**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ДОСЛІДЖЕННЯ РІЗНИХ МЕТОДІВ МАРШРУТИЗАЦІЇ ТА КОМУТАЦІЇ У МЕРЕЖАХ CISCO З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ CISCO TRUSTSEC»**

на здобуття освітнього ступеня магістр
за спеціальності 123 Комп'ютерна інженерія
(код,найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ігор БЕНЕДІКО
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр.КСДМ-62
Ігор БЕНЕДІКО
(ім'я, ПРІЗВИЩЕ)
Керівник: Наталія ЛАЩЕВСЬКА
к.т.н., доцент *(ім'я, ПРІЗВИЩЕ)*
Рецензент:
науковий ступінь, вчене звання *(ім'я, ПРІЗВИЩЕ)*

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти «Магістр»

Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна прорама Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
(ім'я, ПРІЗВИЩЕ)
"____" _____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бенедіко Ігору Володимировичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Дослідження різних методів маршрутизації та комутації у мережах Cisco з використанням технології Cisco Trustsec
керівник роботи Наталія ЛАЩЕВСЬКА к.т.н., доцент
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" 10 2023 р. №145
2. Строк подання кваліфікаційної роботи
3. Вихідні дані кваліфікаційної роботи:
3.1. Інтернет ресурси стосовно методів маршрутизації та комутації.
3.2. Технічна документація стосовно мереж Cisco/
3.3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Основні завдання маршрутизації в комп'ютерних мережах.
4.2. Аналіз методів маршрутизації в комп'ютерних мережах.
4.3. Програмно-обумовлена сегментація мережі на основі Cisco TrustSec.
5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання "19" жовтня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	**Примітка**
1.	Підбір технічної літератури	.2023р. .2023р.	Виконано
2.	Основні завдання маршрутизації в комп'ютерних мережах	.2023р. .2023р.	Виконано
3.	Аналіз методів маршрутизації в комп'ютерних мережах	.2023р. .2023р.	Виконано
4.	Програмно-обумовлена сегментація мережі на основі Cisco TrustSec	.2023р. .2023р.	Виконано
5.	Оформлення роботи, висновки	.2023р. .2023р.	Виконано
6.	Розробка демонстраційного матеріалу, доповідь	.2023р. .2023р.	Виконано

Здобувач вищої освіти Ігор БЕНЕДІКО
(підпис) *(ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Наталія ЛАЩЕВСЬКА
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступеня магістр: 95 стор., 15 рис., 1 табл., 22 джерел.

Мета роботи – забезпечення безпеки мереж та контролю доступу до ресурсів за допомогою використання технології Cisco TrustSec.

Об'єкт дослідження – методи маршрутизації та комутації.

Предмет дослідження – мережі Cisco.

Короткий зміст роботи: У роботі було розглянуто та проаналізовано загальні принципи маршрутизації та комутації комп'ютерних мереж. Визначено основні переваги та недоліки протоколів маршрутизації, та наведено їх порівняльний аналіз. В роботі проаналізовано традиційний підхід до сегментації і його обмеження. Розглядається новий підхід до сегментації на базі технології Cisco TrustSec, що усуває ці обмеження. Розглядається ряд типових завдань ІТ та ІБ, пов'язаних з сегментацією, а також проводиться порівняння рішень цих задач, які пропонуються традиційним і новим підходами.

КЛЮЧОВІ СЛОВА: КОМП'ЮТЕРНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, МЕТОДИ МАРШРУТИЗАЦІЇ, МЕТОДИ КОМУТАЦІЇ, ПРОТОКОЛИ МАРШРУТИЗАЦІЇ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, МЕРЕЖІ CISCO, ТЕХНОЛОГІЯ CISCO TRUSTSEC

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 95 pages, 1 table, 15 figures, 22 sources.

The purpose of the work is ensuring network security and resource access control using Cisco TrustSec technology.

The object of research is routing and switching methods.

The subject of research is Cisco networks.

The work considered and analyzed the general principles of routing and switching of computer networks. The main advantages and disadvantages of routing protocols are determined, and their comparative analysis is given. The paper analyzes the traditional approach to segmentation and its limitations. A new approach to segmentation based on Cisco TrustSec technology is considered, which eliminates these limitations. A number of typical IT and IS tasks related to segmentation are considered, as well as a comparison of solutions to these tasks, which are offered by traditional and new approaches.

КЛЮЧОВІ СЛОВА: КОМП’ЮТЕРНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, МЕТОДИ МАРШРУТИЗАЦІЇ, МЕТОДИ КОМУТАЦІЇ, ПРОТОКОЛИ МАРШРУТИЗАЦІЇ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, МЕРЕЖІ CISCO, ТЕХНОЛОГІЯ CISCO TRUSTSEC

ЗМІСТ

Стор.

ВСТУП

Одним з найбільш актуальних наукових завдань у галузі телекомунікацій є передавання трафіку з дотриманням низки вимог щодо якості обслуговування. Це пов'язано із тим, що множина потоків даних передається по мережі, ресурси якої необхідно розподілити між цими потоками за певною пропорцією. Оскільки дані, які підлягають передаванню, різні за своєю природою та важливістю, то необхідно мати механізми, які дають змогу розв'язувати задачу розподілу ресурсів оперативно, у відповідності до властивостей тих потоків, які передаються у конкретний момент часу через конкретні телекомунікаційні вузли. Такі механізми повинні базуватись на удосконалених методах розподілу ресурсів, що мають високу масштабованість, швидкодію, гнучкість, низьку операційну складність та ресурсоємність.

Для підвищення якості обслуговування (QoS) переданого мережевого трафіку актуальним є пошук гнучких методів управління мережними ресурсами для забезпечення їхнього збалансованого завантаження й гарантованої якості обслуговування трафіку користувачів у комп'ютерних мережах.

Використання мережних ресурсів значною мірою залежить від вибору протоколу маршрутизації.

TrustSec – це архітектура для збільшення безпеки кампусної мережі та датацентру. Допомагає компаніям захистити мережу, дані та ресурси за допомогою:

- технологій мережевої ідентифікації;

- технологій контролю доступу на основі політик та користувальницьких ролей;

- додаткові сервіси для захисту доступу та середовища передачі.

Актуальність дипломної роботи полягає в тому, що безпека мереж стає все більш важливою у сучасному світі, де зростає кількість кібератак та загроз безпеці інформації. Використання технології Cisco TrustSec може допомогти організаціям забезпечити безпеку своїх мереж та контроль доступу до ресурсів. Дослідження

різних методів маршрутизації та комутації у мережах Cisco з використанням цієї технології дозволить виявити найефективніші рішення та рекомендації для практичного застосування.

1 ОСНОВНІ ЗАВДАННЯ МАРШРУТИЗАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1 Сутність поняття маршрутизації

Маршрутизація - це процес пересилання пакетів даних між мережами або підмережами, використовуючи пристрої третього рівня моделі OSI/ISO.

Для маршрутизації використовуються таблиці маршрутизації та протоколи, які реалізують алгоритми маршрутизації для визначення найбільш раціонального шляху для пересилання пакетів даних. Способи маршрутизації в мережах передачі даних представлений на рисунку 1.1.

Рисунок 1.1 - Способи маршрутизації в мережах передачі даних

Пристрій, який визначає більш прийнятний шлях для передачі даних з однієї мережі в іншу, називається маршрутизатором. Принцип дії маршрутизаторів показано на рисунку 1.2.

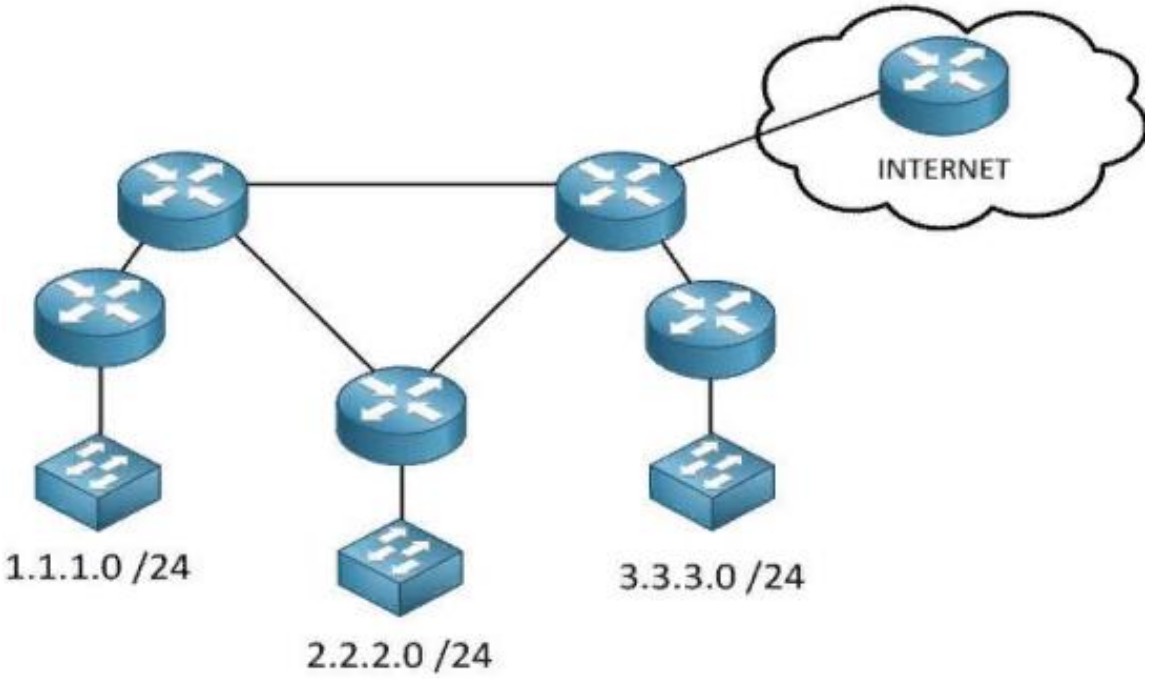

Рисунок 1.2 - Принцип дії маршрутизаторів

Для обміну даних у мережах маршрутизатор веде таблицю маршрутизації. Вона представляє собою список мережевих адрес, а також зберігає дані про місця призначення та з'єднання з наступними переходами. За допомогою цих з'єднань, пристрій розуміє, чи можна дістатися до пункту призначення безпосередньо чи через інші маршрутизатори. Таблиця може зберігати такі типи записів (один запис для кожної мережі):

- статична - інформація про маршрут заповнюється вручну, але цей метод призводить до проблем у випадку зміни топології мережі або відмови на будь-якій ділянці;

- динамічна - заповнення відбувається завдяки обміну даними маршрутизації між пристроями, отриманими за протоколом маршрутизації, тобто маршрутизатори обмінюються інформацією один з одним, передаючи повідомлення про оновлення. Залежно від протоколу, оновлення можуть надходити періодично або лише при зміні топології.

Трапляються ситуації, коли існує кілька способів передачі інформації від джерела до місця призначення. Кожен протокол маршрутизації використовує свої метрики для визначення найкращого шляху. Якщо використовуються різні

протоколи, то прийнятний шлях обирається на основі адміністративної відстані - це число від 0 до 255 (рис. 1.3).

Назва протоколу	Значення відстані
Сумарний маршрут EIGRP	5
BGP, який працює поза рамками автономної системи	20
EIGRP, який працює в рамках автономної системи	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
EIGRP, який працює поза рамками автономної системи	170
BGP, який працює в рамках автономної системи	200

Рисунок 1.3 – Значення адміністративної відстані

Протокол з найменшим значенням вибирається як більш надійний.

Протокол маршрутизації – це набір правил, які маршрутизатор використовує в "комунікації" з іншими маршрутизаторами для визначення шляхів до віддалених мереж, а також для зберігання записів про ці мережі в таблиці маршрутизації . Існують два поняття:

- протокол, що маршрутизується – це будь-який протокол з адресою мережевого рівня, який здійснює пересилку пакетів між хостами. Цей протокол, як правило, не має інформації про весь маршрут від джерела до пункту призначення. Наприклад, протокол IP;

- протокол маршрутизації - дозволяє забезпечити обмін даних маршрутизації даних між мережами та дозволяє створити динамічні таблиці маршрутизації. Маршрутизатор повинен знати, куди відправити пакет, але не його подальший шлях від інших маршрутизаторів.

На рисунку 1.4 представлено протоколи, що маршрутизуються.

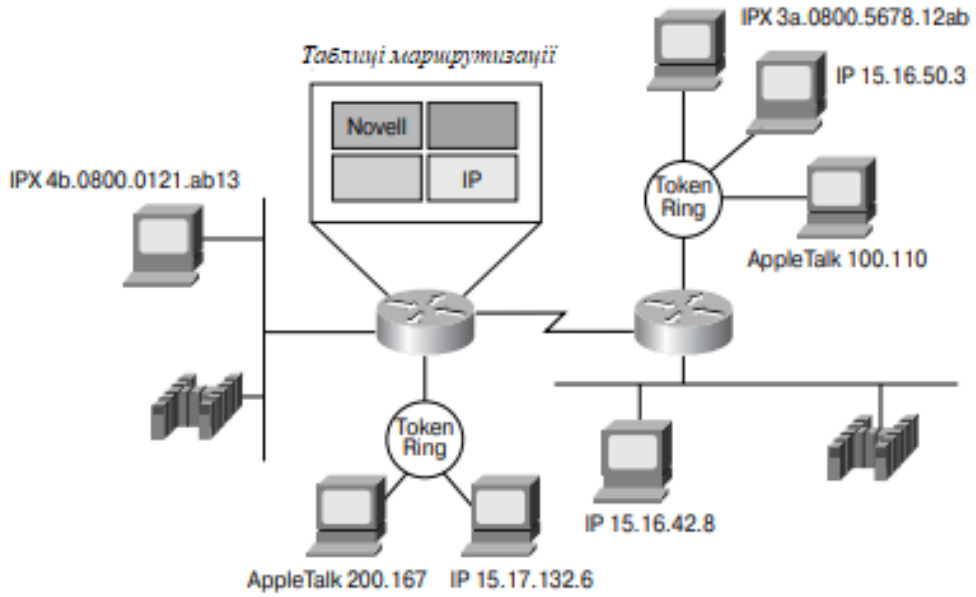

Рисунок 1.4 - Протоколи, що маршрутизуються

Протоколи маршрутизації відрізняються по типу взаємодії між мережами. Ця різниця пов'язана з поняттям автономної системи (рис. 1.5).

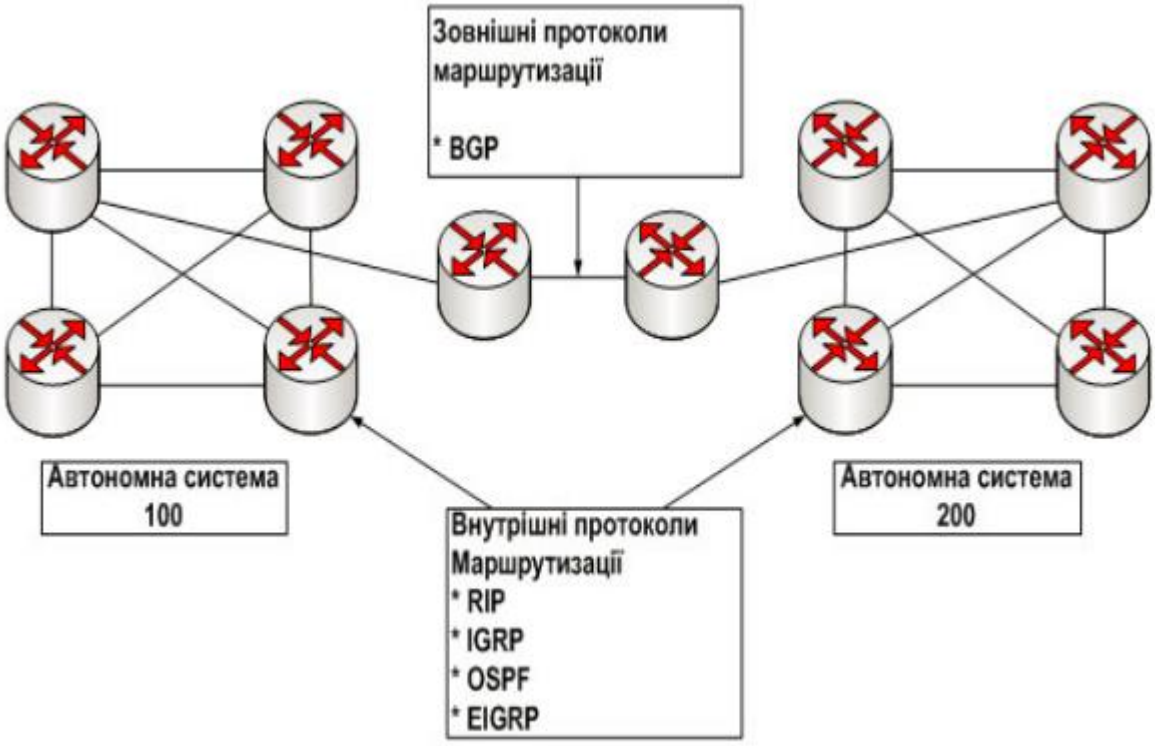

Рисунок 1.5 – Класифікація протоколів маршрутизації по типу взаємодії між мережами

Автономна система (АС) - це сукупність мереж із загальним управлінням, маршрутизатори в АС мають єдині правила маршрутизації. Відповідно до цих понять є два типи протоколів маршрутизації:

- внутрішній протокол маршрутизації - протокол, службовець для обміну інформацією всередині АС. Наприклад: RIP, OSPF, EIGRP та ін.;

- зовнішній протокол маршрутизації - протокол, службовець для обміну інформацією між автономними системами. Наприклад: BGP.

Такий поділ протоколів визначає ієрархічний метод маршрутизації.

Протоколи маршрутизації можна класифікувати по використанню певного алгоритму маршрутизації, який необхідний для визначення оптимального шляху проходження пакетів від джерела до місця призначення.

Вимоги, яким повинні відповідати алгоритми маршрутизації:

- оптимальність - здатність алгоритму вибрати кращий шлях;

- простота - алгоритм не повинен вимагати великої та складної програмної реалізації;

- живучість - алгоритм повинен продовжувати функціонувати в разі непередбачених обставин, таких як відмова обладнання, високі навантаження на мережі і т.д .;

- швидка збіжність - процес угоди між всіма маршрутизаторами по найкращим шляхам. Тобто, наприклад, при відмові будь-якого маршрутизатора, повідомлення про оновлення топології мережі повинні дійти до інших маршрутизаторів з мінімальною затримкою. В результаті маршрутизатори перераховують шлях і вибирають оптимальний. Алгоритми, які сходяться повільно, можуть привести до небажаних наслідків, таких як вихід з ладу всієї мережі;

- гнучкість - алгоритм повинен точно і швидко адаптуватися до змін в мережі. Наприклад, зміна топології мережі, смуги пропускання певних ліній, затримка і т.п.

Розрізняють такі основні алгоритми маршрутизації:

- статичні. Системний адміністратор вручну прописує записи в таблиці маршрутизації. Такий метод маршрутизації непридатний для великих мереж. Так само його складно налаштовувати при зміні топології мережі;

- динамічні. Цей алгоритм враховує зміни в мережі, завдяки повідомленнями, що надходять. При зміні топології відбудеться перерахунок шляхів, після чого відбудеться нова розсилка повідомлень про зміну маршрутів.

Протоколи внутрішньої маршрутизації можна класифікувати по використанню однієї з таких динамічних алгоритмів маршрутизації:

- метод маршрутизації на основі вектору відстаней. Цей метод визначає напрямок і відстань (наприклад, кількість переходів) до будь-якого каналу іншої мережі, шляхом розсилки вектору. При отриманні вектору від сусіда маршрутизатор збільшує відстань, а також додає інформацію про відомі йому мережі і розсилає нове значення вектору по мережі. Мінус цього методу в тому, що у великих мережах широкомовлення негативно позначиться на роботі мережі;

- метод маршрутизації на основі стану каналу. Маршрутизатори обмінюються повідомленнями про стан каналу зі своїми сусідами, при цьому кожен маршрутизатор створює базу даних топології мережі, на основі отриманих повідомлень. Після цього алгоритм видаляє зайві шляхи і становить своє дерево найкоротших шляхів.

Ідеального алгоритму пошуку шляху для всієї мережі не існує.

В алгоритмах маршрутизації використовується багато різних показників, які називаються метрикою. Це число, яке генерує алгоритм для кожного можливого шляху.

Найчастіше менша метрика означає найкращий шлях. Складні алгоритми маршрутизації при виборі маршруту можуть базуватися на безлічі показників або їх комбінації. Нижче перелічені метрики, які найчастіше використовуються в алгоритмах маршрутизації.

- Кількість переходів. Це число показує, скільки переходів через обладнання повинен зробити пакет, щоб дістатися від джерела до місця призначення.

- Швидкість передачі даних в каналі (смуга пропускання).

- Затримка. Час, необхідний для передачі пакета від джерела до місця призначення. Затримка може залежати від багатьох факторів, таких як завантаження мережі, пропускна здатність каналів і т.п.

- Завантаження. Активність мережевого ресурсу, маршрутизатора, каналу й т.д.

- Надійність. Надійність, відноситься до надійності каналу зв'язку. Деякі канали мережі можуть відмовляти частіше, ніж інші. Відмови одних каналів мережі можуть бути усунуті легше або швидше, ніж відмови інших каналів. При призначенні оцінок надійності можуть бути прийняті до уваги будь-які фактори надійності.

- Вартість. Налаштування роздільного значення.

Кожен маршрутизатор може мати дві різні таблиці маршрутизації: стандартна таблиця, що описує набір найкоротших шляхів до місця призначення, і альтернативна таблиця, що описує набір довших шляхів до місця призначення. Вибір між цими таблицями повинен бути зроблений у відповідності з наступним набором політик маршрутизації:

- пріоритетний трафік повинен бути спрямований по стандартному (найкоротшому) шляху, так як цей має більш високу ймовірність забезпечення необхідного рівня обслуговування;

- якщо мережа менш завантажена, трафік що залишився, може використовувати один і той же шлях, так як це не буде заважати роботі з більш високим пріоритетом;

- у міру збільшення навантаження на мережу будуть знайдені альтернативні шляхи, які будуть використовуватися вхідними агрегатними потоками з більш низьким пріоритетом, щоб відповідати рівню обслуговування вже активних потоків і використовувати незадіяні мережеві ресурси.

- у разі серйозного локального перевантаження існуючі агрегатні потоки з більш низьким пріоритетом, можливо, доведеться перенаправити на альтернативний шлях.

Мета маршрутизації при наявності певних обмежень зводиться до виконання наступних завдань: формування згідно з обраними критеріями і параметрами оптимальності набору маршрутів і розподіл по ним потоків трафіку. Серед параметрів оптимізації може бути мінімальна затримка доставки, максимальна пропускна здатність, мінімальна ціна, максимальна надійність або мінімальна ймовірність помилки. При чіткому розподілі навантаження можна управляти числом перевантажених ліній, у яких низька якість обслуговування.

Маршрутизація з урахуванням вимог трафіку має дві основні складові:

- створення набору допустимих маршрутів;

- розподіл трафіку за отриманими маршрутами відповідно до основних параметрів оптимізації.

Для отримання оптимального рішення необхідно одночасний розгляд усіх потоків на повному безлічі маршрутів.

1.2 Завдання маршрутизації

Завдання маршрутизації полягає у визначенні ефективних шляхів проходження потоків трафіку через мережу передачі даних.

Для цього найчастіше застосовується декомпозиція на три рівні:

- резервування необхідної пропускної здатності;

- визначення безлічі допустимих маршрутів;

- розміщення потоків за отриманими допустимими маршрутами.

Завдання першого рівня зводиться до визначення значення доступної пропускної здатності для додаткового трафіку певного класу сервісу через допустиму пропускну здатність лінії і значення реального проходження потоку трафіку по тій же лінії. Другий рівень загальної задачі маршрутизації вирішується за допомогою методу мінімально спрямованих графів (МСГ) для того, щоб знизити складність завдання шляхом накладання додаткових обмежень при пошуку допустимих маршрутів. В результаті побудови мінімального

спрямованого графа утворюється набір допустимих маршрутів, за яким необхідно розподілити потоки інформації. Це є завданням третього рівня.

Мінімізація перевантажень є первинним завданням. Тут мова йде не про короткочасні перевантаження, а про довгострокові, що впливають на поведінку мережі в цілому. Перевантаження зазвичай проявляється двояко:

- коли мережевих ресурсів недостатньо або вони не відповідають існуючому завантаженню;

- коли потоки трафіку неефективно розподілені по наявним ресурсам. Перший тип проблем перевантаження може бути вирішений шляхом:

- розширення ресурсу, або

- застосуванням класичних засобів управління перевантаженням, або

- поєднанням цих підходів.

Класичні способи управління перевантаженням намагаються регулювати запит таким чином, щоб трафік розподілявся на доступні ресурси. Ці способи включають в себе: обмеження потоку, управління шириною вікна для потоку, управління чергами в маршрутизаторі, диспетчеризацію тощо.

Другий тип проблем з перевантаженням, пов'язаний з неефективним розміщенням ресурсів, може бути вирішений за допомогою управління трафіком.

Взагалі, перевантаження, пов'язане з неефективним розміщенням ресурсів, може бути зменшене за допомогою політики балансування навантаження в різних фрагментах мережі. Завданням таких стратегій є мінімізація максимального перевантаження або навпаки мінімізація максимуму використання ресурсу. Коли перевантаження мінімізовано шляхом оптимального розміщення ресурсів, втрати пакетів і затримка доставки падають, а сукупна пропускна здатність зростає.

Таким чином, сприйняття кінцевим користувачем якості мережевого обслуговування стає краще.

1.3 Методи комутації

Будь-які мережі зв'язку підтримують деякий спосіб комутації своїх абонентів між собою. Цими абонентами можуть бути віддалені комп'ютери, локальні мережі, факс-апарати або просто співрозмовники, що спілкуються за допомогою телефонних апаратів. Практично неможливо надати кожній парі взаємодіючих абонентів свою власну фізичну лінію зв'язку, яка не комутується, і якою вони могли б монопольно "володіти" протягом тривалого часу. Тому в будь-якій мережі завжди застосовується який-небудь спосіб комутації абонентів, що забезпечує приступність наявних фізичних каналів одночасно для декількох сеансів зв'язку між абонентами мережі. На рис. 1.6 показана типова структура мережі з комутацією абонентів.

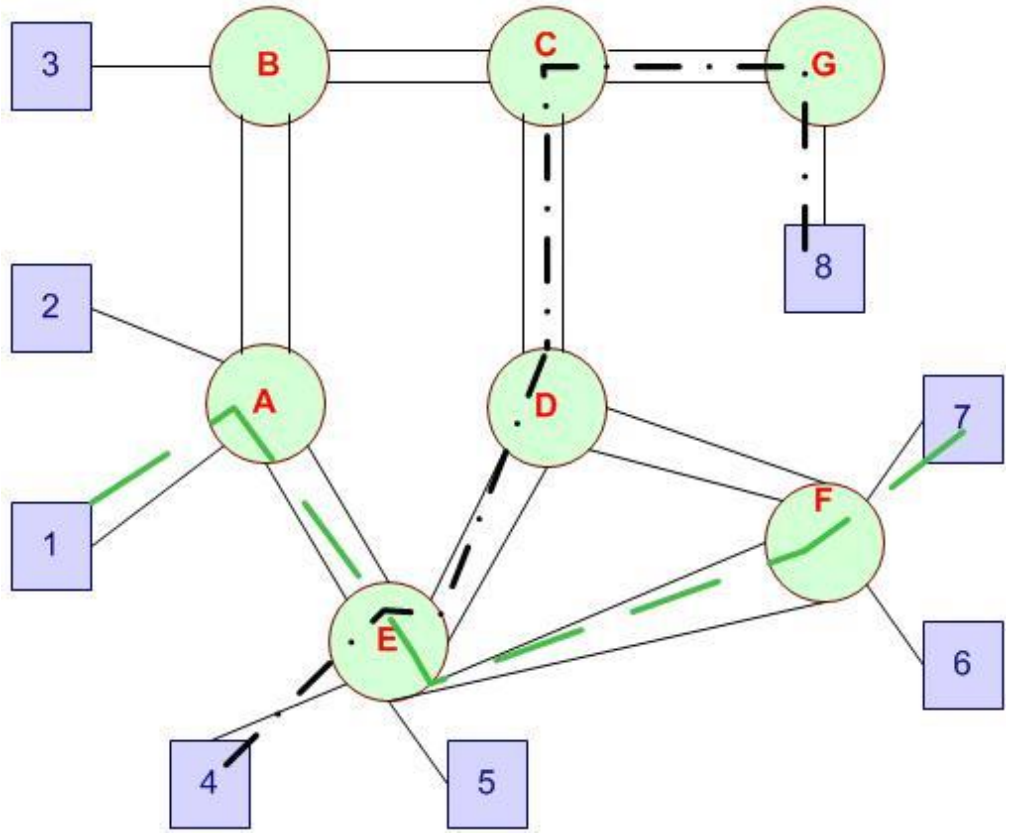

Рисунок 1.6 - Загальна структура мережі з комутацією

Абоненти з'єднуються з комутаторами індивідуальними лініями зв'язку, кожна з який використовується в будь-який момент часу тільки одним,

закріпленим за цією лінією абонентом. Між комутаторами лінії зв'язку розділяються декількома абонентами, тобто використовуються спільно.

Існують три принципово різні схеми комутації абонентів у мережах: комутація каналів (circuit switching), комутація пакетів (packet switching) і комутація повідомлень (message switching). Зовні всі ці схеми відповідають приведеній на мал. 1 структурі мережі, однак можливості і властивості їх різні. Мережі з комутацією каналів мають більш багату історію, вони ведуть своє походження від перших телефонних мереж. Мережі з комутацією пакетів порівняно молоді, вони з'явилися наприкінці 60-х років як результат експериментів з першими глобальними комп'ютерними мережами. Мережі з комутацією повідомлень послужили прототипом сучасних мереж з комутацією пакетів і сьогодні вони в чистому виді практично не існують.

Кожна з цих схем має свої переваги і недоліки, але за прогнозами багатьох фахівців майбутнє належить технології комутації пакетів, як більш гнучкої й універсальний.

Як мережі з комутацією пакетів, так і мережі з комутацією каналів можна поділити на два класи по іншій ознаці — на мережі з динамічною комутацією і мережі з постійною комутацією.

В першому випадку мережа дозволяє встановлювати з'єднання з ініціативи користувача мережі. Комутація виконується на час сеансу зв'язку, а потім (знову ж з ініціативи одного з взаємодіючих користувачів) зв'язок розривається. У загальному випадку будь-який користувач мережі може з'єднатися з будь-яким іншим користувачем мережі. Звичайно період з'єднання між парою користувачів при динамічній комутації складає від декількох секунд до декількох годин і завершується при виконанні визначеної роботи — передачі файлу, перегляду сторінки чи тексту зображення і т.п.

В другому випадку мережа не надає користувачу можливість виконати динамічну комутацію з іншим довільним користувачем мережі. Замість цього мережа дозволяє парі користувачів замовити з'єднання на тривалий період часу. З'єднання встановлюється не користувачами, а персоналом, що обслуговує

мережу. Час, на яке встановлюється постійна комутація, виміряється звичайно декількома місяцями (роками). Режим постійної комутації в мережах з комутацією каналів часто називається сервісом виділених (dedicated) чи орендованих (leased) каналів.

Прикладами мереж, що підтримують режим динамічної комутації, є телефонні мережі загального користування, локальні мережі, мережі TCP/IP.

Найбільш популярними мережами, що працюють у режимі постійної комутації, сьогодні є мережі технології SDH, на основі яких будуються виділені канали зв'язку з пропускною здатністю в декілька гігабіт у секунду. Деякі типи мереж підтримують обидва режими роботи. Наприклад, мережі X.25 і ATM можуть надавати користувачу можливість динамічно зв'язатися з будь-яким іншим користувачем мережі й у той же час відправляти дані по постійному з'єднанню одному цілком визначеному абоненту.

1.4 Якість обслуговування (QoS) в комп’ютерних мережах

QoS - це можливість надавати різні рівні обслуговування різним чином характеризуваним трафіком або потоком руху. Він є основою для пропонування різних класів обслуговування різним сегментам кінцевих користувачів, що дозволяє потім створювати різні рівні ціноутворення, які відповідають різним рівням CoS та QoS. QoS має важливе значення для розгортання в режимі реального часу трафіку, наприклад, голосових чи відеопослуг, а також для розгортання служб передачі даних.

QoS включає визначення вимог пропускної здатності мережі, контроль пріоритету користувача, контроль втрати пакета або стільника, а також контроль затримок як затримки транзиту (що відбувається в кінці), так і варіацій затримки трафіку (тобто тремтіння). Характеристики потоку руху включають визначення допуску затримки та еластичності для цього додатка. Вони також можуть пов'язувати стійкість до затримки та еластичність із програмами та користувачами та, можливо, навіть із сценаріями часу, дня тижня. Ми повинні мати можливість

забезпечувати різні рівні обслуговування; наявність пропускної здатності, затримки від кінця до кінця, відхилення затримки та втрати пакетів, що підтримують відповідну програму; і відносний пріоритет руху. Також QoS асоціюється з контролем дозволу на дотримання політики та з дотриманням правил руху потоків руху.

Інженерна рада інтернету (The Internet Engineering Task Force - IETF) намагається вирішити проблему відсутності QoS в Інтернеті шляхом визначення нових моделей послуг. Перша запропонована модель - Integrated Service (IntServ) - забезпечує суворі гарантії QoS, але погано масштабується для великих мереж. Модель диференційованого обслуговування (DiffServ) вирішила цю проблему і здатна забезпечити QoS для агрегованих потоків трафіку, класифікованих в обмежений набір класів обслуговування.

Є два способи реалізації QoS. Явний QoS означає, що програма вибирає необхідні QoS. Явний QoS означає, що менеджер мережі контролює це рішення.

Багатопротокольна комутація по мітках (MPLS) - це ще одне рішення, яке забезпечує підтримку QoS за допомогою можливостей проектування трафіку, пропонованих нижче мережевого рівня. Щодо QoS всі ці технології повинні співіснувати з мережею. Проте, Diffserv буде грати центральну роль, оскільки він масштабується до мережевого рівня, будучи незалежним від будь-яких технологій доступу або протоколів більш високого рівня.

На сьогоднішній день інтернет-маршрутизація фокусується на можливості підключення: протоколи маршрутизації, такі як Open Shortest Path First (OSPF) або RIP (Routing Information Protocol), здатні справлятися з порушеннями мережі, але не в змозі виконати накладені вимоги обслуговування. новим видом додатків. Трафік між двома кінцевими точками пересилається по одному і тому ж шляху, який зазвичай є найкоротшим, незалежно від стану мережі та вимог QoS пов'язаних потоків. Таким чином, на цих шляхах виникає перевантаження, і вимоги до обслуговування більше не можуть бути задоволені, незважаючи на існування альтернативних недостатньо використовуваних шляхів.

Для вирішення цих проблем було запропоновано кілька протоколів маршрутизації з урахуванням QoS. Якщо мережі передачі даних і телекомунікації зійдуться навколо NGN, проблеми з маршрутизацією QoS стануть дуже важкими для вирішення. Перш за все, ця конвергенція призводить до існування трафіку з різними обмеженнями QoS в одній і тій же мережі, і, згідно з цим, це може збільшити складність маршрутизації, так як пошук допустимого шляху з двома незалежними обмеженнями є повною проблемою NP. По-друге, оскільки стан мережі змінюється дуже часто, може бути важко збирати актуальну інформацію про стан, особливо в великомасштабних середовищах. Використання застарілої інформації по протоколу маршрутизації може погіршити продуктивність мережі. І, нарешті, мережа, в якій ресурси розподіляються між пріоритетами і трафіком Best Effort (BE), важка для управління. Хоча гарантії продуктивності можуть бути забезпечені в пріоритетному трафіку, за допомогою резервування ресурсів пропускна здатність трафіку не постраждає, якщо пропускна здатність мережі буде оптимізована, через втрату шляхів, які можуть використовуватися, зрештою, трафіком. Більшість пропозицій по маршрутизації QoS можуть працювати з інформацією про стан мережі, але не справляються з диференціацією послуг.

1.5 ATM QoS

ATM (asynchronous transfer mode — асинхронний спосіб передачі даних) QoS визначає чотири різні рівні обслуговування (один з яких має дві варіанти), які визначають серію конкретних параметрів QoS, які визначають ряд конкретних параметрів QoS що адаптує соти для розміщення відео, даних, голосу чи змішаного медіа-трафіку. Нижче наведено чотири класи обслуговування:

Постійна швидкість передачі даних (Constant bit rate - CBR) забезпечує постійну, гарантовану швидкість для додатків у режимі реального часу, таких як потокове відео, тому це безперервна смуга пропускання. Він імітує підхід з комутацією ланцюгів і пов'язаний з мінімальними затримками та втратами. CBR - це найвищий клас послуг, який ви можете отримати, і це для дуже вимогливих

програм, таких як потокове медіа, потокове аудіо, потокове відео та відео за запитом. Спочатку CBR потрібно було використовувати для таких речей, як голосова та відеоконференція, але було виявлено, що насправді в цих додатках не обов'язково потрібна безперервна смуга пропускання. Велика частина голосової розмови - це тиша. Якби переносили цю передачу через CBR, коли б там не було тиші, перемикачі ATM заповнювали б порожні соти, щоб підтримувати таку безперервну пропускну здатність, і, звичайно, це надмірність і витрата мережевих ресурсів.

Змінна швидкість передачі даних (Variable bit rate - VBR) BR має дві підмножини: в режимі реального часу (VBR-RT) і в режимі нереального часу (VBR-NRT). VBR забезпечує справедливу частку доступної пропускної здатності відповідно до конкретної політики розподілу, тому має максимальну стійкість до затримок і втрат. VBR - це найвищий клас сервісу в області даних, а також є класом обслуговування голосу в режимі реального часу. VBR-RT може використовуватися власним голосом ATM з стисненням пропускної здатності та придушенням тиші. Тож коли хтось мовчить, VBR-RT використовує наявну смугу пропускання для перенесення чужих сот, що робить VBR відповідним для мультимедійних функцій, таких як відеоконференції.

Доступна швидкість передачі даних (Available bit rate - ABR) підтримує трафік даних VBR із середніми та піковими параметрами трафіку (наприклад, з'єднання локальної мережі та послуги Інтернет-мережі, емуляція локальної мережі, передача критичних даних, що вимагає гарантій обслуговування). Виклики віддалених процедур, розподілені файлові послуги та обмін та пейджинг комп'ютерних процесів - приклади програм, які були б доречні для ABR.

Невизначена швидкість передачі даних (Unspecified bit rate - UBR) не надає гарантій на обслуговування, тому б використовували його для текстових даних, передачі зображень, обміну повідомленнями та розповсюдження інформації, яка є некритичною, коли вам не потрібно встановлювати встановлений час відповіді або гарантію обслуговування.

1.6 MPLS

Останнім словом у розвитку засобів маршрутизації і комутації для магістралей Інтернет стала розробка технології багатопротокольної комутації на основі міток (Multiprotocol Label Switching - MPLS). У ній збережено все краще, що притаманне архітектурі IP over ATM (ефективні мультиплексування і моделювання трафіку, висока продуктивність), і при цьому вона ще більше підвищує масштабованість мереж, спрощує їх побудову та експлуатацію. Важливо і те, що MPLS може використовуватися не тільки з ATM, але і з будьякою іншою технологією канального рівня.

Багатопротокольна комутація інформаційних потоків по мітках (Multiprotocol Label Switching, MPLS) - технологія швидкої комутації пакетів в багато протокольних мережах, заснована на використанні міток.

MPLS поєднує в собі можливості, властиві технологіям канального рівня (Data Link Layer 2), масштабованість і гнучкість протоколів, управління трафіком, характерні для мережевого рівня (Network Link Layer 3). Вибір даної технології обумовлений існуючими сьогодні вимогами обслуговування (QoS) і класів обслуговування (CoS) для додатків у всій мережі, а також вирішення питань масштабованості, керованості і безпеки.

Поява методів багаторівневої комутації і, в кінцевому рахунку, MPLS - це один з кроків на шляху еволюційного розвитку Інтернет в бік спрощення його інфраструктури шляхом інтеграції функцій другого (комутація) та третього (маршрутизація) рівнів. Всі методи багаторівневої комутації, в тому числі і MPLS, базуються на двох основних принципах: поділ функцій пересилання пакетів і управління цим процесом та пересилання пакетів з використанням послідовних міток.

MPLS є гарною платформою для того, щоб здійснити явну маршрутизацію, а також підтримати попередній розрахунок безлічі певних маршрутів для пари джерело - одержувач. Помічено, що комутація по розрахованим заздалегідь шляхах набагато швидче, ніж при визначенні нового маршруту (наприклад,

використовуючи алгоритм найкоротшого шляху), тому час відновлення відмови значно зменшується.

Багаторівнева комутація передбачає чіткий поділ всіх функцій по два компоненти: пересилання пакетів і управління. Керуюча компонента задіє стандартні протоколи маршрутизації (OSPF, IS-IS, BGP4) для обміну інформацією з іншими маршрутизаторами. На основі цієї інформації формується і модифікується спочатку таблиця маршрутизації, а потім, з урахуванням інформації про суміжних системах на кожному інтерфейсі - таблиця пересилання пакетів. Коли система отримує новий пакет, що пересилає компонента аналізує інформацію, що міститься в його заголовку, шукає відповідний запис в таблиці пересилання і направляє пакет на вихідний інтерфейс.

2 АНАЛІЗ МЕТОДІВ МАРШРУТИЗАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

2.1 Метод маршрутизації DARL

Метод DARL при ухваленні рішення про вибір наступного маршруту враховує ймовірність скидання пакету на тому чи іншому мережевому інтерфейсі, а також використовує пакети даних в якості службових повідомлень.

У разі методу DARL метрика є багатокритеріальною. Тому необхідно введення двох нових полів в таблицю маршрутизації: поле «Завантаженість», яке містить кількість пакетів, повернутих шлюзом на даному маршруті за певний проміжок часу, для обчислення якого служить значення в поле «Граничний час».

Підсумкова метрика розраховується за такою формулою:

$$M = \begin{cases} 0, \text{якщо } p = 1; \\ P + L + C, \text{якщо } p < 1, \end{cases} \tag{2.1}$$

де,

p - завантаженість мережевого інтерфейсу маршруту;

P - нормована завантаженість мережевого інтерфейсу;

L - нормована завантаженість маршруту;

C - нормована стандартна метрика маршруту.

Нормована завантаженість мережевого інтерфейсу розраховується за формулою:

$$P = 1 - p \tag{2.2}$$

Нормована завантаженість маршруту розраховується за формулою:

$$L = \begin{cases} 1, \text{якщо } l = 0 \\ \dfrac{1}{l}, \text{якщо } l > 1, \end{cases} \tag{2.3}$$

де,

l – завантаженість маршруту.

Нормована стандартна метрика маршруту розраховується за формулою:

$$C = {}^{1}/_{c}, \tag{2.4}$$

де,

c - метрика стандартного алгоритму.

Використання методу DARL дає наступні переваги:

1. Значне зменшення втрат будь-якого типу трафіку

2. Як наслідок, істотне збільшення продуктивності системи маршрутизації.

3. Зниження вартості доставки даних.

Недоліком методу є незначне збільшення фазового тремтіння цифрового сигналу даних при сильній завантаженості мережі.

$X_R^i=(0,...,X_{R,i+1}^i,...,X_{R,n-1}^i,...,X_{R,n}^i)(i=1,2,...,n-1)$ — двійковий вектор, пов'язаний з маршрутом R для викликів класу i.

Значення перших X_R^i елементів безлічі мають значення 0, а інші елементи $X_{R,j}^i$ $(j = i + 1, ..., n)$ визначаються як:

$$X_{R,j}^i = I\left[\Lambda\left(\frac{\tilde{C}_R - T_j}{b_j^{min(h)}}\right) - \Lambda\left(\frac{\tilde{C}_R - T_j - b_i^h}{b_j^{min(h)}}\right)\right], \tag{2.5}$$

де,

min (h) - означає кількість перельотів в маршруті, який являє собою мінімальний шлях хопу;

$\Lambda[(\tilde{C}_R - T_j)/b_j^{min(h)}]$ означає максимальну кількість викликів класу j (j> i), які можуть бути використані на маршруті R.

l (x) визначається наступним чином:

$$I(x) = \begin{cases} 0 & if \quad x = 0 \\ 1 & if \quad x > 0. \end{cases} \tag{2.6}$$

Тому $X_{R,j}^{i}$ є показником, який показує, чи є зниження максимальної кількості викликів класу j, які можуть бути прийняті за маршрутом R після того, як виклик і пройшов за маршрутом R. Значення $X_{R,j}^{i}$ для j = 1, ..., і встановлюються в 0, тому що ми розглядаємо тільки вплив запитів класу і на більш високих (чим клас і) типах сервісу.

Пропорційне значення M_j між доходами класу j і класу і (тут ми припускаємо, що більш високий клас сервісу має більш високий дохід, ніж нижчий клас) визначається наступним чином:

$$M_j = \frac{\textit{дохід для j запитів}}{\textit{дохід для і запитів}} \tag{2.7}$$

Далі, ми вводимо і строго визначаємо параметр β, який представляє собою компроміс між найкоротшим маршрутом і альтернативним маршрутом для типу сервісу і. Зокрема,

$$\beta_i = \exp\left(\frac{G\rho_i b_i^{\min(h)}}{\sum_{i=1}^{n}\rho_i b_i^{\min(h)}}\right), \tag{2.8}$$

де ρi = λi / μi і G є константою для найвищих типів сервісу n і визначаються наступним чином:

$$G = K\frac{\sum_{i=1}^{n}\rho_i b_i^{\min(h)}}{\rho_n b_n^{\min(h)}}. \tag{2.9}$$

де,

$\gamma_R = \max\{\gamma_l | \gamma_l = (C_l - \tilde{C}_l/C_l, l \in R, R \in S_l\}$ позначає саму найвикористовувану лінію на маршруті, і Ф (x, y) визначається як $\Phi(x,y) = \sqrt{xy}.$

Функція Ф (), яка використовувалася в попередніх відносинах, є складною функцією пропорційного параметра найкоротшого альтернативного маршруту і використовуваної ліній маршруту.

2.2 Метод маршрутизації MODR-S

MODR-S - альтернативний метод маршрутизації, який періодично оновлює таблиці маршрутизації. Він заснований на періодичних оцінках підсумкових транспортних потоків, базується на ієрархічній дворівневої багатоцільової моделі оптимізації маршрутизації мережі.

Завдання маршрутизації сформульовано у вигляді ієрархічної дворівневої багатоцільовий проблеми оптимізації, яка, на мережевому рівні, прагне максимізувати очікуваний дохід мережі та максимальне значення ймовірності блокування послуги, а на прикладному рівні - мінімізувати середню ймовірність блокування послуги та максимальну ймовірність блокування точка-точка для кожної послуги. Цільова функція на першому рівні є критерієм справедливості на мережевому рівні щодо всіх типів послуг, а цільові функції на другому рівні представляють критерії справедливості в межах кожного типу сервісу. Важливо відзначити, що перший рівень цільових функцій має пріоритет над другим рівнем.

Позначимо

Ck - ємність лінії lk;

C - вектор ємностей лінії Ck;

B - матриця ймовірностей блокування запиту B_{ks};

c - матриця випливають сполучних вартостей c_{ks};

$L_r^i(fs)$) - ймовірність блокування на маршруті $r^i(fs)$;

B_{ks} - ймовірність втрати запиту послуги s на лінії зв'язку l_k;

ρ_{ks} - - трафік, що висувається в лінію lk сервісними запитами s.

Нехай

$$\overline{d_k} = (d_{k1}, \ldots, d_{k|S|})$$

$$\overline{\rho_k} = (\rho_{k1}, \ldots, \rho_{k|S|})$$

Тоді $B_{ks} = \mathcal{L}_s\left(\overline{d_k}, \overline{\rho_k}, C_k\right)$

Багатоцільові моделі маршрутизації дають можливість вибору компромісних рішень серед чітких вимог QoS, моделі дозволяють точно представляти цільові функції, доречну для кожного транспортного потоку метрику.

2.3 Алгоритми маршрутизації комп’ютерних мереж

Існує кілька ключових підходів до класифікації алгоритмів маршрутизації. Алгоритми маршрутизації можна диференціювати, ґрунтуючись на декількох ключових характеристиках. По-перше, на роботу результуючого протоколу маршрутизації впливають конкретні завдання, які вирішує розробник алгоритму. По-друге, існують різні типи алгоритмів маршрутизації, і кожен з них по різному впливає на мережу і ресурси маршрутизації. І нарешті, алгоритми маршрутизації використовують різноманітні показники, які впливають на розрахунок оптимальних маршрутів.

Найбільш поширеним є підхід, в якому класифікація ґрунтується на тому, чи впливають зміни параметрів трафіку і стану ліній в мережі на обрані маршрути. На рис. 2.1 нижче представлена класифікація алгоритмів маршрутизації.

Рисунок 2.1 - Класифікація алгоритмів маршрутизації в комп’ютерних мережах

Існують такі способи передачі даних, при яких не потрібна наявність таблиць маршрутизації в пристроях. До таких відносить маршрутизації від джерела. В цьому випадку, при передачі даних повний маршрут прямування потоку трафіку по мережі формується в вузлі-джерелі у вигляді послідовності адрес тих вузлів, через які повинні пройти пакети, щоб досягти вузла-одержувача, і цілком включається до складу цих пакетів. В цьому випадку проміжні компоненти мережі при визначенні подальшого напрямку руху трафіку не приймають самостійно ніяких рішень, а виконують вказівки, що містяться в пакетах. Маршрутизація від джерела легко реалізується на проміжних вузлах в мережі, але вимагає повного знання всіх маршрутів на кінцевих компонентах. Через це кінцеві вузли повинні володіти високою продуктивністю, щоб зберігати всі таблиці маршрутизації. Це особливо стосується мереж з великою кількістю компонентів.

При однокрокової маршрутизації всі компоненти мережі, які беруть участь в передачі потоків, самостійно визначають, якому наступного вузла їх необхідно відправити. Рішення приймається на підставі аналізу знаходиться в пакеті адреси одержувача. При цьому повний маршрут для передачі трафіку складається з однокрокових рішень, прийнятих компонентами мережі. До таких технологій, наприклад, відноситься багатопротокольна комутація інформаційних потоків по мітках (Multiprotocol Label Switching, MPLS).

Залежно від способу формування таблиць маршрутизації, однокрокову маршрутизацію можна розділити на три класи (рис.2.1):

- проста (за замовчуванням);
- фіксована (статична);
- адаптивна (динамічна).

Проста (за замовчуванням) маршрутизація здійснюється за принципом пристроїв канального рівня (повторювачі, комутатори). У загальному випадку для простої маршрутизації на вибір подальшого шляху пакета впливає лише статична апріорний стан мережі. Її поточний стан: завантаження і зміна топології через відмови - не враховується. В алгоритмах простий маршрутизації таблиця маршрутизації або зовсім не використовується, або будується без участі протоколів маршрутизації. Є три види такого способу маршрутизації: випадкова маршрутизація, лавинна маршрутизація і маршрутизація з досвіду (рис.2.1.).

При випадковій маршрутизації кожен маршрутизатор (роутер), отримавши пакет, відправляє його на випадковий інтерфейс. Такий підхід не гарантує швидкого та якісного доставки пакета адресату. А в ряді випадків пакет позагально знищується при перевищенні TTL (Time Te Live) - часу життя. При лавинній маршрутизації роутер посилає пакет за всіма активними інтерфейсами (портам, підключеним до маршрутизатора). Недолік цього алгоритму - засмічення мережі інформацією.

При випадковій та лавинній маршрутизації не використовуються таблиці маршрутизації, в яких відображена топологія мережі на даний момент часу. У найзагальнішому випадку таблиця маршрутизації містить адресу мережі

призначення, адреса наступного вузла на шляху до цієї мережі і метрику (вартість) шляху.

При маршрутизації з досвіду шлюз накопичує інформацію про маршрути, пересилаючи дані лавинним чином. Після складання деякої таблиці, він вчиться направляти пакети по потрібному напрямку.

Алгоритми даного методу маршрутизації прості в реалізації, але при цьому не гарантують доставку пакета за вказаною адресою за прийнятний час і щодо раціонального маршруту без перевантаження мережі. Тому проста маршрутизація не знайшла застосування у великих мережах.

При реалізації фіксованої (статичної) маршрутизації використовується інформація про топологію мережі. При цьому методі здійснюється такий вибір маршрутів, при якому для передачі даних від джерела до адресата використовується єдиний маршрут, описаний в таблиці маршрутизації. Крім того, при завданні фіксованої маршрутизації повинні бути вказані всі взаємозв'язки між логічними мережами, які передбачаються залишатися незмінними. Вся робота по прописування шляхів в таблиці покладається на адміністратора мережі.

При розробці алгоритмів маршрутизації часто намагаються досягти одну або декілька з перерахованих нижче цілей:

- оптимальність;
- простота і низькі непродуктивні витрати;
- живучість і стабільність;
- швидка збіжність;
- гнучкість

Оптимальність.

Оптимальність є найбільш загальною метою розробки. Вона характеризує здатність алгоритму маршрутизації вибирати "найкращий" маршрут. Найкращий маршрут залежить від показників і від "ваги" цих показників, використовуваних при проведенні розрахунку. Наприклад, алгоритм маршрутизації міг би використовувати кілька пересилань з певною затримкою, але при розрахунку

"вага" затримки може бути їм оціненена як дуже значна. Звичайно, що протоколи маршрутизації повинні строго визначати свої алгоритми розрахунку показників.

Простота і низькі непродуктивні витрати.

Алгоритми маршрутизації розробляються якомога більш простими. Іншими словами, алгоритм маршрутизації повинен ефективно забезпечувати свої функціональні можливості, з мінімальними витратами програмного забезпечення і коефіцієнтом використання. Особливо важлива ефективність у тому випадку, коли програма, що реалізує алгоритм маршрутизації, повинна працювати в комп'ютері з обмеженими фізичними ресурсами.

Живучість і стабільність.

Алгоритми маршрутизації повинні мати живучість. Іншими словами, вони повинні чітко функціонувати в разі неординарних або непередбачених обставин, таких як відмова апаратури, умова високого навантаження і некоректні реалізації. Оскільки роутери розташовані в вузлових точках мережі, їх відмова може викликати значні проблеми. Часто найкращими алгоритмами маршрутизації виявляються ті, які витримали випробування часом і довели свою надійність в різних умовах роботи мережі.

Швидка збіжність.

Алгоритми маршрутизації повинні швидко збігатися. Збіжність - це процес згоди між усіма роутерами за оптимальними маршрутами. Коли якась подія в мережі приводить до того, що маршрути або відкидаються, або становляться доступними, роутери розсилають повідомлення про відновлення маршрутизації. Повідомлення про відновлення маршрутизації пронизують мережі, стимулюючи перерахунок оптимальних маршрутів і, як наслідок, змушуючи всі роутери дійти згоди по цих маршрутах. Алгоритми маршрутизації, які збігаються повільно, можуть привести до утворення петель маршрутизації або виходів з ладу мережі.

Гнучкість.

Алгоритми маршрутизації повинні бути також гнучкими. Іншими словами, алгоритми маршрутизації повинні швидко і точно адаптуватися до різноманітних обставин в мережі. Наприклад, припустимо, що сегмент мережі відкинутий.

Багато алгоритмів маршрутизації, після того як вони дізнаються про цю проблему, швидко вибирають наступний найкращий шлях для всіх маршрутів, які зазвичай використовують цей сегмент. Алгоритми маршрутизації можуть бути запрограмовані таким чином, щоб вони могли адаптуватися до змін смуги пропускання мережі, розмірів черги до роутера, величини затримки мережі та інших змінних.

Протоколи маршрутизації призначені для автоматичної побудови таблиць маршрутизації, які використовуються для просування пакетів даних.

Алгоритми маршрутизації можна умовно розділити на дві великі групи: одношляхова маршрутизація і багатошляхова. При одношляховій маршрутизації передача інформації здійснюється по одному каналу зв'язку, при багатошляховій, як можна зрозуміти з назви, для передачі трафіку одночасно використовується кілька маршрутів до одного одержувача. Одними з найважливіших вимог, що пред'являються до протоколів маршрутизації, є надійність і відмовостійкість.

Цим критеріям ефективно задовольняють методи багатошляхової маршрутизації. З цієї причини розробці і дослідженню алгоритмів передачі даних одночасно за кількома маршрутами присвячено безліч наукових робіт. Заслужений інтерес до багатошляхової маршрутизації виявлений завдяки тому, що вона забезпечує стабільність, балансування навантаження, запобігання перевантажень і оптимальне використання ресурсів мережі.

Існують два великі класи алгоритмів маршрутизації: статичні і динамічні. Статичні алгоритми приймають рішення тільки на основі даних, які не змінюються з плином часу. Динамічні алгоритми постійно оновлюють свої локальні структури для оптимізації вибору маршрутів.

Принципова різниця між ними - в ступені обліку зміни топології і навантаження мережі при вирішенні завдання вибору маршруту.

Статична маршрутизація передбачає знаходження декількох шляхів між кожною парою джерело-одержувач заздалегідь. Дані маршрути записуються в таблицю маршрутизації і використовуються при передачі даних. Як правило, такі алгоритми дозволяють враховувати кілька критеріїв при виборі маршруту, але

володіють великою обчислювальною складністю, а, отже, і меншою гнучкістю при зміні навантаження в мережі. Такі алгоритми використовуються в високостабільних надійних мережах, де зміни відбуваються досить рідко і потрібний чіткій заданий коефіцієнт готовності.

Найбільшого поширення набула адаптивна (динамічна) маршрутизація, яка застосовується в великих мережах з різними за характеристиками каналами і надлишковими лініями. При такій маршрутизації враховується і зміна завантаження, і зміна топології, крім того, в процедурі вибору маршруту дозволяється використовувати більше одного шляху. Динамічна маршрутизація передбачає, що маршрутизатор може сам визначати нові шляхи, або модифікувати інформацію про старих.

Адаптивна маршрутизація виконує дві важливі функції:

-динамічне виявлення маршрутів, так що не потрібно попереднє налаштування кінцевих систем і маршрутизаторів між ними при кожній зміні топології;

- припустима зміна маршрутів при виникненні перевантажень або несправностей на лінії, в результаті чого може бути досягнута ефективне балансування навантаження;

Але, тим не менше, динамічна маршрутизація має певні недоліки:

- ускладняється вибір маршрутів, тому маршрутизаторів доводиться більше часу витрачати на обробку інформації;

- в більшості випадків алгоритми адаптивної маршрутизації залежать від інформації про стан мережі, зібраної в одному місці, але використовуваної в іншому. Виникає проблема вибору між якістю цієї інформації і кількістю витрачених ресурсів для її обслуговування. Чим більший обсяг інформації, яким обмінюються маршрутизатори, і чим частіше вони нею обмінюються, тим краще будуть рішення про вибір маршрутів, прийнятих кожним вузлом. Але з іншого боку, ця інформація сама надає навантаження на мережі, викликаючи зниження продуктивності;

- реакція на зміни, що виникають при адаптивної маршрутизації, може виявитися занадто швидкою, що може привести до великого обсягу службової інформації, що викликають перевантаження, або занадто повільною, тобто не встигає за змінами.

- застосування адаптивної стратегії може привести до небажаних ефектів, таким як, наприклад, зациклення.

Динамічні протоколи засновані на лавинних алгоритмах маршрутизації і алгоритмах маршрутизації від джерела і здатні динамічно реагувати на зміни топології мережі. Одним з таких протоколів є Ad hoc On Demand Distance Vector (AODV).

Динамічні протоколи маршрутизації, що застосовуються в даний час в обчислювальних мережах, діляться на три групи, кожна з яких пов'язана з одним з наступних типів алгоритмів:

- дистанційно-векторні протоколи (Distance Vector Algorithms, DVA);

- протоколи стану каналу (Link State Algorithms, LSA);

- гібридні протоколи.

У протоколах дистанційно-векторного типу кожен маршрутизатор періодично і широкомовно розсилає по мережі вектор, компонентами якого є відстані від даного маршрутизатора до всіх відомих йому мереж. Під відстанню зазвичай розуміється число переходів. Можлива й інша метрика, що враховує не тільки число проміжних маршрутизаторів, а й час проходження пакетів по мережі між сусідніми маршрутизаторами. При отриманні вектору від сусіда маршрутизатор нарощує відстані до вказаних у векторі мереж на відстань до даного сусіда. Отримавши вектор від сусіднього маршрутизатора, кожен маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він дізнався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектору по мережі. Кожен маршрутизатор дізнається інформацію про всі наявні в інтермережі мережах і про відстань до них через сусідні маршрутизатори.

Протоколи стану каналу забезпечують кожен маршрутизатор інформацією, достатньою для побудови точного графа зв'язків мережі. Всі маршрутизатори працюють на основі однакових графів, що робить процес маршрутизації стійкішим до змін конфігурації. Широкомовна розсилка використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто. Вершинами графа є як маршрутизатори, так і об'єднані ними мережі. Інформація, що розповсюджується по мережі складається з опису зв'язків різних типів: маршрутизатор - маршрутизатор, маршрутизатор - мережа. Гібридні протоколи працюють за принципами дистанційно-векторних протоколів, але будують таблиці маршрутизації, як протоколи стану каналу.

Гібридні протоколи працюють за принципами дистанційно-векторних протоколів, але будують таблиці маршрутизації, як протоколи стану каналу.

Крім цього, можна виділити чотири види адаптивної маршрутизації: локальна, розподілена, централізована, змішана.

З точки зору розробки і реалізації, найбільш простими є такі методи адаптивної маршрутизації, які будують свої рішення тільки на підставі локально доступною в кожному вузлі інформації. Ці методи відносяться до локальної адаптивної маршрутизації. Інформація, необхідна для прийняття рішення, являє собою заздалегідь завантажені в вузли таблиці маршрутизації, відомості про поточний стан вихідних трактів вузла (відкриті або закриті) і довжинах черг пакетів, які мають бути надіслані по кожному з каналів. Інформація про стан інших компонентів мережі вузлом не використовується. Алгоритм маршрутизації обирає найкращий маршрут з безлічі можливих, заданих таблицями маршрутизації. Цей вибір робиться за допомогою обчислень, що ґрунтуються на відомостях про довжини черг і топології мережі, що відображають перевагу найкращим каналам для досягнення того чи іншого вузла призначення. Недоліком такого методу є обмежена адаптація до змін різного роду в мережі, а також відсутність обміну даними про маршрутизації між вузлами.

Розподілена адаптивна маршрутизація характеризується тим, що вузли між собою обмінюються інформацією, що стосується подальшого розподілу даних. В

результаті, після отримання інформації, кожен вузол заново підраховує таблицю маршрутизації. Рішення про вибір того чи іншого маршруту для передачі трафіку всередині підмережі приймають внутрішні (локальні) маршрутизатори цієї підмережі, а поза підмережі - зовнішні (магістральні) маршрутизатори.

Через постійний обмін інформацією між вузлами в мережі можуть виникати перевантаження. Крім цього, при використанні розподіленої адаптивної маршрутизації з'являються проблеми, що виникають при відключенні одного з вузлів від мережі, - Count to Infinity (рахунок до нескінченності). Таке виходить після відключення однієї з мереж, коли сторонній роутер оповіщає сусіда, що відключена мережу доступна через нього (в разі, якщо сусід не встигне оповістити маршрутизатор про недоступність мережі).

Даний метод маршрутизації використовується в протоколі маршрутизації RIP, який називається також методом рельєфів. Він заснований на алгоритмі Беллмана-Форда і використовується переважно на нижніх рівнях ієрархії мережі.

У розподіленої маршрутизації можна виділити два алгоритми. Алгоритми стану каналу (Link State Algorithm, LSA) направляють потоки маршрутної інформації в усі вузли об'єднаної мережі. Однак кожен роутер посилає тільки ту частину маршрутної таблиці, в якій міститься інформація про найближчих сусідів і мережах, а також відомості про метриці для кожного свого з'єднання. Потім, застосовуючи алгоритм найкоротшого шляху (shortest path first - SPF), який більш відомий як алгоритм Дейкстра, маршрутизатори обчислюють дерево найкоротших маршрутів до кожного віддаленого вузла, поміщаючи себе в корінь цього дерева.

Алгоритми вектора відстані або дистанційно-векторні (Distance Vector Algorithm, DVA) вимагають від кожного маршрутизатора посилки всієї або частини своєї маршрутної таблиці, але тільки своїм сусідам. Вузол оцінює дистанцію до кожного сусіда і розсилає її своїм сусідам, які в свою чергу виконують те ж саме. Під дистанцією або відстанню зазвичай розуміється кількість переходів, пересилань між компонентами мережі (хопи), які необхідно подолати, щоб досягти одержувача, хоча можлива наявність і інших метрик, що

включають швидкість і або вартість передачі пакета по лінії зв'язку. При формуванні таблиці маршрутизації в неї вносяться зміни, так щоб в ній містилися тільки маршрути з найкоротшими відстанями. Основна перевага алгоритму вектору відстаней - його простота. Дійсно, в процесі роботи маршрутизатор спілкується тільки з сусідами, періодично обмінюючись з ними копіями своїх таблиць маршрутизації. Слабка сторона алгоритму вектору відстаней – повільна конвергенція, що може стати причиною утворення петель і "чорних дірок" при зміні топології мережі.

Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. У великих же вони завантажують лінії зв'язку інтенсивним широкомовним трафіком.

Відрізняючись більш швидкої збіжністю, алгоритми стану каналів трохи менше схильні до утворення петель маршрутизації, ніж алгоритми вектору відстані. З іншого боку, алгоритми стану каналу характеризуються більш складними розрахунками в порівнянні з алгоритмами вектору відстаней, вимагаючи більшої процесорної потужності та пам'яті, ніж алгоритми вектору відстаней. Крім того, дистанційно-векторні алгоритми володіють таким недоліком, як проблеми зростання до нескінченності (Count to Infinity). Вона є основною причиною завдання обмежень на максимальну довжину шляху в усіх протоколах вектору відстані. Протоколи, в основі яких лежать алгоритми стану каналу, дають можливість кожному вузлу самостійно обмінюватися інформацією з усіма маршрутизаторами і отримувати уявлення про топологію мережі. Саме тому цього алгоритму не властиві проблеми зростання до нескінченності, а жорсткі обмеження на діаметр мережі відсутні. Вузьким місцем такого підходу є необхідність обов'язкової синхронізації баз даних всіх маршрутизаторів в межах автономної системи. Якщо різні вузли будуть по-різному уявляти собі топологію мережі, з якої вони працюють, то це призведе до утворення петель і до інших проблем. Ще однією перевагою алгоритмів аналізу стану каналу є поліпшена ієрархічна структура (до-пускається розбиття домена на рівні або області), що дозволяє краще виявляти нестабільні ділянки.

Питання, що обговорювали адаптивні алгоритми маршрутизації використовують для своєї роботи або локальну інформацію, яку інформацію, отриману в процесі обміну з сусідніми вузлами. Алгоритми такого типу дуже повільно адаптуються до віддалених подій в мережі, що є наслідком малої швидкості поширення маршрутної інформації по мережі. Тому розробники алгоритмів шукали методи, що засновують свої рішення на інформації про стан всієї мережі. Одним із способів формування уявлення про стан всієї мережі є організація в мережі центру маршрутизації. І тоді мережа буде функціонувати за принципом централізованої адаптивної маршрутизації.

При такій маршрутизації кожен вузол мережі готує повідомлення про свій стан, в якому міститься інформація про поточні довжинах черг, працездатності трактів і т. д.; ці повідомлення будуть надсилатися центру маршрутизації мережі. Із сукупності таких повідомлень центральний вузол становить глобальну картину стану мережі, користуючись якою він може визначити найкращі маршрути для трафіку в мережі. Ці маршрути оформляються у вигляді таблиць маршрутизації, які розсилаються всім вузлам мережі, що знаходяться на певному маршруті.

Залежно від способу збору інформації про стан мережі і розсилки керуючих директив режим маршрутизації в мережі може бути синхронним і асинхронним. Якщо всі вузли посилають свої повідомлення і отримують вказівки центрального вузла через регулярні інтервали часу, то такий спосіб управління трафіком називається синхронним; якщо такі дії здійснюються лише при істотних змінах в мережі, цей спосіб управління називається асинхронним. При синхронному режимі обсяг службової інформації, переданої для цілей маршрутизації, може бути занадто великим, особливо для мереж великої розмірності, і це призводить до великих витрат на маршрутизацію. Асинхронний режим може бути реалізований при значно меншому потоці службової інформації.

Як і всі інші методи, централізована адаптивна маршрутизація не позбавлена своїх недоліків, до яких можна віднести концентрацію службового трафіку біля центру маршрутизації; низьку надійність мережі при відмові

центрального вузла або при ізоляції від нього ділянки мережі; отримання вузлами таблиць маршрутизації в різний час з різною затримкою.

Змішана адаптивна маршрутизація характеризується тим, що рішення про вибір маршруту приймається в вузлах комутації з урахуванням рекомендацій центру управління.

Деякі алгоритми маршрутизації оперують в плоскому просторі, в той час як інші використовують ієрархії маршрутизації. У однорівневій маршрутизації всі роутери рівні по відношенню один до одного. У ієрархічній маршрутизації деякі маршрутизатори формують те, що становить основу (backbone - базу) маршрутизації. Пакети з небазових роутерів переміщаються до базових і пропускаються через них до тих пір, поки не досягнуть загальної області пункту призначення. Починаючи з цього моменту, вони переміщаються від останнього базового маршрутизатора через один або дещо небазових маршрутизаторів до кінцевого пункту призначення. Тобто існує схема розбивки великої мережі на ієрархічну систему підмереж з власної маршрутизацією всередині кожного рівня. У дуже великих мережах можуть існувати додаткові ієрархічні рівні. Роутери найвищого рівня ієрархії утворюють базу маршрутизації. Основною перевагою ієрархічної маршрутизації є те, що вона імітує організацію більшості компаній і, отже, дуже добре підтримує їх схеми трафіку.

2.4 Протоколи маршрутизації

Вибір протоколу маршрутизації в значній мірі залежить від наступних факторів.

- Топологія і складність мережі. Необхідно передбачити наявність резервних ліній зв'язку в мережі, що забезпечують її надійне функціонування (доступність серверів і мережевих сегментів) в разі відмов мережевого обладнання та основних ліній зв'язку. Наприклад, при деревовидній топології мережі з так званим «кореневим маршрутизатором», можливості динамічної маршрутизації зводяться до мінімуму.

- Розміри мережі і необхідність в її подальшому масштабування. Можливості деяких протоколів в цьому сенсі обмежені.

- Завантаженість мережі. Для мереж з високим коефіцієнтом завантаженості ліній зв'язку має значення здатність протоколу до перерозподілу потоків даних.

- Вимоги до надійності мережі. Допустимий час простоїв або нестабільності в роботі мережі через відмову її вузлів залежить від роду діяльності організації, і визначається можливими фінансові збитками або небезпекою порушення виробничого циклу.

- Вимоги до захисту інформації в мережі. Ці вимоги визначаються ступенем ризику, пов'язаного з потраплянням інформації про адреси і маршрутах в мережі в руки зловмисників, що особливо важливо для мереж, що мають зовнішні канали зв'язку.

- Необхідність підключення маршрутизації сегмента до вже існуючої мережі. В цьому випадку слід звернути увагу на сумісність протоколів маршрутизації і засобів їх реалізації.

- Можливість організації програмних маршрутизаторів. При невеликому трафіку в мережі або на окремих її ділянках від маршрутизаторів не потрібна висока продуктивність. У таких випадках з економічної точки зору буває вигідніше використовувати замість апаратного маршрутизатора універсальний комп'ютер з декількома мережевими картами і програмним забезпеченням (ПЗ) з функціями протоколів маршрутизації. Однак не для всіх протоколів маршрутизації є відповідне ПЗ, а від складності протоколів залежить кількість споживаних обчислювальних ресурсів комп'ютера.

- Кваліфікація і суб'єктивні переваги обслуговуючого персоналу. Складність налаштування маршрутизаторів і адміністрування мережі при використанні різних протоколів суттєво відрізняються. При наявності необхідних можливостей в декількох протоколах важливо врахувати зручність і наявність досвіду роботи з одним з протоколів в адміністратора мережі.

2.5 Критерії порівняння протоколів маршрутизації

Так як адаптивна маршрутизація є найбільш поширеною, то і протоколи адаптивної маршрутизації користуються найбільшою популярністю. До таких протоколів відносять RIP, OSPF, IS-IS, BGP та ін.

Для визначення ефективного протоколу маршрутизації, який би задовольняв вимогам конкретної мережі, необхідно провести порівняльний аналіз найбільш відомих протоколів динамічної маршрутизації.

Протоколи маршрутизації діляться на два основні класи: протоколи внутрішніх шлюзів (Interior Gateway Protocols - IGP) і протоколи зовнішніх шлюзів (Exterior Gateway Protocols - EGP). Протоколи класу IGP проектувалися для обміну інформацією про мережі та підмережі між внутрішніми маршрутизаторами однієї автономної системи (Autonomous System - AS), тобто між маршрутизаторами, що знаходяться під єдиним адміністративним керуванням, і використовують один протокол маршрутизації. Такими мережами можуть бути мережі провайдерів послуг Internet, великих урядових і науководослідних організацій, приватних комерційних концернів. Протоколи EGP проектувалися для обміну маршрутною інформацією між прикордонними маршрутизаторами різних автономних систем. Домінуючим EGP-протоколом сьогодні є протокол граничної маршрутизації версії 4 (Border Gateway Protocol version 4 - BGP-4). Цей протокол використовується для обміну маршрутною інформацією між AS мережі Internet.

За методом поширення маршрутної інформації протоколи IGP діляться на дистанційно-векторні і стану каналів зв'язку.

У методі вектору відстаней кожен маршрутизатор через рівні проміжки часу посилає сусіднім маршрутизаторам оновлення всієї або частини своєї таблиці маршрутизації. У міру поширення маршрутної інформації в мережі кожен маршрутизатор може обчислити відстані від нього до всіх мереж і підмереж в межах внутрішньо-корпоративної мережі. Найбільш поширеними протоколами

даного типу є RIP (Routing Information Protocol) і IGRP (Interior Gateway Routing Protocol).

У методі обліку стану каналів зв'язку кожен маршрутизатор корпоративної мережі посилає іншим маршрутизаторів інформацію про своїх безпосередніх з'єднаннях з мережами і маршрутизаторами. На основі отриманої інформації, кожен маршрутизатор здатний побудувати її повний топологічний граф, а потім заповнити свою таблицю, використовуючи складний алгоритм вибору першого найкоротшого шляху (Shortest Path First - SPF). Найбільш відомими протоколами даного типу є OSPF (Open Shortest Path First) і IS-IS (Intermediate System to Intermediate System). Існують також гібридні протоколи, що поєднують в собі переваги обох методів поширення маршрутної інформації. Прикладом гібридного протоколу є EIGRP (Enhanced Interior Gateway Routing Protocol).

Протоколи, засновані на методі вектору відстані, вимагають менше обчислювальних ресурсів маршрутизатора, ніж протоколи з вибором станом каналів зв'язку з їх складними SPF-алгоритмами. З іншого боку, протоколи з вибором стану каналів зв'язку займають меншу частину смуги пропускання мережі (крім початкового етапу вивчення топології мережі) так, як вони поширюють тільки інформацію про зміни, а не всю таблицю маршрутизації, що особливо важливо для великих мереж.

В якості інших критеріїв порівняння протоколів динамічної маршрутизації можна виділити наступні.

- швидкість збіжності. Ця характеристика протоколу визначає тривалість тимчасового інтервалу можливої нестабільної роботи мережі, в перебігу якого протокол виявляє недоступний маршрут, вибирає новий маршрут і поширює нову інформацію по мережі. Швидкість реакції на зміни в мережевий топології особливо важлива при підтримці важливих додатків, що вимагають високого ступеня готовності мережі. Протоколи, засновані на методі вектору відстані, вимагають більшого часу для збіжності, ніж протоколи з вибором станом каналу зв'язку, тому що інформація про новий шляху передається від одного

маршрутизатора до іншого побічно без вказівки джерела її походження в процесі періодичних розсилок;

- можливість обліку в метриці (критерії) вибору найбільш раціонального маршруту різних характеристик маршруту. Метрики можуть розраховуватися на основі однієї або кількох характеристик шляху. До найбільш вживаним характеристикам шляху відносяться:

- кількість переходів (проміжних маршрутизаторів в дорозі);

- пропускна здатність каналів зв'язку;

- затримка пакета в дорозі;

- надійність (частота виникнення помилок каналах зв'язку);

- навантаження (завантаженість маршрутизаторів і каналів зв'язку);

- вартість (довільне значення, яка призначається адміністратором на підставі як перерахованих вище, так і інших міркувань, наприклад фінансових).

Метрики, що обчислюються на основі декількох показників, забезпечують більшу гнучкість при виборі маршруту. Можливості протоколу підтримувати одночасно кілька метрик дозволяють задовольняти вимоги QoS-трафіку (Quality of Service) різних додатків.

- можливість балансування навантаження між декількома маршрутами. Можливість зберігання в таблицях маршрутизації декількох маршрутів до однієї мережі (з рівними або навіть відрізняються метриками) дає можливість маршрутизатора знижувати завантаження ліній зв'язку, шляхом поперемінного відсилання пакетів по кожному з маршрутів. Слід звернути увагу на те, що балансування навантаження може викликати проблеми в тих випадках, коли додаток використовує дейтаграмні протоколи канального і транспортного рівнів, що не нумерують і, отже, не відновлюють порядок проходження пакетів, як це робить, наприклад, транспортний протокол із установленням з'єднання TCP;

- можливість об'єднання маршрутів на співпадаючих ділянках. Наявність даної функції сприяє зниженню відносної складності великої мережі, скорочення кількості записів в таблицях маршрутизаторів і прискоренню пошуку в них. Об'єднання маршрутів вимагає, щоб протокол маршрутизації підтримував маски

підмереж змінної довжини і був здатний поширювати інформацію про мережеві маски разом з інформацією про мережеві маршрути.

- максимальна кількість маршрутизаторів в мережі визначає можливості її масштабування. Це обмеження побічно пов'язане з іншими характеристиками протоколу маршрутизації, що впливають на його здатність працювати у великій мережі (наприклад, швидкістю збіжності, часткою смуги пропускання мережі, необхідної для передачі службових повідомлень протоколу);

- необхідність попередньої логічної підготовки мережі. Деякі протоколи маршрутизації для досягнення відповідного рівня масштабування (зменшення споживання обчислювальних ресурсів маршрутизаторів і пропускної здатності мережі) мають на увазі виділення в мережі логічних областей і зв'язків між ними. впровадження таких протоколів може зажадати серйозної інженерного пропрацювання проекту мережі (її топології та схеми адресації);

- забезпечення безпеки при обміні маршрутною інформацією. Якщо мережа підтримує обмін маршрутною інформацією між підмережами, з'єднаними глобальними зв'язками, то потрапляння такої інформації в руки зловмисників може становити загрозу безпеці мережі. У таких випадках підтримка протоколом маршрутизації методів аутентифікації джерела і шифрування маршрутної інформації набуває важливого значення.

- доступність програмного забезпечення (ПЗ) реалізації протоколу маршрутизації. Протоколи можуть бути відкритими і підтримуватися різними виробниками апаратних маршрутизаторів і ПО для універсальних комп'ютерів, а можуть бути закритими і реалізуватися тільки певними компаніями;

- перспективність - реалізація в протоколі перспективних можливостей (наприклад, протоколу IP6, підтримка трафік інжинірингу).

2.6 Характеристика протоколів маршрутизації

2.6.1 Протокол маршрутизації на базі вектора відстаней – RIP

Одним з найбільш поширених протоколів маршрутизації на основі вектору відстаней, є протокол RIP (Routing Information Protocol). Основні характеристики протоколу RIP:

- дистанційно-векторний протокол маршрутизації; метрика – число переходів;

- максимальне число переходів - 15;

- широкомовна розсилка маршрутизації за замовчуванням - раз в 30 секунд.

RIP призначений для роботи з мережами середнього розміру, що використовують однорідну технологію. Практично використання RIP обмежена мережами, найдовший шлях якого не перевищує 15 стадій.

При запуску маршрутизатор, який підтримує RIP, дізнається з файлів конфігурації, до яких мереж він безпосередньо підключений. Він записує цю інформацію в свою таблицю маршрутизації і розсилає її у вигляді групових повідомлень всім підключеним мережам. Решта маршрутизаторів на цих мережах отримують і записують отриману інформацію в свої таблиці маршрутизації. При наступному обміні інформацією кожен з маршрутизаторів передає свою оновлену таблицю маршрутизації. Інформація передається через фіксовані проміжки часу (30 с), хоча розширення «критичний RIP» дозволяє робити це відразу ж після зміни локальної конфігурації.

Версія 2 RIP, що підтримує маршрути CIDR, не змінює самого протоколу, а вводить розширення в формат повідомлення, яке дозволяє маршрутизаторам колективно використовувати важливу додаткову інформацію.

І хоча RIP не призначений для виконання ролі EGP, він іноді використовується для маршрутизації між автономними системами (АС). Центральні комп'ютери (хости) можуть також використовувати RIP як протокол розпізнавання маршрутизаторів. Такі комп'ютери переглядають («слухають») як

проходить трафік RIP і використовують видобуту з нього інформацію розпізнавання маршрутів для прийняття рішення про вибір конкретного маршрутизатора для використання в якості першої стадії.

Головною перевагою протоколу є легкість конфігурування, що не вимагає високої кваліфікації обслуговуючого персоналу. Протокол є відкритим і підтримується практично всіма виробниками мережевого устаткування.

До недоліків RIP слід віднести:

- таблиці маршрутизації надсилаються повністю і по груповій адресі.

- повільна збіжність і великий обсяг службового трафіка (для адаптації до змін в топології мережі маршрутизатори періодично розсилають повні копії своїх таблиць). Це обмежило сферу застосування протоколу мережами з кількістю маршрутизаторів не більше п'ятнадцяти;

- при відключенні мережі маршрутизатори не отримують про це своєчасної інформації;

- для маршрутизації вибирається шлях з найменшим числом проміжних маршрутизаторів, але не найшвидший або дешевий.

І хоча нові досконаліші протоколи OSPF і IS-IS в цілому перевершують RIP, в невеликих мережах він має ряд переваг, забезпечуючи там менше перевантаження з точки зору використовуваної смуги пропускання і часу адміністративного управління. RIP дуже легко реалізувати особливо в порівнянні з новітніми IGP і витрати на нього швидко окупаються.

Повідомлення RIP містить мінімум маршрутної інформації та великий обсяг вільного місця, що належить відправнику.

Крім того, реалізацій RIP набагато більше, ніж, наприклад, комбінованого використання OSPF і IS-IS OSI. Очікується, що використання RIP продовжиться ще протягом декількох років.

У сучасних мережах протокол RIP не найкраще рішення для вибору в якості протоколу маршрутизації, так як його можливості поступаються більш сучасним протоколам, таким як EIGRP і OSPF. Обмеження на 15 переходів (хопів) не дозволяє застосовувати його у великих мережах. Перевага цього протоколу

являється простота конфігурації. Тому, якщо мережа невелика, то протокол RIP цілком прийнятний як протокол маршрутизації.

2.6.2 Протокол маршрутизації IGRP

Закритий дистанційно-векторний протокол IGRP компанії Cisco Systems був спроектований для усунення ряду недоліків протоколу RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з відмінними характеристиками смуги пропускання і величини затримки. Протокол використовує комбіновану метрику, яка включає затримку, смугу пропускання, надійність і завантаженість маршруту. Вагові коефіцієнти, що визначають внесок цих характеристик в результуючу метрику, задаються користувачем, забезпечуючи гнучку адаптацію до його конкретним завданням. Показники затримки і смуги пропускання конфігуруються для кожної лінії зв'язку попередньо, а показники надійності і завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі. Для підтримки вимог QoS різних додатків можна підготувати кілька маршрутних таблиць, побудованих на основі метрик з різними значеннями вагових коефіцієнтів.

Протокол IGRP забезпечує швидшу збіжність, ніж RIP завдяки застосуванню пакетів оновлення з миттєвою розсилкою (інформація про зміни в мережі відправляється відразу, як тільки стає доступною, не чекаючи чергового часу поновлення). Протокол підтримує балансування навантаження між декількома маршрутами навіть в тому випадку, якщо їх метрики не рівні, але знаходяться в межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів відправлених по кожній колії даних буде пропорційно співвідношенню їх метрик.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини і можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні кошти

аутентифікації при обміні маршрутною інформацією. Непрямим засобом захисту є можливість прийому повідомлень про оновлення маршрутів тільки від тих маршрутизаторів, які даний визначає як «сусідні», а також можливість внесення змін в конфігурацію маршрутизатора тільки на підставі пароля, який зберігається в зашифрованому вигляді. Протокол сумісний з RIP.

2.6.3 Вдосконалений протокол маршрутизації на базі вектору відстаней - EIGRP

Вдосконаленим протоколом маршрутизації на базі вектору відстаней є протокол EIGRP. Він був розроблений компанією Cisco Systems, отже, часто використовується на обладнанні цієї компанії.

Протокол має наступні якості.

- більш швидка збіжність в порівнянні з іншими протоколами на базі вектору відстаней, яка досягається завдяки алгоритму DUAL (Diffusing Update Algorithm). Алгоритм становить таблицю топологій, в якій зазначено два кращих шляхи до мережі призначення (основний і резервний). На обох цих маршрутах не виникають петлі;

- зниження споживання смуги пропускання досягається за рахунок того, що при будь-яких зміни в мережі, алгоритм DUAL відправляє тільки нові оновлення, а не всю таблицю маршрутизації;

- підтримка декількох протоколів мережевого рівня (IP, IPX, AppleTalk);

- безкласовий протокол маршрутизації;

- використання багатоадресної (224.0.0.10) та одноадресної розсилки, замість широкомовної. Завдяки цьому оновленню маршрутизації не впливають непотрібні маршрутизатори.

2.6.3.1 Принцип роботи протоколу EIGRP

Протокол EIGRP спочатку повинен виявити своїх сусідів, для цього він використовує протокол Hello, який в свою чергу розсилає hello- пакети (за замовчуванням кожні 5 секунд). Для відправки пакетів використовується багатоадресна розсилка. Поки hello-пакети приходять від сусіда, маршрутизатор визначає його як функціонуючого. Якщо протягом певного часу (за замовчуванням 15 секунд) від сусіда не прийшов hello- пакет, він вважається недоступним.

Після того, як сусіди встановлені, відбувається обмін інформацією про топологію мережі. Спочатку пересилається інформація про повну топології мережі між маршрутизаторами. А далі, при зміні на мережі, маршрутизатори обмінюються наступними пакетами:

- пакет оновлень маршрутів (Update). У цих пакетах зберігається інформація про зміну маршрутів. Пакети можуть пересилатися по багатоадресній або одноадресній розсилці;

- пакет запитів (Query). Цей пакет необхідний, коли маршрутизатор перераховує будь-який маршрут, і у нього немає резервного. Маршрутизатор відправляє запит сусідам. Якщо у сусідів є маршрут, то вони відповідають шляхом посилки пакета відповіді на запит (Reply). Якщо маршруту немає, то вони відправляють запит уже своїм сусідам.

- пакет підтвердження (Acknowledgment). При отриманні вище зазначених пакетів (update, query, reply), у відповідь надсилається пакети підтвердження. Для надійної і гарантованої доставки відправлених пакетів протокол EIGRP використовує надійний транспортний протокол (Reliable Transport Protocol - RTP). Протокол неодноразово пересилає маршрутну інформацію, якщо повідомлення було втрачено. За рахунок використання протоколу RTP зменшується ймовірність виникнення петель.

Далі відбувається вибір найкращого шляху. Маршрутизатори аналізують топологічну таблицю і вибирають з неї шлях з найменшою метрикою. Протокол

вважає її за допомогою вагових коефіцієнтів (за замовчуванням К1 = 1; К2 = 0; К3 = 1; К4 = 0; К5 = 0), а також смуги пропускання (bandwidth) і затримки (delay).

До переваг протоколу EIGRP відноситься:

- швидка збіжність у великих мережах;
- значно менше завантаження каналів і CPU при роботі протоколу;
- можливість балансування трафіку по нееквівалентним каналам.

Недоліком протоколу EIGRP, є те що він закритий, тобто може бути реалізований тільки на обладнанні компанії Cisco Systems. Протокол добре сумісний з IGRP, а також з RIP.

2.6.4 Протокол маршрутизації на основі стану каналу – OSPF

Одним з поширених протоколів на основі стану каналу є протокол OSPF. Це безкласовий протокол маршрутизації. Технологія роботи протоколу полягає у відстеженні стану каналів і пошуку найкоротших шляхів (Shortest Path First - SPF), використовуючи алгоритм Дейкстри. Протокол підтримує складну топологічну базу даних. Якщо протоколи на базі вектору відстаней не містять інформацію про віддалених мережах, то протоколи на основі стану каналу підтримують всю інформацію про видалені маршрутизатори і їх з'єднання. Стан каналу в цьому протоколі має на увазі опис інтерфейсу (наприклад, IP-адреса, маска, тип мережі і т.п.) і його відношення з сусідніми маршрутизаторами. На основі вище зазначених описів інтерфейсів формується база даних стану каналів. База даних заповнюється завдяки отриманню повідомлень про стан каналу (Link-State Advertisement - LSA), які розподіляються часто або ж відразу після зміни топології мережі, або при будь-яких змінах на маршрутизаторах. Ці повідомлення є невеликими пакетами. В LSA міститься інформація про підключені інтерфейси, метрики і інші параметри. На основі отриманих повідомлень LSA маршрутизатор використовує алгоритм SPF, який будує дерево найкоротших маршрутів. Алгоритм виробляє розрахунок над базою даних топології мережі, видаляючи зайві гілки (гілки - всі можливі шляхи). Отримані маршрути записуються в таблицю маршрутизації.

Протокол може підтримувати різні вимоги IP-пакетів на якість обслуговування (пропускна здатність, затримка і надійність) за допомогою побудови окремої таблиці маршрутизації для кожного з цих показників.

Протокол володіє і іншими перевагами, корисними в великих сучасних мережах. До них відносяться можливість балансування навантаження між каналами з рівними метриками і засоби аутентифікації як по нешифрованому паролю, так і по шифрованому (шляхом додавання до пакету дайджесту ключа і тіла пакета за алгоритмом MD5). Нумерація пакетів виключає їх повторюваність і таким чином можливість повторної атаки.

До недоліків проколу слід віднести високу обчислювальну складність і, отже, високі вимоги, що пред'являються до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає зі збільшенням розмірів мережі. Тому для збільшення масштабованості протоколу застосовується поділ мережі на логічні області, з'єднані магістральної областю. Внутрішня топологічна інформація між областями не віддається. Скорочення обсягів таблиць маршрутизації і зниження службового трафіку при оновленні топологічної інформації служить можливість об'єднання декількох адрес мереж в один при виявленні у них загального префіксу, і заміна широкомовних розсилок – мультикастінговими. З метою економії IP-адрес в з'єднаннях типу «точка-точка» між маршрутизаторами призначати кінцевим точкам адреси не обов'язково. Платою за ці переваги є складність конфігурації і необхідність ретельного попереднього планування мережі для її оптимальної роботи (розбивка на області, виділення магістралі, розподіл функцій між маршрутизаторами з урахуванням їх обчислювальної потужності: рядові, виділені в зоні, прикордонні і т.д.).

Протокол OSPF - внутрішній протокол маршрутизації і працює всередині однієї автономної системи. Її можна розбити на зони або області, які представляють собою логічні розділи автономної системи.

OSPF забезпечує:

- алгоритм вибору оптимального шляху, заснований на пропускній здатності каналів зв'язку, затримки в передачі даних, кількості помилок при передачі в кожному напрямку і інших факторах;

- відсутність службового трафіку після побудови таблиці маршрутизації (передача тільки коротких пакетів між сусідніми маршрутизаторами через певні інтервали часу, що підтверджують їх доступність);

- швидке поширення інформації про зміну топології (кожен маршрутизатор містить повну картину про структуру всієї зони, тому при зміні топології інформація розсилається відразу всім маршрутизаторам зони);

- розподіл повноважень з управління. Наявність в OSPF власних зон дозволяє у великій мережі делегувати повноваження по управлінню різними ділянками (зонами) мережі окремим адміністраторам, зберігаючи загальний контроль за мережею з центру, завдяки наявності так званої центральної (backbone) зони, через яку здійснюється сполучення інших зон між собою;

- автоматичне агрегатування підмереж, тобто уявлення декількох безперервно наступних в адресному просторі підмереж у вигляді однієї мережі в разі, якщо доступ до всіх цих мереж з даного маршрутизатора здійснюється через один сусідній маршрутизатор;

- можливість розподіляти навантаження по передачі трафіку по паралельних каналах, що дозволяє збільшувати пропускну здатність при відсутності каналів зв'язку необхідної пропускної здатності.

Протокол OSPF має ряд переваг:

- маршрути, обчислені протоколом OSPF, не можуть бути циклічними;

- протокол забезпечує масштабованість для великих мереж;

- найшвидша пере налаштування при зміні топології мережі.

До недоліків можна віднести:

- ієрархічна топологія;

- відсутній розподіл навантаження при нееквівалентний шляхах;

- метрика використовує тільки вартість маршруту

2.6.5 Протокол маршрутизації IS-IS

Протокол IS-IS заснований на алгоритмі стану каналів зв'язку і є попередником OSPF. У протоколі обміну даними між проміжними системами ISIS (Integrated Intermediate System-to-intermediate System) використовується той же принцип маршрутизації станом каналів, що і в протоколі OSPF. Обидва ці протоколи відносяться до класу протоколів IGP (Interior Gateway Protocol) і їх головна відмінна особливість - постійно проводиться пошук найкоротшого шляху. Це основна властивість є одночасно як перевагою, так і недоліком. Для передачі даних між двома кінцевими пунктами використовується найкоротший на даний момент маршрут. Але при цьому, для обміну між маршрутизаторами службовою інформацією, доводиться вдаватися до лавинної розсилці пакетів (flooding). Такий процес необхідний для того, щоб кожен маршрутизатор, який є сусіднім до даного, прийнявши чергове повідомлення про зміну стану каналів і оновивши свої таблиці маршрутизації, переслав його далі.

Для запобігання можливих перевантажень при лавинної розсилці пакетів стану каналів LSP (Link State Packet) протокол IS-IS оснащений рядом механізмів контролю. Його принцип полягає в тому, що маршрутизатор ніколи не передасть LSP-пакет тому вузлу, від якого був прийнятий.

Принципи маршрутизації протоколу IS-IS багато в чому схожі з тими, що використовуються в OSPF. Для синхронізації баз даних маршрутизації IS-IS використовує пакети CSNP (Complete Sequence Number Packet) і PSNP (Partial Sequence Number Packet) за своїм значенням приблизно аналогічні пакетам DD (Database Description) і LSR (Link State Request) протоколу OSPF.

У мережевому оточенні IS-IS використовується два різних способу маршрутизації і, відповідно, два методу обробки дейтаграм маршрутизаторами. Сфера дії маршрутизатора першого рівня обмежена своєю областю, а маршрутизатор другого рівня відповідає за маршрутизацію як всередині, так і поза області, домену, локальної мережі.

В даний час цей протокол дуже рідко використовується в корпоративних мережах. Це викликано повною перевагою над ним протоколу OSPF, який, по суті, є вдосконаленим IS-IS. До недоліків протоколу відноситься його нездатність підтримувати маски підмереж змінної довжини, об'єднувати маршрути, а також широкомовний характер розсилок сусіднім маршрутизаторам. Все це негативно впливає на швидкість збіжності, навантаження маршрутизаторів і завантаженість ліній зв'язку.

2.6.6 Протокол маршрутизації BGP-4

Протокол BGP розроблявся як зовнішній для організації маршрутизації між автономними системами в глобальній мережі Internet (максимальне число маршрутизаторів 65534 між AS). В даний час в Internet використовується 4-я версія протоколу BGP-4. Хоча протокол відноситься до зовнішніх протоколів маршрутизації, його іноді застосовують і для внутрішньої маршрутизації. BGP є протоколом, що орієнтується на вектор відстані.

Однак, на відміну від RIP і IGRP протокол BGP не вимагає періодичного оновлення всієї маршрутної таблиці. Обмін повними таблицями виконується між маршрутизаторами тільки при їх початковому підключенні. Надалі відсилаються тільки повідомлення про оновлення в таблицях, причому тільки тим маршрутизаторам, які явно вказані в якості сусідніх. В одному оновленні BGP-4 може бути оголошено про один новий маршрут або анулювання декількох, що перестали існувати. Все це сприяє зниженню службового трафіку.

Метрика BGP є довільне число одиниць, що характеризує ступінь переваги конкретного маршруту, і встановлюються адміністратором мережі, в основному виходячи з міркувань договірних і фінансових переваг, можливо, з обліку інших факторів (за замовчуванням на підставі мінімального числа проміжних AS). У різних маршрутизаторів може використовуватися різна маршрутна політика.

Хоча BGP підтримує маршрутну таблицю всіх можливих шляхів до конкретної мережі, в своїх повідомленнях про коригування він оголошує тільки

про оптимальні маршрути. Наявність в таблиці альтернативних маршрутів прискорює реакцію маршрутизатора на інформацію про недосяжність основного шляху, а також дозволяє підтримувати балансування навантаження. Оскільки протокол орієнтований на обмін даними між різними AS, де при виборі маршрутів переважають, як правило, не технічні, а політичні міркування, то процес балансування навантаження на увазі осмислене розподіл маршрутів між альтернативними каналами за допомогою налаштування відповідних параметрів протоколу. Повідомлення BGP-4 про коригування містять послідовність AS, через які може бути досягнута зазначена мережа, її IP-адреса та довжина маски префіксу (підтримується тільки безкласовості адресація CIDR).

Протокол дозволяє об'єднувати маршрути. Перелік AS використовується для поліпшення збіжності, швидкість якої у протоколу не висока. Для забезпечення безпеки можуть застосовуватися різні способи аутентифікації маршрутизаторів.

Протокол сумісний з RIP і OSPF.

2.7 Порівняльна характеристика протоколів маршрутизації

У таблиці представлена порівняльна характеристика основних протоколів динамічної маршрутизації.

Важливою характеристикою протоколу маршрутизації є швидкість збіжності. Виходячи з аналізу самих алгоритмів можна сказати, що дистанціонно векторний протокол RIP поступається за цим параметром вдосконаленому протоколу IGRP. Ще більшу швидкість збіжності має комбінований протокол EIGRP, який наближається до найбільш швидкісним протоколам OSPF і IS-IS, заснованим на алгоритмі обліку стану каналів зв'язку. Протокол BGP не відноситься до числа швидкісних, як через дистанційно-векторний алгоритм, так і з огляду на його особливості, пов'язані з роботою в якості зовнішнього протоколу (різна маршрутна політика маршрутизаторів, використання надійного транспортного протоколу TCP і т.д.).

Таблиця 2.1 - Порівняльна таблиця основних характеристик протоколів динамічної маршрутизації

Критерії/Протоколи	**RIP v.2**	**IGRP**	**IS-IS**	**OSPF**	**EIGRP**	**BGP v.4**
Безпека	Відкритий пароль або аутентифікація по ключу MD5	-	-	Відкритий пароль або аутентифікація по ключу MD5	Аутентифікація по ключу MD5	Різні методи аутентифікації
Тип алгоритму	Вектор відстані	Вектор відстані	Стан лінії зв'язку	Стан лінії зв'язку	Комбінований	Вектор відстані
Балансування навантаження	-	Різні метрики	Однакові метрики	Однакові метрики	Різні метрики	Різні метрики(під автоматично)
Об'єднання маршрутів	-	-	-	+	+	+
Маски підмережі	+	-	-	+	+	+
Максимальна кількість машрутизаторів в мережі	15	255(реком. < 50)	1024	65534	255	65534
Метрика	Одна загальна	Комбінова на	Одна загальна та 3 додаткові	Одна загальна та 3 додаткові	Комбінована	довільна
Підтримка QoS	-	+	+	+	+	-
Оновлення маршрутної інформації	Вся таблиця	Вся таблиця	Вся таблиця	Тількі зміни	Тількі зміни	Тількі зміни
Доступність реалізації	Відкритий	Тількі на обладнанні Cisco Systems	Відкритий	Відкритий	Тількі на обладнанні Cisco Systems	Відкритий
Підтримка IPv6	-	-	-	+	+	+

Можна зробити висновок, що кращими внутрішніми протоколами маршрутизації є OSPF і EIGRP. Особливо в застосуванні до великих і складних мереж. Але так само ці протоколи, не дивлячись на широкий спектр позитивних якостей, мають і свої мінуси. Протокол OSPF має високі вимоги до ресурсів

маршрутизації через занадто складний обчислювальний розрахунок найкоротших шляхів. Хоча протокол EIGRP виграє в цьому плані, він все ж є закритим. Його реалізація можлива тільки на обладнанні Cisco Systems. Але в наш час в мережах застосовується обладнання різноманітних фірм. Тому у великих мережах вигідніше застосовувати протокол OSPF.

2.8 Методика вибору алгоритму маршрутизації в комп'ютерних мережах

Багато мережевих завдань, таких як завдання знаходження оптимального маршруту проходження трафіку, завдання пошуку найкоротших шляхів, завдання оптимального розподілу мережевих ресурсів тощо, формулюються як задачі теорії графів. На даний момент теорія графів розглядається як потужний інструмент для вирішення великої кількості завдань з різноманітних областей.

Перед тим як описати методику вибору алгоритму слід позначити основні визначення з теорії графів.

Теорія графів - розділ дискретної математики, що вивчає властивості графів.

У загальному сенсі граф представляється як безліч вершин (вузлів), з'єднаних ребрами.

Граф $G=[R,A]$ - це сукупність двох множин: множини точок, які називаються вершинами, і безлічі ребер А. Кожен елемент $a \in A$ є упорядкована пара (p_i, p_j) елементів множини R, вершини pi і pj називаються кінцевими точками або кінцями ребра а. Граф називається кінцевим, якщо безлічі R і А кінцеві.

Теорія графів не враховує конкретну природу множин А і В. Існує велика кількість різних конкретних завдань, при вирішенні яких можна тимчасово забути про специфічний зміст множин та їх елементів. Ця специфіка ніяк не позначається на результаті виконання завдання, незалежно від її складності.

Наприклад, при вирішенні питання про те, чи можна з точки a дістатися до точки b, рухаючись тільки по з'єднучим точки лініях, неважливо, чи маємо ми справу з людьми, містами, числами і т.д. Але, коли задача вирішена, ми отримуємо рішення, вірне для будь-якого змісту, яке було змодельована у вигляді графа. Недивно тому, що теорія графів - один з найбільш затребуваних інструментів при створенні штучного інтелекту: адже штучний інтелект може обговорити зі співрозмовником і питання любові, і питання музики або спорту, і питання вирішення різних завдань, причому робить це без будь-якого переходу (перемикання), без якого в подібних випадках не обійтися людині.

Зв'язний граф - граф, що містить рівно один компонент зв'язності. Це означає, що між будь-якою парою вершин цього графа існує як мінімум один шлях.

Неорієнтовані граф, G-граф - це впорядкована пара G: = (V, E), для якої виконані наступні умови:

- V - це непорожня безліч вершин, або вузлів,

- E - це множина пар (в разі неорієнтованого графа - невпорядкованих) вершин, званих ребрами

- V (а значить і, E, інакше воно було б мульти-множиною) зазвичай вважаються кінцевими множинами. Багато хороших результатів, отриманих для кінцевих графів, невірні (або будь-яким чином відрізняються) для нескінченних графів. Це відбувається тому, що ряд міркувань стає хибним в разі нескінченних множин.

- Вершини і ребра графа називаються також елементами графа.

- Порядок графа - це число вершин в графі | V |.

- Розмір графа - це число його ребер | E |

В мультисервісних мережах у порівнянні зі звичайними мережами передачі даних спостерігається значне збільшення навантаження на мережеві ресурси. А класична IP-маршрутизація не здатна забезпечити ефективну і надійну роботу мережі.

Одним з рішень є запропонований спосіб маршрутизації на основі мінімально спрямованих графів, при якому трафік проходить за мінімально спрямованим графом, побудованому за допомогою алгоритму Йена. Агрегований потік трафіку розподіляється відразу кількома маршрутами, певними при побудові графа. Набір маршрутів створюється при побудові мінімальних спрямованих графів для пари вузлів. При цьому виділяється деяка підмножина маршрутів між заданими вузлами. Для побудови такого підграфу з вихідного графа мережі застосовується метод ранжирування і послідовна нумерація вузлів. Після цього вузли, які опинилися непронумерованими, спільно з інцидентними їм лініями виключаються з розгляду.

Для передачі по мережі різнорідних потоків інформації необхідно, щоб алгоритм маршрутизації враховував вимоги, що пред'являються даними потоками до рівня QoS. Перевагою MPLS є можливість безпосереднього управління маршрутами, за якими будуть слідувати потоки трафіку. Для мультисервісних мереж, в яких реалізуються можливості Traffic Engineering (TE), через велику кількість вузлів розмір завдання маршрутизації може виявитися дуже великим, щоб розв'язати цю проблему за прийнятний час.

Зменшити розмір завдання маршрутизації можна за рахунок формування набору маршрутів для кожної пари вузлів (джерело, одержувач) $б_{ij}$, задовольняючи певні умови, а саме мінімальна або заздалегідь задана обмежена кількість прольотів. Формування множини допустимих маршрутів між кожною парою вузлів (джерело-одержувач) будемо здійснювати, використовуючи резервний алгоритм, в основі якого лежить метод МСГ (мінімальних спрямованих графів).

Суть методу мінімально спрямованих графів полягає в тому, що певний потік трафіку направляється від джерела до одержувача відразу кількома маршрутами, обчисленим при побудові мінімального спрямованого графа, або по одному, але з найбільшим пріоритетом, з набору допустимих маршрутів. При цьому досягається більш збалансоване завантаження, так як враховуються особливості всіх маршрутів. Їх основні параметри збираються на основі

статистичної обробки всієї мережі за певний період. До таких параметрів можна віднести, наприклад, коефіцієнти завантаження в мережі в залежності від часу доби (днів тижня), затримка в мережі при передачі.

Побудова мінімального спрямованого графа необхідна для того, щоб виділити серед безлічі маршрутів між парою вузлів ті, які мають мінімальне або заздалегідь відоме число прольотів (але більше мінімального), і вже серед них провести оптимізацію по одному або кількома параметрами. При цьому слід враховувати, що графи, що містять зациклення, в розгляд не приймаються.

Таким чином, методику вибору алгоритму маршрутизації можна визначити як завдання побудови мінімального спрямованого графа та звести його до чотирьох основних процедур:

Нижче представлений алгоритм побудови мінімального спрямованого графа (рис. 2.2).

Рисунок 2.2 – Алгоритм побудови мінімального спрямованого графа

Процедура усунення «тупікових» маршрутів:

Вихідними даними є вузол $v_k \in V$(V - множина всіх вузлів мережі), у якого була видалена хоча б одна вихідна лінія, і множина Е вхідних і вихідних ліній вузла.

Перевіряється, чи є у даного вузла ще вихідні лінії. Якщо вихідні лінії відсутні, тобто $E_{k\ поч} = 0$ то вузол v_k , виключається з множини розглянутих вузлів. Якщо $E_{k\ поч} \neq 0$ то перейти до п. 5.

По безлічі вхідних ліній вузол $E_{k\ вх}$ визначаються інцидентні йому вузли, які утворюють множини I_k.

У всіх вузлів множини I_k видаляються вихідні лінії до вузла v_k з множини Е.

4. Для кожного вузла з множини I_k, у якого була видалена хоча б одна виходить лінія, запускається процедура усунення тупікових маршрутів, при цьому відповідний вузол виключається з множини I_k.

Якщо всі вузли з множини I_k були розглянуті ($I_k \neq 0$), вихід з процедури.

Схема цієї процедури зображена на рис. 2.3.

Рисунок 2.3 - Схема процедури усунення «тупікових» маршрутів

Алгоритм перевірки зв'язності графа:

При побудові мінімального спрямованого графа після процедури усунення тупікових маршрутів слід запустити алгоритм перевірки зв'язності графа, який для випадків видалення одного прольоту або видалення одного вузла буде різним. Під видаленням вузла розуміється вихід з ладу всіх його інтерфейсів. Але з огляду на те, що ймовірність такої події мала, то її подальший розгляд в даній роботі не є доцільним.

Нижче наводиться опис алгоритму для випадку видалення одного прольоту і схема цього процесу (рис. 2.4). Слід зауважити, що віддаленим може виявитися

проліт в разі будь-якої аварії (наприклад, обрив кабелю або вихід з ладу відповідного інтерфейсу в вузлі) або якщо коефіцієнт завантаження даної ділянки дорівнює або прямує до 100%.

- розглядаються прольоти від вузла нульового рангу до всіх вузлів першого рангу.

- якщо таких прольотів більше одного, то перейти до п. 5. Якщо такий проліт один, то потрібно тимчасово виключити його з розгляду.

- побудувати заново спрямований граф без урахування віддалених прольотів. Якщо в цьому випадку не вдається побудувати спрямований граф, то можливе використання модифікованого алгоритму побудови спрямованого графа.

- додати до отриманого графу тимчасово вилучені прольоти. Тепер кількість прольотів між двома розглянутими рангами більше одного.

- перейти до розгляду всіх прольотів між двома наступними рангами. При цьому розглядається вже новозбудований граф. Якщо наступний ранг відсутній, то перейти до п. 7.

- повторити процедуру, починаючи з п. 2.

- отриманий після виконаних операцій граф залишається зв'язковим навіть при видаленні одного будь-якого прольоту.

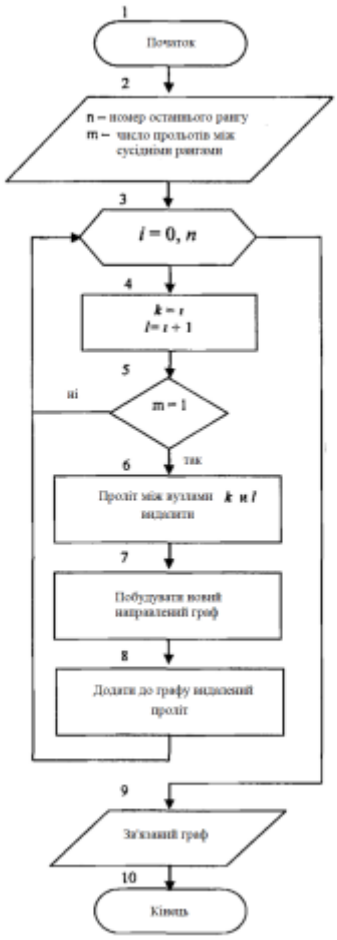

Рисунок 2.4 - Алгоритму для випадку видалення одного прольоту

Пропонується кілька варіантів модифікованого алгоритму побудови спрямованого графа при перевірці зв'язності.

1.При побудові спрямованого графа не слід виключати прольоти між одноранговими вузлами. При цьому номери рангів будуть визначатися за рангом вузла, для якого віддалений проліт є вихідним, а також по найбільшому рангу, який містить більше одного вузла. Якщо віддалений проліт з'єднував вузол джерела і будь-який вузол першого рангу, то не слід видаляти лінії між одноранговими вузлами першого рангу, що містить більше одного вузла.

2. Для створення зв'язного графа потрібно побудувати міні-граф між вузлами двох найближчих рангів, для яких був видалений проліт. При цьому такі вузли приймаються за джерело і приймач відповідно. Після побудови міні-графа його накладають на вихідний спрямований граф, а також додають віддалений раніше проліт.

Для такого варіанту перевірки зв'язність графа очевидними є певні переваги і недоліки. Перевагою є те, що зв'язний графа виходить максимально наближеним до вихідного мінімального спрямованого графу. Недолік такого способу - кількість прольотів (хопів) значно збільшується.

3. Для створення зв'язного графа потрібно побудувати міні-граф між вузлами двох рангів. Джерелом бути вузол, для якого віддалений проліт є вихідним. Приймачем залишається той же вузол, який був призначений для початкової топології. Після побудови такого міні-графа його накладають на вихідний спрямований граф, а також додають віддалений раніше проліт. Такий спосіб є хіба що проміжним між попереднім методом і з самого початку не модифікованим алгоритмом перевірки зв'язності графа.

4. У більшості схожий на вихідний модифікований алгоритм перевірки зв'язності графа. З тією лише різницею, що в даному випадку з розгляду тимчасово виключаються йдуть підряд поодинокі прольоти.

Якщо в процесі перевірки зв'язності графа з використанням модифікованого алгоритму не вдалося побудувати спрямований граф, тобто в разі видалення якого-небудь одиночного прольоту не є можливим знайти резервні маршрути, значить мережу із заданою топологією не гарантуватиме необхідну якість обслуговування QoS про визначення класу сервісу трафіку. Такий потік отримає відмову в обслуговуванні.

Можлива така ситуація, коли після перевірки зв'язності будується початковий граф, тобто виходить та топологія, яка була до початку побудови набору допустимих маршрутів. Таке найімовірніше, коли задана мережа, з невеликою кількістю вузлів. Якщо в такій мережі маршрутизатори (розглядаються в якості вузлів) не здатні обробити таблиці маршрутизації з необхідним обсягом інформації, то слід опустити перевірку зв'язності графа, або не використовувати модифікації алгоритму перевірки зв'язності графа. Для зниження рівня складності завдання розподілу потоків можна також обмежити число можливих допустимих маршрутів кожної пари вузлів джерело - одержувач.

Перевірку зв'язності графа можливо також опустити для випадку, якщо в поданій мережі спочатку існує одиночний проліт між вузлами двох рангів. Щоб це перевірити, необхідно до процесу усунення тупікових маршрутів виявити поодинокі прольоти.

3 ПРОГРАМНО-ОБУМОВЛЕНА СЕГМЕНТАЦІЯ МЕРЕЖІ НА ОСНОВІ CISCO TRUSTSEC

В даному розділі розглядається сегментація мережі - важливий інструмент забезпечення інформаційної безпеки (ІБ), що дозволяє значно знизити ймовірність інцидентів безпеки і пов'язаний з ними збиток навіть у разі проникнення зловмисників всередину периметра корпоративної мережі. Аналізується традиційний підхід до сегментації і його обмеження. Розглядається новий підхід до сегментації на базі технології Cisco TrustSec, що усуває ці обмеження. Розглядається ряд типових завдань ІТ та ІБ, пов'язаних з сегментацією, а також проводиться порівняння рішень цих задач, які пропонуються традиційним і новим підходами.

3.1 Ієрархічна модель мережі від Cisco

3-рівнева ієрархічна модель Cisco націлена на побудову надійної, масштабованої і високопродуктивної мережевої конструкції. Цей високоефективний мережевий ієрархічний підхід забезпечує економічний, модульний, структурований і простий метод (забезпечує нескладний і однаковий проект) для задоволення існуючих і майбутніх потреб зростання мережі. Кожен з рівнів має свої особливості і функціональність, що ще більше спрощує мережі.

Що ж змушує нас переходити до використання 3-рівневого ієрархічного підходу, представлено нижче:

- масштабованість (Scalability) - ефективно пристосовується до майбутнього зростання мережі;

- простота управління і усунення неполадок - ефективне управління і простота в усуненні причини збою;

- більш проста і структурована фільтрація і примусове застосування політик - простіше створювати фільтри/політики і застосовувати їх в мережі;

- надмірність і відмовостійкість - в мережі можуть відбуватися збої/простої пристроїв, і вона повинна продовжувати надавати послуги з тією ж продуктивністю, в разі виходу з ладу основного пристрою;

- висока продуктивність - ієрархічна архітектура для підтримки високої пропускної здатності і високої продуктивності базової активної інфраструктури;

- модульність - забезпечує гнучкість в проектуванні мережі і полегшує просте впровадження та усунення неполадок.

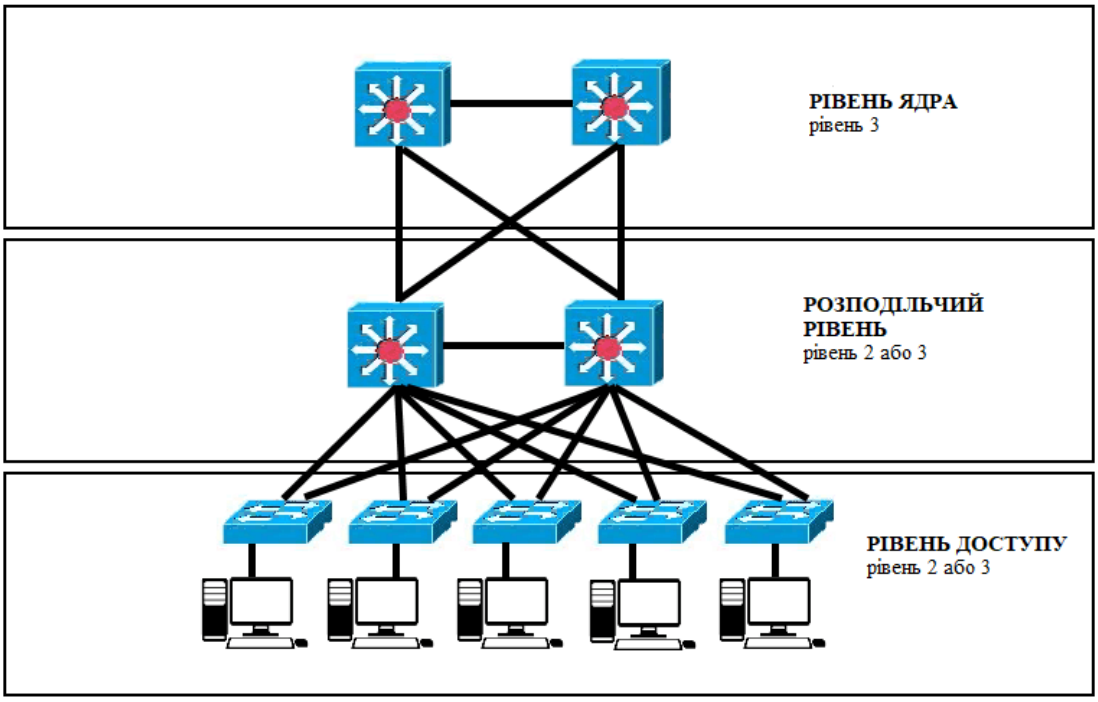

Рисунок 3.1 - Ієрархічна модель мережі від Cisco

3.1.1 Рівень ядра (внутрішній рівень) | core layer

Цей рівень також називається мережевим магістральним рівнем і відповідає за забезпечення швидкого транспорту між розподільними комутаторами в межах кампусу підприємства.

Станціями внутрішнього рівня є комутатори високого класу і високопродуктивні комутатори, які мають модульний форм-фактор. Це повністю резервні пристрої, що підтримують розширені функції комутації рівня 3 і

протоколи динамічної маршрутизації. Основним тут є збереження конфігурації якомога більше мінімальної на рівні ядра.

Через дуже високу критичність цього шару, проектування його вимагає високого рівня стійкості для швидкого і плавного відновлення, після будь-якої події збою мережі в межах блоку ядра.

Нижче наведені основні характеристики внутрішнього рівня:

- висока продуктивність і наскрізна комутація;
- забезпечення надійності та відмовостійкості;
- маштабованість.

Ось деякі моделі комутаторів Cisco, що працюють на рівні ядра: Catalyst серії 9500/6800/6500 і nexus серії 7000.

3.1.2 Розподільчий рівень | distribution layer

Розподільчий рівень розташований між рівнями доступу та ядра. Основна функція цього рівня - забезпечити маршрутизацію, фільтрацію і WAN-доступ, а також візуалізувати зв'язок між рівнями доступу та ядра. Крім того, комутатори рівня розподілу можуть надавати висхідні служби для багатьох комутаторів рівня доступу. Рівень розподілу гарантує, що пакети маршрутизуються між підмережами і Inter/Intra VLAN в середовищі кампуса. Як стандартний підхід, шлюзи за замовчуванням для всіх VLAN будуть комутаторами рівня розподілу. Насправді серверні пристрої не повинні бути безпосередньо підключені до розподільчих комутаторів. Цей підхід забезпечує економію витрат на один порт за рахунок високої щільності портів при менш дорогих комутаторах рівня доступу.

Основні функції розподільчого рівня перераховані нижче:

- акумулювання каналів LAN/WAN;
- контроль доступу та фільтрація, такі як ACLs і PBR;
- маршрутизація між локальними мережами і VLAN, а також між доменами маршрутизації;
- надмірність і балансування навантаження;

-підсумовування підмереж і агрегування маршрутів на кордонах/до рівня ядра;

-управління широкомовним доменом. Пристрій рівня розподілу діє як демаркаційна точка між широкомовними доменами.

Основними моделями комутаторів Cisco, що працюють на розподільному рівні, є Catalyst серії 6800/6500/4500/3850

3.1.3 Рівень доступу | access layer

Цей рівень включає в себе комутатори рівня 2 і точки доступу, що забезпечують підключення до робочих станцій і серверів. На висхідних лініях зв'язку пристрою рівня доступу підключаються до розподільчих комутаторів. Ми можемо управляти контролем доступу і політикою, створювати окремі колізійні домени і забезпечувати безпеку портів на рівні доступу. Комутатори рівня доступу забезпечують доставку пакетів на кінцеві пристрої.

Рівень доступу виконує ряд функцій, в тому числі:

- комутація рівня 2;
- висока доступність;
- безпека портів;

3.2 Сегментація мережі

Корпоративна мережа стала критично важливим інструментом бізнесу багатьох компаній, оскільки саме вона забезпечує роботу безлічі бізнес-процесів, пов'язаних з передачею інформації. У той же час загрози інформаційної безпеки безперервно еволюціонують, і потреба в ефективних засобах захисту зростає з кожним днем.

Довгий час увагу фахівців з інформаційної безпеки було зосереджено в основному на захисті периметра мережі. Але в сучасних мережах класичне поняття периметра поступово розмивається. Користувачі підключаються до

мережі різними способами, включаючи доступ через дротові і бездротові сегменти, а також VPN-підключення. При цьому в рамках IT-інфраструктури організації, як правило, існує безліч типів користувачів і пристроїв, яким для виконання своєї роботи потрібен доступ до різних ресурсів мережі. Реалізація належного розмежування доступу в сучасних розподілених і динамічних IT-інфраструктурах є досить непростим завданням. З урахуванням великої кількості векторів атаки, що дозволяють зловмисникам і шкідливому програмному забезпеченню проникати в корпоративну IT-інфраструктуру, ймовірність порушення інформаційної безпеки можна вважати вкрай високою, як правило, це питання часу.

Однією з популярних заходів, спрямованих на зниження шкоди від проникнення зловмисника в корпоративну IT-інфраструктуру, є сегментація мережі. Мається на увазі попереднім етапом сегментації є поділ користувачів і ресурсів мережі на ізольовані одна від одної групи (закриті групи користувачів і ресурсів). Обмін даними між цими групами контролюється або взагалі блокується в залежності від вимог політики безпеки організації.

Принципи, які використовуються для поділу користувачів на групи, визначаються прийнятою в організації політикою безпеки. В якості одного з типових варіантів поділу користувачів і пристроїв за категоріями можна навести такий: співробітники, тимчасовий персонал, гості, користувачі з пристроями, що не відповідають корпоративній політиці (карантин), інженерні підсистеми будівель і так далі. Крім того, співробітники можуть бути розміщені не в одну групу, а розділені на кілька груп, наприклад рядові співробітники, керівництво, топ-менеджмент, бухгалтерія тощо.

Сегментація мережі допомагає значно знизити ризики інформаційної безпеки за рахунок обмеження можливостей зловмисників по нанесенню збитку в разі їх проникнення всередину, периметру, що захищається.

Поділ користувачів на групи і сегментація мережі не є самоціллю, але можуть бути дуже важливими для підвищення безпеки бізнес-процесів. У цьому сенсі такі бізнес-процеси спираються на сегментацію. Політика безпеки

організації може вимагати, щоб співробітники різних категорій отримували доступ тільки до тих корпоративних ресурсів, до яких їм необхідно мати доступ для виконання своєї роботи. Наприклад, доступ до групи серверів системи ERP з конфіденційною бізнес-інформацією може надаватися тільки керівництву, а доступ до конфіденційних баз HR - тільки співробітникам HR-підрозділу і, можливо, керівництву. У той же час персонал нижчої ланки або тимчасові співробітники можуть отримувати доступ тільки до обмеженого набору корпоративних додатків, наприклад до кооперативної системи CRM і електронної пошті, і не мати права доступу до всіх інших ресурсів мережі.

Вплив сегментації на бізнес-процеси в описуваних випадках полягає в тому, що сегментація важлива для забезпечення інформаційної безпеки, а оскільки інциденти в області ІБ можуть призводити до порушення доступності, то сегментація також сприяє підвищенню доступності бізнес-процесів.

Крім того, існує ціла група бізнес-процесів, впровадження яких при відсутності сегментації є вкрай небажаною. Наприклад, до цієї групи належать процеси, пов'язані з доступом до корпоративної мережі користувачів, які не є співробітниками організації. Типовим прикладом є надання доступу в мережу (або в Інтернет) так званим гостьовим користувачам. В якості інших варіантів можна згадати доступ співробітників компанії-партнера, доступ аудиторів, підключення в мережу пристроїв, що належать іншим організаціям, наприклад банкоматів, цифрових вивісок, платіжних терміналів. Ще одним сценарієм, в якому рекомендується використання сегментації, є розмежування доступу між співробітниками афілійованих структур, що використовують одну і ту ж мережу.

Подібних сценаріїв може бути багато, але всі вони призводять до задачі реалізації сегментації на практиці.

3.2.1. Традиційні методи сегментації мережі

При реалізації сегментації мережі необхідно вирішити 3 ключові завдання:

- визначити приналежність користувача до потрібної групи при його підключенні до мережі (задача 1).

Ізолювати трафік користувача даної групи від трафіку користувачів інших груп при передачі по мережі (задача 2).

Забезпечити доступ користувача до тих ресурсів, до яких він повинен мати доступ і, як правило, заблокувати доступ до всіх інших ресурсів (завдання 3).

Завдання 1 зазвичай вирішується за допомогою аутентифікації та авторизації з використанням протоколу 802.1x на RADIUS-сервері (часто з використанням даних з корпоративної служби каталогів, наприклад Active Directory). Можливе застосування і інших методів - статичного приміщення користувачів в залежності від порту підключення, VLAN'a, IP-підмережі, авторизації по MAC-адресу і так далі в залежності від можливостей використовуваного сервера AAA і обладнання.

Завдання 2 традиційно вирішується шляхом створення окремих віртуальних топологій для кожної групи користувачів. Як правило, це робиться за допомогою тих чи інших засобів віртуалізації мережі. У разі невеликих мереж цими засобами зазвичай є VLAN'и і транки 802.1Q. Також часто використовуються технології Рівня 3, наприклад Multi-VRF CE (VRF-Lite). Для великих мереж характерно застосування MPLS VPN.

Завдання 3, як правило, вирішується пакетною фільтрацією на основі IP-адрес. Контроль доступу може бути реалізований такими «грубими» засобами, як списки контролю доступу (ACL) на елементах мережевої інфраструктури, так і «тонкою» фільтрацією на системах захисту нового покоління (NGFW, NGIPS), але фундаментальний принцип залишається тим же - базовим критерієм для прийняття рішення про допуск/недопуск є IP-адреса. Фільтрація проводиться в одному або декількох місцях, призначених для обміну трафіком між групами користувачів.

Іноді пакетну фільтрацію використовують без створення віртуальних топологій, тобто пакетні фільтри одночасно служать для вирішення як завдання 2, так і завдання 3.

3.2.2 Обмеження традиційних методів сегментації

Традиційні методи вирішення завдань (2) і (3) можуть призводити до значного обсягу ручної роботи, особливо в процесі експлуатації мережі.

Ця обставина стає тим відчутніше, чим більше динаміки в середовищі сегментації, наприклад:

У мережі можуть змінюватися правила контролю доступу - як в зв'язку з оновленням вимог служби безпеки, так і зі змінами в складі ресурсів і користувачів.

У мережі може змінюватися склад груп користувачів - наприклад, в зв'язку з реорганізаціями всередині компанії, змінами в складі ресурсів мережі і т.д.

Можливі зміни в географії груп користувачів, через що може знадобитися поширення сегментації на нові частини мережі.

Підтримка сегментації стає тим складніше, чим з бульшою кількістю закритих груп користувачів доводиться мати справу.

Ситуація ускладнюється тим, що правила контролю доступу спираються на IP-адреси. З такими правилами важко працювати і легко помилитися. Крім того, застосування IP-адрес як базового критерію для контролю доступу значно обмежує можливості внесення змін в схему адресацію, а в деяких випадках робить зміни практично неможливими. Крім того, IP-адреса не може ідентифікувати користувача/пристрій/стан і її легко підмінити.

Часто списків контролю доступу стає так багато, а в самих списках - настільки багато рядків (Access Control Entries, ACE), що адміністратори не можуть згадати, для чого конкретно потрібен той чи інший рядок, і побоюються змінювати або видаляти ці рядки. Згодом списки розростаються і їх обслуговування стає ще складніше. Це відбувається тому, що кількість рядків ACE визначається множенням ACE = S * D * P, де S - кількість адрес джерел (sources), D - кількість адрес призначення (destinations), а P - кількість дозволів доступу (permit). Наприклад, навіть в разі відносно невеликої мережі, в якій правила доступу стосуються 4 VLAN'ів, з яких дозволяється доступ в 30 підмереж

до 4 додатків (що вимагає хоча б 4 записи permit в ACL), адміністратори мають справу не менше ніж з 4 * 30 * 4 = 480 рядками. Що вже говорити про великі мережі з безліччю підмереж і додатків!

Висока трудомісткість роботи зі списками контролю доступу іноді призводить до того, що деякі організації взагалі не використовують сегментацію або відмовляються від неї в процесі росту мережі. Але і ті, хто використовують сегментацію, часто змушені витрачати багато часу і сил на координацію між департаментами IT, ІБ, бізнесу, на обмін заявками і т.д.

У підсумку на персонал служб IT та ІБ лягає значне навантаження, що займає робочий час рутинними, але відповідальними операціями, що вимагають великої концентрації уваги. Типові слідства:

Зростають ризики ІБ через можливі помилки і «дірки», що виникають в результаті правок списків контролю доступу вручну.

Зростають ризики збоїв бізнес-процесів через помилки, що виникають в результаті внесення змін до конфігурації обладнання.

Багато часу йде лише на підтримку сегментації в актуальному стані. Займатися важливими, але не терміновими справами немає часу, і часто вони і не робляться. Іде на рутину час, який можна було б використовувати для вирішення стратегічних, творчих завдань - наприклад, пов'язаних з розвитком мережі, плануванням, оптимізацією підтримки бізнес-процесів, оптимізацією роботи мережі і т.д. Як правило, часу не залишається навіть на підтримання документації в актуальному стані, що знову підвищує ризики ІБ і збоїв бізнес-процесів!

Довше time-to-market: йде більше часу на запуск нових додатків або досягнення бізнес-результатів, в тій чи іншій мірі пов'язаних з сегментацією мережі.

3.3 Технологія Cisco TrustSec

TrustSec - це технологія сегментації, розроблена компанією Cisco і дозволяє подолати розглянуті вище проблеми за рахунок автоматизації. На рисунку 3.2 показано Приклад домену мережі Cisco TrustSec.

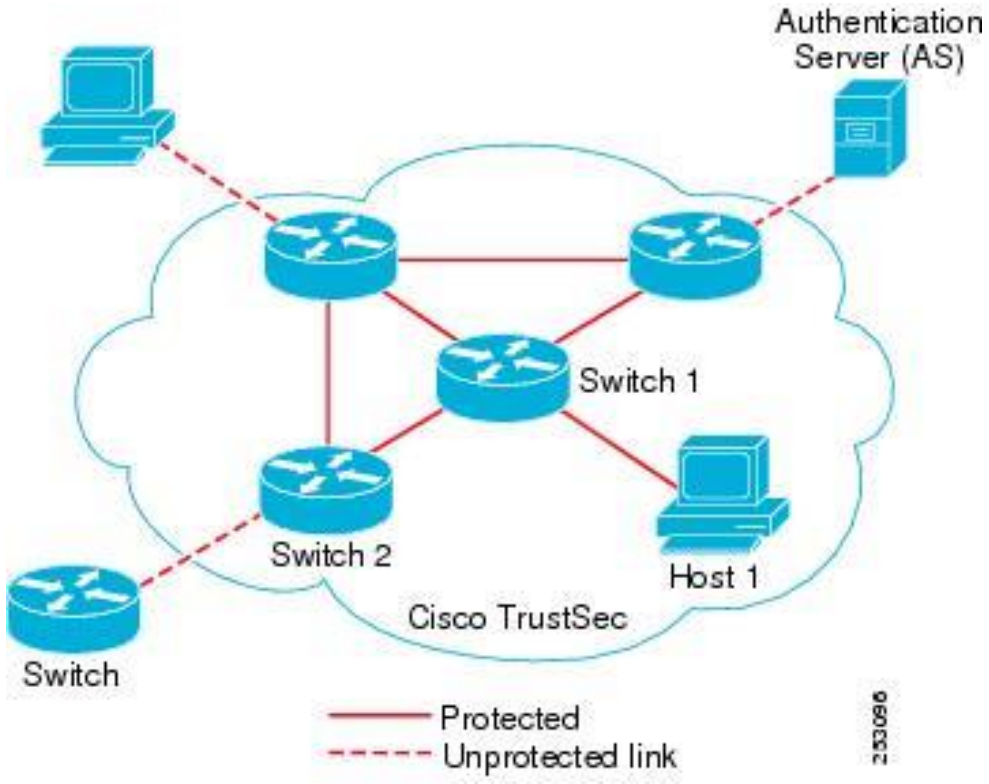

Рисунок 3.2 - Приклад домену мережі Cisco TrustSec

Як і у випадку традиційних методів, Cisco TrustSec передбачає вирішення завдання розміщення користувача в потрібну групу (завдання 1, в термінології TrustSec - Classification, класифікація) шляхом аутентифікації і авторизації користувача по протоколу 802.1x за допомогою сервера контролю доступу, в якості якого виступає Cisco Identity Services Engine (Cisco ISE). Сервер Cisco ISE може проводити аутентифікацію і авторизацію з використанням як внутрішньої бази даних користувачів, так і зовнішніх каталогів, наприклад Active Directory. TrustSec не вимагає застосування будь-яких конкретних типів облікових даних користувачів (user credentials) - можливі варіанти, наприклад MSCHAPv2, Generic Token Card (GTC), одноразовий пароль RSA і так далі. Також можливі

альтернативні методи, такі як MAC Authentication Bypass, Web Authentication, Passive Identity (Easy Connect) на основі AD і т.п. Крім того, доступні статичні методи - на основі VLAN, IP-адрес, інтерфейсів і т.п.

Але далі підходи принципово різняться. Cisco TrustSec передбачає призначення трафіку кожній закритій групі користувачів відповідної 16-бітної мітки безпеки (Security Group Tag, SGT) при підключенні до мережі, точніше, при вході в межі домену TrustSec. Зазвичай це робиться на комутаторі доступу або іншому пристрої на кордоні корпоративної мережі.

Багатство можливостей класифікації і призначення міток групам користувачів і підключень всіх типів - дротовим, бездротовим, VPN, підключенням серверів в ЦОД та інших організацій - дозволяє створити на базі TrustSec єдину, всеосяжну політику доступу для всіх типів пристроїв і підключень (рис. 3.3)

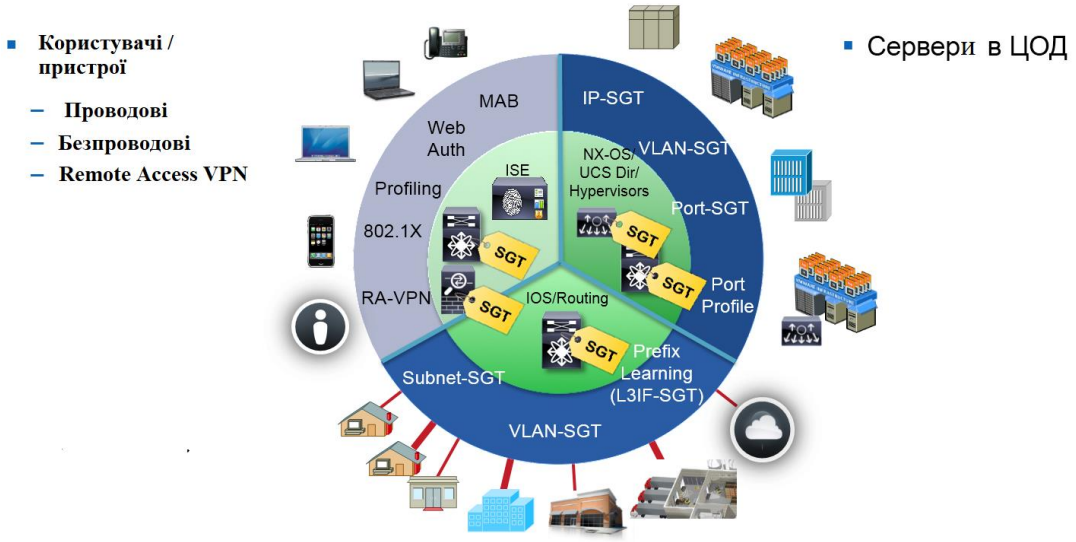

Рисунок 3.3 - Технологія Cisco TrustSec

Рисунок 3.3 Cisco TrustSec дозволяє створити єдину, всеосяжну політику доступу для всіх типів пристроїв і підключень

Мітка SGT призначається динамічно сервером Cisco ISE або статично елементом мережевої інфраструктури, а далі TrustSec працює з мітками.

В цьому і полягає принципова відмінність рішення задачі ізоляції трафіку (завдання 2, в термінології TrustSec - Propagation, поширення). У традиційному підході для цього необхідне створення віртуальної топології для кожної групи. У TrustSec це не потрібно, так як TrustSec передбачає призначення трафіку кожної групи мітки SGT. Це позбавляє від необхідності створення віртуальних топологій і значно спрощує мережу: всі закриті групи користувачів можуть працювати на базі єдиної мережевої топології.

Далі, TrustSec пропонує принципово інше, більш просте і ефективне, рішення задачі контролю доступу (завдання 3, в термінології TrustSec - Enforcement, застосування політик). Традиційний підхід передбачає застосування списків контролю доступу, заснованих на IP-адреси (ACL). TrustSec працює зі списками контролю доступу, заснованими не на IP-адресах, а на мітках SGT. Ці списки називаються Cisco TrustSec Security Group ACL (SGACL). Використання SGACL дозволяє значно спростити роботу: замість численних і важких в супроводі ACL, заснованих на IP-адресах, адміністратори мають справу з SGACL, заснованими на мітках груп і не залежать ні від адрес, ні від наявності віртуальних топологій.

Ця концепція реалізована в матриці TrustSec Policy сервера Cisco ISE. Замість безлічі розрізнених списків контролю доступу адміністратор працює з централізованою матрицею (рис. 3.4). Ряди матриці представляють собою групи-джерела трафіку (sources), колонки - групи-адресати (destinations). Політики доступу задаються в комірках-пересіченнях в вигляді SGACL. Можливі як найпростіші правила (permit / deny) для будь-якого трафіку), так і більш складні SGACL з деталізацією дозволяємого і забороняємого трафіку аналогічно тому, як це робиться в ACL, тільки джерела і адресати визначаються мітками SGT, а не IP-адресами.

Sources	Destinations: Company Database	Public Cloud	External Partner	Internet
Guest	Deny	Deny	Deny	Permit
Employee BYOD	Permit	Define Access	Deny	Web Apps
Building Mgmt.	Permit	Deny	Deny	Deny
Employee	Permit	Permit	Define Access	Permit

Рисунок 3.4 - Ілюстрація концепції матриці доступу Cisco TrustSec Policy Management Matrix

Заповнювати всі осередки матриці необов'язково - незаповнені клітини слідують політиці Default Policy, яка може забороняти або дозволяти за замовчуванням весь трафік. Заповнені клітинки відповідають налаштованим в SGACL правилам, після яких виконується Default Policy.

Концепція матриці доступу і динамічне призначення міток дозволяють реалізувати політику доступу централізовано, зручно, консистентно. TrustSec поширює цю політику по мережі шляхом динамічної передачі міток SGT і правил SGACL.

Мітки SGT можуть поширюватися по мережі трьома способами - від вузла до вузла в складі заголовків фреймів або пакетів трафіка (це метод inline), за допомогою протоколу SGT Exchange Protocol (SXP), що працює поверх TCP, або за допомогою технології Cisco Platform Exchange Grid (pxGrid).

Перший спосіб забезпечує дуже високу масштабованість і зручність, тому що мітки передаються разом з трафіком, але пристрій повинен мати можливості роботи з мітками, впровадженими у фрейми або пакети. Це доступно не завжди, особливо в разі роботи з мітками в складі фреймів Ethernet, які вимагають апаратної реалізації в інтегральних мікросхемах (ASIC). Крім того, реалізацію

TrustSec можуть мати не всі пристрої мережі і тоді може виникнути завдання об'єднання «ізольованих областей» TrustSec між собою. У таких випадках можна скористатися другим способом - передачею міток по протоколу SXP. Третій спосіб - на базі pxGrid - забезпечує інтеграцію з іншими рішеннями інформаційної безпеки Cisco і її партнерів.

На даний момент Cisco реалізувала технологію TrustSec вже в десятках лінійок своїх продуктів, включаючи комутатори для корпоративних і промислових мереж, центрів обробки даних, міжмережеві екрани, маршрутизатори, контролери БЛВС і т.д. Крім того, хоча TrustSec і є фірмовою розробкою Cisco, в 2014 р Cisco опублікувала інформаційний драфт IETF з описом протоколу Source-group tag eXchange Protocol (SXP), щоб відкрити функціонал TrustSec і іншим вендорам.

Що стосується поширення правил SGACL, то елементи мережевої інфраструктури автоматично завантажують їх з сервера Cisco ISE. Коли адміністратор вносить зміни в політики TrustSec, він може негайно поширити їх по мережі, скориставшись push-командою в інтерфейсі Cisco ISE. Крім того, є можливість оновити політику TrustSec локально на пристрої за допомогою команди в CLI. Пристрої також періодично оновлюють політики у міру закінчення їх часу життя (expiry timeout).

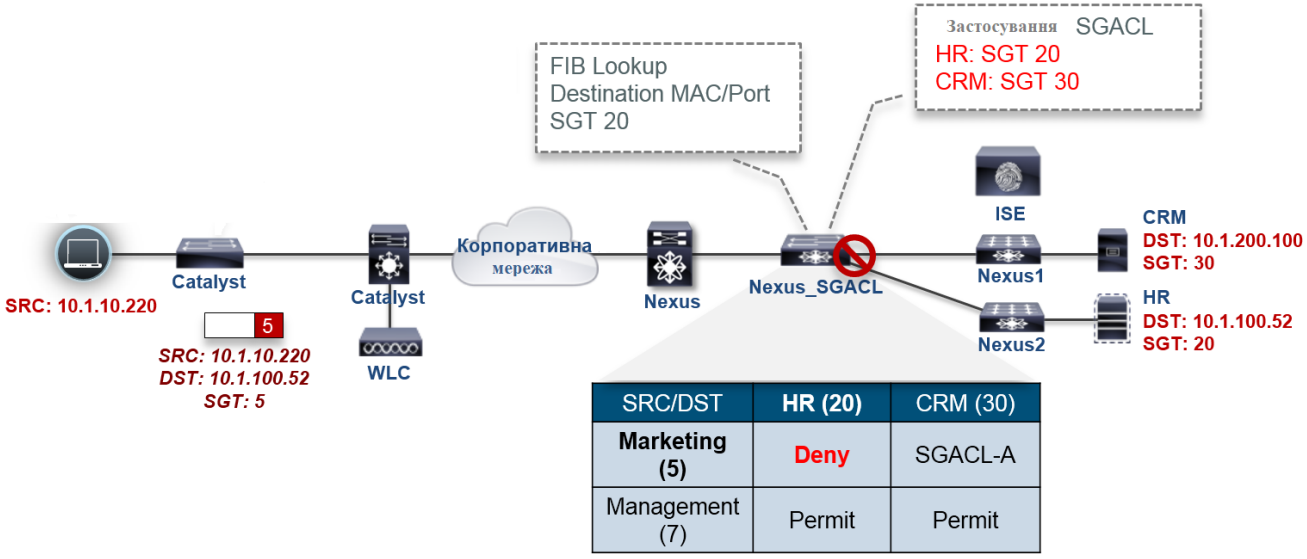

Рисунок 3.5 - Приклад застосування політики TrustSec

Розглянемо застосування політики TrustSec на прикладі (рис. 3.5). Користувач Аліса підключилася до мережі, пройшла аутентифікацію і авторизацію на сервері Cisco ISE і за результатами авторизації була призначена в групу 5 (Marketing). Комутатор доступу призначає пакетам, що надходять в мережу від її комп'ютера, мітку SGT 5. Припустимо для простоти, що всі зображені на малюнку комутатори охоплені доменом TrustSec, а політики TrustSec застосовуються на інтерфейсах комутатора Nexus_SGACL, до яких підключені комутатори Nexus1 і Nexus2 (хоча політики можуть застосовуватися і на інших маршрутизованих і комутованих інтерфейсах домену TrustSec). Адміністратор налаштував на Cisco ISE і розповсюдив в домені TrustSec політику доступу, зображену в таблиці на рис 3.5.

Припустимо, комп'ютер Аліси відправив IP-пакет сервера групи HR, що належить до групи HR. Пакет передається через мережу і приходить на комутатор Nexus_SGACL, який застосовує вже завантажену з сервера Cisco ISE політику. Як ми пам'ятаємо, матрицю доступу треба читати по мнемонічному правилу «зліва-направо-знизу-вгору», тому представлена в прикладі політика передбачає Deny для всього трафіку групи Marketing (мітка 5), спрямованого адресатам групи HR (мітка 20). Оскільки сервер HR з адресою 10.1.100.52 належить групі HR, комутатор видаляє пакет Аліси, виконуючи таким чином вимогу політики сегментації.

Комутатори застосовують SGACL апаратно на швидкості каналу зв'язку, тому фільтрація на базі міток не впливає на продуктивність комутації.

Детально ознайомитися з деталями налаштування політик TrustSec на сервері Cisco ISE можна в технічній документації. Також в документації можна знайти і докладні відомості про налаштування TrustSec на елементах мережевої інфраструктури, наприклад комутаторах Catalyst. На сайті Cisco доступні і Design Guides по темі TrustSec.

Таким чином, Cisco TrustSec пропонує динамічне поширення політик контролю доступу в рамках всієї мережі, в тому числі можливість охопити всі

види доступу в мережу - дротові, бездротові, VPN - в рамках єдиної, централізованої політики.

Cisco TrustSec охоплює не тільки мережеву інфраструктуру і сервер Cisco ISE. Завдяки інтерфейсу pxGrid TrustSec інтегрується з іншими рішеннями Cisco (і її партнерів), наприклад Cisco Firepower, Cisco Web Security Appliance (WSA), Cisco Stealthwatch і т.д. Зокрема, така інтеграція дозволяє створити на базі міток SGT дуже тонкі і гранулярні політики доступу до додатків і мікрододатків, користуючись арсеналом функцій міжмережевих екранів наступного покоління Cisco Firepower. Інший приклад - застосування на базі міток SGT різних привілеїв доступу до веб-ресурсів за допомогою Cisco WSA. Третій приклад - розробка політик Stealthwatch для боротьби зі спрямованими погрозами з урахуванням приналежності користувача до тієї чи іншої групи SGT. Четвертий приклад - окремий випадок можливостей рішення Cisco Rapid Threat Containment. У цьому прикладі Cisco Stealthwatch або Cisco Advanced Malware Protection виявляють загрозу ІБ (наприклад, інфікований комп'ютер) і передають на Cisco ISE запит на обмеження доступу на вашому комп'ютері за допомогою інструментарію TrustSec (динамічне приміщення в карантинну групу).

Крім того, TrustSec, по суті будучи технологією програмно-визначаємої сегментації, інтегрується з архітектурою програмно-обумовленого ЦОД Cisco Application Centric Infrastructure (ACI). Інтеграція встановлює взаємну відповідність між закритими групами користувачів, сегментованих за допомогою міток SGT, і додатками з їх компонентами, сегментованими на групи Endpoint Groups (EPG) технології ACI. В результаті з'являється можливість створити наскрізні програмно-визначаємі політики безпеки, що охоплюють і мережу, і ЦОД.

Обидві технології - TrustSec і ACI - спрямовані на оптимізацію та автоматизацію процесів в областях безпеки і ЦОД. У цьому сенсі технології взаємно доповнюють одна одну і, коли використовуються разом, пропонують додаткові синергетичні вигоди.

Розглянемо ряд типових завдань департаментів IT та ІБ і порівняємо очікувані результати від вирішення цих завдань в сценаріях мережі, в якій сегментація реалізована на базі традиційних методів (умовно назвемо її мережу AS-IS) і мережі з сегментацією на базі технології Cisco TrustSec (мережа TO- BE).

Для визначеності припустимо, що в обох сценаріях користувачі поміщаються в потрібну групу (завдання 1) в результаті аутентифікації і авторизації 802.1x на RADIUS-сервері з використанням служби каталогів Active Directory. Таким чином, рішення цього завдання в обох сценаріях принципово не відрізняється.

Але ізоляція трафіку користувачів (завдання 2) реалізується в мережі AS-IS шляхом створення віртуальних топологій або застосування ACL, а в мережі TO-BE - шляхом призначення фреймам міток SGT.

Контроль доступу (завдання 3) в сценарії мережі AS-IS реалізується за допомогою ACL, а в сценарії мережі TO-BE - за допомогою Security Group ACL (SGACL), динамічно поширюються по мережі з сервера Cisco ISE.

Виходимо з того, що обладнання мережі в сценарії AS-IS підтримує необхідні технології віртуалізації, а в сценарії TO-BE - функціонал TrustSec.

3.3.1 Операції по створенню/зміненню/видаленню списків контролю доступу (ACL)

До завдань цього виду відносяться операції, пов'язані з контролем доступу вже наявних користувачів до ресурсів мережі.

У разі вихідної мережі (AS-IS) завдання вирішується шляхом ручних правок списків контролю доступу (ACL), налаштованих на одному або на багатьох елементах мережевої інфраструктури. Особливо багато правок може знадобитися в разі, коли ACL використовуються як для ізоляції трафіку (замість віртуальних топологій), так і для контролю доступу.

Щоб впоратися з великою кількістю ACL в рамках традиційного підходу, можна спробувати централізувати їх застосування до трафіку. Для цього буде

потрібно, по-перше, реалізувати віртуальні топології для ізоляції трафіку закритих груп користувачів (рішення задачі 2), а по-друге, реалізувати обмін трафіком між цими топологиями і застосування ACL (рішення задачі 3) в мінімально прийнятній кількості точок мережі.

Подібна централізація обміну трафіком може допомогти зменшити кількість ACL, але не усуває проблеми традиційного підходу повністю. Крім того, вона сприяє виникненню додаткових «пляшкових шийок» в мережі, а також зниженню оптимальності маршрутів трафіку між групами. Неоптимальні шляхи трафіку між групами можуть з'явитися від того, що трафіку потрібно обов'язково пройти через точку обміну, яка може і не бути на найкоротшому шляху. Різниця між найкоротшим і фактичним шляхами в деякій англомовній літературі називається network stretch. В цілому, застосування політик зазвичай збільшує network stretch.

У мережі з TrustSec (TO-BE) рішення задачі автоматизується. Контроль доступу до ресурсів реалізується шляхом налаштування матриці TrustSec Policy Management Matrix, централізованої на сервері контролю доступу Cisco ISE. Політики доступу динамічно поширюються по елементах мережевої інфраструктури і реалізуються в SGACL.

Також відпадає необхідність ставити певні ACL на відповідних інтерфейсах, як було в мережі AS-IS. Замість цього на інтерфейсах активується застосування політик TrustSec, але самі правила SGACL пристрої отримують динамічно. Тому більше немає необхідності централізувати обмін трафіком між групами, його можна зробити розподіленим. В результаті з'являється можливість знизити network stretch, оптимізувати шляхи обміну трафіком між групами, зменшити кількість «пляшкових шийок».

Таким чином, TrustSec пропонує:

- значне зниження витрат праці і часу на внесення змін;

- значне зниження ймовірності недоступності додатків, пов'язаних з ними збоїв бізнес-процесів і інцидентів ІБ, що виникають через помилки в конфігурації ACL і інших проявів «людського фактора»;

- негайний вступ в силу нових політик доступу;

- зміна статичного контролю доступу на динамічний;
- автоматизовану сегментацію мережі;
- непряму оптимізацію шляхів передачі трафіку між групами користувачів.

3.3.2 Створення/зміна/видалення ресурсів і закритих груп користувачів

Завдання цього типу можуть бути пов'язані зі створенням або видаленням закритих груп користувачів, запуском або видаленням ресурсів мережі, що спираються у своїй роботі на сегментацію, зміною географічного охоплення груп користувачів. Такі завдання можуть виникати в тому числі в рамках концепції «agile office».

3.3.2.1 Створення / видалення закритих груп користувачів

У сценарії мережі AS-IS закриті групи користувачів реалізуються шляхом створення віртуальних топологій за допомогою таких засобів, як VLAN, VRF, MPLS VPN, тунелі, тощо. Альтернативним варіантом є застосування ACL і для сегментації, і для контролю доступу.

Додавання нових груп або видалення старих вимагає значних витрат часу і ручної праці, а також часто пов'язано з помилками в налаштуванні і простоями бізнес-процесів через «людський фактор».

У сценарії мережі з TrustSec (TO-BE) додавання або видалення закритої групи користувачів реалізується шляхом створення або видалення мітки групи (SGT) на сервері Cisco ISE і призначення користувачів в потрібні групи. При цьому зміни в конфігурації мережі, як правило, не потрібні.

В результаті TrustSec забезпечує:

Значний виграш часу обслуговуючого персоналу, який можна використовувати не на рутину, а на рішення більш творчих, стратегічних завдань, на які часто не вистачає часу (наприклад, планування розвитку мережі, підготовка

та актуалізація документації, оптимізація налаштувань мережевого обладнання і т.п.).

Значне прискорення запуску нової закритої групи користувачів або нового бізнес-процесу, що спирається на сегментацію мережі.

Запобігання помилок, які можуть виникати при виконанні великого числа рутинних операцій. Перевірити матрицю доступу (як в робочому порядку, так і в процесі формального аудиту) набагато простіше, ніж сотні записів ACE, розподілених між десятками списків ACL.

3.3.2.2 Зміна географічного охоплення груп користувачів

Сценарій передбачає зміну географічного охоплення закритих груп користувачів. Наприклад - включення в групу користувачів з іншої будівлі, офісу в іншому місті, фізичні переміщення груп користувачів при переїзді або зміни в складі відділів, в рамках концепції «agile office», тощо.

У сценарії мережі AS-IS недостатньо одного разу виконати комплекс робіт по сегментації - об'єднати VLAN'и і VRF'и в віртуальні топології, застосувати ACL (можливо, на численних мережевих інтерфейсах) і т.п. Подібні роботи необхідно проводити і надалі, при змінах в політиці сегментації.

Тому якщо спочатку реалізувати сегментацію для всіх груп по всій мережі, за це доведеться платити ще більше високою трудомісткістю експлуатації. Здавалося б, можна знизити гостроту проблеми, якщо впровадити сегментацію в мережі лише частково, прокладаючи віртуальні топології тільки в ті частини мережі і для тих груп, які там необхідні в даний момент. Але коли вимоги до географії груп поміняються, за це доведеться розплачуватися додатковими витратами часу і праці на впровадження сегментації в потрібній області мережі - трудомісткими змінами конфігурації і пов'язаними з ними помилками в налаштуванні і простоями бізнес-процесів.

TrustSec в сценарії мережі (TO-BE) дозволяє звести витрати праці адміністраторів практично до нуля. TrustSec впроваджується в мережі один раз,

навіть на цьому етапі вимагаючи набагато менших трудовитрат, ніж створення віртуальних топологій і / або безлічі ACL на елементах мережевої інфраструктури. І TrustSec не вимагає переналаштування обладнання при змінах політик. Тому міркування трудомісткості експлуатації не заважають реалізувати TrustSec у всій мережі спочатку, при її створенні або модернізації.

Але все ж якщо при зміні географії груп користувачів виявляється, що з яких-небудь причин TrustSec спочатку не впроваджений в потрібній частині мережі, це можна зробити швидше, ніж в сценарії AS-IS, шляхом застосування набору команд, єдиного для всіх груп користувачів і не залежить від їх кількості.

Якщо ж TrustSec вже впроваджений в потрібній частині мережі, то з боку адміністраторів не потрібно взагалі ніяких дій з налаштування обладнання, тому що політики TrustSec поширюються по мережі динамічно.

3.3.3 Запобігання інцидентів ІБ

TrustSec дозволяє реалізувати сегментацію користувачів і контроль доступу з набагато більш високою швидкістю і гранулярністю, ніж базові засоби мережі AS-IS.

Ефект від впровадження TrustSec тим більше, чим більше динаміки в конфігурації закритих груп користувачів компанії, тому що TrustSec автоматизує ці зміни замість трудомісткої ручної роботи.

Також ефект від TrustSec тим більше, ніж більш затребувана гранулярність сегментації користувачів на групи. У разі традиційної сегментації на базі віртуальних топологій чим більше груп користувачів, тим більше топологій і тим вище трудомісткість. В результаті кількість топологій (і груп користувачів) може виявитися не оптимальним з точки зору безпеки, а меншим - щоб досягти компромісу між безпекою та трудомісткістю. У свою чергу, такий компроміс вже йде не на користь безпеки. Завдяки автоматизації TrustSec усуває це обмеження і дозволяє розділити користувачів саме на таку кількість груп, яке буде оптимально саме з точки зору безпеки.

TrustSec дозволяє створити єдину, всеосяжну політику доступу для всіх типів пристроїв і підключень, тим самим допомагаючи забезпечити високий рівень безпеки. Дуже серйозні додаткові можливості відкриває інтеграція TrustSec з іншими рішеннями інформаційної безпеки завдяки технології pxGrid.

Крім того, TrustSec забезпечує підвищений рівень безпеки за рахунок суворої взаємної аутентифікації елементів мережевої інфраструктури і можливості шифрування трафіку на канальному рівні.

Завдяки описаним перевагам Cisco TrustSec дозволяє значно знизити ймовірність і збитки, пов'язані з інцидентами інформаційної безпеки.

Так як TrustSec дозволяє сегментувати користувачів на закриті групи значно гранулярніше, ніж традиційні методи, то в разі виникнення інциденту ІБ (наприклад, при проникненні зловмисника або попаданні інфекції в мережу) очікуваний збиток буде набагато менше, ніж в мережі AS-IS.

Крім того, з цієї причини TrustSec заощадить час персоналу на усунення наслідків інциденту.

Інша перевага - TrustSec дозволить усунути наслідки інциденту, зберігаючи доступ користувачів до мережі за рахунок їх перенесення в окрему ізольовану групу. Це особливо важливо, коли мова йде про VIP-користувачів. Наприклад, з'являється можливість усунути наслідки зараження комп'ютерів топ-менеджменту, зберігши їх доступ в мережу, причому з мінімальними ризиками для незаражених комп'ютерів.

Так як TrustSec дозволяє реалізувати набагато більш гранулярну сегментацію користувачів, ніж в разі мережі AS-IS, розслідування інцидентів зажадає аналізу меншої кількості пристроїв. В результаті можна значно прискорити і полегшити розслідування інцидентів інформаційної безпеки.

ВИСНОВКИ

В дипломній роботі проаналізовано традиційний підхід до сегментації мережі та її обмеження. Розглядається новий підхід до сегментації на основі технології Cisco TrustSec, що усуває ці обмеження. Розглядається ряд типових завдань IT та ІБ, пов'язаних із сегментацією, а також проводиться порівняння рішень цих завдань, що пропонуються традиційним та новим підходами. Розглядається низка типових завдань, пов'язаних із сегментацією, а також проводиться порівняння рішень цих завдань, що пропонуються традиційним та новим підходами. Докладно аналізуються нові можливості та переваги для бізнесу, які пропонує Cisco TrustSec.

Для сучасного бізнесу характерна дедалі більша динаміка. Мережа, а також реалізовані в ній політики, повинні оперативно підлаштовуватися під вимоги бізнесу, що змінюються. Критично важлива і належна робота бізнес-процесів, що спираються на мережу та залежать від сегментації. Будь-які зміни політики сегментації мають бути реалізовані як швидко, а й надійно. Тому традиційні засоби сегментації, розглянуті у роботі, вже не відповідають запитам бізнесу сьогоднішнього та завтрашнього днів. Підтримувати ці запити можна за допомогою сучасної технології сегментації мережі Cisco TrustSec.

TrustSec відповідає сучасним вимогам бізнесу та пропонує інструментарій, що реалізує зміни середовища сегментації швидко та надійно за рахунок автоматизації та зведення до мінімуму «людського фактору».

У результаті Cisco TrustSec пропонує бізнесу виграш, як мінімум, у трьох областях:

Зниження витрат. Ефект Expected Value за рахунок зниження ризиків ІБ та зниження ризиків простоїв бізнес-процесів.

Зменшення робочого часу. Виражений у людино-годинах виграш робочого дня персоналу з допомогою зниження обсягів рутинної роботи. З'являється можливість зосередитись на вирішенні стратегічних, творчих завдань, які часто відкладаються або взагалі не виконуються.

Оптимізація часу. Виражене у тижнях чи днях загальне прискорення запуску нових сервісів/додатків та отримання бізнес-результатів, які тією чи іншою мірою спираються на сегментацію мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Building the Carrier-Class IP Next-Generation Network. //[Електронний ресурс], 2017. – Режим доступу: http://www.cisco.com/en/US/prod/collateral/routers/ps5763/prod_white_paper0900aecd802e2a52_ns573_Networking_Solutions_White_Paper.html

2. ITU-T Recommendation Y.2201, “NGN release 1 requirements,” to be approved in April 2017.

3. Hiroyuki, S. Traffic Engineering using Multiple Multipoint-to-Point LSPs [Електронний ресурс] / S. Hiroyuki, M. Yasuhiro, Makiko Y. - Режим доступу: http://www.ieee-infocom.org/2000/papers/533.pdf. - 3.12.2017.].

4. S. Chen and K. Nahrstedt, “An Overview of Next-Generation HighSpeed Networks: Problems and Solutions,” IEEE Network.

5. Плешаков В. Основы маршрутизации. // [Електронний ресурс] – Режим доступу: http://www.citforum.ru/nets/ito/2.shtml

6. Martins L, Craveirinha J, Climaco J (2013a), A new multiobjective dynamic routing method for multiservice networks – modeling and performance evaluation, Technical report, INESC– Coimbra.

7. CISCO Internetworking Technology Overview , Сервер Марк-ИТТ, Владимир Плешаков. // [Електронний ресурс] - Режим доступу: http://citforum.ru/nets/ito/index.shtml

8. Розробка структурної схеми маршрутизатора. // [Електронний ресурс] - Режим доступу: http://ukrefs.com.ua/page,6,171661-Razrabotkastrukturnoiy-shemy-marshrutizatora.html

9. Класифікація алгоритмів маршрутизації. // [Електронний ресурс] - Режим доступу: http://um.co.ua/2/2-7/2-74318.html

10. Canfeng Chen Weiling Wu Zheng Li.Multipath Routing Modeling in Ad Hoc Networks / In Proc. of IEEE Globecom. — St. Louis, Missouri, USA, 2015. Pp. 259-2598.

11. Збірник наукових праць ВІТІ № 2 – 2019 Симоненко О.А. (ВІТІ) Троцько О.О. (ВІТІ) Кушніренко Д.М. (ВІТІ) - Аналіз методів багатошляхової маршрутизації в програмно конфігурованих телекомунікаційних мережах .

12. Бачинський, В.Ш. Гіоргізова-Гай, 2021 Системні дослідження та інформаційні технології, 2021, № 1

13. Володимир Щербо - Протоколи маршрутизації Internet. // [Електронний ресурс] - Режим доступу: https://www.osp.ru/os/1999/11-12/177881/

14. Dimitri B., Robert G., “Data Networks – 2nd ed”. Prentice Hall, New Jersey, ISBN 0-3-200916-1.].

15. Yee, J.R., “On the International routing protocol enhanced interior gateway routing protocols: is it optimal?” in International Transactions in Operational Research, v 13, n 3, pp. 177-94, May 2016

16. Хабракен Д. Маршрутизатори Cisco. Практичне застосування. / Д. Хабракен. – 2012. – 316 с.

17. Lammle Todd. Ccna data center: introducing cisco data center technologies study guide. exam 640-916. Lammle Todd /John Wiley & Sons Limited. - ISBN: 9781118763209.

18. Огляд блейд-серверів Cisco UCS серії B [Електронний ресурс] – Режим доступу до ресурсу: s://www.cisco-parts.ru/catalog-cisco/blade-servers-cisco-ucs-b-series/

19. Огляд серверного обладнання Cisco UCS [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco-parts.ru/catalog-cisco/cisco-ucs-servers/.

20. Нові рішення і переваги програмного забезпечення управління Cisco UCS [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco-parts.ru/catalog-cisco/cisco-ucs-managment-software/.

21. Cisco UCS Management [Електронний ресурс] – Режим доступу до ресурсу:https://www.cisco.com/c/en/us/products/servers-unified-computing/cisco_ucs_management.html.

22. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ua/about/press/2016/0222c.html.

ДЕМОНСТРАЦІЙНІ МАТЕРІЛИ