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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Аналіз протоколів маршрутизації у сучасних комп’ютерних мережах для швидкості поширення маршрутної інформації і обчислення оптимальних шляхів

Виконав(ла): студент(ка) 6 курсу, групи СНнм-61
спеціальності 122 «Комп’ютерні науки»
(шифр і назва спеціальності)

(підпис) Шевченко Н.А. (прізвище та ініціали)

Керівник (підпис) Щербак Л.М. (прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Боднарчук І.О. (прізвище та ініціали)

Рецензент (підпис) Стадник М.А. (прізвище та ініціали)

Тернопіль
2021

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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 202 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

студенту Шевченко Назарію Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз протоколів маршрутизації у сучасних комп'ютерних мережах для швидкості поширення маршрутної інформації і обчислення оптимальних шляхів

Керівник роботи Щербак Леонід Миколайович, д.т.н., професор каф. КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 202 року № _____
2. Термін подання студентом завершеної роботи 18.05.2021
3. Вихідні дані до роботи Літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз проблематики дослідження. 2. Аналіз протоколів маршрутизації. 3. Дослідження динамічного протоколу OSPF. 4. Практична реалізація наукових досліджень Висновки. Перелік літературних джерел. Додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема, мета, завдання. 2. Повільна збіжність і зациклення маршрутизації,.
3. Порівняння внутрішніх протоколів маршрутизації.
4. Принцип функціонування маршрутизуючого протоколу.
5. Типи маршрутизаторів OSPF.
6. Типи мереж OSPF.
7. Налаштування маршрутизаторів Cisco.
8. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	к.т.н., доцент Дмитроца Л.П.		
Безпека в надзвичайних ситуаціях	д.т.н., професор Стадник І.Я.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.10.2020-28.20.2020	*Виконано*
2.	Підбір наукових джерел щодо підвищення ефективності роботи книгарні за рахунок сегментації споживачів	29.10.2020-21.11.2020	*Виконано*
3.	Переклад та опрацювання наукових джерел щодо підвищення ефективності роботи протоколів маршрутизації	22.11.2020-21.12.2020	*Виконано*
4.	Виконання дослідження щодо підвищення ефективності протоколів маршрутизації	22.12.2020-10.01.2021	*Виконано*
5.	Оформлення розділу «Аналіз проблематики дослідження»	11.01.2021-21.02.2021	*Виконано*
6.	Оформлення розділу «Аналіз протоколів маршрутизації»	22.02.2021-01.03.2021	*Виконано*
7.	Оформлення розділу «Дослідження динамічного протоколу OSPF»	02.03.2021-11.03.2021	*Виконано*
8.	Оформлення розділу «Практична реалізація наукових досліджень»	02.03.2021-11.03.2021	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці»	12.03.2021-20.03.2021	*Виконано*
10.	Виконання завдання до підрозділу «Безпека в надзвичайних ситуаціях»	21.03.201-28.03.2021	*Виконано*
11.	Оформлення кваліфікаційної роботи	29.03.201-29.04.2021	*Виконано*
12.	Нормоконтроль	30.04.2021-06.05.2021	*Виконано*
13.	Перевірка на плагіат	07.05.2021	*Виконано*
14.	Попередній захист кваліфікаційної роботи	10.05.2021	*Виконано*
15.	Захист кваліфікаційної роботи	25.05.2021	

Студент _____ Шевчекно Н.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Щербак Л.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз протоколів маршрутизації у сучасних комп’ютерних мережах для швидкості поширення маршрутної інформації і обчислення оптимальних шляхів // Дипломна робота ОР «Магістр» // Шевченко Назарій Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНнм–61 // Тернопіль, 2021 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: ЗБІЖНІСТЬ, МЕРЕЖА, ДОСЛІДЖЕННЯ, ДАНІ, ПРОТОКОЛ, АЛГОРИТМ, МАРШРУТИЗАЦІЯ, АЛГОРИТМ, ДИНАМІЧНИЙ

В першому розділі проведено опис: маршрутизації маршрутизованих протоколів у комп’ютерних мережах, види маршрутизації, класи протоколів маршрутизації, класифікації алгоритмів маршрутизації, маршрутизації одноадресної передачі, особливості протоколів маршрутизації стану посилань та проведено опис відкритого протоколу маршрутизації найкоротшого шляху (OSPF).

В другому розділі проведено огляд протоколів маршрутизації таких як: інформаційний протокол маршрутизації (RIP), інформаційний протокол маршрутизації (RIP) V1 і V2, протокол EIGRP та наведено особливості вдосконаленого протоколу маршрутизації внутрішніх шлюзів (EIGRP).

В третьому розділі проведено опис протоколу маршрутизації OSPF, наведено ролі маршрутизатора та найкоротший шлях (OSPF) і його налаштування, описано стани протоколу (OSPF) та наведено відкриття найкоротшого шляху в OSPF.

В четвертому розділі проведено розробку початкових налаштувань маршрутизації протоколів «OSPF та EIGRP» для обладнання компанії Cisco.

ABSTRACT

Analysis of routing protocols in modern computer networks aimed at quick spread of route information and the most efficient ways calculation // Diploma work degree “Master” // Shevchenko Nazariy Andriyovych // Ternopil Ivan Pul'uj National Technical University, Faculty of computer-information systems and software engineering, Department of computer science, a group SNnm-61 // Ternopil, 2021 // P.- , Fig. - Table. - , Draws. - , Add. - , Ref. - .

Keywords: CONVERGENCE, NETWORK, RESEARCH, DATA, PROTOCOL, ALGORITHM, ROUTING, ALGORITHM, DYNAMIC

The first section describes: routing of routing protocols in computer networks, types of routing, classes of routing protocols, classification of routing algorithms, unicast routing, features of link state routing protocols and a description of the open path routing protocol (OSP).

The second section provides an overview of routing protocols such as: Routing Information Protocol (RIP), Routing Information Protocol (RIP) V1 and V2, EIGRP protocol, and features of the Advanced Internal Gateway Routing Protocol (EIGRP).

The third section describes the OSPF routing protocol, describes the roles of the router and the shortest path (OSPF) and its settings, describes the protocol states (OSPF), and provides the discovery of the shortest path in OSPF.

In the fourth section, the initial routing settings of the OSPF and EIGRP protocols for Cisco equipment were developed.

ЗМІСТ

ВСТУП

Актуальність теми роботи. Протоколи маршрутизації – це набір визначених правил, що використовуються маршрутизаторами для зв’язку між джерелом і призначенням. Вони не переміщують інформацію джерела до пункту призначення, а лише оновлюють таблицю маршрутизації, що містить інформацію.

Протоколи мережевих маршрутизаторів допомагають визначити спосіб взаємодії маршрутизаторів між собою. Це дозволяє мережі вибирати маршрути між будь-якими двома вузлами в комп'ютерній мережі.

Метою наукового дослідження є аналіз протоколів маршрутизації

Згідно до виконання мети роботи потрібно виконати завдання:

– провести аналіз проблематики дослідження;

– зробити аналіз видів маршрутизації;

– провести аналіз протоколів маршрутизації та навести їх порівняльну характеристику;

– провести дослідження динамічного протоколу OSPF;

– провести розробку початкових налаштувань маршрутизації протоколів.

Наукова новизна: методика дослідження, яка була використана у даній роботі, сформульована за допомогою такого стандарту, як RFC, який в свою чергу дозволяє привести методику роботи протоколів маршрутизації «OSPF та EIGRP», що в свою чергу дозволяють провести аналіз та оцінку даних протоколів.

Об’єктом дослідження є комп’ютерна мережа.

Апробація результатів роботи. Результати роботи представлені на двох наукових конференціях:

1. Огляд моделей хмарних послуг / Н. А. Шевченко, М. В. Валігула, Т. О. Маєвський, Г. В. Шимчук // Матеріали міжнародної наукової конференції „Іван Пулюй: життя в ім’я науки та України“ (до 175-ліття від дня народження), 28-30

вересня 2020 року. — Т. : ФОП Паляниця В. А., 2020. — С. 109–110. — (Важливі аспекти практичного застосування здобутків сучасної науки і новітніх технологій).

2. Шевченко Н. Аналіз протоколу OSPF / Н. Шевченко., Ю. Горбуляк, Т. Маєвський // Матеріали IV Міжнародної студентської науково - технічної конференції / Тернопіль: Тернопільський національний технічний університет ім. І.Пулюя (м. Тернопіль, 28-29 квітня 2021 р.),. — Т. : ТНТУ, 2021. — С. 21-22.

1 АНАЛІЗ ПРОБЛЕМАТИКИ ДОСЛІДЖЕННЯ

1.1 Маршрутизація маршрутизованих протоколів у комп'ютерних мережах

Мережевий рівень моделі OSI відповідає за забезпечення логічної адресації, яку маршрутизатори використовують для вибору найкращого шляху для маршрутизації пакетів. На цьому шарі використовуються два типи пакетів:

1. Пакети даних – дані користувача передаються в підмережі цими пакетами даних. Маршрутизовані протоколи – це ті протоколи, які підтримують такий трафік даних Прикладами маршрутизованих протоколів є IPv4, IPv6 та AppleTalk.

2. Пакети оновлення маршруту – інформація про мережі, підключені до всіх маршрутизаторів, оновлюється до сусідніх маршрутизаторів через пакети оновлення маршруту. Протоколи маршрутизації відповідають за їх надсилання. Прикладами протоколів маршрутизації є «RIP (Routing Information Protocol), EIGRP (Enhanced Internal Gateway Routing Protocol) та OSPF (Open Shortest Path First)».

А тепер давайте візьмемо реальну аналогію, щоб краще зрозуміти різницю між протоколами маршрутизації.

Припустимо, ви хочете піти додому після семестрових іспитів. Ви забронюєте таксі або їдете автобусом додому. На шляху своєї подорожі ви зустрічаєте кілька табличок із знаками, які допоможуть вам пройти правильний або найкращий шлях, або Google Maps допоможе вам вибрати найкращий маршрут.

За цією аналогією розгляньте себе як «ДАНІ», автобус чи кабіну як «ПРОТОКОЛ МАРШРУТУ», а дошки вивісок чи GPS, встановлений у телефоні вашого водія, як «ПРОТОКОЛ МАРШРУТУ». Подібним чином, у мережі маршрутизатори використовують протоколи маршрутизації, щоб визначити найкращий шлях для того, щоб пакет ефективніше переміщався по підмережах.

Маршрутизовані протоколи призначаються інтерфейсу і визначають спосіб доставки пакету.

Тепер давайте перейдемо до різних типів протоколів маршрутизації.

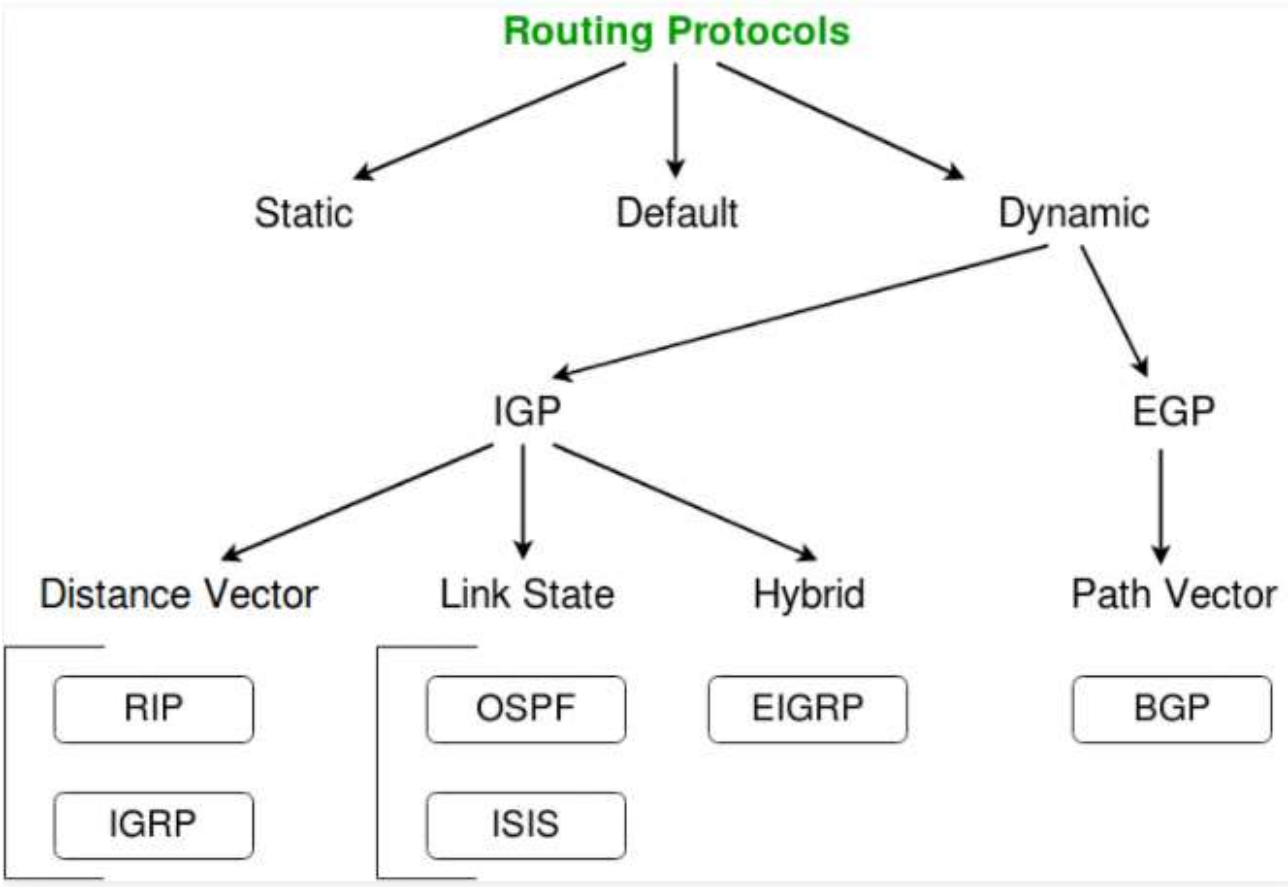

Рисунок 1.1 – Типи маршрутизації

IGP – Протокол внутрішніх шлюзів.

EGP – Протокол зовнішніх шлюзів.

RIP – Протокол інформації про маршрутизацію.

IGRP – Протокол маршрутизації внутрішніх шлюзів

OSPF – Протокол динамічної маршрутизації.

ISIS – Протокол маршрутизації проміжних систем.

EIGRP – Покращений протокол маршрутизації внутрішніх шлюзів.

BGP – Протокол маршрутизації між автономними системами.

1.2 Види маршрутизації

Маршрутизація – це процес, який виконується пристроями рівня 3 (або мережевого рівня) з метою доставки пакету шляхом вибору оптимального шляху від однієї мережі до іншої.

Існує 3 типи маршрутизації:

1. Статична маршрутизація – статична маршрутизація – це процес, при якому ми повинні вручну додавати маршрути в таблиці маршрутизації.

Переваги

- Немає накладних витрат на маршрутизатор для процесора маршрутизатора, що означає, що для маршрутизації можна використовувати дешевий маршрутизатор.
- Це додає безпеки, оскільки лише адміністратор може дозволити маршрутизацію лише до певних мереж.
- Відсутність використання смуги пропускання між маршрутизаторами.

Недоліки

- Для великої мережі адміністратору є важке завдання вручну додавати кожен маршрут для мережі до таблиці маршрутизації на кожному маршрутизаторі.
- Адміністратор повинен добре знати топологію. Якщо приходить новий адміністратор, він повинен вручну додати кожен маршрут, щоб він мав дуже добре знати маршрути топології.

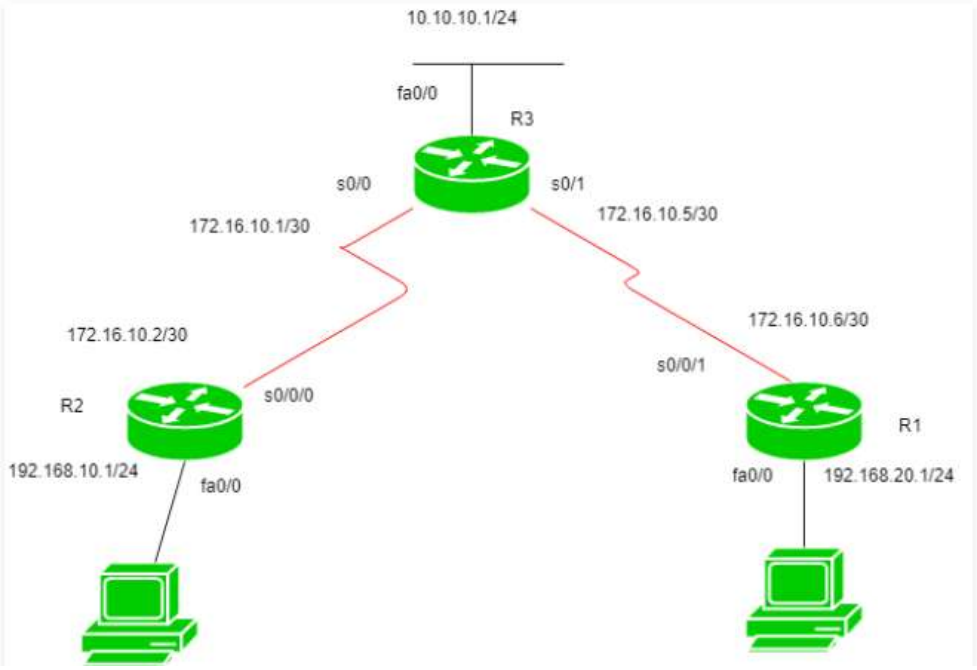

Рисунок 1.2 – Конфігурація мережі

R1, що має IP-адресу 172.16.10.6/30 на s0 / 0/1, 192.168.10.1/24 на fa0 / 0. R2, що має IP-адресу 172.16.10.2/30 на s0 / 0/0, 192.168.20.1/24 на fa0 / 0. R3, що має IP-адресу 172.16.10.5/30 на s0 / 1, 172.16.10.1/30 на s0 / 0, 10.10.10.1/24 на fa0 / 0.

Налаштовуємо статичні маршрути для маршрутизатора R3:

```
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2
R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6
```

Це вказано маршрут для мережі 192.168.10.0, де 192.168.10.0 є її мережею I, а 172.16.10.2 та 172.16.10.6 – наступною адресою переходу.

Налаштування для R2:

```
R2(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.1
R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1
R2(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.1
```

Аналогічно для R1:

```
R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5
R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5
R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5
```

2. Маршрутизація за замовчуванням – це спосіб, при якому маршрутизатор налаштований на передачу всіх пакетів до одного маршрутизатора (наступний стрибок). Не має значення, до якої мережі належить пакет, він передається маршрутизатору, який налаштований на маршрутизацію за замовчуванням. Зазвичай він використовується із заглушеними маршрутизаторами. Маршрутизатор заглушки – це маршрутизатор, який має лише один шлях для досягнення всіх інших мереж.

Використаємо ту саму топологію, яку ми використовували для статичної маршрутизації раніше (див. рис. 1.2).

У цій топології R1 та R2 є маршрутизаторами-заглушками, тому ми можемо налаштувати маршрутизацію за замовчуванням для обох цих маршрутизаторів.

Налаштування маршрутизації за замовчуванням для R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0  172.16.10.5
```

Тепер налаштовуємо маршрутизацію за замовчуванням для R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0  172.16.10.1
```

3. Динамічна маршрутизація робить автоматичне коригування маршрутів відповідно до поточного стану маршруту в таблиці маршрутизації. Динамічна маршрутизація використовує протоколи для виявлення мережевих пунктів призначення та маршрутів до них. RIP та OSPF – найкращі приклади протоколу динамічної маршрутизації. Автоматичне регулювання буде здійснено для досягнення пункту призначення мережі, якщо один маршрут піде вниз.

Динамічний протокол має такі особливості:

1. Маршрутизатори повинні мати однаковий динамічний протокол для обміну маршрутами.

2. Коли маршрутизатор виявляє зміну в топології, тоді маршрутизатор рекламує це всім іншим маршрутизаторам.

Переваги

- Простота налаштування.

– Більш ефективно вибрати найкращий маршрут до віддаленої мережі призначення, а також виявити віддалену мережу.

Недоліки

– Споживає більше пропускної здатності для спілкування з іншими сусідами.

– Менш безпечний, ніж статична маршрутизація.

1.3 Класи протоколів маршрутизації

Розглянемо протокол векторної маршрутизації відстані та протокол маршрутизації стану зв'язку Маршрутизація – це процес, при якому пристрої рівня 3 (або маршрутизатор, або комутатор рівня 3) знаходять оптимальний шлях для доставки пакету з однієї мережі в іншу. Протоколи динамічної маршрутизації використовують метрику, вартість та кількість стрибків, щоб визначити найкращий шлях із шляху, доступного для мережі призначення. В основному існує 3 різні класи протоколів маршрутизації:

1. Протокол векторної маршрутизації відстані. Ці протоколи вибирають найкращий шлях на основі підрахунку стрибків для досягнення цільової мережі у певному напрямку. Динамічний протокол, такий як RIP, є прикладом протоколу векторної маршрутизації відстані. Кількість переходів – це кожен маршрутизатор, який відбувається між джерелом та мережею призначення. Шлях із найменшим числом стрибків буде обраний найкращим шляхом.

Особливості

– Проходить обмін інформації при оновлені мережі.

– Оновлення (інформація про маршрутизацію) завжди транслюється.

– Повні таблиці маршрутизації надсилаються в оновленнях.

– Маршрутизатори завжди довіряють інформації про маршрутизацію, отриману від сусідніх маршрутизаторів.

Недоліки

– Оскільки інформація про маршрутизацію періодично обмінюється, генерується непотрібний трафік, який споживає доступну пропускну здатність.

– Оскільки повні таблиці маршрутизації обмінюються, то це має проблеми із безпекою. Якщо до мережі увійде уповноважена особа, то всю топологію буде дуже легко зрозуміти.

– Також трансляція мережі періодично створює непотрібний трафік.

2. Протокол маршрутизації стану зв'язку. Ці протоколи знають про роботу в мережі більше, ніж будь-який інший протокол векторної маршрутизації відстані. Вони також відомі як протокол SPF (Shortest Path First). OSPF є прикладом протоколу маршрутизації стану зв'язку.

Особливості

– «Привіт повідомлення», також відомі як повідомлення про підтримку, використовуються для виявлення та відновлення сусідів.

– Використовується концепція ініційованих оновлень, тобто оновлення ініціюються лише тоді, коли відбувається зміна топології.

– Обмінюється лише стільки оновлень, які запитує сусідній маршрутизатор.

Протокол маршрутизації стану зв'язку підтримує три таблиці, а саме:

1. Таблиця сусідів – таблиця, яка містить інформацію лише про сусідів маршрутизатора, тобто до яких приєднано.

2. Таблиця топології. Ця таблиця містить інформацію про всю топологію, тобто містить як найкращі, так і резервні маршрути до певної рекламованої мережі.

3. Таблиця маршрутизації. Ця таблиця містить усі найкращі маршрути до рекламованої мережі.

Переваги

– Оскільки він підтримує окремі таблиці як для найкращого маршруту, так і для резервного маршруту (ціла топологія), тому він має більше знань про міжмережу, ніж будь-який інший протокол векторної маршрутизації відстані.

– Використовується концепція ініційованих оновлень, тому більше не спостерігається зайвого споживання смуги пропускання, як у протоколі векторної маршрутизації відстані.

– Часткові оновлення запускаються, коли відбувається зміна топології, а не повне оновлення, як протокол векторної маршрутизації відстані, де обмінюється вся таблиця маршрутизації.

3. Розширений протокол векторної маршрутизації відстані – Він також відомий як гібридний протокол маршрутизації, який використовує концепцію як протоколу векторної дистанції, так і протоколу маршруту стану зв'язку. Розширений протокол маршрутизації внутрішніх шлюзів (EIGRP) є прикладом цього класу, якщо протокол маршрутизації. EIGRP діє як протокол маршрутизації стану зв'язку, оскільки використовує концепцію протоколу Hello для виявлення сусідів та формування суміжності. Крім того, часткові оновлення запускаються, коли відбувається зміна. EIGRP діє як протокол векторної маршрутизації відстані, оскільки вивчав маршрути від безпосередньо підключених сусідів.

1.4 Класифікація алгоритмів маршрутизації

Маршрутизація – це процес встановлення маршрутів, якими повинні йти пакети даних для досягнення пункту призначення. У цьому процесі створюється таблиця маршрутизації, яка містить інформацію про маршрути, за якими йдуть пакети даних. Різні алгоритми маршрутизації використовуються для того, щоб вирішити, яким маршрутом вхідний пакет даних повинен бути переданий, щоб ефективно дістатись до пункту призначення.

Алгоритми маршрутизації можна класифікувати наступним чином:

1. Адаптивні алгоритми – це алгоритми, які змінюють рішення про маршрутизацію, коли змінюється топологія мережі або навантаження трафіку. Зміни в рішеннях про маршрутизацію відображаються на топології, а також на трафіку мережі. Також відомі, як динамічна маршрутизація, вони

використовують динамічну інформацію, таку як поточна топологія, навантаження, затримка тощо для вибору маршрутів. Параметри оптимізації – це відстань, кількість стрибків та розрахунковий час проходження інформації.

Далі вони класифікуються таким чином:

– Ізольовані. У цьому методі кожен вузол приймає рішення про маршрутизацію, використовуючи інформацію, яку він має, не шукаючи інформацію в інших вузлах. Відправляючі вузли не мають інформації про стан певного посилання. Недоліком є те, що пакет може надсилатися через перевантажену мережу, що може призвести до затримки.

– Централізовані. У цьому методі централізований вузол має всю інформацію про мережу і приймає всі рішення про маршрутизацію. Перевага цього методу полягає в тому, що для збереження інформації всієї мережі потрібен лише один вузол. Алгоритм стану посилання називається централізованим алгоритмом, оскільки він знає про вартість кожного посилання в мережі.

– Розподілені. У цьому методі вузол отримує інформацію від своїх сусідів, а потім приймає рішення про маршрутизацію пакетів. Недоліком є те, що пакет може затримуватися, якщо між інтервалами, в яких він отримує інформацію та відправляє пакет, змінюється інтервал. Він також відомий як децентралізований алгоритм, оскільки він обчислює найменш витратний шлях між джерелом і пунктом призначення

2. Неадаптивні алгоритми – це алгоритми, які не змінюють рішення про маршрутизацію після того, як їх було вибрано. Вони також відомі, як статична маршрутизація, оскільки маршрут, який потрібно пройти, обчислюється заздалегідь і завантажується на маршрутизатори при завантаженні маршрутизатора.

Вони класифікуються таким чином:

– «Flooding». Адаптує техніку, при якій кожен вхідний пакет надсилається на кожну вихідну лінію, за винятком тієї, з якої він надійшов. Однією з проблем цього є те, що пакети можуть йти в циклі, і в результаті вузол

може отримувати повторювані пакети. Ці проблеми можна подолати за допомогою порядкових номерів, кількості стрибків.

– «Random walk» У цьому методі пакети передаються хостом за хостом або вузлом за вузлом до одного із сусідів випадковим чином. Це надзвичайно надійний метод, який зазвичай реалізується шляхом надсилання пакетів на посилання, яке найменше знаходиться в черзі.

1.5 Маршрутизація одноадресної передачі

Обов’язкова умова: маршрутизація відстані вектора, алгоритм Дейкстра, маршрутизація відстані вектора v/s, маршрутизація стану каналу, OSPF, RIP.

Unicast означає передачу від одного відправника до одного одержувача. Це точка-точка зв'язку між відправником та одержувачем. Існують різні одноадресні протоколи, такі як TCP, HTTP тощо.

– TCP – це найбільш часто використовуваний одноадресний протокол. Це протокол, орієнтований на з'єднання, який передає сигнал підтвердження з боку приймача.

– HTTP розшифровується як «Hyper Text Transfer Protocol». Це об’єктно-орієнтований протокол для спілкування.

Існує три основних протоколи одноадресної маршрутизації:

1. Відстань вектор маршрутизації.
2. Маршрутизація стану посилань.
3. Маршрутизація шляху-вектора.

Маршрутизація стану каналу – це друге сімейство протоколів маршрутизації. У той час як маршрутизатори векторів відстані використовують розподілений алгоритм для обчислення своїх таблиць маршрутизації, маршрутизація стану каналу використовує маршрутизатори стану зв'язку для обміну повідомленнями, які дозволяють кожному маршрутизатору вивчити всю топологію мережі. На основі цієї вивченої топології кожен маршрутизатор

потім може обчислити свою таблицю маршрутизації, використовуючи обчислення найкоротшого шляху.

1.6 Особливості протоколів маршрутизації стану посилань

– Пакет стану зв'язку – невеликий пакет, що містить інформацію про маршрутизацію.

– База даних стану посилання – інформація про колекцію, зібрана з пакету стану зв'язку.

– Перший алгоритм найкоротшого шляху (алгоритм Дейкстри) – обчислення, проведене на базі даних, у найкоротший шлях.

– Таблиця маршрутизації – список відомих шляхів та інтерфейсів.

Розрахунок найкоротшого шляху. Щоб знайти найкоротший шлях, кожен вузол повинен запустити відомий алгоритм Дейкстри. Цей відомий алгоритм використовує наступні кроки:

– Крок 1: Вузол береться і вибирається як кореневий вузол дерева, це створює дерево з одним вузлом, і встановлюється загальна вартість кожного вузла до деякого значення, на основі інформації в базі даних стану посилань.

– Крок 2: Вузол вибирає один вузол серед усіх вузлів, що не належать до структури, подібної до дерева, яка є найближчою до кореня, і додає це до дерева.

– Крок 3: Після того, як цей вузол додано до дерева, вартість усіх вузлів, що не є у дереві, потрібно оновити, оскільки шляхи можуть бути змінені.

– Крок-4: Вузол повторює кроки 2. і 3., поки всі вузли не будуть додані в дерево.

Протоколи стану зв'язку у порівнянні з протоколами дистанційного вектора:

1. Вимагають великого обсягу пам'яті.
2. Для обчислення найкоротших шляхів потрібно багато процесорних кіл.

3. Якщо мережа використовує невелику пропускну здатність; він швидко реагує на зміни топології.

4. Всі елементи бази даних повинні надсилатися сусідам для формування пакетів стану посилань.

5. Всім сусідам потрібно довіряти топологію.

6. Механізми автентифікації можна використовувати, щоб уникнути небажаного суміжності та проблем.

7. Жодні методи розділеного горизонту неможливі при маршрутизації стану зв'язку.

1.7 Відкритий протокол маршрутизації найкоротшого шляху (OSPF)

– Open Shortest Path First (OSPF) – це одноадресний протокол маршрутизації, розроблений робочою групою робочої групи Інженерної інженерії (IETF).

– Це внутрішньодоменний протокол маршрутизації.

– Це протокол з відкритим кодом.

– Це схоже на протокол маршрутизації інформації (RIP)

– OSPF – це безкласовий протокол маршрутизації, що означає, що в своїх оновленнях він включає підмережу кожного маршруту, про який він знає, таким чином, дозволяючи маски підмережі змінної довжини. За допомогою масок підмережі змінної довжини IP-мережу можна розбити на безліч підмереж різного розміру. Це надає мережевим адміністраторам додаткову гнучкість конфігурації мережі. Ці оновлення являють собою багатоадресну передачу за певними адресами (224.0.0.5 та 224.0.0.6).

– OSPF реалізований як програма на мережевому рівні з використанням послуг, що надаються Інтернет-протоколом

– IP дейтаграма, яка несе повідомлення з OSPF, встановлює значення поля протоколу на 89.

– OSPF базується на алгоритмі SPF, який іноді називають алгоритмом Дейкстри.

– OSPF має дві версії – версію 1 та версію 2. В основному використовується версія 2.

Повідомлення OSPF. OSPF – дуже складний протокол. Він використовує п’ять різних типів повідомлень:

1. Повідомлення "Привіт" (тип 1) – воно використовується маршрутизаторами, щоб представити себе іншим маршрутизаторам.

2. Повідомлення з описом бази даних (тип 2) – Зазвичай воно надсилається у відповідь на повідомлення Hello.

3. Повідомлення про запит стану зв'язку (Тип 3) – воно використовується маршрутизаторами, яким потрібна інформація про конкретний пакет стану зв'язку.

4. Повідомлення про оновлення стану зв'язку (тип 4) – це основне повідомлення OSPF для побудови бази даних стану зв'язку.

5. Повідомлення про підтвердження стану зв'язку (тип 5) – воно використовується для створення надійності в протоколі OSPF.

1.8. Висновки до 1 розділу

В даному розділі проведено опис: маршрутизації маршрутизованих протоколів у комп’ютерних мережах, види маршрутизації, класи протоколів маршрутизації, класифікації алгоритмів маршрутизації, маршрутизації одноадресної передачі, особливості протоколів маршрутизації стану посилань та проведено опис відкритого протоколу маршрутизації найкоротшого шляху (OSPF).

2 АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

2.1 Інформаційний протокол маршрутизації (RIP)

Інформаційний протокол маршрутизації (RIP) – це динамічний протокол маршрутизації, який використовує кількість переходів як метрику маршрутизації для пошуку найкращого шляху між джерелом та мережею призначення. Це протокол векторної маршрутизації відстані, який має значення AD 120 і працює на прикладному рівні моделі OSI. RIP використовує номер порту 520.

Кількість переходів – це кількість маршрутизаторів, що відбуваються між джерелом та мережею призначення. Шлях з найнижчим числом стрибків вважається найкращим маршрутом для досягнення мережі і, отже, розміщується в таблиці маршрутизації. RIP запобігає циклам маршрутизації, обмежуючи кількість стрибків, дозволених на шляху від джерела та пункту призначення. Максимальна кількість стрибків, дозволена для RIP, становить 15, а кількість стрибків 16 вважається недосяжною для мережі.

Особливості RIP:

1. Періодично проводиться оновлення мережі.

2. Оновлення (інформація про маршрутизацію) завжди транслюються.

3. Повні таблиці маршрутизації надсилаються в оновленнях.

4. Маршрутизатори завжди довіряють інформації про маршрутизацію, отриманій від сусідніх маршрутизаторів.

Версії RIP: Існує три версії протоколу інформації про маршрутизацію – RIP Version1, RIP Version2 і RIPng.

RIP v1	RIP v2	RIPng
Надсилає оновлення як трансляцію	Надсилає оновлення як багатоадресне	Надсилає оновлення як багатоадресне
Трансляція за 255.255.255.255	Багатоадресна передача на 224.0.0.9	Багатоадресне передавання на FF02 :: 9 (RIPng може працювати лише в мережах IPv6)
Не підтримує автентифікацію повідомлень про оновлення	Підтримує автентифікацію повідомлень про оновлення RIPv2	-

Рисунок 2.1 – Версії протоколу RIP

RIP v1 відомий як Classful Routing Protocol, оскільки він не надсилає інформацію про маску підмережі під час оновлення маршрутизації. RIP v2 відомий як безкласовий протокол маршрутизації, оскільки надсилає інформацію про маску підмережі під час оновлення маршрутизації.

>> Use debug command to get the details :

```
# debug ip rip
```

>> Use this command to show all routes configured in router, say for rou ter R1 :

```
R1# show ip route
```

>> Use this command to show all protocols configured in router, say for router R1 :

```
R1# show ip protocols
```

Рисунок 2.2 – Приклад виконання протоколу RIP

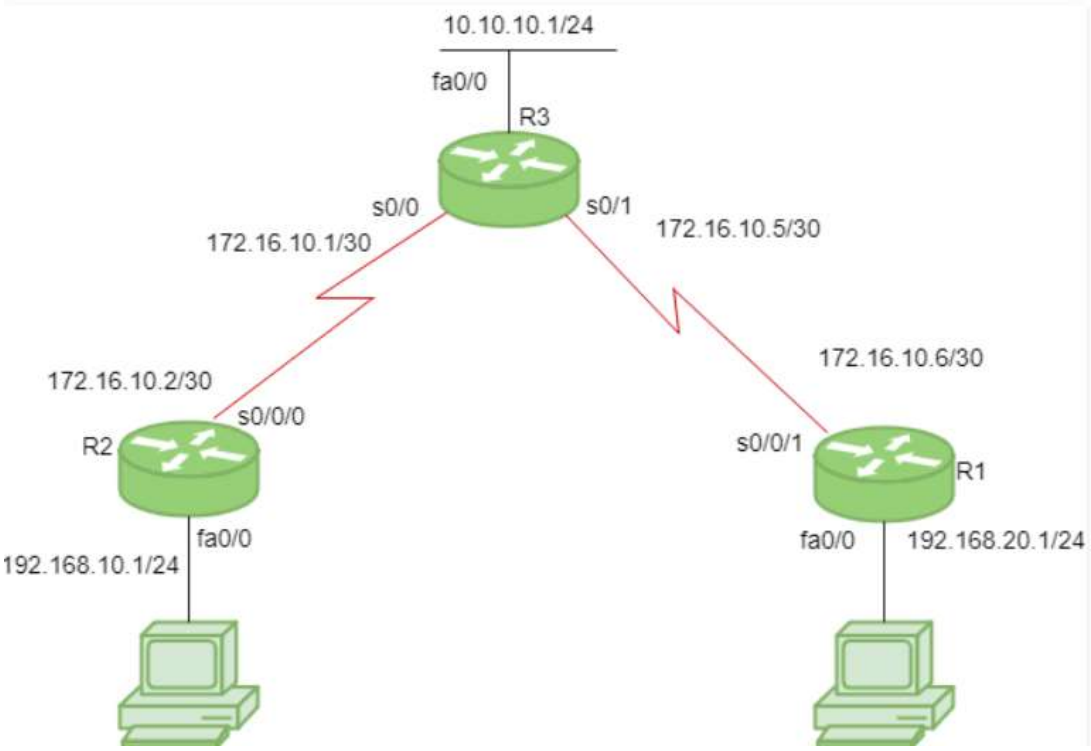

Рисунок 2.3 – Конфігурація мережі

Розглянемо наведену вище топологію, яка має 3-маршрутизатори R1, R2, R3. R1 має IP-адресу 172.16.10.6/30 на s0 / 0/1, 192.168.20.1/24 на fa0 / 0. R2 має IP-адресу 172.16.10.2/30 на s0/0/0, 192.168.10.1/24 на fa0 / 0. R3 має IP-адресу 172.16.10.5/30 на s0 / 1, 172.16.10.1/30 на s0 / 0, 10.10.10.1/24 на fa0 / 0.

Налаштування RIP для R1:

```
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

«No auto-summary» команда вимикає автоматичне підведення підсумків. Якщо ми не виберемо жодного автоматичного підведення підсумків, то маска підмережі буде розглядатися як класична у Версії 1.

Налаштування RIP для R2:

```
R2(config)# router rip
R2(config-router)# network 192.168.10.0
R2(config-router)# network 172.16.10.0
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

Подібним чином налаштовується RIP для R3:

```
R3(config)# router rip
R3(config-router)# network 10.10.10.0
R3(config-router)# network 172.16.10.4
R3(config-router)# network 172.16.10.0
R3(config-router)# version 2
R3(config-router)# no auto-summary
```

Таймери RIP:

- Таймер оновлення: Типовий час для інформації про маршрутизацію, якою обмінюються маршрутизатори, що працюють на RIP, становить 30 секунд. За допомогою таймера оновлення маршрутизатори періодично обмінюються таблицею маршрутизації.
- Недійсний таймер: якщо оновлення не надходить до 180 секунд, то маршрутизатор призначення вважає його недійсним. У цьому випадку маршрутизатор призначення позначає кількість стрибків як 16 для цього маршрутизатора.
- Утримання таймеру: це час, протягом якого маршрутизатор чекає відповіді від сусіднього маршрутизатора. Якщо маршрутизатор не може відповісти протягом певного часу, він оголошується мертвим. За замовчуванням це 180 секунд.
- Час змиву: Це час, через який введення маршруту буде змито, якщо воно не відповість протягом часу змиву. За замовчуванням це 60 секунд Цей таймер запускається після визнання маршруту недійсним і через 60 секунд, тобто час становитиме 180 + 60 = 240 секунд.

Всі ці часи можна регулювати. Використовуються команди, щоб змінити таймери:

```
R1(config-router)#  timers basic
R1(config-router)#  timers basic 20   80    80    90
```

2.2 Інформаційний протокол маршрутизації (RIP) V1 і V2

Протокол маршрутизації інформації (RIP) – це внутрішньодоменний (внутрішній) протокол маршрутизації, який базується на векторній маршрутизації відстані і використовується всередині автономної системи. Перший стовпець таблиці маршрутизації – адреса призначення. Вартість метрики в цьому протоколі – це кількість переходів, яка є кількістю мережі, яку потрібно передати для досягнення пункту призначення. Тут нескінченність визначається фіксованим числом, яке становить 16, це означає, що за допомогою RIP мережа не може мати більше 15 стрибків.

Версія RIP-1 – це протокол відкритого стандарту, що означає, що він працює на різних постачальниках маршрутизаторів. Він працює на більшості маршрутизаторів, це класний протокол маршрутизації. Оновлення транслюються. Його адміністративне значення відстані становить 120, це означає, що воно не є надійним. Чим менше адміністративне значення відстані, тим надійність набагато більше. Його показник – кількість переходів, а максимальна кількість переходів – 15. У мережі буде всього 16 маршрутизаторів. Коли до пункту призначення буде стільки ж стрибків, Rip починає виконувати балансування навантаження. Збалансування навантаження означає, що якщо є три шляхи до пункту призначення і кожен шлях має однакову кількість маршрутизаторів, тоді пакети будуть відправлятися на кожен шлях для досягнення пункту призначення. Це зменшує трафік, а також навантаження збалансовано. Він використовується в невеликих компаніях, у цьому протоколі таблиці маршрутизації оновлюються кожні 30 секунд. Щоразу,

коли посилання розривається, RIP трасу’ інший шлях до пункту призначення. Це один із найповільніших протоколів.

Переваги RIP ver1 -

1. Простий у налаштуванні, статичний маршрутизатор складний.
2. Менше накладних витрат/
3. Ніякої складності.

Недолік RIP ver1 -

1. Використання смуги пропускання дуже велике, оскільки трансляція проводиться кожні 30 секунд.
2. Він не є масштабованим, оскільки кількість переходів становить лише 15. Якщо в мережі буде потрібно більше маршрутизаторів, це буде проблемою.
3. Збіжність відбувається дуже повільно, витрачає багато часу на пошук альтернативного шляху.

Версія RIP-2:Через деякі недоліки в оригінальній специфікації RIP, версія RIP 2 була розроблена в 1993 році. Вона підтримує безкласову міждоменну маршрутизацію (CIDR) і має здатність передавати інформацію про підмережі, її метрика також становить кількість переходів, а максимальна кількість переходів 15 така ж, як RIP-версія 1. Він підтримує автентифікацію, робить підмережі та багатоадресну передачу. Автозведення можна зробити на кожному маршрутизаторі. У RIPv2 маски підмережі включені в оновлення маршрутизації. RIPv2 багатоадресно передає всю таблицю маршрутизації на всі сусідні маршрутизатори за адресою 224.0.0.9, на відміну від RIPv1, який використовує широкомовну передачу (255.255.255.255).

Переваги RIP ver2:

1. Це стандартизований протокол.
2. Він сумісний з VLSM.
3. Забезпечує швидку конвергенцію.
4. Він надсилає ініційовані оновлення при зміні мережі.

5. Працює з маршрутизацією знімків – робить її ідеальною для набірних мереж.

Недолік RIP ver2 – Є також деякі недоліки:

1. Максимальна кількість стрибків 15, через вразливість «відлік до нескінченності».

2. Жодної концепції сусідів.

3. Обмінюється цілою таблицею з усіма сусідами кожні 30 секунд (крім випадків запущеного оновлення).

RIP Ver1	RIP Ver2
RIP v1 використовує те, що називається класичною маршрутизацією	RIP v2 - це безкласовий протокол, який підтримує маскування підмережі змінної довжини (VLSM), CIDR та узагальнення маршрутів
Оновлення маршрутизації RIPv1 транслюються	Оновлення маршрутизації RIP v2 багатокастові
RIPv1 не має автентифікації	RIP v2 підтримує автентифікацію
RIP v1 не містить маску в оновленнях	RIP v2 несе маску в оновленнях, тому підтримує VLSM
RIP v1 - це застарілий, вже не використовуваний протокол маршрутизації	IP v2 може бути корисним у невеликих, плоских мережах або на межі великих мереж через простоту конфігурації та використання

Рисунок 2.4 – RIP ver1 проти RIP ver2

2.3 Протокол EIGRP

Протокол динамічної маршрутизації виконує ту саму функцію, що і протокол статичної маршрутизації. У протоколі динамічної маршрутизації, якщо адресат недоступний, тоді може бути використаний інший запис у таблиці маршрутизації до того самого пункту призначення. Одним з протоколів маршрутизації є EIGRP.

EIGRP – розширений протокол маршрутизації внутрішнього шлюзу (EIGRP) – це протокол динамічної маршрутизації, який використовується для пошуку найкращого шляху між будь-якими двома рівнями 3 пристрою для доставки пакету. EIGRP працює над протоколом мережевого рівня моделі OSI і використовує номер протоколу 88. Він використовує метрику, щоб знайти найкращий шлях між двома пристроями рівня 3 (маршрутизатором або комутатором рівня 3), що працюють з EIGRP. На рисунку 2.5 показано адміністративні відстані для EIGR.

Маршрути EIGRP	Значення AD
Зведені маршрути	5
Внутрішні маршрути	90
зовнішні маршрути	170

Рисунок 2.5 – Адміністративні відстані для EIGR

Він використовує деякі повідомлення для зв'язку з сусідніми пристроями, які експлуатують EIGRP:

1. «Привіт, повідомлення» – ці повідомлення є повідомленнями про підтримку, якими обмінюються два пристрої, що працюють за допомогою EIGRP. Ці повідомлення використовуються для виявлення/відновлення сусідів,

якщо є якийсь пристрій, що працює з EIGRP, або якщо якийсь пристрій (що працює з EIGRP) знову з'являється. Ці повідомлення використовуються для виявлення сусідів, за допомогою багатоадресного пересилання на 224.0.0.10. Він містить такі значення, як номер AS, значення k тощо. Ці повідомлення використовуються як підтвердження під час одноадресної передачі. В якості підтвердження використовується привіт без даних.

2. Оновлення NULL. Використовується для обчислення SRTT (плавний таймер зворотного переїзду) та RTO (тайм-аут повторної передачі). SRTT: пакет займає час, щоб дістатися до сусіднього маршрутизатора, і підтвердження пакету, щоб дістатися до локального маршрутизатора. RTO: якщо багатоадресна передача не вдається, тоді одноадресні передаються на цей маршрутизатор. RTO – це час, протягом якого локальний маршрутизатор чекає підтвердження пакета.

3. Повне оновлення – після обміну «привітальними» повідомленнями або після формування сусідства ці повідомлення обмінюються. Це повідомлення містить усі найкращі маршрути.

4. Часткове оновлення. Цими повідомленнями обмінюються, коли відбувається зміна топології та додаються нові посилання. Він містить лише нові маршрути, а не всі маршрути. Ці повідомлення є багатоадресними.

5. Повідомлення запиту – ці повідомлення є багатоадресними, коли пристрій оголошено мертвим, і він не має до нього маршрутів у своїй таблиці топології.

6. Відповідь – ці повідомлення є підтвердженням повідомлення про запит, надісланого ініціатору повідомлення із запитом, у якому вказано маршрут до мережі, на який відбувся запит у повідомленні про запит.

7. Повідомлення про підтвердження Використовується для підтвердження оновлення EIGRP, запитів та відповідей. Acks – це привіт-пакети, які не містять даних.

«Привіт пакети» підтвердження не вимагають. Відповіді, запити, оновлення повідомлень є надійними повідомленнями, тобто вимагає підтвердження.

Складена матриця. Розрахунок складеної метрики EIGRP може використовувати до 5 змінних, але за замовчуванням використовуються лише 2 (K1 та K3). Складеними метричними значеннями є:

1. K1 (пропускна здатність).
2. K2 (навантаження).
3. K3 (затримка).
4. K4 (надійність).
5. K5 (MTU).

Найменша пропускна здатність, навантаження, затримка, надійність, MTU на шляху між джерелом і пунктом призначення враховується у складеній матриці для розрахунку вартості.

Як правило, для розрахунку метрики за допомогою EIGRP використовуються лише значення k1 та k3. Значення складають 10100 для k1, k2, k3, k4, k5 відповідно. Для формування сусідства EIGRP ці критерії повинні бути виконані:

1. значення k повинні збігатися;
2. номер автономної системи повинен збігатися. (AS – це група мереж, що працюють під єдиним адміністративним контролем);
3. автентифікація повинна відповідати (якщо застосовується). EIGRP підтримує лише автентифікацію MD5;
4. маска підмережі повинна бути однаковою.

2.4 Особливості вдосконаленого протоколу маршрутизації внутрішніх шлюзів (EIGRP)

Розширений протокол маршрутизації внутрішніх шлюзів (EIGRP) – це запатентований Cisco протокол гібридної маршрутизації, який містить

особливості протоколів маршрутизації відстані-вектора та стану зв'язку. Це протокол мережевого рівня, який працює за протоколом номер 88.

Деякі його особливості:

1. Швидка конвергенція. EIGRP використовує алгоритм DUAL для підтримки швидкої конвергенції. Якщо маршрут до мережі йде вниз, тоді може бути використаний інший маршрут (можливий наступник). Якщо до цієї мережі в таблиці топологій також немає маршруту, тоді повідомлення із запитом здійснюється багатоадресно, щоб знайти альтернативний шлях до цієї мережі.

2. Скорочення використання смуги пропускання. EIGRP не надсилає періодичні оновлення, як це робить інший протокол векторної маршрутизації відстані. Протокол векторної маршрутизації відстані, такий як RIP, надсилає повну таблицю маршрутизації протягом певного періоду, тому витрачає доступну пропускну здатність без потреби, але EIGRP використовує часткові оновлення, якщо є якісь зміни у топології, тобто оновлення ініціюються лише у тому випадку, якщо відбувається якась подія, тому споживає пропускну здатність, коли це необхідно. Крім того, оновлення EIGRP поширюються на маршрутизаторах лише тим, хто цього потребує.

3. Підтримка всіх протоколів та топологій передачі даних LAN та WAN – EIGRP підтримує мережу з декількома доступами, як FDDI, кільце маркерів тощо, та всі топології WAN, такі як орендована лінія, посилання точка-точка. EIGRP не вимагає будь-якої додаткової конфігурації для протоколів рівня 2, таких як ретрансляція кадрів.

4. Підтримує автоматичне підведення підсумків. В EIGRP автоматичне підведення підсумків увімкнено за замовчуванням. Автоматичне підведення підсумків – це функція, яка дозволяє протоколам маршрутизації автоматично узагальнювати свої маршрути до своїх класичних мереж, тобто маршрутизатори отримуватимуть підсумовані маршрути автоматично. EIGRP: наприклад, 1.1.1.1/24 буде автоматично підведено до класичного 1.1.1.1/8

5. Підтримує нерівномірне вирівнювання витрат навантаження. В EIGRP можливе нерівномірне вирівнювання навантаження за рахунок зміни

значення дисперсії. За замовчуванням дисперсія дорівнює 1, тому підтримує рівномірне балансування витрат навантаження, але якщо ми хочемо використовувати нерівномірне балансування навантаження, тоді ми можемо змінити значення дисперсії відповідно до кількості трафіку, який ми хочемо розділити на різні шляхи. Доступна відстань множиться таким чином, що вона стає більшою, ніж величина можливої відстані наступника.

6. Зв'язок за допомогою протоколу надійної передачі (RTP). EIGRP залежить від власного протоколу RTP для управління зв'язком між мовними маршрутизаторами EIGRP. EIGRP використовує 224.0.0.10 як адресу багатоадресної розсилки. Для кожного багатоадресного повідомлення, яке він відправляє, маршрутизатор готує та підтримує список маршрутизаторів (говорячи EIGRP). Якщо підтвердження багатоадресної розсилки не отримано, то ті самі дані передаються через 16 одноадресних повідомлень. Якщо підтвердження не отримано навіть після 16 одноадресних спроб, воно оголошується померлим. Цей процес відомий як надійне багатоадресне передавання.

7. Вибір найкращого шляху за допомогою DUAL. EIGRP використовує алгоритм дифузійного оновлення (DUAL), щоб з’ясувати найкращий шлях, доступний мережі. Мовні маршрутизатори EIGRP підтримують таблицю топологій, в якій підтримуються всі маршрути до мережі. Якщо найкращий шлях (наступник) падає, тоді з таблиці топологій використовується другий найкращий шлях (можливий наступник). Якщо у таблиці топології немає доступного шляху, він надсилає повідомлення із запитом для вирішення запиту.

8. В основному він підтримує 3 різні таблиці: (a) таблиця сусідів: вона містить інформацію про маршрутизатори, з якими було сформовано сусідство Він містить SRTT, RTP. Він також містить значення кількості черг для повідомлень про привіт, які не підтверджуються. (b) Таблиця топології: містить усі маршрути, доступні мережі (як можливий наступник). (c) Таблиця маршрутизації: вона містить усі маршрути, які використовуються для

прийняття поточних рішень про маршрутизацію. Маршрути в цій таблиці розглядаються як наступні (найкращі) шляхи.

9. Контроль трафіку. Припустимо, якщо один із інтерфейсів маршрутизатора підключений до провайдера, тоді ми не хочемо, щоб цей інтерфейс був частиною процесу EIGRP. Для цього сценарію EIGRP надає функцію, за допомогою якої ми можемо позначити інтерфейс як пасивний, тобто не брати участь у процесі EIGRP.

10. Підтримка маски підмережі змінної довжини (VLSM).

11. Підтримка IPv4 та IPv6.

2.5 Висновки до 2 розділу

В даному розділі проведено огляд протоколів маршрутизації таких як: інформаційний протокол маршрутизації (RIP), інформаційний протокол маршрутизації (RIP) V1 і V2, протокол EIGRP та наведено особливості вдосконаленого протоколу маршрутизації внутрішніх шлюзів (EIGRP).

3 ДОСЛІДЖЕННЯ ДИНАМІЧНОГО ПРОТОКОЛУ OSPF

3.1 Протокол маршрутизації OSPF

(OSPF) – це протокол маршрутизації стану каналу, який використовується для пошуку найкращого шляху між джерелом та маршрутизатором призначення за допомогою власного алгоритму найкоротшого шляху (SPF). Протокол маршрутизації стану зв'язку – це протокол, який використовує концепцію ініційованих оновлень, тобто, якщо в таблиці маршрутизації спостерігається зміна, то ініціюються його оновлення, а не протокол маршрутизації з відстанню, де знаходиться таблиця маршрутизації.

OSPF розроблений Інженерною робочою групою (IETF) як один із протоколів внутрішніх шлюзів (IGP), тобто протокол, який спрямований на переміщення пакету у великій автономній системі або домені маршрутизації. Це протокол мережевого рівня, який працює над протоколом номер 89 і використовує значення AD 110. OSPF використовує багатоадресну адресу 224.0.0.5 для звичайного зв'язку та 224.0.0.6 для оновлення до призначеного маршрутизатора (DR) / резервного призначеного маршрутизатора (BDR).

Для формування сусідства в OSPF існують критерії для обох маршрутизаторів:

1. Він повинен бути присутнім в тій же області.
2. Маршрутизатор повинен бути унікальним.
3. Маска підмережі повинна бути однаковою.
4. «Hello and dead timer» повинні бути однаковими.
5. Стаб-прапор повинен збігатися.
6. Аутентифікація повинна збігатися.

OSPF підтримує NULL, звичайний текст, аутентифікацію MD5.

Обидва маршрутизатори (сусіди) повинні мати ввімкнену автентифікацію одного типу, наприклад – якщо у одного сусіда увімкнено автентифікацію MD5, тоді для іншого також повинна бути ввімкнена автентифікація MD5.

OSPF використовує певні повідомлення для зв'язку між маршрутизаторами, що працюють з OSPF.

– «Hello message» – це повідомлення для збереження життя, що використовуються для виявлення / відновлення сусідів. Вони обмінюються кожні 10 секунд. Сюди входить така інформація: маршрутизатор I, інтервал Hello / dead, область I, пріоритет маршрутизатора, IP-адреса DR та BDR, дані автентифікації.

– Опис бази даних (DBD) – це маршрути OSPF маршрутизатора. Він містить топологію AS або області (домен маршрутизації).

– Запит стану зв'язку (LSR) – коли маршрутизатор отримує DBD, він порівнює його зі своїм власним DBD. Якщо отриманий DBD має більше оновлень, ніж його власний DBD, тоді LSR надсилається своєму сусіду.

– Оновлення стану зв'язку (LSU) – коли маршрутизатор отримує LSR, він відповідає повідомленням LSU, що містить запитувані дані.

– Підтвердження стану зв'язку – це забезпечує надійність процесу обміну станом зв'язку. Він надсилається як підтвердження LSU.

– (LSA) – це пакет даних OSPF, який містить інформацію про маршрутизацію стану каналу, що передається лише маршрутизаторам, до яких сформовано суміжність.

Таймери

– «Hello timer» – Інтервал, протягом якого маршрутизатор OSPF надсилає привітне повідомлення на інтерфейс. За замовчуванням це 10 секунд.

– «Dead timer» – Інтервал, через який сусід буде оголошено померлим, якщо він не зможе надіслати «Hello timer». За замовчуванням воно становить 40 секунд. Зазвичай це в 4 рази більше інтервалу привітання, але його можна налаштувати вручну відповідно до потреб.

OSPF має такі переваги:

– Використовується для протоколу IPv4, так і IPv6.

– Балансування навантаження з однаковою важливістю маршрутів для одного пункту призначення.

– VLSM та підведення підсумків маршрутів.

– Необмежена кількість стрибків.

– Тригерні оновлення для швидкої конвергенції.

– Безциклова топологія з використанням алгоритму SPF.

– Запускається на більшості маршрутизаторів.

– Безкласовий протокол.

Є деякі недоліки OSPF, наприклад, він вимагає додаткового процесу процесора для запуску алгоритму SPF, вимагає більше оперативної пам'яті для зберігання топології суміжності та більш складний в налаштуванні та важкий для усунення несправностей.

3.2 Ролі маршрутизатора та найкоротший шлях (OSPF) і його налаштування

(OSPF) – це протокол маршрутизації стану каналу, який використовується для пошуку найкращого шляху між джерелом та маршрутизатором призначення за допомогою власного алгоритму SPF.

Відкритя ролі маршрутизатора з найкоротшим шляхом (OSPF) – це група суміжних мереж і маршрутизаторів. Маршрутизатори, що належать до однієї області, мають спільну таблицю топології та область. Область, яку пов’язується з інтерфейсом маршрутизатора, оскільки маршрутизатор може належати більше ніж до однієї області.

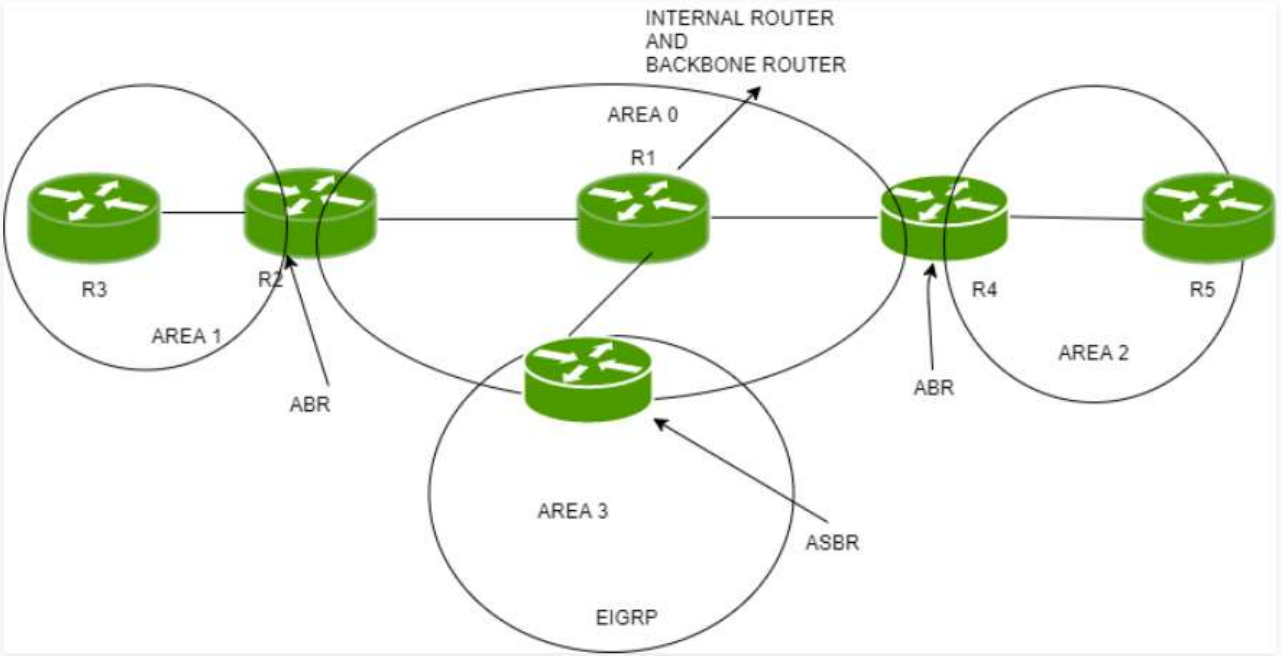

Рисунок 3.1 – Ролі маршрутизатора в OSPF

Є кілька ролей маршрутизатора в OSPF:

1. Магістральний маршрутизатор – область 0 відома як магістральна область, а маршрутизатори в області 0 відомі як магістральні маршрутизатори. Якщо маршрутизатори частково існують у зоні 0, то це також магістральний маршрутизатор.

2. Внутрішній маршрутизатор – це маршрутизатор, який має всі свої інтерфейси в одній області.

3. Маршрутизатор граничних площ (ABR) – маршрутизатор, який з'єднує магістральну область з іншою областю, називається маршрутизатором граничних площ. Він належить не одній області. Отже, ABR підтримують безліч баз даних про стан зв'язку, що описують як основну топологію, так і топологію інших областей.

4. Підсумковий прикордонний маршрутизатор (ASBR) – коли маршрутизатор OSPF підключений до іншого протоколу, такого як EIGRP, або Border Gateway Protocol, або будь-якого іншого протоколу маршрутизації, тоді він відомий як AS. Маршрутизатор, який має дві різні AS (в одному з інтерфейсів працює OSPF), відомий як Router Summary Border Router. Ці маршрутизатори

виконують перерозподіл. ASBR запускають як OSPF, так і інший протокол маршрутизації, такий як RIP або BGP, ASBR проводить обмін зовнішньою інформацією про маршрутизацію по всій їх AS.

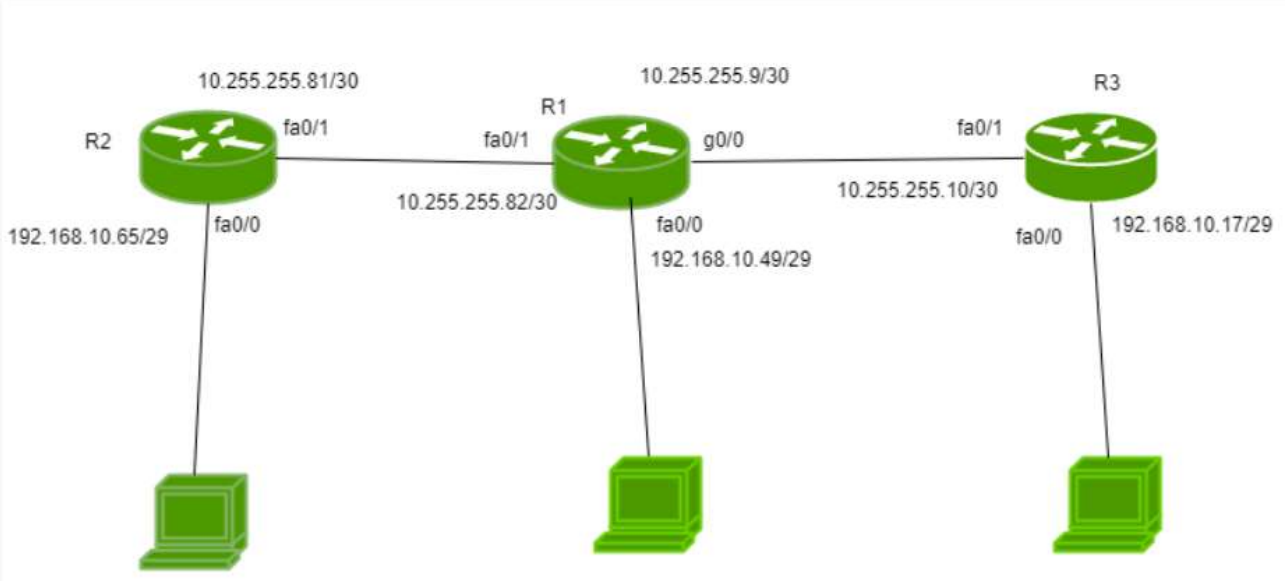

Рисунок 3.2 – Конфігурація мережі за допомогою трьох маршрутизаторів

Наведемо невелику топологію, в якій є 3 маршрутизатори, а саме R1, R2, R3, підключені між собою. R1 підключений до мереж 10.255.255.80/30 (інтерфейс fa0/1), 192.168.10.48/29 (інтерфейс fa0/0) та 10.255.255.8/30 (інтерфейс gi0/0) На рисунку 3.2 наведені IP-адреси з їх інтерфейсами, для того, щоб провести рекламування мережі потрібно написати мережу «I'd». R2 підключений до мереж 192.168.10.64/29 (інтерфейс fa0/0), 10.255.255.80/30 (інтерфейс fa0/1). R3 підключений до мереж 10.255.255.8/30 (int fa0/1), 192.168.10.16/29 (int fa0/0).

Тепер налаштовуємо OSPF для R1:

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.48 0.0.0.7 area 1
R1(config-router)#network 10.255.255.80 0.0.0.3 area 1
R1(config-router)#network 10.255.255.8 0.0.0.3 area 1
```

1 – це екземпляр OSPF або процес. Він може бути однаковим або різним (не має значення). Тут використовується підстановочна маска, а використана область дорівнює 1. Тепер, налаштовуюєм R2:

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.10.64 0.0.0.7 area 1
R2(config-router)#network 10.255.255.80 0.0.0.3 area 1
```

Налаштовуємо R3 аналогічно:

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.10.16 0.0.0.7 area 1
R3(config-router)#network 10.255.255.8 0.0.0.3 area 1
```

Щоб перевірити конфігурацію потрібно набрати команду:

```
R3#show ip protocols
```

3.3 Стани протоколу (OSPF)

(OSPF) – це протокол маршрутизації стану каналу, який використовується для пошуку найкращого шляху між вихідним та цільовим маршрутизатором за допомогою власного «Найкоротшого шляху спочатку». OSPF розроблений Інженерною робочою групою (IETF) як один із протоколів внутрішніх шлюзів (IGP), тобто протокол, який спрямований на переміщення пакету у великій автономній системі або домені маршрутизації. Це протокол мережевого рівня, який працює з протоколом номер 89 і використовує значення AD 110. OSPF використовує багатоадресну адресу 224.0.0.5 для нормального зв'язку та 224.0.0.6 для оновлення до призначеного маршрутизатора (DR) / резервного призначеного маршрутизатора (BDR).

Умови OSPF:

1. «Router I'm» – Це найвища активна IP-адреса, присутня на маршрутизаторі. Спочатку враховується найвища адреса зворотного зв'язку. Якщо жодна петля не налаштована, то враховується найвища активна IP-адреса на інтерфейсі маршрутизатора.

2. Пріоритет маршрутизатора – це 8-бітове значення, присвоєне маршрутизатору, що працює OSPF, і використовується для вибору DR та BDR в широкомовній мережі.

3. Призначений маршрутизатор (DR). Він обраний, щоб мінімізувати кількість утворених збіжностей. DR розподіляє LSA на всіх інших маршрутизаторах. DBD обирається в широкомовній мережі, до якої всі інші маршрутизатори діляться своїми DBD. У широкомовній мережі запити маршрутизатора на оновлення DR відповідають на цей запит оновленням.

4. Маршрутизатор, призначений для резервного копіювання (BDR). BDR робить резервну копію для DR у широкомовній мережі. Коли DR падає, BDR стає DR і виконує свої функції.

Вибори DR та DBD відбуваються в мережі мовлення або мережі з багатьма доступами. Ось критерії виборів:

1. Маршрутизатор, що має найвищий пріоритет маршрутизатора, буде оголошений як DR.

2. Якщо є рівність у пріоритеті маршрутизатора, тоді буде враховано найвищий маршрутизатор. По-перше, розглядається найвища адреса зворотного зв'язку. Якщо жодна петля не налаштована, то враховується найвища активна IP-адреса на інтерфейсі маршрутизатора.

Стани OSPF. Пристрій, що працює з OSPF, проходить певні стани. Це такі стани:

1. Down – у цьому стані на інтерфейс не надійшов жоден «привіт-пакет». Стан Down не означає, що інтерфейс фізично не працює. Тут це означає, що процес примикання OSPF ще не розпочався.

2. INIT. У такому стані «привіт пакет» отримано від іншого маршрутизатора.

3. 2WAY. У стані 2WAY обидва маршрутизатори отримали пакети привіт від інших маршрутизаторів. Встановлено двонаправлений зв’язок.

4. Exstart. У цьому стані обмінюються NULL DBD. Маршрутизатор, що має вищий маршрутизатор, стає головним, а інший стає дочірним. Ці вибори вирішують, який маршрутизатор першим надішле свій DBD.

5. Обмін. У цьому стані обмінюються фактичні DBD.

6. Завантаження. У цій стані обмінюються LSR, LSU та LSA (підтвердження стану посилання). Коли маршрутизатор отримує DBD від іншого маршрутизатора, він порівнює власний DBD з іншим DBD маршрутизатора. Якщо отриманий DBD є більш оновленим, ніж його власний DBD, маршрутизатор надішле LSR іншому маршрутизатору із зазначенням необхідних посилань. Інший маршрутизатор відповідає LSU, що містить необхідні оновлення. Натомість маршрутизатор відповідає повідомленням про стан зв'язку.

7. Повний. У цьому стані відбувається синхронізація всієї інформації. Маршрутизація OSPF може розпочатися лише після повного стану.

3.4 Відкриття найкоротшого шляху в OSPF

OSPF скорочено називається Open Shortest Path First. OSPF – це внутрішньодоменний протокол маршрутизації, який є реалізацією протоколу маршрутизації стану зв'язку, і він потрапляє в групу внутрішніх протоколів шлюзу (IGP), що працюють в рамках однієї автономної системи (AS). OSPF був розроблений як протокол внутрішнього шлюзу. Він використовується в автономній системі, такі як локальна мережа (LAN).

Щоб ефективно та вчасно обробляти маршрутизацію, цей протокол розділяє автономну систему на області. Область – це колекція маршрутизаторів, хостів, мереж, що містяться в автономній системі. Автономну систему можна розділити на багато різних областей, але в той же час всі мережі всередині певної області повинні бути з'єднані.

Протокол OSPF підтримує автентифікацію, а його оновлення надсилаються за адресою багатоадресної розсилки 224.0.0.5/6. Якщо одне з

посилань не опитуєтьсяя, протокол знаходить інший найкоротший шлях до пункту призначення, отже він має більш швидку конвергенцію. У той час як пакети hello зв'язку надсилаються кожні 10 секунд, і коли відповідь не отримана протягом 40 секунд, це вважається тайм-аутом. Також при незначних змінах у конфігурації маршрутизатора (додані/видалені маршрутизатори) таблиця маршрутизації оновлюється дуже швидко. Він базується на протоколі маршрутизації стану зв'язку.

Як випливає з назви, «спочатку найкоротший шлях», OSPF обчислює найкоротший шлях до пункту призначення через мережу на основі алгоритму. Він використовує алгоритм DISJKTRA для обчислення найкоротшого шляху.

Зв'язок також відомий як посилання, також може бути з'єднанням між двома маршрутизаторами/мережами. У OSPF визначено чотири різні типи посилань:

Точка до точки: Ці типи посилань присутні між двома маршрутизаторами, і, оскільки це точка-точка, між двома підключеними маршрутизаторами немає хостів, маршрутизаторів.

Перехідне посилання. Якщо існує велика кількість маршрутизаторів, підключених до мережі. Це може бути LAN, WI-FI, кілька різних маршрутизаторів, тоді ця конфігурація називається перехідною ланкою. Вона може бути представлена двома топологіями: реалістичною та нереалістичною.

1. Заглушка. Це мережа, яка пов’язана з єдиною мережею. Пакети даних надсилаються та отримуються через один і той же маршрутизатор.
2. Віртуальне посилання. Може статися якась ситуація, коли посилання порушено з якоїсь причини. На той час адміністратор мережі створює віртуальний зв’язок між двома зв’язаними маршрутизаторами. Такі типи посилань називаються віртуальними.

У протоколі OSPF існує п’ять різних типів пакетів, і це:

1. Пакет привіт.
2. Опис бази даних.
3. Запит стану посилання.

4. Оновлення стану посилання.
5. Підтвердження стану посилання.

Коли виникає ситуація передачі пакета, питання полягає в тому, до якої мережі він повинен передаватися і чому? Рішення базується на оптимізації. Один із способів – призначити вартість проходження через мережу, і ця вартість називається метричною. Однак показник, призначений кожній мережі, залежить від типу протоколу. Такий протокол, як OSPF, дозволяє адміністратору призначати вартість проходження через мережу на основі типу послуги. Він може базуватися на максимальних затримках, максимальній пропускній здатності, швидкості та помилках тощо. Може бути кілька таблиць маршрутизації на основі різних типів послуг.

OSPF використовує еталонну пропускну здатність 100 Мбіт/с для розрахунку вартості. Формулою для розрахунку вартості є еталонна пропускна здатність, поділена на пропускну здатність інтерфейсу. Наприклад, у випадку Ethernet, це 10 Мбіт/с / 10 Мбіт/с = 1.

3.5 Висновки до розділу 3

В даному розділі проведено опис протоколу маршрутизації OSPF, наведено ролі маршрутизатора та найкоротший шлях (OSPF) і його налаштування, описано стани протоколу (OSPF) та наведено відкриття найкоротшого шляху в OSPF.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ НАУКОВИХ ДОСЛІДЖЕНЬ

В даному розділі наведемо параметри мережі, які мають протоколи OSPF та EIGRP. Це дає змогу на практиці описати використання маршрутизаторів Cisco, що в свою чергу дає можливість врахувати те, що ці протоколи в основному використовуються цією компанією.

4.1 Маршрутизатори Cisco Systems та її особливості

Наведемо основні компоненти маршрутизаторів Cisco Systems:

1. Оперативна пам'ять. Дає можливість зберігати таблиці маршрутизації в кеш протоколу ARP, що в свою чергу забезпечує зберігання пакетів в інтерфейсах ще до обробки центральним процесором. Дає можливість забезпечувати тимчасову пам’ять для конфігурування файлів маршрутизатора коли він включений. Після того коли маршрутизатор виключити, пам’ять очищується.

2. NVRAM – це енергонезалежна пам’ять, що містить стару або резервну копію файлу конфігурування. Після того як виключити маршрутизатор пам’ять не очущується.

3. Flash – пам'ять. Пам’ять яка має можливість перепрограмовуватись і стиратись. В ній розміщується образ операційної системи. Дає можливість проводити оновлення програмного забезпечення.

4. ПЗП та RAM. Розміщується мікрокод для того щоб мати можливість проводити початкове завантаження і проводити обслуговування маршрутизатора. Робить перевірку цілісності маршрутизатора, а зокрема процесора, пам’яті і т.д. В ПЗП зберігаються ОС Cisco, для відновлення опереційної системи. Після того як виключити маршрутизатор пам’ять не очущується.

5. Інтерфейс це мережеве з'єднання, за допомогою якого дані передаються на пристрій.

6. Центральний процесор забезпечує обробку даних та запитів до застосувань і служб безпеки.

Коли виключити живлення маршрутизатора Cisco будуть виконуватись наступні умови:

1. Перевірка працездатності компонентів маршрутизатора.
2. Проводиться виконання коду завантаження, що в свою чергу є мікрокомандою ПЗП.
3. За допомогою коду завантаження можна визначити місцезнаходження програмного забезпечення ОС, що запускається. В основному образ програмного забезпечення зберігається у flash-пам’яті.
4. Наступний крок це коли код завантажувальника проводить розпаковку програмного забезпечення в ОЗП і в подальшому запускає його.
5. Знаходження конфігурації. За замовчуванням «strtup-config» розміщується в енергонезалежній пам’яті.
6. Завантаження конфігурації.
7. Проводиться запуск відлагодженого програмного забезпечення ОС.

Наведемо основні функції маршрутизаторів:

1. Це процес читання заголовку пакетів мережевих протоколів, що завантажуються в буфер обміну у кожен порт маршрутизатора.
2. Приймає рішення про наступний маршрут спрямування.
3. Підключає локальні мережі до глобальної мережі.

4.2 Проведення налаштування маршрутизатора Cisco

Налаштування маршрутизаторів Cisco можна проводити через інтерфейс командного рядка, за допомогою консолі або за допомогою терміналу. ПЗ Cisco ОС використовує інтерпретатор «EXEC».

Маршрутизатор дає можливість працювати в декількох режимах.

Розглянемо користувацький режим. За допомогою цього режиму проводиться перевірка стану маршрутизатора. Щоб вийти з маршрутизатора потрібно використати команду exit.

Розглянемо привілейований режим. За допомогою цього режиму можна провести налаштування маршрутизатора. Щоб увійти протрібно набрати команду enable, після цього вводимо пароль (при наявності).

```
RouterX>
RouterX>password
RouterX>enable
RouterX#
RouterX#disable
RouterX>
```

Щоб переглянути список команд в будь-якому режимі потрібно ввести знак ?. Cisco ОС дає можливість скорочувати команди, для прикладу можна написати enab, а не enable. Коли на маршрутизаторі відсутня подібна команда, маршрутизатор зрозуміє цю команду.

В режимі глобальної конфігурації можна получити доступ до спеціального режиму конфігурування маршрутизатора, для прикладу можна привести, як конфігурування інтерфейсу, лінії та протоколу.

```
RouterX>
RouterX>enable
RouterX#configure terminal
RouterX(config)#
```

Для прикладу можна навести налаштування маршрутизатора:

```
RouterX>
RouterX>enable
RouterX#configure terminal
RouterX(config)#interface fa 0/0 - налаштування певного інтерфейсу
RouterX(config - if)#ip address  - привласнення IP-адреси і маски
192.168.1.1 255.255.255.0
RouterX(config - if)#no shutdown - включення інтерфейсу
```

Щоб переглянути налаштування маршрутизатора потрібно набрати команду show interface.

Щоб налаштувати локальну мережу потрібно присвоїти кожному комп'ютерну цієї мережі IP-адресу. Налаштування відбувається або вручну, або за допомогою протоколу DHCP. Відповідно цей протокол працюза по принципу клієнт-сервер. Сервер DHCP дає змогу виділяти IP-адреси хостам автоматично, тобто або присвоєння адреси відбувається на постійній основі, або динамічно на певний проміжок часу.

```
RouterX(config)# service dhcp – включення dhcp-сервера
RouterX(config)# ip dhcp pool LAN – оголошуємо пул
RouterX(config – pool)# network 192.168.20.0 255.255.255.0
RouterX(config – pool)# default – router – вказування шлюзу по
замовчуванню 192.168.20.1
```

Для того, щоб провести виключення IP-адрес з наданого пулу, потрібно:

```
RouterX(config – pool)# ip dhcp – виключення однієї адреси
excluded – addresses 192.168.0.2
RouterX(config – pool)# ip dhcp – виключення діапазону адрес
excluded – addresses 192.168.0.128 192.168.0.255
```

Підсумовуючи, що краща збіжність відповідає таким протоколам, як EIGRP, OSPF, наведемо налаштування наших маршрутизаторів за допомогою цих протоколів.

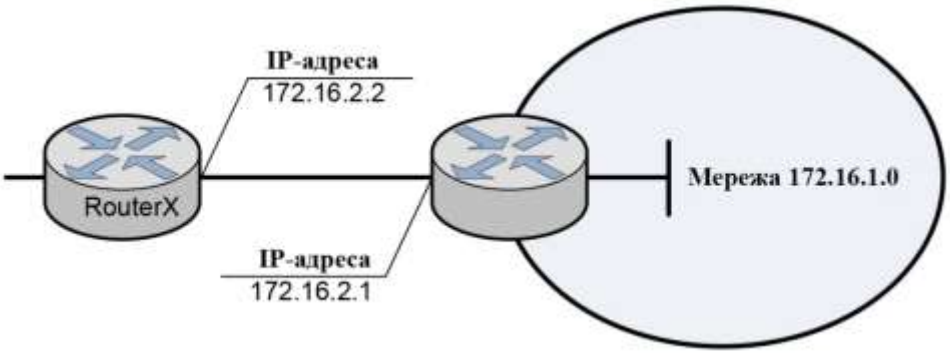

Рисунок 4.1 – «Налаштування статичної маршрутизації»

`RouterX(config)#ip route`	– статичний маршрут
`172.16.1.0`	– адреса статичного маршруту до мережі призначення
`255.255.255.0`	– маска підмережі
`172.16.2.1`	– адреса наступного переходу

На рисунку 4.2 наведено налаштування протоколу OSPF.

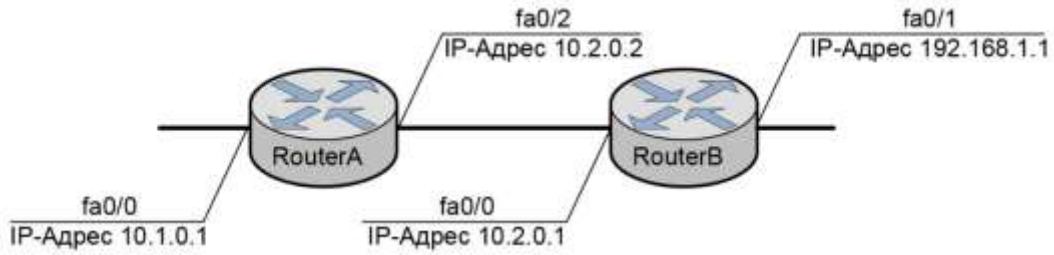

Рисунок 4.2 – Протоколу OSPF та його налаштування

101 – ідентифікатор процесу маршрутизації, випадковий номер;

10.2.0.1 – адреса інтерфейсу (так само може бути записана адреса мережі або підмережі);

0.0.0.0 – wildcard mask, зворотна маска, яка показує, яка частина (скільки біт) IP -адреса можуть мінятися. 0.0.0.0 – всі біти фіксовані;

Area 0 - ідентифікатор області.

За допомогою команди «show ip route» проводиться виведення таблиці маршрутизації. На початку відображаються коди, які вказують на то яким способом отримана інформація.

Коди: C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external (зовнішній), O - OSPF, IA - OSPF inter area (міжобласний), N1 - OSPF NSSA external type 1 (зовнішній маршрут NSSA першого типу), N2 - OSPF NSSA external type 2 (зовнішній маршрут NSSA другого типу), E1 - OSPF external type 1, E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary, L1 - IS-IS level - 1, L2 - IS-IS level - 2, ia - IS-IS inter area, * – candidate default (вказує останній, використаний шляха для пересилки маршрутів), U – per-user static

route (користувацький статичний маршрут), o – ODR (маршрут на вимогу), P – periodic downloaded static route (періодично завантажуваний статичний маршрут).

Далі відображається сама таблиця маршрутизації. В ній вказуються усі записи про всі відомі мережі, які так само позначаються буквою коду. У записах з віддаленою мережею, так само є поля з вказуванням адміністративної відстані джерела даних, метрики маршруту, адреси наступного переходу, часу, що пройшов з моменту останнього оновлення, а так само інтерфейсу, через який можна отримати доступ до віддаленої мережі.

Рисунок 4.3 – Процес виведення таблиці маршрутизації

На рисунку 4.3 наведено налаштування протоколу EIGRP.

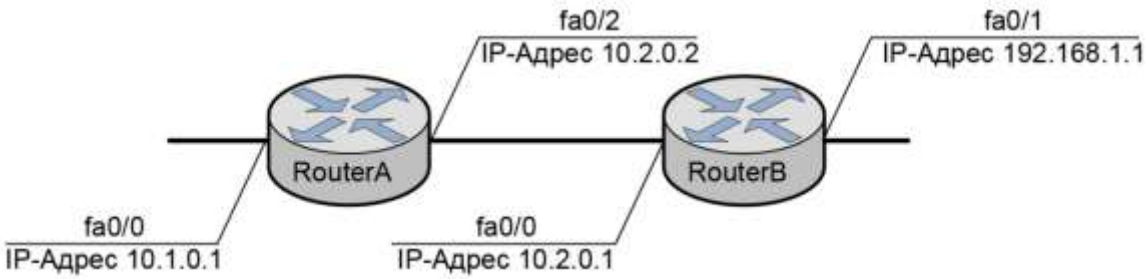

Рисунок 4.4 – Протокол EIGRP та його налаштування

```
RouterB(config)#router eigrp 100
RouterB(config - router)#network 10.2.0.0
RouterB(config - router)#network 192.168.1.0
```

100 – це номер системи в автономному режимі. Цей номер можу бути зареєстрованим або приватним. При цьому маршрутизатори, які працюють в одній автономній системи, використовують один номер цієї системи щоб обмінюватись інформацією.

За замовчуванням протокол EIGRP проводить балансування навантаження, зокрема з 4 маршрутами в яких використовується однинакова метрика. Для відключення балансування навантаження, встановлюємо кількість маршрутів, який рівний 1. Щоб провести зміну кількості маршрутів, потрібно:

```
RouterX(config – router)# maximum – paths 6
```

В залежності від того, як буде проходити обробка пакету на маршрутизаторі пакетів балансування навантаження, потрібно виконати таку коменду, як «per-packet» це застосовується для кожного пакету, або «perdestination», застосовується до кожного адресата.

Балансування навантаження по адресатові призначення означає, що маршрутизатор розподіляє пакети на основі адреси призначення. За наявності двох шляхів доступу до однієї мережі, всі пакети для призначення 1 в цій мережі пересилаються по першому шляху, а усі пакети для призначення 2 в цій мережі пересилаються по другому шляху і так далі. При цьому зберігається порядок пакетів з потенційно нерівномірним використанням каналів.

Балансування навантаження по пакетах означає, що маршрутизатор відправляє один пакет для призначення 1 по першому шляху, а другий пакет для цього ж призначення 1 по другому шляху і так далі. Балансування навантаження по пакетах гарантує рівномірний розподіл навантаження між усіма каналами. Проте існує ймовірність порушення порядку дотримання пакетів, коли вони досягають адресата призначення, через можливе існування диференціальної затримки в мережі.

EIGRP може розподіляти трафік між декількома маршрутами з різною метрикою. Це регулюється завданням variance:

```
RouterX(config - router)# variance 2
```

Зокрема саме значення «variance» може знаходитись в межах від 1 і до 128. Це зокрема множник на який буде проводитись множення «FD», тобто поточного маршруту щоб провести визначення «feasible «маршрутів.

Зокрема саме балансування навантаження буде виконуватись тільки між «feasible routes», при потраплянні в таблицю маршрутизації.

В свою чергу маршрут можна вважати «feasible» коли будуть виконані дві умови:

– FD при кращому маршруті буде більший ніж AD, що в свою чергу проводить анонсування сусіднього маршрутизатора. Можна сказати так, що слідуючий маршрутизатор на шляху має знаходитись ближче до «destination», ніж сам локальний маршрутизатор, щоб запобігти петлі маршрутизації;

– FD при кращому маршруті буде помножене на «variance», яке в свою чергу має бути більше, ніж FD для альтернативного маршруту.

4.3 Висновки до 4 розділу

В даному розділі проведено розробку початкових налаштувань маршрутизації протоколів «OSPF та EIGRP» для обладнання компанії Cisco.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Охорона праці

Тема дипломної роботи присвячена аналізу протоколів маршрутизації у сучасних комп'ютерних мережах. Оскільки, проведення робіт з аналізу протоколів маршрутизації у сучасних комп'ютерних мережах передбачає використання електронно-обчислювальної (комп'ютерної) техніки, то важливим є дотримання норм організації робочого місця, забезпечення комфортних та зручних умов праці осіб, які беруть участь у процесі, а це вимагає дослідження та дотримання вимог з охорони праці і техніки безпеки.

5.1.1 Вимоги охорони праці при виконанні робіт на персональному комп'ютері

Робочі місця офісних працівників, обладнані персональними комп'ютерами, повинні відповідати вимогам «Правил охорони праці під час експлуатації електронно – обчислювальних машин», затверджених Наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від 26.03.2010 року №65 та «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно – обчислювальних машин», затверджених постановою Головного державного санітарного лікаря України від 10.12.1998 року №7 (ДСанПіН 3.3.2-007-98). Правила поширюються на всіх суб'єктів господарювання незалежно від форм власності, які у своїй діяльності здійснюють роботу, пов'язану з персональними комп'ютерами, у тому числі на тих, які мають робочі місця, обладнані персональними комп'ютерами і периферійними пристроями [42].

Вимоги щодо розміщення і планування приміщень для роботи з комп'ютером:

Робочі місця, обладнані персональними комп'ютерами, заборонено облаштовувати у підвальних або цокольних приміщеннях будівель. При

обладнанні приміщень забороняється використання полімерних матеріалів, що виділяють шкідливі хімічні речовини. Також слід приділити увагу забезпеченню достатнім для здійснення роботи рівнем освітлення (природного та штучного – у темну пору доби) та звукоізоляції. Для регуляції рівня освітлення природним світлом бажано застосовувати жалюзі. Окрім того, у приміщеннях, де здійснюється робота з комп'ютерами, щодня має здійснюватися вологе прибирання з метою недопущення запиленості підлоги та меблів.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), мають бути надійно захищені діелектричними щиткам або сітками з метою недопущення потрапляння людини під напругу [42].

Особливої уваги заслуговують заходи дотримання протипожежної безпеки. Так, у всьому офісі лінії електромережі мають бути захищені від виникнення короткого замикання, а також від перепадів мережевої напруги, що може спричинити збої в роботі електронно–обчислювальної техніки. Приміщення (окрім тих, де розташовуються сервери) мають бути оснащені системою автоматичної пожежної сигналізації та вогнегасниками. Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, застосовувати негорючу ізоляцію. У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

5.1.2 Вимоги щодо організації та обладнання робочих місць

Площа, відведена на одне робоче місце має становити не менше 6 кв.м., а об'єм – не менше 20 куб.м. Конструкція робочого місця повинна забезпечувати підтримання оптимальної робочої пози, тобто такої, яка дозволяє працівникові виконувати роботу з мінімальним напруженням тіла, і яка дозволяє уникнути

перевтоми в ході і після закінчення робочого процесу. Раціональна робоча поза має важливе значення для збереження здоров'я працівника, оскільки тривале перебування його в незручній і напруженій позі може призвести до таких захворювань, як сколіоз (викривлення хребта), варикозне розширення вен, плоскостопість тощо. Установлено, що робота в зігнутому положенні збільшує затрати енергії на 20%, а при значному нахиленні – на 45% порівняно з прямим положенням корпуса [43].

За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 – 2 м.

Робочі місця слід розташовувати відносно джерела природного світла (вікон) таким чином, щоб світло падало збоку, переважно зліва. Також робоче місце має відповідати сучасним вимогам ергономіки [43]:

– стіл повинен мати висоту поверхні 680 – 800 мм, ширину 600 – 1400 мм і глибину 800 – 1000 мм. Такі параметри забезпечують можливість виконання операцій в зоні досяжності працівника;

– робочий стілець має бути підйомно – поворотним, з можливістю регулювання висоти, бажано зі стаціонарними або змінними підлікотниками і напівм'якою нековзкою поверхнею сидіння, що легко чиститься і не електризується;

– екран комп'ютера має розташовуватися на оптимальній відстані від користувача, що становить 600 – 700 мм, але не менше 600 мм з урахуванням літерно – цифрових знаків і символів;

– відстань між бічними поверхнями персональних комп'ютерів повинна бути не менше 1,2 метри;

– відстань від тильної поверхні одного персонального комп'ютера до екрана іншого – 2,5 метри.

– персональний комп'ютер та його комплектуючи (монітор та інші периферійні пристрої) не повинні потрапляти під прямі промені сонячного світла

та під дію інших джерел тепла (батареї опалення та інші прилади для обігріву приміщень).

5.1.3 Вимоги безпеки під час роботи з комп'ютером

Щодня перед початком роботи оператор повинен [44]:

– оглянути своє робоче місце: про виявлення ознак пошкодження обладнання інформувати свого безпосереднього керівника;

– відрегулювати освітленість на робочому місці, переконатися в відсутності відблисків на екрані комп'ютера, відсутності зустрічного світла;

– перевірити правильність підключення обладнання ЕОМ до електромережі;

– очистити екран комп'ютера від пилу та інших забруднень;

– перевірити правильність організації робочого місця й за необхідності провести відповідні коригування.

Оператор під час роботи зобов'язаний:

– виконувати тільки ту роботу, яку йому було доручено;

– підтримувати порядок і чистоту на робочому місці;

– тримати відкритими всі вентиляційні отвори обладнання;

– коректно закрити всі активні завдання у разі припинення роботи з комп'ютером;

– негайно відключити комп'ютером від електричної мережі у разі виникнення аварійної ситуації.

5.2 Безпека в надзвичайних ситуаціях

5.2.1 Міжнародний тероризм

Терор (лат. terror – страх, жах) – має ознаку «усувати», «закривати». Ця обставина і визначає терор як особливу форму політичного насильства, що характеризується жорстокістю, цілеспрямованістю й уявленою ефективністю. Ці особливості визначили широке використання терору упродовж людської історії

як засобу політичної боротьби в інтересах держави, організацій чи окремих угруповань. Безпосередньо сам факт привселюдної страти кримінальних чи політичних злодіїв, чи процес «аутодафе» в період середньовікової інквізиції, є класичною формою терору в інтересах держави чи католицької церкви.

Правовою основою боротьби з міжнародним тероризмом є «Декларація про заходи для ліквідації міжнародного тероризму», що затверджена на 49-й сесії Генеральної асамблеї ООН (резолюція 49/60 від 9 грудня 1994 р.)

Цей документ встановлює принципи відносин світової спільноти і програму заходів з метою ліквідації такого огидного суспільного явища, як міжнародний тероризм, а також встановлює подальше співробітництво між державами для невідкла-деної ліквідації будь-яких форм і проявів терористичної діяльності. Характерним для розвитку світової спільноти є те, що наявність лідера (провідної країни чи провідної сили) народжує відповідну реакцію – формування нижчого за рангом (рівнем) іншого лідера (іншої країни чи іншої провідної сили). Має місце формування біполярності, виникають реалії антагонізму на різних рівнях світового суспільства, в т.ч. суперечності на рівні «держава»↔«держава», «держава»↔«внутрішня організація» (організація зовнішня), «держава»↔«партія» та ін. Крім того, у світовій практиці мають місце комбіновані види із вищезгаданих «пар», з яких формуються інші групи (сили), в т.ч. політичні, злочинні та ін. відповідні сили чи угруповання. На другому етапі формування ці сили (групи) шукають собі відповідні «ніші» існування; економічну, політичну, наукову та інші види підтримок; формують свої озброєні сили, відповідні професійні кадри, джерела озброєння, територію знаходження тощо. При цьому використовуються всі «блага» цивілізації особистого розвитку і поширення впливу на світову спільноту.

Міжнародний тероризм, створюючи свій плацдарм, може викликати кризи (системні) в світовій, моральній, політичній, економічній системі відносин і зруйнувати та усунути всі передумови розвитку світової спільноти.

В Україні, за даними служби безпеки, за останні два роки скоєно понад 560 злочинів терористичного характеру, внаслідок цього 90 осіб (із них 15

представників владних структур) загинуло. В Україні зростає активність міжнародних терористичних організацій, насамперед із країн Ближнього Сходу («Хезболах», «Абу Ніджаль», «Хамас», «Брати мусульмани»), які прагнуть використати територію України для транзиту своїх бойовиків до країн західної Європи, підготовки терористичних акцій.

Головними принципами попередження та боротьби з міжнародним тероризмом має стати постійне удосконалення відповідної законодавчої бази, співробітництво з правоохоронними організаціями, консолідація з іншими країнами й організація напрямів запобігань поширенню будь-яких терористичних організацій і угруповань.

Терористичний акт не має безпосередніх можливостей досягнення оголошеної кінцевої мети і звичайно складається з таких елементів: насильницька дія у різноманітних її формах, політичний мотив в основі здійснення самого терористичного акту; сам акт спрямовано проти осіб, організацій, націй, національностей і меншин, державних інститутів чи їх представників з метою їх залякування чи виконання окремих вимог. Терор щодо націй, етнічної, расової чи релігійної групи, що здійснюється для її повного чи часткового усунення, розглядається світовою спільнотою вже як акт геноциду.

Варіанти комбінацій за спрямованістю суб'єкт—об'єкт здійснення терористичного акту багатоспрямовані, тому важко дати універсальне визначення «терору». Проте деякі критерії певної класифікації можна встановити:

– індивідуальний, організований терор і терор як політика держави;

– терор як метод внутрішньополітичної боротьби і терористичні акти міжнародного характеру.

5.2.2 Структура системи БЖД

Поняття «життєдіяльність» стосується тільки людини. Людина живе і працює в безпосередньому зв’язку з навколишнім середовищем.

Життєдіяльність (ЖД) – це складна фізіологічна система, яка має назву «система ЖД».

Системою називають сукупність взаємозв'язаних елементів, функціонування яких спрямоване на досягнення певної загальної мети.

Система ЖД складається із взаємопов'язаних елементів: життя, діяльності людини, навколишнього середовища, – і має підтримувати комфортне та безпечне існування людини, забезпечити сталий розвиток людства.

Розглянемо характеристики елементів системи ЖД.

Життя – це форма існування матерії, яка характеризується обміном речовин, здатністю до розмноження і розвитку, вмінням пристосовуватись до навколишнього середовища.

Людина – вища форма розвитку живої матерії, і її існування – дуже складний процес, що не тільки підтримує її фізіологічний стан, але й задовольняє духовні потреби. Крім того, на життя людини суттєво впливають умови проживання та праці, медичний догляд і багато інших факторів, що виникають завдяки діяльності самих людей.

Діяльність – це специфічна форма ставлення людей до навколишнього середовища та одне до одного, яка має задовольняти потреби та інтереси людини. Це соціальна категорія, нерозривно зв'язана із суспільством. Тільки завдяки діяльності людини створено всі блага, які має людство.

Основні види діяльності такі:

- виробнича;
- наукова;
- мистецька;
- освітня.

Однією із специфічних форм діяльності людини є праця – перша й основна умова існування людини (людства).

Праця – цілеспрямована діяльність людини, у процесі якої вона впливає на природу і використовує її з метою виробництва матеріальних та інших благ, необхідних для задоволення своїх потреб.

Потреби – це необхідність для людини того, що забезпечує її існування і самозабезпечення (фізіологічне, матеріальне, соціальне, духовне та ін.).

Навколишнє середовище (довкілля) або середовище існування – це все, що оточує людину впродовж її життя. Навколишнє середовище, у свою чергу, поділяють на такі види:

- природне середовище;
- штучне середовище.

Природне середовище (біосфера) – це частина Землі і простору навколо неї, де зосереджено все живе. Біосфера включає:

- атмосферу (газоподібна частина);
- гідросферу (рідка водна частина);
- літосферу (тверда частина).

На ЖД людей найбільше впливає частина біосфери від поверхні Землі вглиб на 15–20 км і до висоти 20–22 км, де починається озоновий шар. Природне середовище є джерелом природних ресурсів для існування людини: повітря, води, деревини, корисних копалин, ґрунту та ін.

Штучне середовище – це складова довкілля, створена людством за тривалий час його існування. Штучне середовище умовно можна поділити на два види:

- виробниче середовище;
- побутове середовище.

Виробничим називають середовище, в якому людина реалізує свою трудову діяльність (підприємства, установи, навчальні заклади тощо).

Побутовим є середовище, де люди мешкають або проводять вільний час. Воно охоплює сукупність житлових будинків, комунально-побутових об’єктів, місця відпочинку та ін.

Організм людини може нормально функціонувати тільки тоді, коли умови (параметри) зовнішнього середовища відповідають оптимальним. Якщо умови середовища змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальні механізми, які зберігають постійність параметрів

внутрішнього середовища (всередині організму) чи змінюють їх у межах допустимого.

Можливість функціонування організму в середовищі, параметри якого постійно змінюються, забезпечується завдяки механізму, який називають адаптацією.

Адаптація (лат. adapto – пристосування) – динамічний процес пристосування організму до мінливих умов зовнішнього середовища, який спостерігається в будь-якому виді діяльності щоразу, коли виникають значні зміни в системі «людина – середовище». Адаптація може бути фізіологічною, психологічною, соціальною.

Отже, для функціонування системи ЖД середовище має обов'язково відповідати природним параметрам. Відхилення можливі в межах допустимого, коли організм людини здатний адаптуватися, захистити себе, підтримувати існування. Усе, що існує за цими межами, становить загрозу життю, тому виникає потреба захисту ЖД людей. Отже, безпека – важлива складова системи ЖД.

Розглядаючи систему ЖД як взаємодію людей з навколишнім середовищем, слід зауважити, що вона завжди підпорядкована певним принципам, правилам, умовам життя, природним умовам, традиціям тощо.

Система ЖД має такі характерні ознаки:

– її функціонування підпорядковане об'єктивним законам природи;

– це динамічна система, яка розвивається, удосконалюється, пристосовується до змін умов існування;

– тяжіє до сталого розвитку, вживаючи заходів захисту від упливу негативних факторів.

Основні принципи забезпечення ЖД такі:

– своєчасність, достатність, якість забезпечення людей необхідними для життя засобами високої якості і заходами в потрібний час у належній кількості;

– безпека ЖД (захист ЖД від упливу негативних факторів, що виникають унаслідок як природних явищ, так і діяльності людей).

Рівень реалізації цих принципів значною мірою залежить від способів забезпечення ЖД. Виходячи із сказаного, можна визначити такі головні способи забезпечення ЖД:

1. Організація ефективної трудової діяльності людей в суспільстві з максимальним залученням усіх ресурсів (створення робочих місць, упровадження високопродуктивного виробництва і технологій, нормування праці тощо).

2. Організація та удосконалення освіти і підготовка кадрів, розвиток науки відповідно до вимог часу.

3. Розвиток сфери послуг (комунальних, транспортних, торговельних, побутових і т. ін.).

4. Розширення мережі культурних, спортивних, розважальних установ.

5. Проведення заходів щодо збереження здоров’я людей (диспансеризація, оздоровлення, кваліфіковане медичне обслуговування і лікування, санітарно-епідеміологічний стан).

6. Розроблення законодавчих і нормативно-правових актів із забезпечення прав, свобод і захисту людей і суспільства в цілому.

Залежно від того, якою мірою реалізуються принципи та способи забезпечення ЖД, визначається рівень життя людей окремих країн і загальний розвиток людства.

5.2.3 Елементи теорії, що відповідають моделі безпеки життєдіяльності

Модель у широкому розумінні – це предмет, явище, система (опис, схема, знак, графік, план, макет та ін.), які за певних умов відіграють роль замінника або представника будь-якого іншого предмета, явища чи системи.

З точки зору науки модель – це матеріальна чи уявна система, що відображає чи імітує принципи внутрішньої організації, функціонування, певні

властивості чи характеристики об'єкта дослідження, безпосереднє вивчення якого неможливе. Модель може замінити цей об'єкт у пізнавальному процесі з метою отримання нових знань про нього. Таким чином, відношення «модель—оригінал» не природне, а зумовлене процесом пізнання, і питання про їх співвідношення, ступінь їх подібності, адекватності – одне з найважливіших і найскладніших у процесі використання моделей у науковому пізнанні.

Сам процес моделювання – це непрямий, опосередкований метод наукового дослідження об'єктів пізнання на їх моделях, коли з певних причин безпосереднє їх вивчення неможливе.

Моделі в дисципліні «Безпека життєдіяльності» можна систематизувати за об'єктом зв'язків. Усі моделі можна умовно поділити на дві множини залежно від обсягу зв'язків, які вони демонструють.

Перша множина об'єднує моделі, що характеризуються структурою зв'язків.

Друга множина об'єднує моделі парних зв'язків. Певна умовність щодо цієї множини пов'язана з тим, що запровадження глибокого аналізу дозволяє уявити механізми реалізації цих зв'язків діючих великих систем.

Для характеристики довкілля на глобальному, державному і регіональному рівні використовують поняття структури зв'язків (на світовому рівні – навіть загальної). Відповідно до визначеної послідовності рівнів (за територією, від світового до регіонального) зменшується кількість таких зв'язків – з одного боку, а з іншого – збільшується рівень їх деталізації.

Під державним рівнем у цьому випадку розуміють сукупність діючих галузей виробництва як джерел забруднення і географічні чинники території, що одержує це забруднення. Відповідно до двох визначених рівнів подано моделі, що формують уявлення про стан світового довкілля і держави (на прикладі сільськогосподарської галузі). На регіональному рівні модель, що формує стан довкілля, може бути представлена у вигляді взаємодій комплексу діючих (діючого) підприємств із середовищем виробництва.

Для визначення умов роботи підприємства найбільшу увагу для застосування привертають моделі, що відображають зв'язки:

– «регіональний природно-виробничий комплекс – середовище виробництва»;

– «виробниче підприємство – довкілля»;

– «виробниче середовище виробничого підприємства (середовище робочого місця) – людина».

Здобуття найбільш деталізованої інформації за взаємодії можливе на рівні парних (взаємодій) у вигляді: забруднювач середовища (джерелом є підприємство) – елемент довкілля. Таким чином, необхідно розробити відповідні моделі парної взаємодії.

До таких моделей (як зразок) належать:

– модель розповсюдження елемента забруднення в середовищі (елементи довкілля – атмосфера, гідросфера, літосфера);

– моделі обігу елемента забруднення в елементах довкілля;

– моделі обігу елементів середовища;

– моделі взаємних впливів на елементи довкілля;

– моделі взаємодій екологічних компонентів і організації екосистем;

– моделі впливів небезпечних і шкідливих чинників;

– моделі ієрархії екосистем та ін.

У рамках пари «виробниче середовище – людина» певний зміст взаємодій реалізується на базі спрощення уявлення «виробниче середовище» і представлення його як «технологічний процес, обладнання, види господарських робіт тощо».

В період виконання «технологічного процесу...» виникають небезпеки. Це може бути ініційовано як з боку «технологічного процесу, обладнання, видів господарських робіт», так і з боку – «людини». Виходячи з цього, у схемі розгляду нещасного випадку необхідно йти двома шляхами відносно:

– технологічного процесу, обладнання, видів господарських робіт та ін.;

– «людини» як джерела небезпек.

Розвиток подій вивчають за допомогою ступеневих логіко-імітаційних моделей. Характер ступеневої суті моделі визначає перехід від події до події. Події і переходи за змістом формуються трьома складовими: 1) технологічний процес, його операції й елементи; 2) конструкція обладнання; 3) стан охорони праці при їх взаємодії.

За наявності небезпечних обставин під час виконання будь-яких робіт людина сприяє, усвідомлює, приймає і реалізує відповідні рішення в послідовності.

Обидві моделі в межах поєднання свого змісту дають змогу усвідомити комплексний розвиток подій, причини аварій та ін., сприяють створенню безпечних умов праці і запобіганню травматизму.

5.3 Висновки до 5 розділу

В розділі опрацьовано наступні питання: вимоги охорони праці при виконанні робіт на персональному комп’ютері, вимоги щодо організації та обладнання робочих місць, вимоги безпеки під час роботи з комп’ютером, міжнародний тероризм, структура системи БЖД, елементи теорії, що відповідають моделі безпеки життєдіяльності.

ВИСНОВКИ

Під час виконання дипломної роботи ОР «Магістр» виконано наступні завдання:

– Проведено аналіз проблематики дослідження.

– Проведено аналіз видів маршрутизації.

– Проведено аналіз протоколів маршрутизації та наведено їх порівняльну характеристику.

– Проведено дослідження динамічного протоколу OSPF.

– Проведено розробку початкових налаштувань маршрутизації протоколів.

Під час аналізу динамічного протоколу маршрутизації OSPF було досліджено, що він має такі переваги:

– маршрути для протоколу OSPF, не будуть циклічними;

– даний протокол забезпечує масштабованість, що в свою чергу цю особливість можна застосувати до великих мереж;

– можливість швидкого переналаштування, зокрема коли змінюється топологія мережі.

Недоліки:

– складна ієрархічна топологія;

– неможливість довільно узагальнити та фільтрувати в будь-якій точці мережі;

– вища складність (LSA) порівняно з іншими IGP.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. RFC 1131. OSPF Specification Version 1 (J. Moy, Oct. 1989).
2. RFC 1245. OSPF Protocol Analysis (J. Moy, July 1991).
3. RFC 1246. Experience with the OSPF Protocol (J. Moy, July 1991).
4. RFC 1247. OSPF Version 2 [obsoletes 1131] (J. Moy, July 1991).
5. RFC 1248. OSPF Version 2 Management Information Base (F. Baker & R. Coltun, July 1991).
6. RFC 1252. OSPF Version 2 Management Information Base [obsoletes 1248] (F. Baker & R. Coltun, July 1991).
7. RFC 1253. OSPF Version 2 Management Information Base [obsoletes 1252] (F. Baker & R. Coltun, Aug. 1991).
8. RFC 1364. BGP OSPF Interaction [obsoletes 1247 and 1267] (K. Varadhan, Sept. 1992; IAB; L. Chapin, Oct. 1992).
9. RFC 1370. Applicability Statement for OSPF (IAB; L. Chapin, Oct. 1992).
10. RFC 1371. Choosing a "Common IGP"for the IP Internet (\ESG; P. Gross, Oct. 1992).
11. RFC 1403. BGP OSPF Interaction [obsoletes 1364] (K. Varadhan, Jan. 1993).
12. RFC 1583. OSPF Version 2 [obsoletes RFC1247] (J. Moy, March 1994).
13. RFC 1584. Multicast Extensions to OSPF (L Moy, March 1994).
14. RFC 1585. MOSPF: Analysis and Experience (J. Moy, March 1994).
15. RFC 1586. Guidelines For Running OSPF Over Frame Relay Networks (O. deSouza and M. Rodriguez, March 1994).
16. RFC 1587. The OSPF NSSA Option (V. Fuller & R. Coltun, March 1994).
17. RFC 1745. BGP4/IDRP for IP-OSPF Interaction (K. Varadhan, S. Hares, Y. Rekhter, Dec. 94).
18. RFC 1765. OSPF Database Overflow (L Moy, March 1995).

19. RFC 1793. Extending OSPF to Support Demand Circuits (J. Moy, April 1995).

20. RFC 1850. OSPF Version 2 Management Information Base [obsoletes 1253] (F. Baker & R. Coltun, Nov. 1995).

21. RFC 2178. OSPF Version 2 [obsoletes 1583](L Moy, July 1997).

22. RFC 2328. OSPF Version 2 [obsoletes 2178] (J. Moy, April 1998).

23. RFC 2370. The OSPF Opaque ISA Option (R. Coltun, July 1998).

24. RFC 2676. QoS Routing Mechanisms and OSPF Extensions (G. Apostolopoulos,

25. D. Williams, S. Kamat, R. Guerin, A. Orda, T. Przygienda, August 1999).

26. RFC 2740. OSPF for IPv6 (R. Coltun, D. Ferguson, J. Moy, December 1999).

27. RFC 2844. OSPF over ATM and Proxy PAR (T. Przygienda, P. Droz, R Haas, May 2000).

28. OSPF // Википедия. Свободная энциклопедия. – Режим доступа: ru.wikipedia.org/wiki/OSPF. – Дата доступа: октябрь 2018 года. – Заглавие с экрана.

29. OSPF Design Guide // CISCO. – Режим доступу: www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html. – Дата доступу: листопад 2018 року. – Заголовок з екрану.

30. В.Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / Олифер В.Г., Олифер Н.А. – СПб.: Питер, 2010. – 944 с. – ISBN: 978-5-49807-389-7

31. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. – Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с. : ил.

32. Жуков І. А., Дрововозов В. І., Масловський Б. Г. Експлуатація комп’ютерних систем та мереж. Навч. Посібник. – К.: НАУ.2007.-368с.

33. Запечников, С.В. Основы построения виртуальных частных сетей [Текст]: Учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И.

Толстой. – М.: Горячая линия-Телеком, 2003. – 249 с. ; 20 см. – 3000 экз. – ISBN 5-93517-139-2.

34. Збіжність // Всесвітні енциклопедичні знання. – Режим доступу: http://uk.swewe.net/word_show.htm/?20332_3&%D0%97%D0%B1%D1%96%D0%B6%D0%BD%D1%96%D1%81%D1%82%D1%8C. – Дата доступу: листопад 2018 року. – Заголовок з екрану.

35. Зегжда Д. П. Как построить защищенную информационную систему. Технология создания безопасных систем [Текст] / Д. П. Зегжда, А. М. Ивашко ; под научн. ред. П. Д. Зегжды, В. В. Платонова. – СПб.: Мир и Семья-95, Интерлайн, 1998. – 256 с. : ил. ; 20 см. – 500 экз.

36. Олгри, Терри. Модернизация и ремонт сетей, 4-е издание. / Терри Олгри; пер. с англ. И.В. Берштейна, Л.М. Ильичевой, Е.Л. Полонской, А.П. Сергеева, Т.А. Шамренко; [глав. Ред. С.Н. Тригуб] – М.: Издательский дом „Вильямс”, 2005. – 1328 с. – ISBN: 5-8459-0688-1.

37. Плешаков Владимир. Глава 2. Основы маршрутизации / Владимир Плешаков // CIT Forum. – Режим доступа: http://citforum.ru/nets/ito/2.shtml. – Дата доступа: ноябрь 2018 года. – Заглавие с экрана.

38. Сходимость сети // marshrutizatciia.ru. – Режим доступа: http://marshrutizatciia.ru/sxodimost-seti.html. – Дата доступа: ноябрь 2018 года. – Заглавие с экрана.

39. Тарасова В.В. Екологічна статистика (з блочномодульною формою контролю знань). Підручник. / В.В. Тарасова – К.: Центр учбової літератури, 2008. – 392 с. – ISBN 978-966-364-669-5.

40. Томас, Том М. II Структура и реализация сетей на основе протокола OSPF, 2-е изд. : Пер. с англ. – М.: Издательский дом "Вильяме", 2004. – 816с.: ил.

41. Цапко В.Г. Безпека життєдіяльності: Навч. посіб. / За ред. В.Г. Цапка. – 3-тє вид., стер. – К.: Знання, 2004. – 397 с. – ISBN 966-8148-39-8.

42. Інструкція з охорони праці при роботі на персональному комп’ютері [Електронний ресурс] – Режим доступу: https://uteka.ua/ua/publication/special-24-

formy-ta-systemy-oplaty-praci-127-instrukciya-po-oxrane-truda-pri-rabote-na-personalnom-kompyutere-obrazec – Дата доступу: 07.05.21 – Назва з екрана.

43. Вимоги безпеки щодо організації робочих місць [Електронний ресурс] – Режим доступу: https://buklib.net/books/31185/ – Дата доступу: 07.05.21 – Назва з екрана.

44. Вимоги безпеки під час роботи на ПК [Електронний ресурс] – Режим доступу: https://sites.google.com/site/ohoronapraci44/33-vimogi-bezpeki-pid-cas-roboti-na-pk – Дата доступу: 07.05.21 – Назва з екрана.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національна академія наук України
Тернопільський національний технічний університет імені Івана Пулюя
Західний науковий центр НАН України і МОН України
Тернопільська державна обласна адміністрація
Тернопільська обласна рада
Тернопільська міська рада
Наукове товариство імені Шевченка
Віденський університет (Австрія)
Чеський технічний університет (Чехія)
Університет імені П'єра і Марії Кюрі Сорбона Париж (Франція)
Університет прикладних наук Шмалькайдена (Німеччина)
Технічний університет у Кошице (Словаччина)
Опольський технологічний університет (Польща)
Науково-технічне товариство (Тернопіль)

Матеріали міжнародної наукової конференції «ІВАН ПУЛЮЙ: ЖИТТЯ В ІМ'Я НАУКИ ТА УКРАЇНИ»

(до 175-ліття від дня народження)

28–30 вересня 2020 року

ТЕРНОПІЛЬ, 2020

УДК 004.056

Н.А. Шевченко, М.В. Валігула, Т.О. Маєвський, Г.В. Шимчук
Тернопільський державний технічний університет імені Івана Пулюя

ОГЛЯД МОДЕЛЕЙ ХМАРНИХ ПОСЛУГ

N. Shevchenko, M. Valihula, T. Mayevs'kyy, H. Shymchuk

OVERVIEW OF CLOUD SERVICE MODELS

Сучасні організації залежать від можливостей обробки даних, витрат і накладних витрат на управління своїми обчислювальними ресурсами. Концепція хмарних обчислень призначена звільнити організації та їх співробітників від додаткових витрат пов'язаних з IT. Клієнт може перенести зберігання даних, обробку інформації або навіть всю інформаційну інфраструктуру до провайдера послуг, що дозволяє сфокусуватися на своїй основній діяльності і залишити IT професіоналам [1].

У той час як концепція хмарних обчислень надає новий підхід до обробки інформації, проблеми безпеки виходять на перший план. Вимоги безпеки є ключовим чинником для прийняття рішення про використання інформаційно-технічних послуг і, зокрема, для вирішення про перехід до середовища публічних хмарних обчислень [2].

Виходячи з даних Morgan Stanley Research [3], перше місце серед всього списку проблем хмарних обчислень займає проблема забезпечення безпеки. У рамках даного дослідження, відсутність достатніх гарантій безпеки зберігання даних було названо найбільшою перешкодою при переході в «хмару» (24 % респондентів), це вдвічі більше, ніж наступна проблема - неочевидність економічної вигоди (12 % респондентів).

Основна ідея хмарних обчислень - надання ресурсів високої надійності, масштабованості та доступності в розподіленому середовищі на вимогу. Незважаючи на простоту ідеї, термін Cloud Computing розуміється і подається по-різному [4], загальноприйнятого визначення немає. Компанія Cisco Systems визначає Cloud Computing як IT-ресурси та послуги, які абстраговані від інфраструктури та надаються на вимогу «в необхідному масштабі» в середовищі множинної оренди. У свою чергу Лабораторія інформаційних технологій Національного інституту стандартів і технологій США (NIST) опублікувала наступне визначення хмарних обчислень [5]: «Хмарні обчислення - це модель, що забезпечує зручний мережевий доступ на вимогу до загальних конфігурованих обчислювальних ресурсів (мереж, серверів, сховищ даних, додатків і сервісів), який оперативно надається з мінімальними зусиллями з управління та взаємодії з сервіс-провайдером». Визначення хмарних обчислень описує п'ять основних характеристик (самообслуговування на вимогу, широкий мережевий доступ, оперативна еластичність, пул ресурсів, розрахунок вартості послуги), три сервісні моделі (SaaS, PaaS, IaaS) і чотири моделі розгортання (приватні хмари, публічні хмари, групові хмари, гібридні хмари). Концептуально, хмарні послуги класифікуються як сервіси (XaaS): TaaS (тестування як послуга), SaaS (програмне забезпечення як послуга), PaaS (платформа як послуга), HAAS (апаратне забезпечення як послуга).

На даний момент існує безліч сервіс провайдерів, які надають різні сервіси (Amazon EC2, Google App Engine (GAE), SalesForce.com (SFDC), Microsoft Azure, IBM Blue Cloud, 3Tera). Поточний етап еволюції хмарних обчислень характеризується наявністю різнорідних пропозицій від сервіс-провайдерів. Важливо зауважити, що концепція хмарних обчислень не нова, а являє собою наступний етап еволюції декількох ініціатив останніх років, включаючи розподілені обчислення, грід обчислення, комунальні (utility) обчислення, віртуалізацію, кластерізацію [6].

Хмарні обчислення працюють на основі сервісно-орієнтованої бізнес-моделі. Іншими словами, апаратні ресурси і ресурси платформи надаються як сервіс та на

вимогу. Варіанти хмари систематизуються за моделями служб та залучення ресурсів: пропоновані послуги можуть бути згруповані у три категорії: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) і інфраструктура як послуга (IaaS) [7].

Інфраструктура як послуга (IaaS) абстрагує обладнання (сервер, сховище і мережеву інфраструктуру) і об'єднує його у вигляді можливостей обчислення, зберігання та підключення, які поставляються як послуги з ціною, встановленою за фактичним використанням. Її мета полягає в наданні гнучкого стандартного віртуального операційного середовища, що стає основною для PaaS і SaaS. [8]

IaaS, як правило, забезпечує стандартизований віртуальний сервер. Споживач бере на себе відповідальність за конфігурацію і операції гостьової ОС, ПО і бази даних (БД). Обчислювальні можливості (такі як швидкодія, смуга пропускання та доступ до сховища) також стандартизовані. Рівні обслуговування охоплюють швидкодію і доступність інфраструктури, яка віртуалізується. Споживач бере на себе операційні ризики, які існують крім інфраструктури.

Платформа як послуга (PaaS) надає служби виконання додатків, такі як час виконання, зберігання та інтеграція, для додатків, створених для заздалегідь зазначеної архітектури. Ця модель забезпечує ефективний і гнучкий підхід до передбачуваної економічно ефективної роботи горизонтально масштабованих додатків. PaaS відноситься до надання ресурсів рівня платформи, включаючи операційні системи та підтримку фреймворку розробки програмного забезпечення. Приклади PaaS провайдерів включають Google App Engine, Microsoft Windows Azure і Force.com.

Програмне забезпечення як послуга (SaaS) забезпечує бізнес-процеси і додатки, такі як управління відносинами з клієнтами, спільна робота і електронна пошта, у вигляді стандартизованих можливостей, вартість яких визначається за фактичним використанням відповідно до встановленого рівня обслуговування, відповідного бізнес-потребам. Ця модель відрізняється великою ефективністю витрат та доставки при мінімальних налаштуваннях і знімає операційні ризики зі споживача, покладаючи на постачальника. Вся інфраструктура і функції експлуатації IT абстраговані від споживача.

Література:

3. W. Wang, R. Owens, Z. Li, B. Bhargava. Secure and Efficient Access to Outsourced Data. Proceedings of the 2009 ACM workshop on Cloud computing security. Pages 55-65, 2009.
4. W. Jansen, T.Grance. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology Draft Special Publication 800-144. 60 pages, Jan. 2011.
5. Adam Holt, Keith Weiss, CFA1, Katy Huberty, CFA1, Ehud Gelblum. Cloud Computing Takes Off. Market Set to Boom as Migration Accelerates. //Morgan Stanley Research. - May 23, 2011.
6. Cloud Computing and Grid Computing 360-Degree Compared / Foster I., Zhao Y., Raicu I., Lu S.: Grid Computing Environments Workshop, 2008. GCE '08.
7. National Institute of Standards and Technology. [Електронний ресурс]. Режим доступу: http://www.nist.gov/index.html.
8. Eric Brewer. Towards Robust Distributed Systems. – Brewer E. : Principles of Distributed Computing, Portland, Oregon, 2000.
9. Tharam Dillon. Cloud Computing: Issues and Challenges. / Dillon T., Wu C., Chang E.: 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
10. Что такое инфраструктура как услуга. [Електронний ресурс]: Documentation – Режим доступу: https://technet.microsoft.com/ru-ru/cloud/hh744751.aspx

Міністерство освіти і науки України,
Тернопільський національний технічний університет
імені Івана Пулюя
Маріборський університет (Словенія)
Технічний університет в Кошице (Словаччина)
Каунаський технологічний університет (Литва)
Львівський національний університет
імені Івана Франка,
Гірничо-металургійна академія ім. Станіслава Сташиця
(Польща)
Луцький національний технічний університет,
Чернівецький національний університет
імені Юрія Федьковича,
Вроцлавський економічний університет (Польща)
Донбаська державна машинобудівна академія

Студентське наукове товариство

IV МІЖНАРОДНА

студентська науково - технічна конференція

"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ.

АКТУАЛЬНІ ПИТАННЯ"

28-29 квітня 2021 р.

(збірник тез конференції)

Тернопіль 2021

УДК 004.04
Шевченко Н. – ст. гр. СНмн-61, Горбуляк Ю. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя
Маєвський Т. – ст. гр. КІ-206
Технічний коледж Тернопільського національного технічного університету імені Івана Пулюя

АНАЛІЗ ПРОТОКОЛУ OSPF

Науковий керівник: старший викладач Шимчук Г.

Shevchenko N., Horbulyak YU.
Ternopil Ivan Pul'uj National Technical University
Mayevs'kyy T.
Technical college Ternopil Ivan Puluj National Technical University

OSPF PROTOCOL ANALYSIS

Supervisor: Senior Lecturer Shymchuk G.

Ключові слова: IGP, LAN, SPF, ARPANET, OSPF, RFC 1131, DECnet, RIP, BGP, RIPv2, ABR, IS-IS, EIGRP
Key words: IGP, LAN, SPF, ARPANET, OSPF, RFC 1131, DECnet, RIP, BGP, RIPv2, ABR, IS-IS, EIGRP

OSPF був розроблений, як протокол внутрішнього шлюзу (IGP) для використання в автономній системі, такій як локальна мережа (LAN). Він реалізує алгоритм Дейкстри, також відомий, як алгоритм найкоротшого шляху (SPF). Як протокол маршрутизації стану зв'язку він базувався на алгоритмі стану зв'язку, розробленому для ARPANET в 1980 році, та протоколі маршрутизації IS-IS. Вперше OSPF був стандартизований у 1989 році як RFC 1131, який тепер відомий як OSPF версія 1. Роботи з розробки OSPF до його кодифікації як відкритого стандарту проводились переважно Digital Equipment Corporation, яка розробила власні протоколи DECnet [1].

Протокол маршрутизації, такий як OSPF, розраховує найкоротший шлях до пункту призначення через мережу на основі алгоритму. Перший широко впроваджений протокол маршрутизації, «Інформаційний протокол маршрутизації» (RIP), розраховував найкоротший маршрут на основі стрибків, тобто кількість маршрутизаторів, яким IP-пакет повинен був пройти, щоб досягти хоста призначення. RIP успішно реалізував динамічну маршрутизацію, де таблиці маршрутизації змінюються, якщо змінюється топологія мережі. Але RIP не адаптовував свою маршрутизацію відповідно до мінливих мережевих умов, таких як швидкість передачі даних. Зростав попит на динамічний протокол маршрутизації, який міг розрахувати найшвидший маршрут до пункту призначення. OSPF був розроблений таким чином, що найкоротший шлях через мережу обчислювався на основі маршруту з урахуванням пропускної здатності, затримки та навантаження [1]. Таким чином, OSPF проводить розрахунок маршруту на основі параметрів зв'язку, які можуть бути зважені адміністратором. OSPF був швидко прийнятий, оскільки він став відомим для надійного розрахунку маршрутів через великі та складні локальні мережі [1].

Як протокол маршрутизації стану каналу зв'язку, OSPF підтримує бази даних стану каналів зв'язку, які насправді є картами топології мережі, на кожному

маршрутизаторі, на якому він реалізований. Стан даного маршруту в мережі – це важливість, а алгоритм OSPF дозволяє кожному маршрутизатору розрахувати важливість маршрутів до будь-якого даного доступного пункту призначення [1]. Якщо адміністратор не зробив конфігурацію, важливість каналу зв'язку, підключеного до маршрутизатора, визначається швидкістю передачі даних (1 Гбіт/с, 10 Гбіт/с тощо) інтерфейсу. Потім інтерфейс маршрутизатора з OSPF буде рекламувати свою важливість зв'язку із сусідніми маршрутизаторами за допомогою багатоадресного передавання, відомого як процедура hello [1]. Усі маршрутизатори з реалізацією OSPF продовжують надсилати hello-пакети, і, отже, зміни у важливості їх посилань стають відомимі сусіднім маршрутизаторам [1]. Інформація про важливість посилання, тобто швидкість з'єднання від точки до точки між двома маршрутизаторами, потім каскадується через мережу, оскільки маршрутизатори OSPF рекламують інформацію, яку вони отримують від одного із сусіднього маршрутизатора, до всіх інших сусідніх маршрутизаторів. Цей процес «розливу» інформації зв'язку через мережу відомий як синхронізація. На основі цієї інформації всі маршрутизатори з реалізацією OSPF постійно оновлюють свої бази даних стану каналів інформацією про топологію мережі та коригують свої таблиці маршрутизації [1].

Мережа OSPF може бути структурована або поділена на області маршрутизації для спрощення адміністрування, оптимізації використання трафіку та використання ресурсів. Райони ідентифікуються 32-розрядними числами, вираженими або просто в десяткових, або часто в одних і тих же крапково-десяткових позначеннях, що використовуються для адрес IPv4. За домовленістю, область 0 (нуль) або 0.0.0.0 представляє ядро або магістральну область мережі OSPF. Хоча ідентифікації інших областей можуть бути обрані за бажанням, адміністратори часто вибирають в якості ідентифікатора області IP-адресу основного маршрутизатора в певній області. Кожна додаткова область повинна мати зв'язок із магістральною областю OSPF. Такі зв'язки підтримуються маршрутизатором, що з'єднується між собою, відомий як маршрутизатор прикордонної зони (ABR). ABR веде окремі бази даних стану каналів зв'язку для кожної області, яку обслуговує, та підтримує узагальнені маршрути для всіх областей мережі.

OSPF виявляє зміни в топології, наприклад, збої каналів, і сходиться на новій структурі маршрутизації без циклу протягом секунд [1].

OSPF став популярним протоколом динамічної маршрутизації. Іншими часто використовуваними протоколами динамічної маршрутизації є RIPv2 та протокол прикордонного шлюзу (BGP) [2]. Сьогодні маршрутизатори підтримують принаймні один внутрішній протокол шлюзу для реклами своїх таблиць маршрутизації в локальній мережі. Крім OSPF, часто впроваджуваними протоколами внутрішніх шлюзів є RIPv2, IS-IS та EIGRP (Enhanced Internal Gateway Routing Protocol) [3].

Література:

1. Martin P. Clark (2003). Data Networks, IP and the Internet: Protocols, Design and Operation. John Wiley & Sons. ISBN 9780470848562.
2. OSPF Convergence, August 6, 2009, retrieved June 13, 2016
3. J. Moy (April 1998). OSPF Version 2. Network Working Group, IETF. doi:10.17487/RFC2328. OSPFv2., Updated by RFC 5709, RFC 6549, RFC 6845, RFC 6860, RFC 7474, RFC 8042.

З М І С Т

Секція: **Інформаційні технології**