ядра, перш ніж інші процеси отримають можливість запуску. IOS розглядає кожен процес як окремий потік і привласнює йому пріоритетне значення, так що процеси з високим пріоритетом виконуються на ЦП перед поставкою в чергу процесів з низьким пріоритетом, але процеси з високим пріоритетом не можуть переривати виконання процесів з низьким пріоритетом.

Монолітне ядро Cisco IOS не забезпечує захист пам'яті для даних різних процесів. Вся фізична пам'ять відображається в одному віртуальному адресному просторі. Ядро Cisco IOS не виконує підкачування або обмін пам'яті. Тому адресується пам'ять обмежена фізичної пам'яттю мережевого пристрою, на якому встановлена операційна система. Однак IOS підтримує псевдонім дубльованого вмісту віртуальної пам'яті в тій же фізичної пам'яті. Ця архітектура була реалізована Cisco для забезпечення продуктивності системи і мінімізації операційних витрат операційної системи.

Недолік архітектури IOS полягає в тому, що вона збільшує складність операційної системи, може призвести до пошкодження даних, оскільки один процес може перезаписати дані іншого, а один процес може дестабілізувати всю операційну систему або навіть викликати програмний збій. У разі збою IOS операційна система автоматично перезавантажується і перезавантажує збережену конфігурацію.

1.5 Теоретичні відомості про списки доступу (ACL)

Access-list (ACL) - це набір правил, визначених для контролю мережевого трафіку і зниження мережевої атаки. ACL використовуються для фільтрації трафіку на основі набору правил, визначених для вхідної або вихідної мережі.[21]

Особливості ACL:

1. Певний набір правил відповідає послідовному, тобто зіставлення починається з першого рядка, потім з 2-й, потім з 3-й і так далі.
2. Пакети зіставляються доти, поки не будуть відповідати правилу. Як тільки правило порівнювати, подальше порівняння не виконується, і це правило буде виконано.
3. В кінці кожного ACL існує неявна заборона. Якщо не знайдено жодного умови або правила, пакет буде відкинутий.

Як тільки список доступу створений, його слід застосувати до вхідного або вихідного інтерфейсу:

1. Списки вхідного доступу - коли список доступу застосовується до вхідних пакетів інтерфейсу, спочатку пакети обробляються відповідно до списку доступу, а потім направляються на вихідний інтерфейс.
2. Списки вихідного доступу - коли список доступу застосовується до вихідних пакетів інтерфейсу, то спочатку пакет маршрутизироваться, а потім оброблятися на вихідному інтерфейсі.

Існує два основних типи доступу, а саме:

1. Стандартний список доступу - це список доступу, який складений лише за допомогою оригінального IP-адреси. Ці списки ACL дозволяють або забороняють весь набір протоколів. Вони не розрізняють IP-трафік, такий як TCP, UDP, Https і т. Д. Використовуючи номера 1-99 або 1300-1999, маршрутизатор буде розуміти його як стандартний ACL і вказану адресу як IP-адреса джерела.

2. Розширений список доступу - це ACL, який використовує IP-адреса джерела і одержувача. В ACL такого типу ми також можемо вказати, який IP-трафік повинен бути дозволений або заборонений. Вони використовують діапазон 100-199 і 2000-2699.

Останнім часом Access-list (ACL) використовувалися для фільтрації та захисту пакетів. ACL працює по послідовності правил, наданої адміністратором. Правила складаються з різних дозвільних і заборонних умов. Але недоліком ACL є те, що він фільтрує трафік тільки до транспортного рівня.

Тому для функціональності брандмауера з низьким бюджетом використовується маршрутизатор Cisco з правильною версією IOS. Ми можемо реалізувати міжмережевий екран на базі IOS двома способами:

1. Функції управління доступом на основі контексту (CBAC)

2. Зональний міжмережевий екран

ACL забезпечують фільтрацію і захист трафіку до транспортного рівня, в той час як CBAC забезпечує ту ж функцію на рівні додатків. За допомогою конфігурації CBAC маршрутизатор може діяти як міжмережевий екран.

CBAC просто працює як рефлексивний Access-list, але на додаток до цього він підтримує таблицю станів, в якій сеанси зберігаються в пам'яті. Коли сеанс ініціюється пристроєм в мережі, динамічна запис поміщається в таблицю станів, і виходить (що виходить) трафіку дозволяється проходити через маршрутизатор (міжмережевий екран на основі IoS). За допомогою цього запису відповідь вихідного трафіку може проходити через маршрутизатор (міжмережевий екран на основі IoS), оскільки він має запис для трафіку, ініційованого в мережі. Це досягається за допомогою механізму CBAC

брандмауера на основі IoS, оскільки він відкриває тимчасові діри в списку доступу (застосовується до вхідного трафіку), щоб дозволити відповідні пакети.

Деякі функції CBAC:

1. Перевірка трафіку - CBAC підтримує інформацію TCP / UDP, яка необхідна для більш глибокої перевірки корисного навантаження пакета.

2. Фільтрація трафіку - CBAC фільтрує трафік, що виходить із довіреної мережі, який проходить через брандмауер і дозволяє відповіді, тільки якщо у нього є запис у таблиці станів. Він має можливість інтелектуальної фільтрації трафіку до рівня 7.

3. Виявлення вторгнення - CBAC перевіряє швидкість, з якою було встановлено з'єднання, за допомогою якого він може виявляти такі атаки, як Dos-атака, TCP-атака Syn і т. д. На підставі цього механізм CBAC може змусити з'єднання відновлювати або відкидати шкідливі пакети.

4. Генерація попереджень та аудитів - маршрутизатор, що працює з механізмом CBAC, реєструє інформацію про встановлені з'єднаннях, кількості відправлених байтів, IP-адресу джерела і призначення.

Обмеження. Деякі з обмежень механізмів CBAC:

1. CBAC непросте для розуміння, тобто вимагає докладного знання протоколів і операцій, які ми хочемо виконати.

2. Механізм CBAC не може перевіряти трафік, що виходить від самого маршрутизатора (на якому ми налаштували CBAC).

3. Ні таблиці зі збереженням стану при відмові підтримки. У разі збою одного маршрутизатора інший резервний маршрутизатор можна використовувати в якості брандмауера CBAC, але таблиця статків не буде дублюватися, тому необхідно перебудувати таблицю станів, в результаті чого буде відновлено деякий з'єднання.

4. Він не перевіряє зашифровані пакети, такі як IPsec.

Стандартний список доступу - це список який складений лише за допомогою оригінального IP-адреси. Ці списки ACL дозволяють або забороняють весь набір протоколів. Вони не розрізняють IP-трафік, такий як

TCP, UDP, Https і т. Д. Використовуючи номера 1-99 або 1300-1999, маршрутизатор буде розуміти його як стандартний ACL і вказану адресу як IP-адреса джерела.

Стандартний список доступу використовується рідше в порівнянні з розширеним списком доступу, оскільки весь набір протоколів IP буде дозволений або заборонений для трафіку, оскільки він не може розрізнити трафік іншого протоколу IP.

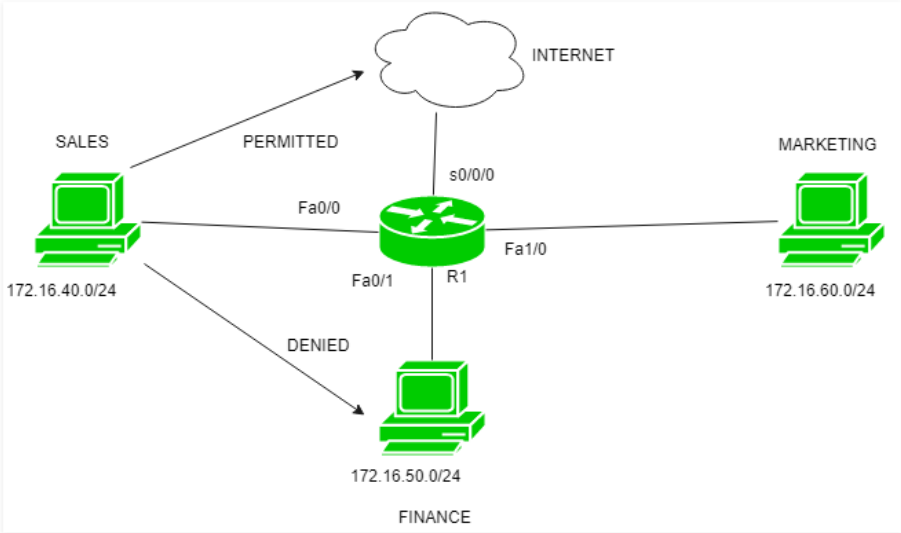


Рис. 1.1. Приклад топології

Ось невелика топологія, в якій є 3 відділи: продаж, фінанси і маркетинг. Відділ продажів з мережею 172.16.40.0/24, фінансовий відділ з мережею 172.16.50.0/24 і відділ маркетингу з мережею 172.16.60.0/24. Тепер ви хочете заборонити зв'язок між відділом продажів і фінансовим відділом і дозволити іншим доступ до цієї мережі.

Насамперед налаштуйте нумерований стандартний доступ - список для заборони будь-якого IP-з'єднання від відділу продажів до фінансового відділу.

Наприкінці кожного списку доступу є неявна заборона, що означає, що якщо трафік не відповідає жодному з правил списку доступу, то трафік буде відкинутий. Вказуючи будь-яких заходів, джерело, що має будь-який трафік IP-адреси, потрапить в фінансовий відділ, за винятком трафіку, який відповідає зазначеним вище правилам.

Висновки до розділу 1.

В результаті детального вивчення інформації про компанію Cisco було обрано її обладнання. Також детально проаналізовані данні про міжмережеву операційну систему Cisco (IOS) що використовуються на багатьох маршрутизаторах Cisco Systems і існуючих мережевих комутаторах Cisco.

Були переглянуті загальні відомості про протокол динамічної маршрутизації OSPF заснований на технології відстеження стану каналу.

Також розглянуті теоретичні відомості про списки доступу (ACL) та переглянуті два їх типи: стандартні та розширені.

РОЗДІЛ 2. РОЗРОБКА ТА ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМПЮТЕРНОЇ МЕРЕЖІ

2.1 Вибір мережевої топології

Оперативний взаємозв'язок між комп'ютерами по локальній мережі здійснюється за допомогою ліній зв'язку. Вся система, в залежності від фізичного підключення вузлів, а також, самого геометричного розташування вузлів мережі, називають мережевою топологією [19].

Існують логічна і фізична топології, які є незалежними між собою. Фізична топологія здійснює в мережі геометрію побудови, а логічна – встановлює в мережі для всіх потоків даних їх напрямок і спосіб передачі.

У локальних мережах найбільш затребувані фізичні топології, такі як:

1. «Шина» (bus);
2. "Зірка" (star);
3. "Кільце" (ring);
4. також, логічне «кільце» (або Token Ring).

В мережі з наявністю шинної топології для передачі даних використовується коаксікальний кабель (моноканал), на кінцях його встановлюються термінатори, або кінцева опора. Підключення кожного комп'ютера до кабелю відбувається через Т-роз'єм (Т-коннектор). Через передавальний вузол мережі дані по шині передаються в обидві сторони, при цьому відбиваються від термінаторів. Іншими словами, термінатори гасять сигнали, які досягають до кінця каналів передачі даних. Таким чином, інформація, що передається проходить через всі вузли, але приймається і фіксується тільки одним, якому і призначалася. Логічна шинна топологія забезпечує в мережі спільну і одночасну передачу інформації до всіх ПК, і навпаки, всі дані від ПК в усі напрямки передаються по мережі. Такий вид передачі сигналів називають ще широкомовним.

Мережі шинної топології мають і свої переваги:

1. легко налаштовується і конфігуруються;

2. стійкість даної мережі до окремих неполадок в вузлах;

3. якщо один з вузлів виходить з ладу, це ніяк не впливає на працездатність всієї мережі.

Але є й недоліки:

1. обмеження в кількості робочих станцій і довжині кабелю;
2. може зупинитися вся робота мережі в разі розриву кабелю;
3. складно визначати дефекти в з'єднаннях.

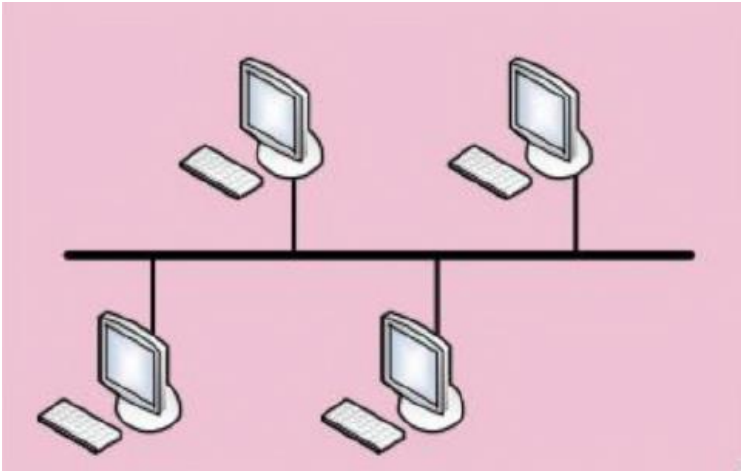


Рис.2.1. Топологія "Шина"

Топологія мережі - "зірка". В даній мережі кожна окрема робоча станція кабелем (звита пара) приєднана до хабу або концентратора, що забезпечує для всіх ПК паралельне з'єднання (всі комп'ютери мережі можуть один з одним спілкуватися).

Дані, які відправляються від однієї передавальної станції, через хаб і всі лінії йдуть на усі ПК. Іншими словами, інформація може надходити на будь-яку робочу станцію, але приймати її можуть лише ті станції, яким вона призначена. Оскільки передача сигналів даної типології фізична «зірка» і вона широкомовна, то логічна топологія в такій локальній мережі буде логічної шиною. В основному

застосовується для локальних мереж, що мають архітектуру 1 OBase-TEthemet.

Переваги даної топології зірка:

1. просте підключення нового ПК;

2. централізоване управління;

3. стійкість до розривів в окремих з'єднання ПК.

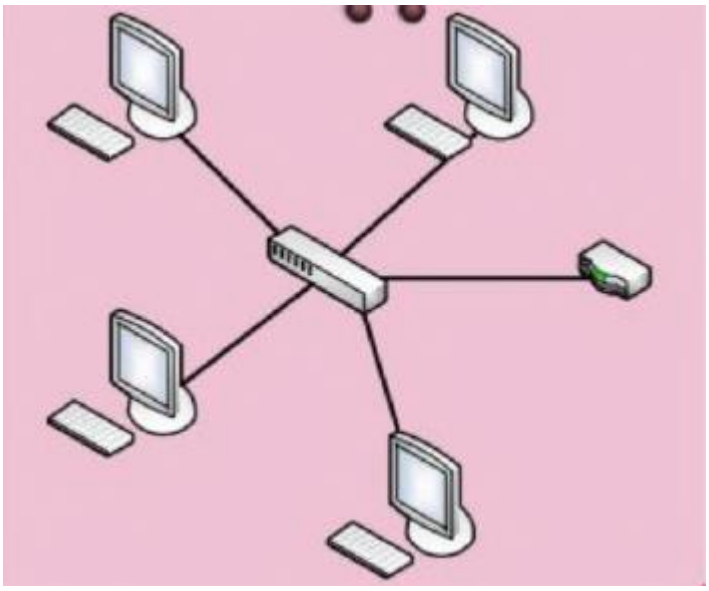


Рис.2.2. Топологія "Зірка"

Топологія мережі "кільце". Нерозривне кільце, за допомогою якого передається інформація між ПК, в топології мережі забезпечується з'єднанням усіх вузлів каналами зв'язку. Завдяки цьому, вся інформація рухається по колу в одному напрямку.

Робоча станція, яка приймає сигнали, розпізнає дані і отримує тіьки ті повідомлення, які їй адресовані. У даній топології мережі застосовується маркерний доступ, що надає право на певний порядок використання кільця. Логічна топологія в даному випадку - логічне кільце.

Така мережа легко створюється і налаштовується. Єдиний недолік мережі топології кільце - якщо хоч в одному місці пошкоджена лінія зв'язку або вийшов з ладу, порушується працездатність всієї мережі.

Через деякій ненадійності, в чистому вигляді даний вид топології рідко застосовується. На практиці в основному застосовують модифікації різних кільцевих топологій.

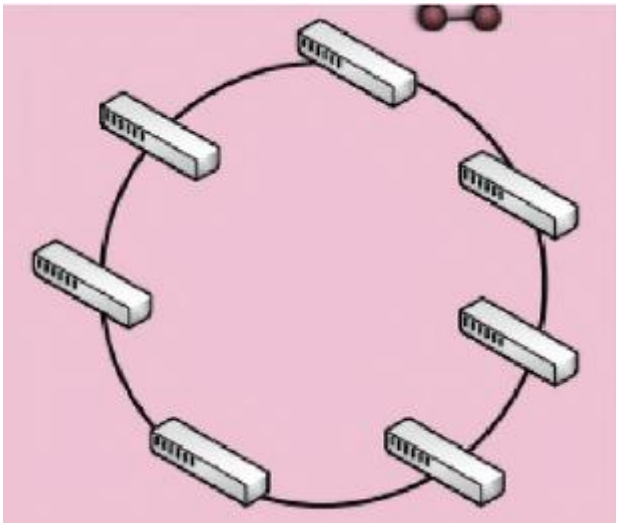


Рис.2.3. Топологія "Кільце"

Топологія мережі - Token Ring. Така топологія ґрунтується на топології мережі «фізичне кільце із застосуванням типу зірка». Передбачає підключення всіх робочих станцій доцентрального концентратора (або Token Ring), так само як при топології «фізична зірка». Таким чином, центральний концентратор за допомогою перемичок здійснює послідовне з'єднання виходів з одних станцій з входами інших станцій.

Концентратор забезпечує з'єднання кожної станції тільки з двома сусідніми станціями - попередньої і наступної. Робочі станції пов'язані між собою петлею кабелю, яка забезпечує передачу даних між станціями, тобто окрема станція ретранслює інформацію далі. Для забезпечення цього, кожна робоча станція обладнана спеціальними приймально-передавальними пристроями, що дозволяють управління проходження даних в мережі.

Система Token Ring зроблена таким чином, що маркер передається по логічному кільцю між вузлами. Передача маркера має фіксований напрямок. Якщо станція має маркер, вона передає інформацію на наступну станцію.

Але для такої передачі даних робоча станції спочатку повинні дочекатися появи вільного маркера. Отриманий маркер містить всі адреси станції, яка направила цей маркер, в тому числі і станції, для якого він призначався. Наступна станція передає маркер далі по мережі, для наступної станції, і так далі по колу.

Головний вузол мережі (в основному це файл-сервер) маркер створює, далі цей маркер відправляється в мережу по кільцю. В даному випадку, такий вузол є активним монітором і строго стежить за рухом маркера, який не повинен загубитися або зруйнуватися.

До переваг такої топології Token Ring можна віднести:

1. однаковий доступ до робочих станцій;

2. надійність системи;

3. стійкість до несправностей деяких станцій або при розривах з'єднань.

Недоліки Token Ring - це дуже велика витрата матеріалів на підключення, а відповідно, найдорожча розводка для ліній зв'язку.

2.2 Вибір обладнання для організації роботи мережі

Для забезпечення функціонування даної мережі організації було обрано оптимальні обладнання корпорації Cisco, котре має адаптованість під модернізацію модулями та підтримували б протокол маршрутизації OSPF. Також потрібно приділити особливу увагу технологіям, котрі необхідні для мережі, зокрема це підтримка GigabitEthernet та Ethernet (FastEthernet) [3].

Комутатор покоління 2960 (рис. 2.4) ідеально підходить для даної мережі.



Рис.2.4. Маршрутизатор Cisco 2960

Catalyst 2960 - це комутатор Ethernet, до якого можна підключати робочі станції, точки бездротового доступу Cisco, IP-телефони Cisco і інші мережеві пристрої, в тому числі сервери, маршрутизатори та інші комутатори. Пристрій Catalyst 2960 на 24 і 48 портів можуть використовуватися в якості магістральних комутаторів для агрегування Ethernet-трафіку 10BASE-T, 100BASE-TX і 1000BASE-T, одержуваного від інших мережевих пристроїв. Компактні 8-портові комутатори Catalyst 2960 володіють такими ж

можливостями підключення Ethernet, але можуть також використовуватися поза традиційної комутаційної середовища, наприклад в офісах і аудиторіях.

При установці в комутатори Catalyst 2960 модулі SFP 1000BASE-T працюють зі швидкістю 10, 100 або 1000 Мбіт / с в повнодуплексному режимі і 10 або 100 Мбіт / с в напівдуплексному режимі. Порти 10/100 і 10/100/1000 виконують автоузгодження швидкості і підтримують повнодуплексний або напівдуплексний режим. Деякі комутатори Catalyst 2960 мають роз'єм RPS для опціональних резервних систем Cisco RPS 2300 або Cisco RPS 675, які працюють на змінному струмі і забезпечують комутатор резервним живленням постійного струму.

Порти 10/100 комутатора Catalyst 2960-24-S пронумеровані в такий спосіб: перший член пари (порт 1) розташований над другим членом (порт 2), порт 3 розташований над портом 4 і т. д.

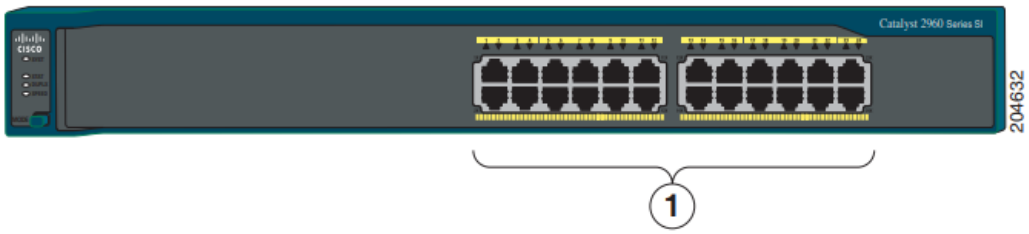


Рис. 2.5. Передня панель комутатора

Порти 10/100 на комутаторах Catalyst 2960-24TC-S і 2960-48TC-пронумеровані так само, як і на комутаторах серії 2960-24-S. Ці комутатори мають порти подвійного призначення, порти 10/100/1000 1 і 2 можуть використовуватися для підключення модуля SFP або роз'єму RJ-45, але не допускають їх одночасного підключення. Щоб налаштувати тип роз'єму для цих портів, використовується програмне забезпечення.

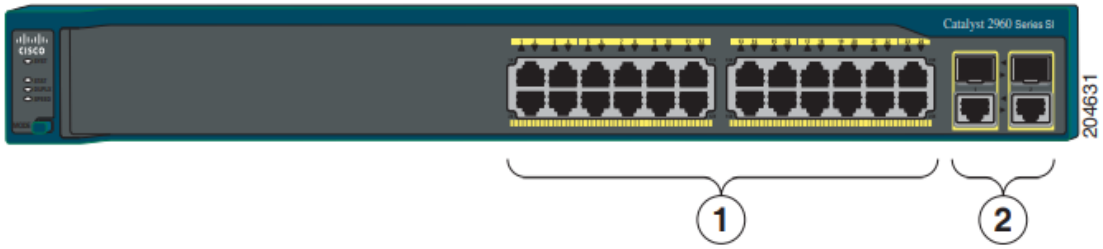


Рис.2.6. Передня панель комутатора Catalyst 2960-24TC-S

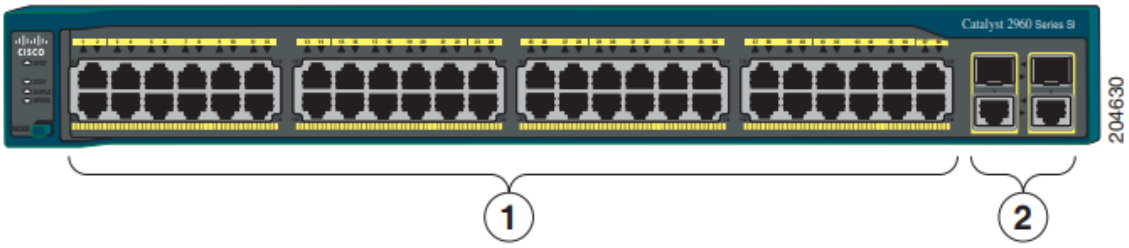


Рис.2.7. Передня панель комутатора Catalyst 2960-48TC-S

Порти 10/100 комутатора Catalyst 2960-48TT-S пронумеровані в такий спосіб: перший член пари (порт 1) розташований над другим членом (порт 2), порт 3 розташований над портом 4 і т. д. Комутатор оснащений 2 портами каскадування 10/100/1000 з нумерацією 1 і 2. (Див. рис.2.8).

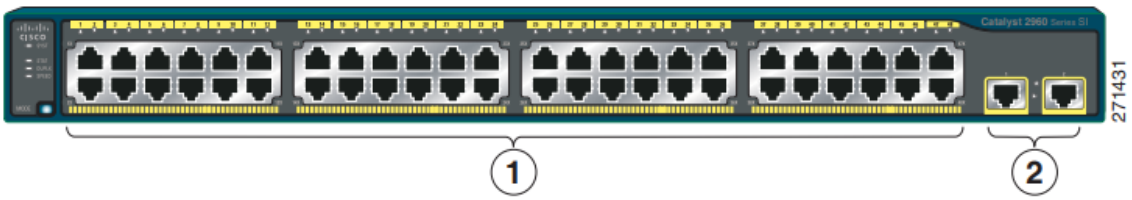


Рис.2.8. Передня панель комутатора Catalyst 2960-48TT-S

Порти 10/100 на комутаторах згруповані в пари. Перший член пари (порт 1) розташований над другим членом (порт 2), порт 3 над портом 4 і т. д. Фіксовані порти 10/100 на комутаторах Catalyst 2960-24PC-L і 2960-24PC-S є портами PoE (див. рис. 2.9 - 2.10). Порти з 1 по 8 на комутаторі Catalyst 2960-24LC-S є портами PoE (див. рис. 2.11).

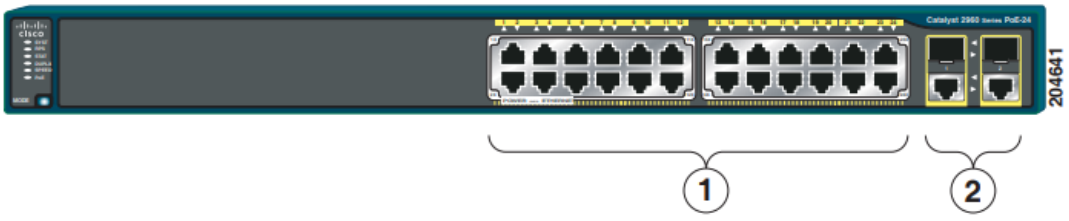


Рис.2.9. Передня панель комутатора Catalyst 2960-24PC-L

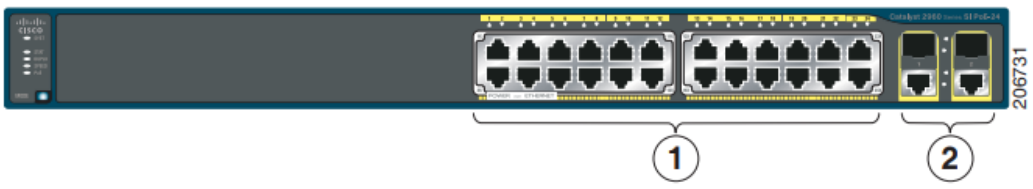


Рис.2.10. Передня панель комутатора Catalyst 2960-24PC-S

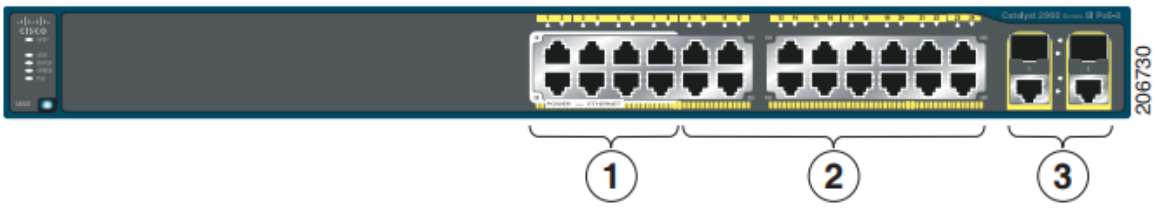


Рис.2.11. Передня панель комутатора Catalyst 2960-24LC-S

Комутатори Catalyst 2960-24TC-L і Catalyst 2960-48TC-L обладнані портами подвійного призначення, т. б. порти 10/100/1000 1 і 2 можуть використовуватися для підключення модуля SFP або роз'єму RJ-45, але не і того й іншого одночасно. Щоб налаштувати тип роз'єму для цих портів, використовується програмне забезпечення.

Вибір маршрутизатора впав на Cisco 2800 серії. Це сімейство маршрутизаторів включає наступні моделі:

1. Cisco 2801 Integrated Services Router
2. Cisco 2811 Integrated Services Router
3. Cisco 2821 Integrated Services Router
4. Cisco 2851 Integrated Services Router



Рис.2.12. Маршрутизатор 2801



Рис.2.13. Маршрутизатор 2811



Рис.2.14. Маршрутизатор 2821



Рис.2.15. Маршрутизатор 2851

Маршрутизатор Cisco 2801 серії є маршрутизатори з інтеграцією сервісів (Integrated Services Routers, ISR), оптимізовані для безпечної передачі даних, голосу і відео на швидкості каналу зв'язку. Маршрутизатор мають вбудовані засоби апаратного прискорення шифрування (DES, 3DES, AES 128, AES 192, AES 256; підтримуються у версіях ПЗ Cisco IOS Software з функціональністю забезпечення мережевої безпеки). Також, на борту є вбудовані порти Fast Ethernet 10/100 (в Cisco 2801 і 2811) і Gigabit Ethernet 10/100/1000 (в Cisco 2 821 і 2851). Пристрої Cisco 2800 серії оснащені слотами для установки мережевих модулів (NME), для встановлення інтерфейсних модулів (HWIC), для підтримки додаткових голосових інтерфейсів (EVM), а також Спеціальний слотами на системній платі маршрутизатора для установки модулів обробки голосу і сервісних модулів (PVDM і AIM). Інтерфейси NME і HWIC мають зворотну сумісність з модулями NM і WIC відповідно.

Дані пристрої призначені для підключення до мереж середніх компаній, а також філій і представництв великих компаній. Вони забезпечують захист

мережі від зовнішніх вторгнень, виконуючи функції брандмауера з інспекцією пакетів, антивірусним захистом, контролем трафіку, функціями URL-фільтрації та авторизацією підключень.

Маршрутизатор серії 2800 надають розширені можливості по створенню високопродуктивних VPN-з'єднань на базі мереж загального користування для створення захищених каналів зв'язку між віддаленими офісами. Опціонально підтримується до 1500 одночасних VPN-тунелів з апаратного шифрування переданих даних. Також за допомогою модулів розширення можна організувати передачу харчування по кручений парі (PoE), що спростить процедуру інсталяції окремих вузлів мережі.

Кожна модель в серії має більше одного WAN-порту з метою підвищення продуктивності каналу (балансування навантаження) або підвищення надійності системи на випадок відмови основної лінії зв'язку. Маршрутизатор серії 2800 підтримують більше 90 різних модулів розширення.

Основні параметри маршрутизаторів Cisco серії 2800 в стандартному виконанні наведені в табл. 2.1.

Таблиця 2.1

Основні параметри маршрутизаторів Cisco серії 2800

Модель маршрутизатора	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
DRAM	128Mb(384Mb)	256Mb(768Mb)	256Mb(1Gb)	256Mb(1Gb)
Compact Flash	64Mb(128Mb)	64Mb(256Mb)	64Mb(256Mb)	64Mb(256Mb)
USB 1.1 Ports	1	2	2	2
Інтегровані LAN порти	2-10/100	2-10/100	2-10/100/1000	2-10/100/1000
Слоти для мережевих модулів	0	1 NME	1 NME or NME-X	1 NME, NMD, NME-X or NME-XD
Слоти для інтерфейсних карт	4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules 1 slot supports WIC, VIC, or VWIC type modules 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules
Слотів для голосового модуля расширения	0	0	1	1
Форм фактор	10	10	20	20
Console Port (up to 115.2 kbps)	1	1	1	1
Інтегровані PVDM (DSP) слоти	2	2	3	3

Управління маршрутизаторами може здійснюватися через WEB-інтерфейс або на базі Cisco IOS Software - інтерфейсу командного рядка, в тому числі віддалено. Є набір встановлених сценаріїв налаштування, який полегшує адміністрування.

Розробка схеми адресації пристроїв

Для забезпечення функціонування мережі, перш за все були виконано розрахунок параметрів IP-адресації. Під час розрахунку параметрів IP-адресації особлива увага була приділена економії IP-адрес, тому мережі було розбито на підмережі з оптимальними масками, згідно кількості вузлів у кожній з них (назва таблиці). Також було приділено увагу можливості розширення деяких підмереж.

Таблиця 2.2

Параметри адресації мережі

Підмережа / Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адрес	Маска підмережі	Префікс
Підмережа A	—	192.158.1.0	255.255.255.0	/24
Підмережа B	—	192.138.2.0	255.255.255.0	/24
Підмережа C	—	10.0.0.0	255.255.255.252	/30
Підмережа D	—	10.0.1.0	255.255.255.252	/30
Підмережа E	—	192.168.3.0	255.255.255.0	/24
Підмережа F	—	192.168.1.0	255.255.255.0	/24
Підмережа G	—	10.0.3.0	255.255.255.252	/30
Підмережа H	—	192.168.5.0	255.255.255.0	/24
Підмережа I	—	192.168.10.0	255.255.255.0	/24
Підмережа J	—	10.0.2.0	255.255.255.252	/30
Підмережа K	—	172.20.1.0	255.255.255.0	/24
Підмережа L	—	172.16.2.0	255.255.255.0	/24
Підмережа M	—	10.0.2.4	255.255.255.252	/30
Підмережа N	—	10.0.2.7	255.255.255.252	/30
Підмережа O	—	10.0.1.8	255.255.255.252	/30
Підмережа P	—	10.0.1.4	255.255.255.252	/30

Продовження таблиці 2.2

Підмережа / Пристрій	**Інтерфейс/Мережевий адаптер/Шлюз**	**IP-адрес**	**Маска підмережі**	**Префікс**
Маршрутизатор R1	Fastethernet0/0	10.0.1.9	255.255.255.252	/30
	Fastethernet0/1	10.0.1.6	255.255.255.252	/30
	Fastethernet6/0	192.168.1.1	255.255.255.0	/24
Маршрутизатор R2	Fastethernet0/0	10.0.1.10	255.255.255.252	/30
	Fastethernet3/0	10.0.1.1	255.255.255.252	/30
	Fastethernet4/0	192.168.5.1	255.255.255.0	/24
	Fastethernet5/0	10.0.0.1	255.255.255.252	/30
	Fastethernet6/0	10.0.3.1	255.255.255.252	/30
Маршрутизатор R3	Fastethernet0/1	10.0.1.6	255.255.255.252	/30
	Fastethernet3/0	10.0.1.2	255.255.255.252	/30
	Fastethernet6/0	192.168.3.1	255.255.255.0	/24
Маршрутизатор R4	Fastethernet0/0	10.0.2.10	255.255.255.252	/30
	Fastethernet0/1	10.0.0.3	255.255.255.252	/30
	Fastethernet2/0	10.0.2.1	255.255.255.252	/30
	Fastethernet4/0	192.168.10.1	255.255.255.0	/24
	Fastethernet6/0	10.0.3.2	255.255.255.252	/30
Маршрутизатор R5	Fastethernet0/0	10.0.2.9	255.255.255.252	/30
	Fastethernet0/1	10.0.2.6	255.255.255.252	/30
	Fastethernet6/0	172.16.2.1	255.255.255.0	/24
Маршрутизатор R6	Fastethernet0/1	10.0.2.5	255.255.255.252	/30
	Fastethernet2/0	10.0.2.2	255.255.255.252	/30
	Fastethernet6/0	172.20.1.1	255.255.255.0	/24
Маршрутизатор R7	Fastethernet0/0	10.0.0.2	255.255.255.252	/30
	Fastethernet0/1	192.158.1.1	255.255.255.0	/24
	Fastethernet1/0	192.138.2.1	255.255.255.0	/24
Робоча станція PC-1	Fa0/1	DHCP		
Робоча станція PC-2	Fa0/1	DHCP		

Продовження таблиці 2.2

Підмережа / Пристрій	**Інтерфейс/Мережевий адаптер/Шлюз**	**IP-адрес**	**Маска підмережі**	**Префікс**
Робоча станція PC-3	Fa6/0	DHCP		
Робоча станція PC-4	Fa6/0	DHCP		
Робоча станція PC-5	Fa6/0	DHCP		
Робоча станція PC-6	Fa6/0	DHCP		
Робоча станція PC-7	Fa4/0	DHCP		
Робоча станція PC-8	Fa4/0	DHCP		
Робоча станція PC-9	Fa4/0	DHCP		
Робоча станція PC-10	Fa4/0	DHCP		
Робоча станція PC-11	Fa6/0	DHCP		
Робоча станція PC-12	Fa6/0	DHCP		
Робоча станція PC-13	Fa6/0	DHCP		
Робоча станція PC-14	Fa6/0	DHCP		
Робоча станція PC-15	Fa1/0	DHCP		
Робоча станція PC-16	Fa1/0	DHCP		

Висновки до розділу 2.

Була спроектована мережева топологія. Сформовані таблиці параметрів інтерфейсів пристроїв та адресації підмереж.

Обрані пристрої, на яких базуватиметься мережа. Описані можливості обладнання, які можуть використовуватись для поставленого завдання, обрані та обґрунтовані основні з них.

Розроблена базова політика безпеки системи, реалізація якої дозволить забезпечити надійний інформаційний захист кожного елемента мережі.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Налагодження пристроїв мережі

Розглянемо лістинги налаштування. Для зручності налаштування були змінені стандартні імена елементів мережі (рис. 3.1).

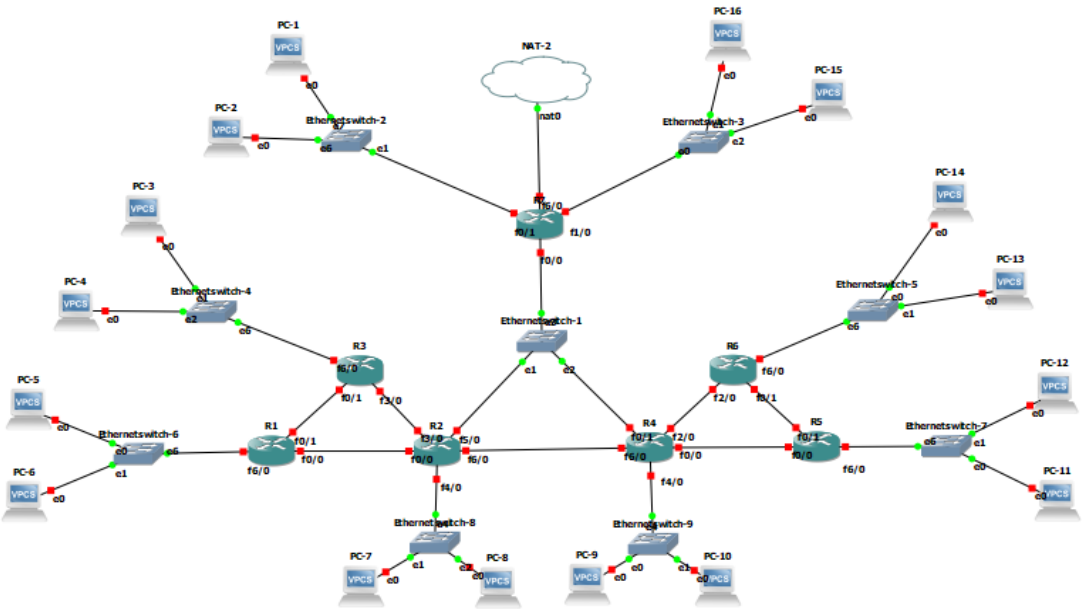


Рис. 3.1.Загальна топологія мережі

В даному етапі розглянуто базис налаштування пристроїв мережі. Для загального розуміння, який пристрій в даний час налаштовується, зручності конфігурування та перевірки працездатності зв'язку між пристроями були змінені на ті, які відповідають проекту (рис. 3.1).

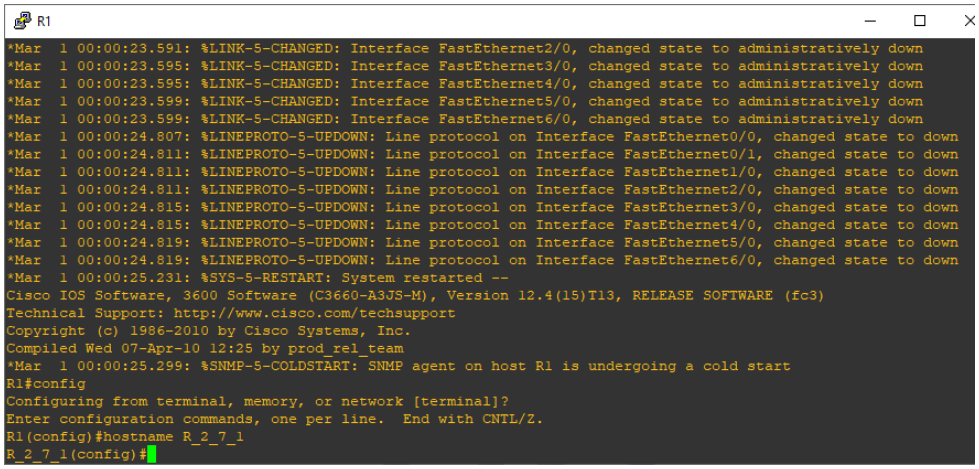


Рис. 3.2. Надання Hostname маршрутизатору R1

Основою будь-якої мережі в першу чергу є адресація, спираючись на це після заміни імен було впроваджено статичну адресацію інтерфейсів мережі. Оскільки статичні адреси конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних адрес відповідно до змін.

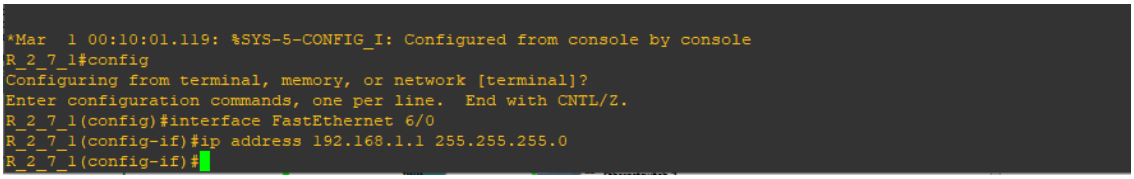


Рис. 3.3. Надання статичної IP-адреси інтерфейсу FastEthernet6/0

Адреса IP складається з двох частин: номера мережі та номера вузла. Уразі ізольованості мережі її адреса може бути обрана адміністратором з навмисно зарезервованих для таких мереж блоків адрес.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор входить відразу до кількох мереж. Тому кожен порт маршрутизатора має власну адресу IP. Кінцевий вузол також може входити до кількох мереж IP. У цьому випадку комп'ютер повинен мати кілька IP- адрес, за числом мережних зв'язків. Таким чином, адреса IP характеризує не окремий комп'ютер чи маршрутизатор, а одне мережне з'єднання.

IP-адресу називають статичною (постійною, незмінною), якщо вона задається користувачем у налаштуваннях пристрою, або якщо надається автоматично при підключенні пристрою до мережі та не може бути присвоєна іншому пристрою.

IP-адресу називають динамічною (непостійною, змінною), якщо вона надається автоматично при підключенні пристрою до мережі і використовується протягом обмеженого проміжку часу, зазначеного в службі, яка надала IP-адресу (DHCP).

Протокол DHCP робить можливим динамічне призначення адрес без необхідності переналаштування комп'ютера клієнта, що підключається. Таким чином, ви можете бути користувачем Інтернету з динамічною IP-адресою,

навіть не помічаючи цього. DHCP є розширенням протоколу BOOTP, що використовувався раніше для забезпечення бездискових робочих станцій IP-адресами при їхньому завантаженні. DHCP зберігає зворотну сумісність з BOOTP.

```
R1(config)#hostname R1_2_7_1
R1_2_7_1(config)#interface FastEthernet 6/0
R1_2_7_1(config-if)#ip address 192.168.1.1 255.255.255.0
R1_2_7_1(config-if)#exi
R1_2_7_1(config)#ip dhcp pool DHCP_AREA_1_R1
R1_2_7_1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1_2_7_1(dhcp-config)#default-router 192.168.1.1
R1_2_7_1(dhcp-config)#dns-server 8.8.8.8
R1_2_7_1(dhcp-config)#exi
R1_2_7_1(config)#ip dhcp excluded-address 192.168.1.1
R1_2_7_1(config)#
```

Рис. 3.4.Налаштування DHCP-серверу на маршрутизаторі R1

Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP.

Деякими з найбільш часто використовуваних опцій є:

```
R1_2_7_1(dhcp-config)#default-router 192.168.1.1
```

Рис. 3.5.IP-адреса маршрутизатора за замовчуванням

```
R1_2_7_1(config-if)#ip address 192.168.1.1 255.255.255.0
```

Рис. 3.6. Маска підмережі

```
R1_2_7_1(dhcp-config)#dns-server 8.8.8.8
```

Рис. 3.7. Адреса сервераDNS

Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах, включаючи:

Динамічний розподіл - адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запросити IP-

адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп'ютери.

Автоматичне виділення - сервер DHCP буде постійно призначати вільний IP-адрес з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих завдань IP і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережних підключень.

Статичний розподіл - сервер DHCP робить призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначена мережева адреса.

Протокол DHCP побудований так, що клієнт може звертатися із запитом відразу до декількох серверів. Клієнт DHCP, що потребує адресу, посилає широкомовний пакет DHCPDISCOVER в пошуках сервера. Пакет містить апаратну адресу запитувача клієнта. Потім один або кілька серверів DHCP розглядають запит і посилають у відповідь пакет DHCPOFFER, що містить IP-адресу і "час оренди".

Сервер посилає підтвердження (DHCPACK) і процес узгодження завершується. Пакет DHCPACK містить обумовлені адресу та час оренди. Сервер позначає виділену адресу як зайняту - до закінчення терміну оренди цю адресу не можна буде присвоїти іншому клієнту. Клієнту залишилося тільки сконфігурувати себе відповідно до надісланих даних і можна приступати до роботи в мережі.

3.2 Налагодження захисту мережі

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з таких проблем — забезпечення надійного захисту інформації. На даному етапі

ми впровадимо технології захисту на прикладі комп'ютерної мережі на базі протоколу OSPF.

Для початку нам необхідно створити vlan інтерфейс, призначити йому відповідний ip адресу і дозволити проходження трафіку через фізичний інтерфейс.

```
R_2_7_3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R_2_7_3(config)#router ospf 1
R_2_7_3(config-router)#network 192.168.3.0 0.0.0.255 area 1
R_2_7_3(config-router)#network 10.0.1.4 0.0.0.3 area 1
R_2_7_3(config-router)#network 10.0.1.0 0.0.0.3 area 1
R_2_7_3(config-router)#passive-interface FastEthernet6/0
R_2_7_3(config-router)#
```

Рис. 3.8.Налагодження динамічної маршрутизації за допомогою протоколу OSPF на маршрутизаторі R_2_7_3

При налагодженні протоколу OSPF, власне як і решти протоколів, рекомендується зменшувати об’єм службового трафіка, що передається по мережі. Для цього використаємо команду passiveinterface. Вона призначена для встановлення пасивного стану роботи того чи іншого інтерфейсу маршрутизатора, тобто переведення інтерфейсу у такий режим, коли OSPF-оновлення у підключену до нього мережу не пересилаються. Цю команду доцільно використовувати у випадку, коли до інтерфейсу маршрутизатора підключена певна тупикова локальна мережа, з метою зменшення потоку службового трафіка в цю мережу.

```
R_2_7_3(config-router)#passive-interface FastEthernet6/0
R_2_7_3(config-router)#
```

Рис. 3.9. Використання команди passive-interface

Протокол OSPF прекрасно працює в будь-якій мережі, проте, мережа велика, то необхідно розділити її на зони. Кожен маршрутизатор повинен зберігати в базі даних повну інформацію про підключених маршрутизаторах і інтерфейси всієї мережі. Маршрутизатор однієї зони не знають топологію мережі іншої зони, тобто не отримують оновлення з іншої зони і таким чином

зменшується навантаження на маршрутизатор. Щоб зменшити навантаження на мережу і маршрутизатори протоколом OSPF передбачено поділ мережі на зони:

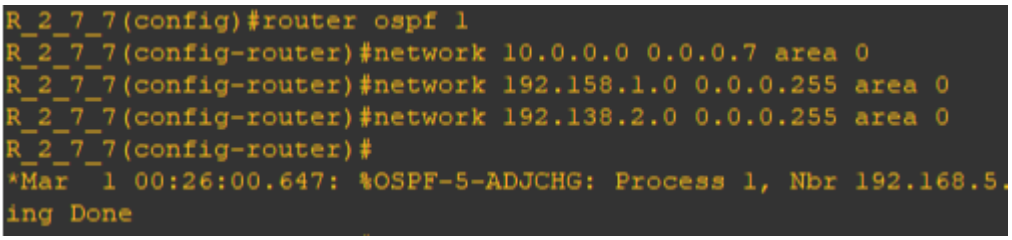


Рис. 3.10.Налагодження зониarea0 протоколу OSPF

У OSPF зона 0 (Area 0) завжди є магістральною (backbone), до якої підключаються інші зони. Зв'язок між зонами завжди здійснюється тільки через магістральну зону.

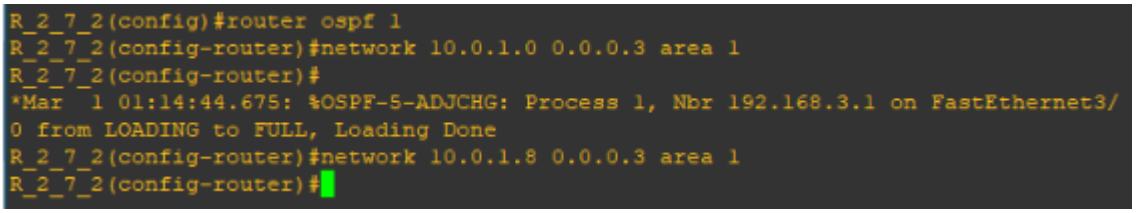


Рис. 3.11.Налагодження зони area1 протоколу OSPF

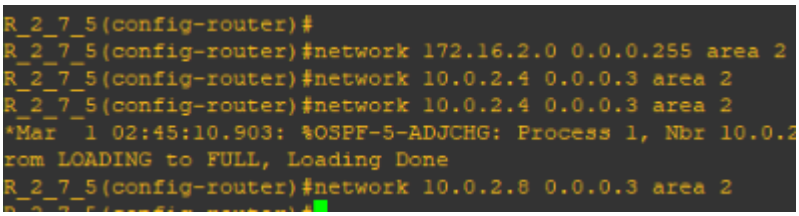


Рис. 3.12.Налагодження зони area2 протоколу OSPF

На наступному етапі ми займемося налаштуванням списків доступу. Функціонал ACL складається в класифікації від трафіку, потрібно його спочатку перевірити, а потім щось з ним зробити в залежності від того, куди ACL застосовується. ACL бувають двох видів: стандартні і розширені. В даній роботі ми використовуємо стандартні. ACL - це набір правил. Кожне правило складається з дії (permit, deny) і критерію (для стандартних ACL –IP-адреса відправника, для розширених - безліч критеріїв).

Команда ip access-list з опцією standard використовується для створення та редагування стандартних списків доступу (config-std-nacl). Стандартні

списки доступу використовуються для фільтрації пакетів тільки по IP-адресою відправника (джерела) пакетів.

```
R_2_7_3(config)#ip access-list standard CLOSE
```

Рис. 3.13. Створення стандартного списку доступу

Команда ip access-list з опцією extended використовується для створення та редагування розширених списків доступу (config-ext-nacl). Розширені списки доступу використовуються для більш гнучкою фільтрації пакетів - по IP-адресою відправника пакета, IP-адресою одержувача пакета, за типом протоколу, порту відправника пакета і порту одержувача.

Надалі ми прив'яжемо список доступу до інтерфейса. Список доступа буде використаний для фільтрації трафіка на даному інтерфейсі.

```
R_2_7_3(config)#interface FastEthernet 6/0
R_2_7_3(config-if)#ip access-group CLOSE in
R_2_7_3(config-if)#ip access-group CLOSE out
R_2_7_3(config-if)#no ip access-group CLOSE in
```

Рис. 3.14. Прив`язка списку доступу до інтерфейсу FastEthernet 6/0

Якщо вказується не вірний список доступних, то всі наявні пакети на інтерфейсі будуть пропущені.

Для захисту наших пристроїв від несанкціонованого використання застосуємо пароль. В обладнанні Cisco розглядається настройка пароля на консолі, паролі підключення по telnet і ssh, і такий же пароль для доступу в привілейований режим роботи пристрою. Паролі налаштовуються однаково для маршрутів та комутаторів.

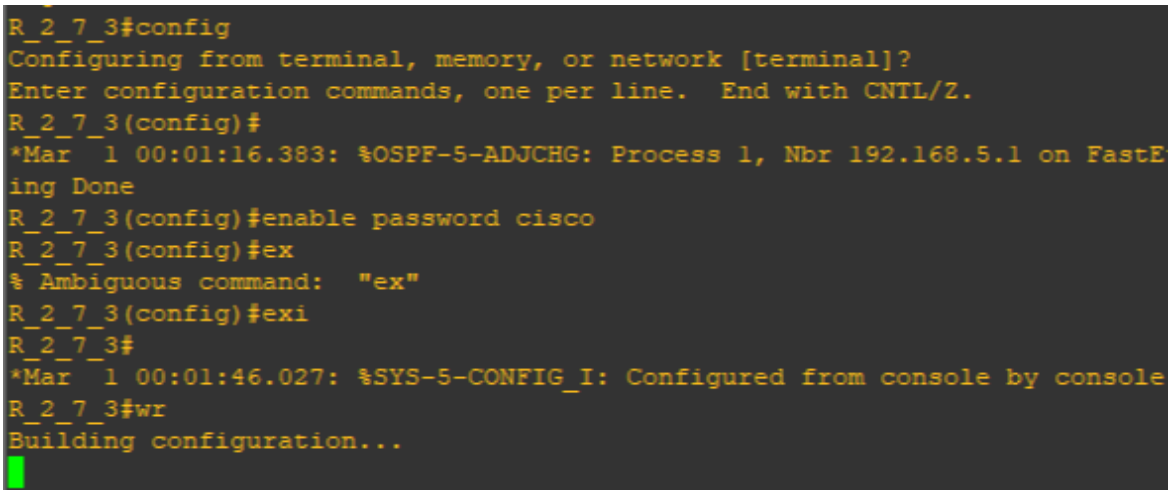


Рис. 3.15.Встановлення паролю на привілейований режим маршрутизатора R_2_7_3

Цей пароль використовується для переходу з користувальницького режиму в привілейований. При вході на пристрій, незалежно від того, робимо ми це через VTY або через консоль, ми потрапляємо в призначений для користувача режим. Далі можна здійснити перехід в привілейований. Якщо встановлено пароль на привілейований режим, то його потрібно ввести, якщо не заданий - то все залежить від того способу, за яким ми підключилися до пристрою. При підключенні по консолі і відсутньому паролі на enable, перехід в привілейований режим відбудеться без введення пароля, якщо ж доступ здійснюється через Telnet або SSH, то без пароля на enable, нас в цей режим не пустять якщо пароль не заданий. Пароль на enable можна задати двома різними командами обидві з яких вводяться в режимі глобальної конфігурації

3.3 Перевірка працездатності мережі

Тестування комп'ютерної мережі це фінальний етап її налаштування, а окрім того й необхідна умова прийняття в експлуатацію. Тестування дає можливість переконатися в коректній роботі системи, нормальному функціонуванню всіх її частин та гарантування того що проект відповідає існуючим нормативним актам. Об'єктивна перевірка надає можливість ліквідувати як і не значні так і серйозні недоліки в її роботі, тим самим забезпечить подальшу економію в її експлуатації.

Тестування комп'ютерних мереж реалізується за допомогою тестового обладнання, так і з використанням програмного забезпечення. Процедура тестування включає в себе наступні пункти.

1. Ліквідація несправностей;
2. Внесення необхідних доповнень і коректив;
3. Оцінка захищеності мережі від втручань;
4. Фінальне регулювання налаштувань обладнання;
5. Детальне вивчення роботи мережі.

Таким чином, тестування мережі - це процес активного впливу на мережу з метою перевірки її працездатності та визначення потенційних можливостей по передачі мережевого трафіку.

Використання всіляких методів тестування і діагностування комп'ютерних мереж дозволяє своєчасно виявити помилки в роботі мережі, що дозволить значно підвищити ефективність роботи комп'ютерних мереж, а також збільшити експлуатаційний термін.

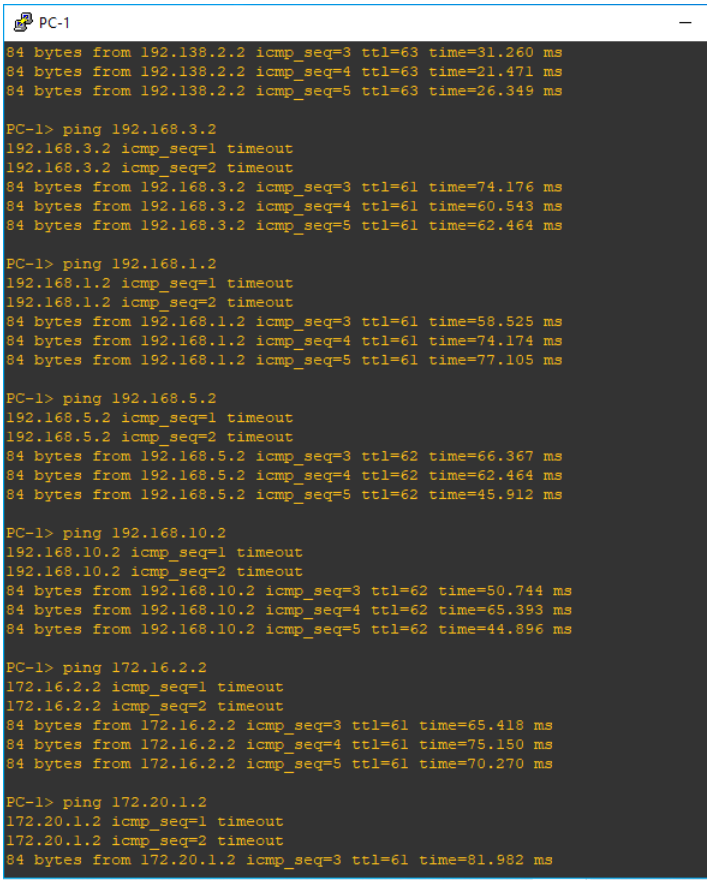


Рис. 3.16.Тестування доступу до мереж

Нагадаємо, що статичний NAT є зіставлення внутрішнього і зовнішнього адреси один до одного. Він дозволяє зовнішніх пристроїв ініціювати підключення до внутрішніх з використанням статично назначеної статичної адреси.

Корисною командою для перевірки роботи NAT є команда show ip nat translations. Ця команда показує активні трансляції NAT. Статичні переклади, на відміну від динамічних перекладів, завжди знаходяться в таблиці NAT.

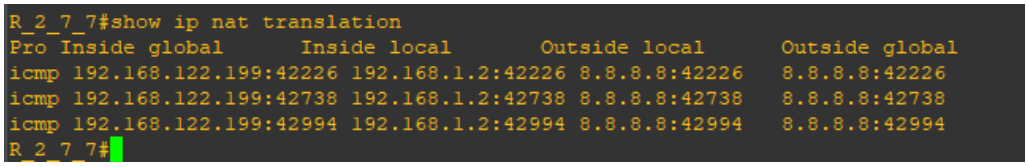


Рис. 3.17. Демонстрація роботи команди show ip nat translation

Також використаємо команду show ip nat statistics яка відображає інформацію про загальну кількість активних перекладів, параметрах конфігурації NAT, кількість адрес в пулі і кількості переведених адрес.

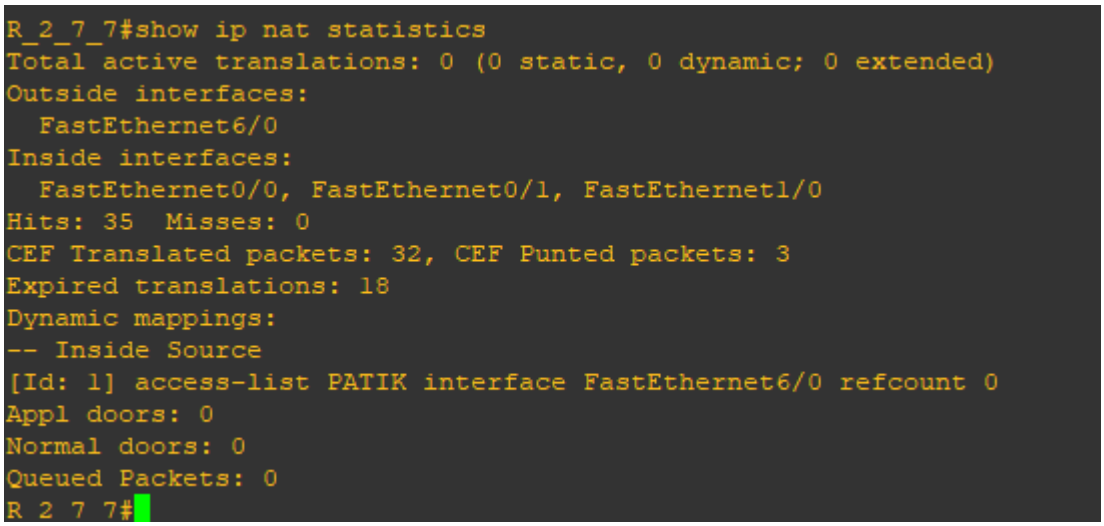


Рис. 3.18. Демонстрація роботи команди show ip nat translation

Оскільки у нас тут використовуються списки доступу ACL, то для їх перевірки можна використовувати команду show access-lists.

```
R_2_7_7#show access-lists
Standard IP access list PATIK
    10 permit 192.168.1.0, wildcard bits 0.0.0.255 (1 match)
    20 permit 192.168.3.0, wildcard bits 0.0.0.255
    30 permit 192.168.5.0, wildcard bits 0.0.0.255 (4 matches)
    40 permit 192.168.10.0, wildcard bits 0.0.0.255
    50 permit 172.16.2.0, wildcard bits 0.0.0.255 (3 matches)
    60 permit 172.20.1.0, wildcard bits 0.0.0.255
    70 permit 192.158.1.0, wildcard bits 0.0.0.255 (5 matches)
    80 permit 192.138.2.0, wildcard bits 0.0.0.255 (5 matches)
R_2_7_7#
```

Рис. 3.19.Демонстрація роботи команди show access-list

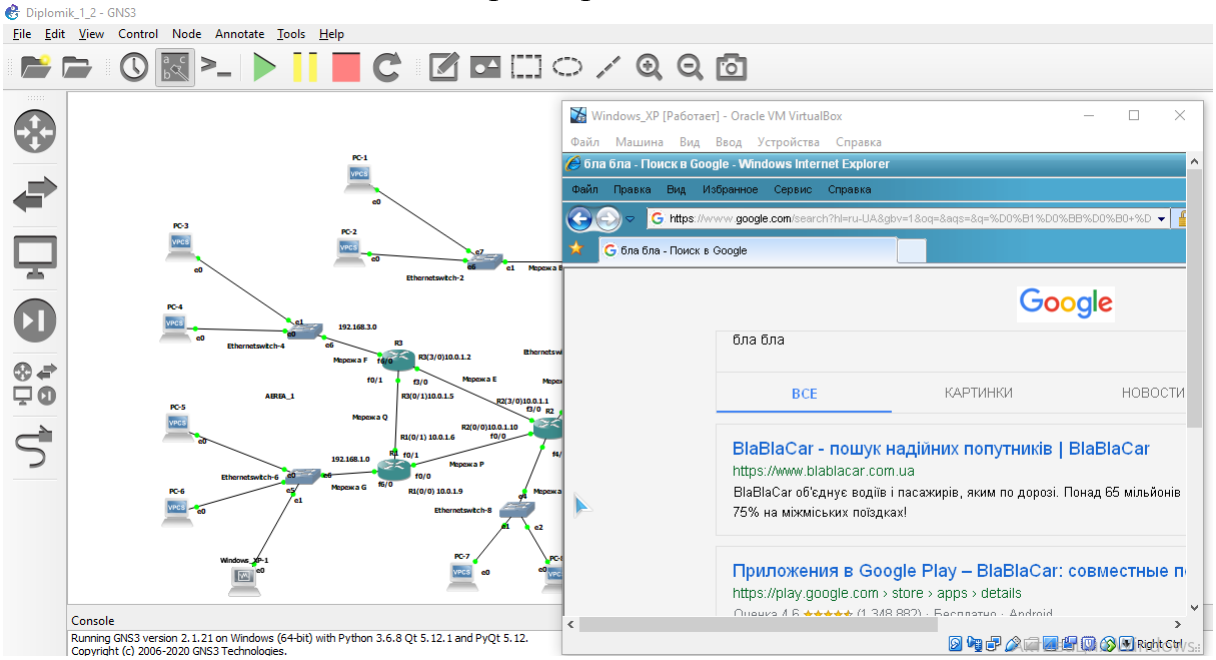


Рис. 3.20.Перевірка доступу до мережі Інтернет

На наступному етапі займемось перевіркою працездатності протоколу OSPF. Існує цілий перелік команд для його перевірки, таких як: show ip protocols, show ip ospf, show ip ospf interface.

Команда show ip protocols дає можливість швидким способом перевірити існуючу інформацію про конфігурацію OSPF таку як: ID процесу OSPF, ID маршрутизатора, мережі, які маршрутизатор поширює, сусідів, від яких маршрутизатор отримує оновлення, і адміністративну відстань за замовчуванням.

```
R_2_7_7#show ip protocol
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.158.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.0.0.7 area 0
    192.138.2.0 0.0.0.255 area 0
    192.158.1.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.1         110      01:01:43
    192.168.5.1          110      01:01:43
  Distance: (default is 110)

R_2_7_7#
```

Рис. 3.21.Демонстрація роботи команди show ip protocols

Команда show ip ospf може також використовуватися, щоб досліджувати ID процесу OSPF і ID маршрутизатора. Додатково, ця команда виводить на екран інформацію по області OSPF, так само як і час, коли алгоритм SPF був обчислений в минулий раз. Як можна бачити з демонстраційного виведення, OSPF є дуже стійким протоколом маршрутизації

```
R_2_7_7#show ip ospf
Routing Process "ospf 1" with ID 192.158.1.1
Start time: 00:01:29.208, Time elapsed: 01:05:22.148
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
   Area BACKBONE(0)
       Number of interfaces in this area is 4
       Area has no authentication
       SPF algorithm last executed 01:05:05.004 ago
       SPF algorithm executed 2 times
       Area ranges are
       Number of LSA 20. Checksum Sum 0x0A2542
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

Рис. 3.22.Демонстрація роботи команди show ip ospf

Кожен раз, коли маршрутизатор отримує нову інформацію про топології (додавання, видалення або модифікація зв'язку), маршрутизатор, повинен повторно запустити алгоритм SPF, щоб створити нове дерево SPF і оновити таблицю маршрутизації. Алгоритм SPF інтенсивний для ЦП, і час, який потрібен для обчислення, залежить від розміру області. Розмір області вимірюється числом маршрутизаторів і розміром бази даних стану каналу.

Мережа, яка циклічно переходить зі стану up в down і навпаки, називають хитається зв'язком. Коливання зв'язок може змусити маршрутизатори OSPF в області постійно повторно обчислювати алгоритм SPF, запобігаючи належну збіжність. Щоб мінімізувати цю проблему, маршрутизатор очікує 5 секунд (5000 msecs) після отримання LSU перш, ніж виконувати алгоритм SPF. Це відомо як затримка розкладу SPF. Щоб запобігти маршрутизатор від постійного виконання алгоритму SPF, є додаткове Час затримки 10 секунд (10000 msecs). Маршрутизатор очікує через 10 секунд після виконання алгоритму SPF перш, ніж знову запустити алгоритм повторно.

Найшвидший спосіб перевірити інтервал Hello і Мертвий інтервал полягає в тому, щоб використовувати команду show ip ospf interface. Як показано на малюнку, додавання імені і номера інтерфейсу до команди відображає висновок для певного інтерфейсу.

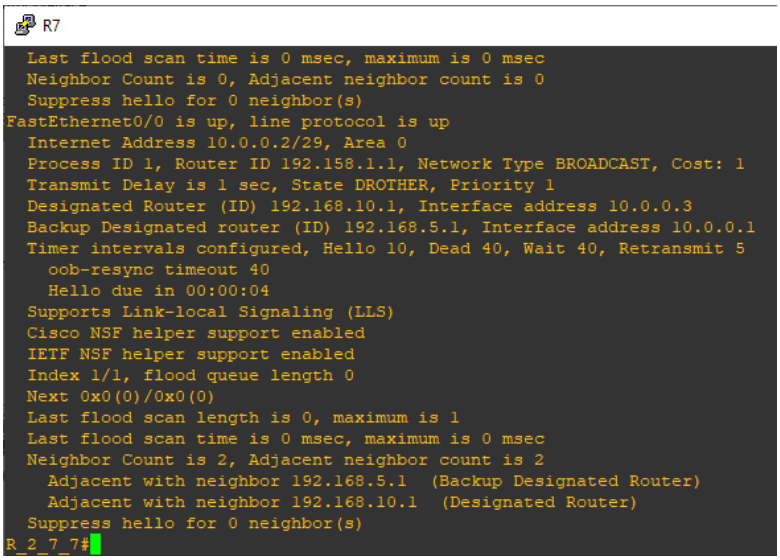


Рис. 3.23.Демонстрація роботи команди show ipospf interface на маршрутизаторі R7

Ці інтервали включаються в Пакети hello OSPF, що відправляються між сусідами. OSPF може мати відмінні інтервали hello і мертві інтервали на різних інтерфейсах, але для маршрутизаторів OSPF, щоб стати сусідами, їх OSPF інтервал hello і мертвий інтервал повинні бути ідентичними. Наприклад, на малюнку, R7 використовує інтервал "Привіт", що дорівнює 10, і мертвий інтервал 40 на інтерфейсі FastEthernet 0/0. Сусідній маршрутизатор повинен також використовувати ті ж самі інтервали на своєму інтерфейсі , або ці два маршрутизатора не будуть формувати суміжність.

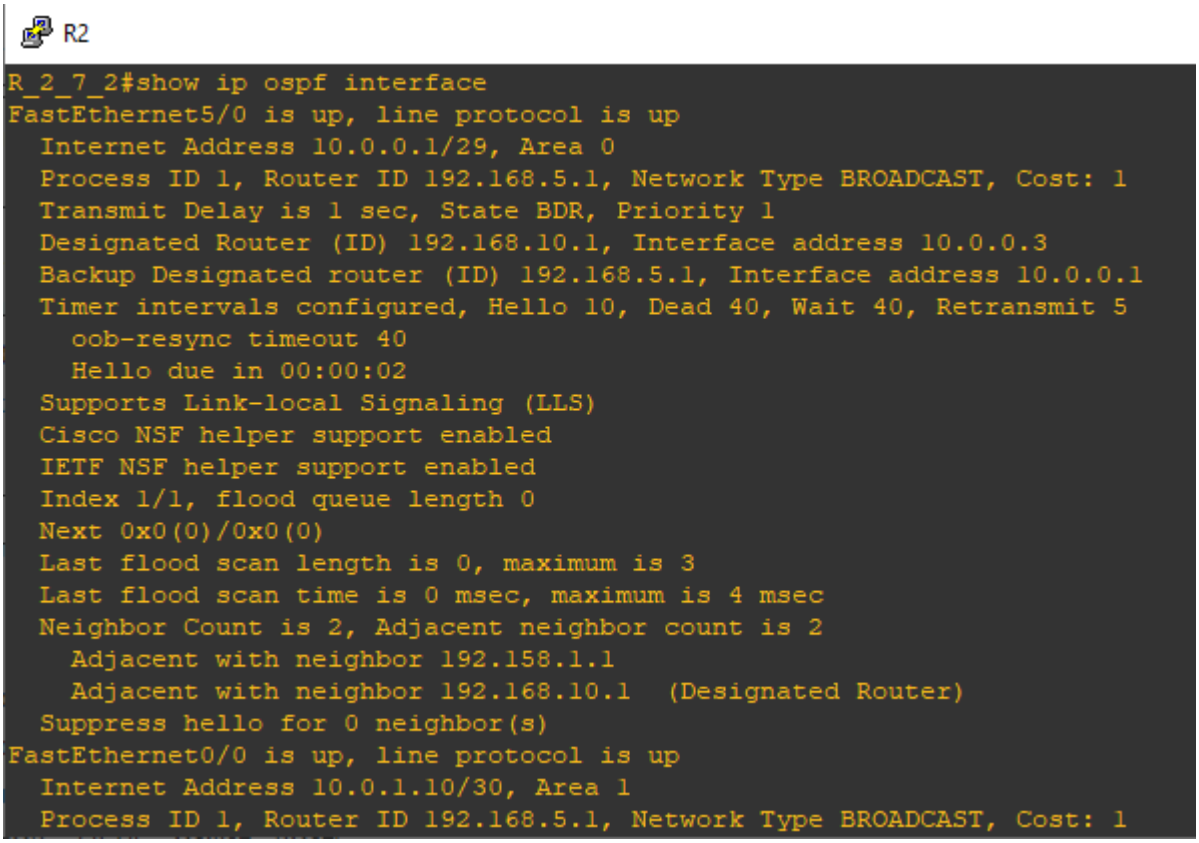
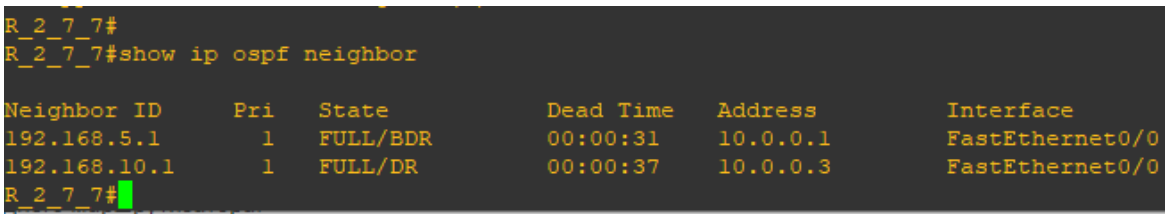


Рис. 3.24.Демонстрація роботи команди show ipospf interface на маршрутизаторі R2

Команда *show ip ospf neighbor* може використовуватися, щоб перевірити і діагностувати відносини суміжності OSPF.



3.25.Демонстрація роботи командиshow ipospfneighbor

Для кожного сусіда ця команда виведе на екран наступну інформацію:

1. Neighbour ID - ID сусіднього маршрутизатора.

2. Pri - пріоритет інтерфейсу OSPF.

3. State - Стан OSPF інтерфейсу. Стан FULL означає, що у маршрутизатора і його сусіда ідентичні бази даних стану каналу OSPF.

4. Dead Time - Час який маршрутизатор буде очікувати, щоб отримати hello пакет OSPF від сусіда перш, ніж оголосити сусіда як втраченого. Це значення зникає, коли інтерфейс отримує пакет hello.

5. Address - IP-адреса інтерфейсу сусіда, з яким безпосередньо взаємодіє цей маршрутизатор.

Проводячи діагностику мережі OSPF, команда show ip ospf neighbor може використовуватися, щоб перевірити те що маршрутизатор сформував суміжність зі своїми сусідніми маршрутизаторами. Якщо ID маршрутизатора сусіднього маршрутизатора не виводиться на екран, або його стан не відображається як FULL, ці два маршрутизатора не сформована суміжність OSPF. Якщо два маршрутизатора не встановили суміжності, то інформацією про стан каналу вони не обміняються. Неповні бази даних стану каналу можуть викликати неточні дерева SPF і таблиці маршрутизації. Маршрути до цільових мережне будуть існувати або буде обраний не найкращий шлях.

Висновки до розділу 3.

В даному розділі були описані базові налаштування пристроїв мережі: статична та динамічна адресація, статична маршрутизація та маршрутизація по протоколу OSPF. Для зручності роботи з обладнанням також були налаштовані імена пристроїв та мережні об’єкти.

На мережних пристроях було проведене налагодження технології NAT. Також списки доступу в мережі. Проведено тестування функціонування мережі: обмін трафіком всередині підмереж, обмін трафіком з глобальною мережею.

Проведено аналіз результатів тестування та сформовано висновки щодо модернізації та можливостей покращення роботи мережі.

ВИСНОВКИ

На сьогоднішній день розробка і впровадження локальних інформаційних систем є однією з важливіших завдань в області інформаційних технологій. З'являється потреба у використанні новітніх технологій для передачі інформації. Інтенсивне використання інформаційних технологій вже зараз є важливим аргументом в конкурентній боротьбі, що розгорнулася на світовому ринку.

В даній кваліфікаційній роботі були поставлені і успішно вирішені завдання вибору мережевої архітектури, конфігурації мережевого устаткування, розглянуті питання управління мережевими ресурсами та користувачами мережі, питання безпеки мережі.

Був проаналізований протокол динамічної маршрутизації OSPF. Протокол визначений у стандарті RFC 1583, являє собою відкритий протокол з широкими функціональними можливостями, який забезпечує взаємодію мереж різних виробників за допомогою сімейства протоколів TCP / IP. Переваги OSPF це швидка конвергенція, VLSM, аутентифікація, ієрархічна сегментація, сумовування і агрегування маршрутів. Всі ці можливості необхідні для роботи великих і складних мереж.

Також були розглянуте обладнання одного з провідних виробників мережевого обладнання – корпорації Cisco. Був проаналізований асортимент, можливості налаштувань та експлуатації обладнання для захисту локальних мереж від не бажаних втручань.

В проекті була використана технологія NAT. Вона допомогла впоратися з дефіцитом IP-адрес, який стає все більш гострим у міру зростання кількості комп'ютерів. Забезпечила безпеку внутрішньої мережі. Комп'ютери локальної мережі, захищені маршрутизатором з активованим NAT-протоколом стають недоступними для зовнішніх чинників. Хоча протокол NAT не замінює брандмауер, він все ж є важливим елементом безпеки.

Були застосовані списки доступу ACL. Вони використовуються для підвищення рівня безпеки та мінімізації ризиків і ефективності прямих втручань. Також захищаючи маршрутизатор від непотрібного трафіку і спаму.

За допомогою проведеного аналізу була спроектована мережа уявної організації. Були сформовані таблиці параметрів інтерфейсів пристроїв та адресації підмереж для цього проекту.

У роботі виконано моделювання мережі підприємства у мережевому емуляторі Graphical Network Simulator-3. Тестування мережі показало вірність виконаних налаштувань і працездатність мережі.

Проведено аналіз результатів тестування та сформовано висновки щодо модернізації та можливостей покращення роботи мережі.

Реалізована мережа є повністю готовим макетом реальної реалізації проекту. Конфігурації можуть бути застосовані для налаштування реального обладнання мережі. Макет може використовуватись для дослідження різних атак на подібні або аналогічні мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Протокол OSPF [Електронний ресурс] – Режим доступу до ресурсу:https://uk.wikipedia.org/wiki/OSPF
2. Протокол OSPF [Електронний ресурс] – Режим доступу до ресурсу:http://xgu.ru/wiki/OSPF
3. Маршрутизатори серії 7200[Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/routers/7200-series-routers/series.html#~tab-documents
4. Open Shortest Path First (OSPF) [Електронний ресурс] – Режим доступу до ресурсу:https://www.cisco.com/c/en/us/products/ios-nx-os-software/open-shortest-path-first-ospf/index.html
5. Принципы работы протокола EIGRP [Електронний ресурс] – Режим доступу до ресурсу:https://habr.com/ru/post/420667/
6. Enterprise routing protocols: VRRP, STP, RIP, OSPF, and BGP[Електронний ресурс] – Режим доступу до ресурсу:https://cradlepoint.com/resources/blog/enterprise-routing-protocols-vrrp-stp-rip-ospf-and-bgp/
7. Configure Route Leaking Between Global and VRF Routing Table without Next-Hop[Електронний ресурс] – https://www.cisco.com/c/ru_ru/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html
8. TCP/IP[Електронний ресурс] –https://uk.wikipedia.org/wiki/TCP/IP
9. Основы компьютерных сетей. Тема №3. Протоколы нижних уровней (транспортного, сетевого и канального)[Електронний ресурс] – https://habr.com/ru/post/308636/
10. Комп'ютерна мережа[Електронний ресурс] – https://uk.wikipedia.org/wiki/Комп'ютерна_мережа
11. Локальні обчислювальні мережі[Електронний ресурс] – https://uareferat.com/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D

1%8C%D0%BD%D1%96_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D1%8E%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96_2

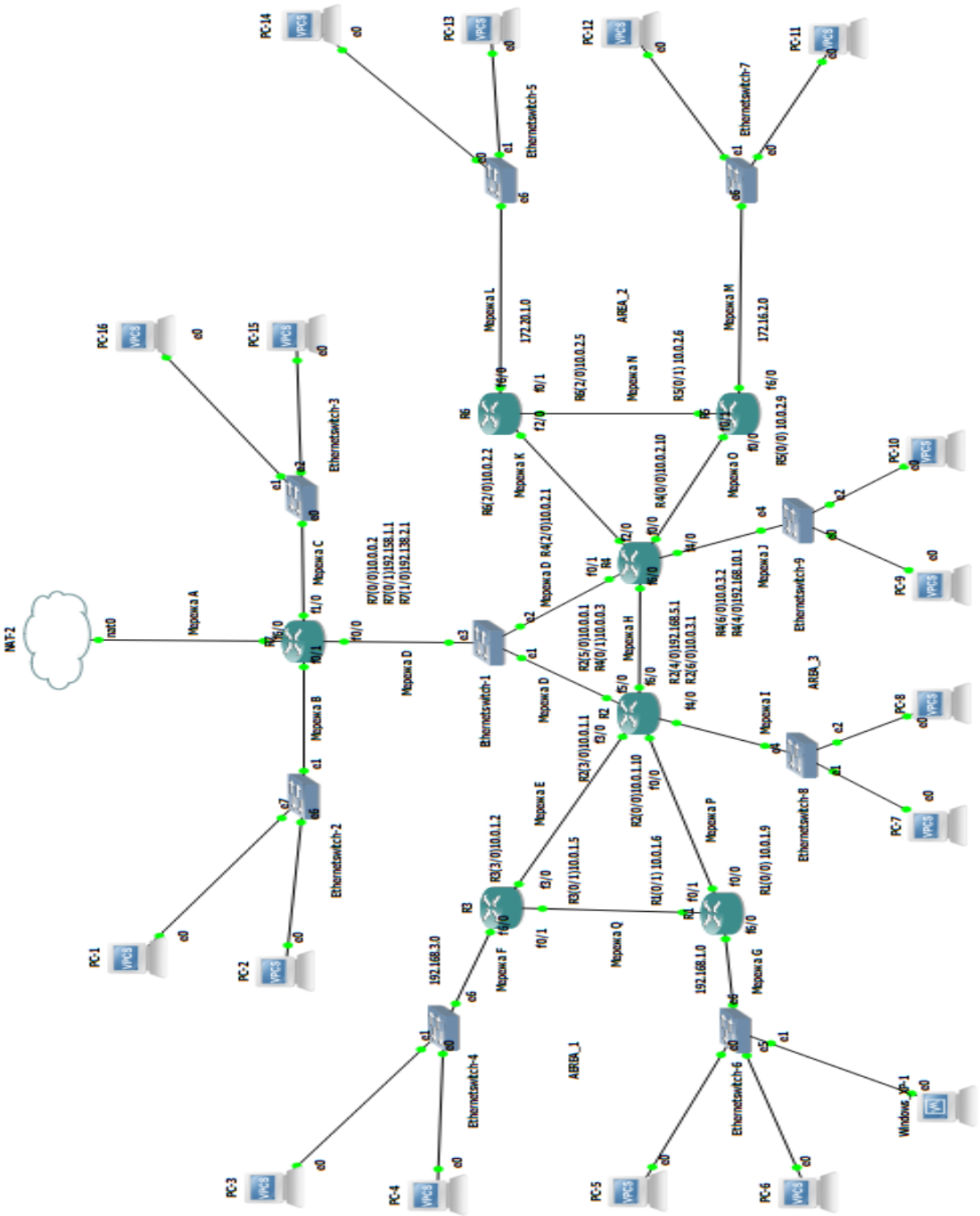
12. Маршрутизатор [Електронний ресурс] – https://www.wikizero.com/uk/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80
13. Cisco Systems [Електронний ресурс] – https://uk.wikipedia.org/wiki/Cisco_Systems
14. Компютерні мережі [Електронний ресурс] – https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/4.9.3.html
15. OSPF[Електронний ресурс] –https://uk.wikipedia.org/wiki/OSPF
16. OSPF (Open Shortest Path First) [Електронний ресурс] – https://wiki.cuspu.edu.ua/index.php/OSPF
17. Адресація в IP-мережах [Електронний ресурс] – https://uk.wikipedia.org/wiki/Адресація_в_IP-мережах
18. Мережева модель OSI[Електронний ресурс] – https://uk.wikipedia.org/wiki/Мережева_модель_OSI
19. Мережева модель OSI [Електронний ресурс] – https://uk.wikipedia.org/wiki/Протокол_маршрутизації
20. ACL (Access Control List) [Електронний ресурс] – https://ru.bmstu.wiki/ACL_(Access_Control_List)
21. ACL: списки контроля доступа в Cisco IOS[Електронний ресурс] – https://habr.com/ru/post/121806/
22. Пример конфигурации: EtherChannel между коммутаторами Catalyst, работающими под управлением ПО CatOS и Cisco IOSIOS [Електронний ресурс] –https://www.cisco.com/c/ru_ru/support/docs/lan-switching/etherchannel/12029-71.html
23. Что такое ACL и как его настраивать[Електронний ресурс] – http://ciscotips.ru/acl

24. Cisco IOS ACLsнастраивать[Електронний ресурс] – https://habr.com/ru/post/154879/
25. Транспортный уровень стека TCP/IP. Описание и принцип работы протоколов TCP и UDP[Електронний ресурс] –https://easy-network.ru/5-urok-4.html
26. Топологія мереж[Електронний ресурс] – https://uk.wikipedia.org/wiki/Топологія_мереж
27. Топологіямереж[Електронний ресурс] – https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/qa_c67_553891.html
28. Выставить приоритет между сетями с двумя шлюзами[Електронний ресурс] – https://qna.habr.com/q/197527

Додатки

Додаток А

Топологія мережі



Додаток Б

Лістинги конфігураційних файлів

```
R_2_7_7#show run
Building configuration...

Current configuration : 2359 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2_7_7
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 192.158.1.1
ip dhcp excluded-address 192.138.2.0
!
ip dhcp pool DHCP_AREA_0_R7_1
   network 192.158.1.0 255.255.255.0
   dns-server 8.8.8.8
   default-router 192.158.1.1
!
ip dhcp pool DHCP_AREA_0_R7_2
   network 192.138.2.0 255.255.255.0
   default-router 192.138.2.1
   dns-server 8.8.8.8
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.248
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.158.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.138.2.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 192.138.2.0 0.0.0.255 area 0
 network 192.158.1.0 0.0.0.255 area 0
!
no ip http server
ip forward-protocol nd
!
!
ip nat inside source list PATIK interface
FastEthernet6/0 overload
!
!
ip access-list standard PATIK
 permit 192.168.1.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.5.0 0.0.0.255
 permit 192.168.10.0 0.0.0.255
 permit 172.16.2.0 0.0.0.255
 permit 172.20.1.0 0.0.0.255
 permit 192.158.1.0 0.0.0.255
 permit 192.138.2.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

```
R_2_7_2#show run
Building configuration...

Current configuration : 1839 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2_7_2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 172.40.2.1
!
ip dhcp pool DHCP_AREA_3_R2
   network 192.168.5.0 255.255.255.0
   default-router 192.168.5.1
   dns-server 8.8.8.8
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.1.10 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 ip address 10.0.1.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet4/0
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet5/0
 ip address 10.0.0.1 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address 10.0.3.1 255.255.255.252
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 10.0.1.0 0.0.0.3 area 1
```

```
 network 10.0.1.8 0.0.0.3 area 1
 network 10.0.3.0 0.0.0.3 area 3
 network 192.168.5.0 0.0.0.255 area 3
!
no ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet5/0
!
!
!
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

```
hostname R_2_7_3
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.3.1
!
ip dhcp pool DHCP_AREA_1_R3
   network 192.168.3.0 255.255.255.0
   dns-server 8.8.8.8
   default-router 192.168.3.1
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 10.0.1.5 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 ip address 10.0.1.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address 192.168.3.1 255.255.255.0
 ip access-group CLOSE out
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet6/0
 network 10.0.1.0 0.0.0.3 area 1
 network 10.0.1.4 0.0.0.3 area 1
 network 192.168.3.0 0.0.0.255 area 1
!
no ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet3/0
!
!
!
ip access-list standard CLOSE
 deny   192.168.1.0 0.0.0.255
 permit any
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

```
hostname R_2_7_4
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 172.50.1.1
!
ip dhcp pool DHCP_AREA_3_R4
   network 192.168.10.0 255.255.255.0
   dns-server 8.8.8.8
   default-router 192.168.10.1
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.2.10 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.3 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 10.0.2.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet4/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address 10.0.3.2 255.255.255.252
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.7 area 0
 network 10.0.2.0 0.0.0.3 area 2
 network 10.0.2.8 0.0.0.3 area 2
 network 10.0.3.0 0.0.0.3 area 3
 network 192.168.10.0 0.0.0.255 area 3
!
no ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
!
!
```

```
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

```
hostname R_2_7_6
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 172.20.1.1
!
ip dhcp pool DHCP_AREA_2_R6
   network 172.20.1.0 255.255.255.0
   default-router 172.20.1.1
   dns-server 8.8.8.8
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 10.0.2.5 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 ip address 10.0.2.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address 172.20.1.1 255.255.255.0
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet6/0
 network 10.0.2.0 0.0.0.3 area 2
 network 10.0.2.4 0.0.0.3 area 2
 network 172.20.1.0 0.0.0.255 area 2
!
router ospf 2
 log-adjacency-changes
!
no ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0
!
!
!
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

```
hostname R1_2_7_1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool DHCP_AREA_1_R1
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.1.9 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.1.6 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet6/0
 network 10.0.1.4 0.0.0.3 area 1
 network 10.0.1.8 0.0.0.3 area 1
 network 192.168.1.0 0.0.0.255 area 1
!
no ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
!
```

```
!
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```