УДК 004.9:658
DOI: https://doi.org/10.53920/ITS-2023-2-7

Андрій Вікторович ЛЕМЕШКО,
доктор філософії, доцент,
доцент кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-8003-3168
Артем Васильович АНТОНЕНКО,
кандидат технічних наук, доцент,
доцент кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-9397-1209
Олександр Максимович МАТВІЙЧУК,
магістр кафедри комп'ютерної інженерії, ДУІКТ
ORCID ID: 0009-0002-8198-9668
Олександр Сергійович ДМИТРЕНКО,
магістр кафедри комп'ютерної інженерії, ДУІКТ
ORCID ID: 0009-0005-2483-600X
Вадим Юрійович БЕРЕЗДЕЦЬКИЙ,
магістр кафедри комп'ютерної інженерії, ДУІКТ
ORCID ID: 0009-0004-1007-975X

УПРАВЛІННЯ ТРАФІКОМ В ГІБРИДНІЙ ПРОГРАМНО-ВИЗНАЧЕНІЙ МЕРЕЖІ

У статті досліджується питання безпеки та доступності в гібридних програмно-визначених мережах (SDN) з використанням контролера та протоколу маршрутизації EIGRP. Особлива увага приділяється методу управління навантаженням з використанням протоколу onePK. У статті розглядається проблема управління трафіком в мережах, яка є актуальною у зв'язку зі зростанням кількості підключених пристроїв та збільшенням об'єму переданих даних. Пропонується використовувати гібридну SDN мережу, яка поєднує в собі переваги традиційної та програмно-визначеної мережі. Для управління трафіком в такій мережі використовується контролер, який керує роботою мережі та маршрутизацією. Для забезпечення безпеки пропонується використовувати протокол маршрутизації EIGRP, який дозволяє забезпечити безпеку та надійність передачі даних. Окрім цього, протокол EIGRP дозволяє використовувати балансування навантаження, що забезпечує рівномірне розподілення навантаження між маршрутизаторами та покращує швидкість передачі даних. Для ефективного управління навантаженням в гібридній SDN мережі пропонується

використовувати метод управління трафіком з використанням протоколу onePK. Цей протокол дозволяє збільшити продуктивність мережі та забезпечити більш ефективне використання ресурсів мережі. Крім того, використання протоколу onePK дозволяє простіше та швидше налаштування та управління мережею, що забезпечує більшу доступність та надійність роботи мережі. У статті розглядаютьсяє актуальні проблеми управління трафіком в мережах та пропонує ефективні методи розв'язання цих проблем з використанням гібридної програмно-визначеної мережі, контролера, протоколу маршрутизації EIGRP та протоколу onePK. Застосування запропонованих методів дозволяє забезпечити безпеку та доступність мережі, а також покращити швидкість та ефективність передачі даних. Робота присвячена методу управління трафіком у високонавантаженій гібридній програмно-визначеній мережі. Як метод дослідження застосовується експеримент. У статті наведено універсальні програмні моделі реалізації запропонованого методу управління трафіком. Наведено формалізовану модель запропонованого методу управління трафіком, а також його універсальну програмну модель реалізації.

Ключові слова: *доступність, безпека, програмно-визначена мережа, контролер, навантаження, EIGRP, onePK.*

Andriy LEMESHKO
Doctor of Philosophy, Associate Professor,
associate professor of the department of computer engineering,State University of information and communication technologies
Artem ANTONENKO
candidate of technical sciences, associate professor,
associate professor of the department of computer engineering,
State University of information and communication technologies
Oleksandr MATVIICHUK,
Oleksandr DMYTRENKO,
Vadym BEREZDETSKYI
masters of computer engineering department,
State University of information and communication technologies

MODELING OF WIRELESS NETWORKS IN OMNET ++ ENVIRONMENT INVOLVING INET FRAMEWORK

The paper investigates security and availability in hybrid software-defined networks (SDN) using a controller and the EIGRP routing protocol. Special attention is paid to the method of load management using the onePK protocol. The article considers the problem of traffic management

in networks, which is relevant in connection with the growth of the number of connected devices and the increase in the volume of transmitted data. It is proposed to use a hybrid SDN network, which combines the advantages of a traditional and software-defined network. To manage traffic in such a network, a controller is used, which controls the operation of the network and routing. To ensure security, it is suggested to use the EIGRP routing protocol, which allows you to ensure the security and reliability of data transmission. In addition, the EIGRP protocol allows the use of load balancing, which ensures an even distribution of the load between routers and improves data transfer rates. For effective load management in a hybrid SDN network, it is suggested to use the traffic management method using the onePK protocol. This protocol allows you to increase network performance and ensure more efficient use of network resources. In addition, the use of the onePK protocol allows easier and faster network configuration and management, which ensures greater availability and reliability of network operation. The article examines current problems of traffic management in networks and offers effective methods for solving these problems using a hybrid software-defined network, a controller, the EIGRP routing protocol, and the OnePK protocol. The application of the proposed methods allows to ensure the security and availability of the network, as well as to improve the speed and efficiency of data transmission. The work is devoted to the method of traffic management in a highly loaded hybrid software-defined network. An experiment is used as a research method. The article provides universal software models for implementing the proposed traffic management method. A formalized model of the proposed traffic management method is given, as well as its universal software implementation model.

Keywords: *availability, security, software-defined networking, controller, EIGRP, load, onePK.*

Постановка проблеми. В даний час концепція SDN (Software Defined Network або програмно-визначена мережа) стрімко завойовує світ мережевих технологій. Швидке зростання обсягу трафіку призводить до зростання інфраструктури, яка дозволить його опрацювати. Це, у свою чергу, призводить до того, що управління будь-якими мережами стає громіздким, малоефективним і складним.

Програмно-визначені мережі надають можливості для більш ефективного та гнучкого управління мережею, зокрема, для управління трафіком. Однак, використання SDN вимагає вирішен-

ня ряду проблем, зокрема, забезпечення доступності та безпеки мережі. Крім того, потрібні ефективні методи управління трафіком в SDN, які б дозволяли забезпечувати ефективність мережі та запобігали перевантаженням мережі.

У зв'язку з цим, постановка проблеми полягає в необхідності розробки методу управління трафіком в гібридній програмно-визначеній мережі з використанням контролера та протоколу маршрутизації EIGRP, який би дозволяв забезпечувати ефективність та безпеку мережі, а також уникати перевантажень мережі. Для досягнення цієї мети необхідно дослідити доступні методи управління трафіком в SDN, зокрема з використанням контролерів та протоколів маршрутизації, та знайти найефективніші підходи для застосування їх у гібридній програмно-визначеній мережі.

Аналіз останніх досліджень і публікацій. На сьогоднішній день тема програмно-визначених мереж є досить актуальною в галузі телекомунікацій та мережевих технологій. У світі багато вчених та фахівців займаються дослідженнями та розробками у цій галузі. Розглянемо кілька останніх джерел з цієї теми, які надруковані в українських та зарубіжних виданнях.

Одним з останніх джерел з даної теми є стаття «Програмно-визначені мережі: переваги, недоліки, можливості» авторів Клименка М. та Шмарди О., яка була опублікована в журналі «Інформаційні технології та комп'ютерна інженерія» в 2017 році. У статті автори описують архітектуру програмно-визначених мереж та їх функції, а також наводять приклади застосування таких мереж у практичних ситуаціях. Стаття містить важливу інформацію про особливості програмно-визначених мереж та їх переваги в порівнянні з традиційними мережами.

Ще одним джерелом є стаття «Управління трафіком в програмно-визначених мережах» авторів Маринченко І. та Нікітіна А., яка була опублікована в журналі «Комп'ютерні системи та мережі» в 2018 році. У статті автори розглядають роль програмно-визначених мереж у підвищенні ефективності управління інформаційними потоками в організаціях. Інше джерело на дану тему — стаття «Програмно-визначені мережі: аналіз стану розробки» авторів Шевчука С. та Мелешко В., яка була опублікована в журналі «Комп'ютерні науки та інформаційні технології» в 2017 році. У статті автори досліджують питання безпеки програмно-визначених мереж та наводять різні методи її забезпечення. Вони

аналізують потенційні загрози та вразливості програмно-визначених мереж та надають пропозиції щодо їх протидії.

Другим джерелом з даної теми є стаття «Основні напрями розвитку програмно-визначених мереж» авторів Арлова О. та Селезньова Д., яка була опублікована в журналі «Науковий вісник Національного гірничого університету» в 2019 році. У статті автори проводять порівняльний аналіз двох протоколів маршрутизації OSPF та EIGRP в програмно-визначених мережах. Вони досліджують переваги та недоліки кожного з цих протоколів та надають рекомендації щодо їх використання.

Загалом, дослідження та розробки в галузі програмно-визначених мереж здійснюються як українськими вченими та фахівцями, так і дослідниками з інших країн. Це свідчить про високий інтерес до даної теми у науковому та практичному середовищі. Важливо продовжувати дослідження та розробки в галузі програмно-визначених мереж з метою покращення доступності та безпеки мереж та підвищення ефективності управління трафіком [1-20].

Метою статті є розгляд методу управління трафіком в гібридній програмно-визначеній мережі з використанням контролера та протоколу маршрутизації EIGRP.

Виклад основного матеріалу дослідження. У роботах розглянутих вище джерел запропоновано рішення щодо забезпечення механізму маршрутизації в SDN з урахуванням виконання вимог до якості обслуговування (QOS) для максимально можливої кількості потоків та в умовах змінного навантаження.

На основі висновків, розглянемо гібридну модель SDN з урахуванням протоколу маршрутизації EIGRP.

Цей протокол відноситься до типу distance-vector, однак, на відміну від RIP та IGRP, використовує як основу своєї роботи алгоритм дифузійних обчислень. Подробиці роботи даного алгоритму наведені у [6] та [7].

Маршрутизатори, що беруть участь у роботі EIGRP, обмінюються інформацією про префікси, що знаходяться в таблиці маршрутизації кожного з них. Інформація про префікси містить:

- IP-адреса мережі;
- маску підмережі;
- смугу пропускання сегмента цієї мережі;
- затримку на інтерфейсі маршрутизатора, який представляє даний сегмент мережі;

- навантаження, яке діє на інтерфейсі, що представляє даний сегмент мережі;
- надійність, розрахована на інтерфейсі цього сегмента мережі;
- розмір MTU.

В якості смуги пропускання сегмента мережі передається мінімальна смуга пропускання мережевим шляхом, через який проходить маршрут до заданої мережі. В якості затримки передається сумарне значення затримки передачі пакета по всіх каналах на маршруті до заданої мережі. Як навантаження передається максимальне значення параметра txload по всіх каналах на маршруті до заданої мережі, який автоматично розраховується на кожному інтерфейсі маршрутизатора. При цьому важливо враховувати, що передається значення навантаження, яке генерується трафіком, що передається у бік префікса-призначення. В якості надійності передається мінімальне значення відношення кількості вірно прийнятих пакетів до загальної кількості прийнятих пакетів по всім каналам на маршруті до заданої мережі. Значення навантаження та надійності обчислюється кожним маршрутизатором окремо на інтерфейсі, підключеному до каналу, який є частиною маршруту до заданої мережі. Процес передачі інформації про префікс представлений на рисунку 1.

Рис. 1. Передача маршрутної інформації протоколом EIGRP

На основі отриманої інформації про префікс маршрутизатор обчислює метрику [8, 9, 10]. В стандарті, що описує роботу EIGRP, визначено два варіанти метрики: стандартна та розширена. Стандартна метрика розраховується маршрутизатором за формулою (1):

$$CM = (K_1 \cdot BW_s + K_2 \cdot \frac{BW_s}{256 - Lo_{max}} + K_3 \cdot D_s) \cdot \frac{K_5}{K_4 + R_{min}}, \quad (1)$$

де $BW_s = \frac{256 \cdot 10^7}{Bandwidth_{min}}$, $Lo_{max} = Load$, $D_s = 256 \cdot Delay_{summed}$, $R - Reliability$.

Як, видно, з формули (1), при розрахунку метрики для конкретного префіксу використовується параметр (навантаження), максимальне його значення по всім каналам на маршруті до заданого префіксу.

Коефіцієнти K_1, K_2, K_3, K_4, K_5 представляють собою вагові коефіцієнти, що змінюються від 0 до 255, вони необхідні для того, щоб при розрахунку метрики той чи інший параметр мав більший чи менший вплив на кінцевий результат розрахунку. Верхній поріг – 255 визначений необхідністю масштабування метрики до розміру в 32 біти – максимального розміру значення метрики в таблиці маршрутизації. У всіх поточних реалізаціях EIGRP реальну роль при розрахунку метрики грають затримка та пропуска спроможність.

Крім того, можна використовувати також розширену метрику, яка розраховується за формулою (2).

$$WM = (K_1 \cdot T_{min} + K_2 \cdot \frac{T_{min}}{256 - Lo_{max}} + K_3 \cdot La_{summed} + K_6 \cdot ExtM) \cdot (\frac{K_5}{K_4 - R_{min}}), \quad (2)$$

де $T_{min} = \frac{65536 \cdot 10^7}{Bandwidth_{min}}$, $La_{summed} = \sum_1^{Hop\ Count} \frac{65536 \cdot Delay_{interface}}{10^6}$.

Використання розширеної метрики обумовлено використанням в даний час каналів з пропускною здатністю 1 Гбіт/с і вище [8, 9, 10]. З формули (1) видно, що при використанні таких каналів відмінностей у метриках не буде, тому при розрахунку розширеної метрики використовуються великі значення чисельників.

При включенні до розрахунку параметра Load, тобто при встановленні значення коефіцієнта > 1, цей параметр враховується тільки при початковому розрахунку метрики для маршруту. Після пер-

шого розрахунку та отримання значення метрики навіть при зміні параметра Load ці зміни не враховуються та перерахунок метрики не провадиться. Ця особливість пов'язана з такими складнощами. Як відомо з положень теорії масового обслуговування, навантаження (трафік), що генерується підключеними до мережі пристроями, має імовірнісну природу, тобто значення навантаження, що є в мережі не завжди і змінюється в часі випадковим чином. Розподіл ймовірностей дії навантаження трафіку при цьому різниться, залежно від типу сервісів, що надаються мережею та типу пристроїв, підключених до мережі. В результаті зміна параметра Load, який відображає зміну навантаження, що діє на інтерфейсі маршрутизатора, має нелінійну природу; зміна також відбувається відповідно до чинного в цій мережі закону розподілу ймовірностей, через що значення параметра може приймати значення, що сильно різняться за абсолютною величиною, на короткому інтервалі часу. В результаті, частий перерахунок метрики з значеннями параметра Load, що сильно розрізняються, може призводити до частої зміни маршруту для проходження трафіку до заданого префіксу, що:

- збільшує затримку при передачі трафіку;
- призводить до втрати деяких пакетів у моменти нестабільності мережі;
- викликає зміни в послідовності пакетів, що передаються.

Ілюстрація цієї ситуації наведено на рисунку 2.

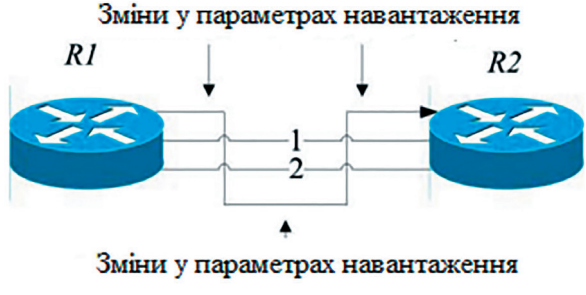

Рис. 2. Проблема з нестабільністю маршрутів в EIGRP

Крім того, зміна метрики маршруту викликає роботу механізмів дифузійних обчислень, закладені в EIGRP, через що інформація про часті зміни метрики, і, відповідно, маршруту, передається

до інших маршрутизаторів, які беруть участь у роботі EIGRP, які також перераховують метрику і змінюють рішення про маршрутизацію, що, в результаті, призводить до постійної частої зміни всіх маршрутів та нестабільності мережі [9, 10], в результаті яких негативні фактори, перераховані вище, посилюються і збільшується кількість відмов в обслуговуванні, що позначається на доступності інформації, що передається по мережі.

З усіх зазначених причин, як було зазначено вище, після першого розрахунку та отримання значення метрики навіть при зміні параметра Load ці зміни не враховуються та перерахунок метрики не провадиться.

Розглянемо алгоритм перерахунку навантаження. Поточні реалізації протоколу не використовують параметри Load для розрахунку метрики. Для того, щоб обійти ці обмеження, можна використовувати адаптивний алгоритм реагування на зміни навантаження, який задається різницевим рівнянням (3):

$$Load = \alpha \cdot Load + (1 - \alpha) \cdot Load_{new} \quad 0 \leq \alpha \leq 1 \tag{3}$$

Відповідно до особливостей різницевого рівняння, значення параметра Load, що обчислюється за поточний інтервал на контролері, буде залежати від значень параметра Load, обчисленого на попередньому інтервалі та значень параметра Load, отриманого за поточний інтервал від маршрутизатора. При цьому вага останнього в результаті обчислень поточного такту буде залежати від значення коефіцієнта a [11]. Зі збільшенням даного коефіцієнта зменшується чутливість даного алгоритму до змін у навантаженні, зі зменшенням даного коефіцієнта збільшується чутливість алгоритму до змін у навантаженні. Питання про те, яке значення коефіцієнта вибрати у разі конкретних топології та моделі трафіку (закону розподілу ймовірностей навантаження) є відкритим і вимагає подальшого дослідження.

На рівні контролера задається граничне значення, яке забезпечує умову реакції на зміни в навантаженні, спільно із завданням коефіцієнта α визначається загальна реакція алгоритму на зміни навантаження в мережі. Оскільки при обчисленні метрики для маршруту маршрутизатором використовуються цілі значення параметрів (пропускної спроможності, затримки, навантаження, надійності), то і обчислення на рівні контролера має сенс роби-

ти з цілими числами, тоді результат обчислень слід округлювати до найближчого цілого значення, щоб згодом передавати маршрутизатору. Обчислення здійснюється для кожного інтерфейсу маршрутизатора, параметри якого може отримати контролер.

Крім питання про вибір коефіцієнта, α також постає питання про застосування запропонованого механізму у разі конкретної мережевої топології. Він також вимагає окремого дослідження, але можна сказати про крайні випадки такого питання. Немає сенсу використовувати запропонованої механізм у мережі з топологією, зображеної на рисунку 3.

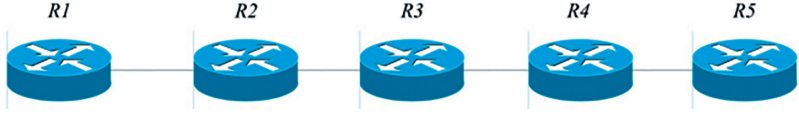

Рис. 3. Мережева топологія

Оскільки така топологія є послідовністю маршрутизаторів, з'єднаних між собою послідовно, існує єдиний маршрут до будь-якої з мереж-призначення. Внаслідок цього перерахунок метрики та обчислення алгоритму не мають сенсу і займають процесорний час контролера та маршрутизаторів мережі.

Після того, як внаслідок зміни значення навантаження було досягнуто певного (заданого адміністратором) граничного значення цього параметра, контролер передає на маршрутизатори (один або кілька) рішення про перерахунок маршруту. Оскільки маршрутизатору, який бере участь у роботі EIGRP, відомі поточні значення параметра навантаження, передача цих параметрів не потрібна. Після отримання рішення про перерахунок маршрутів маршрутизатор запускає обчислення метрики для всіх маршрутів, або для тих маршрутів, які дотичні значенням метрики, що змінилося, відповідно до поточних специфікацій EIGRP без будь-яких змін. Така кінцева реалізація запропонованого методу задіяє механізми та алгоритми, що вже є на мережевих пристроях, і не вимагає змін ні в апаратній, ні в програмній реалізації мережевих пристроїв. Запропонований алгоритм разом з усіма обчисленнями розгортається на контролері, у ролі якого може виступати будь-яка платформа, апаратна чи програмна з підтримкою відповідних програмних інтерфейсів. Архітектура запропонованого рішення наведено на рисунку 4.

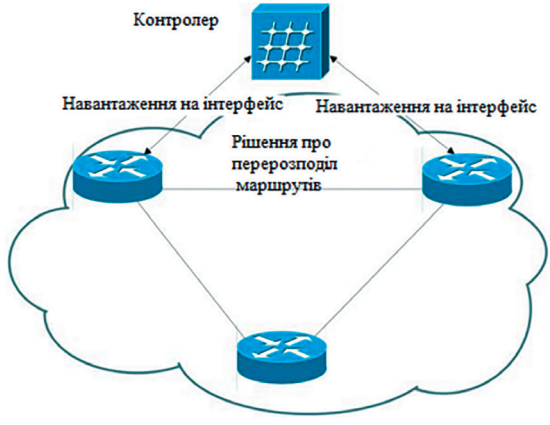

Рис. 4. Пропоноване рішення щодо обліку навантаження в мережі ПД

Якщо високе навантаження діє на всіх каналах у мережі, то перерахунок метрики не дозволить перенаправити частину трафіку менш завантаженим каналом, оскільки останніх у мережі немає.

Розглянемо механізм збору інформації з вузла мережі. Розглянутий алгоритм пропонується використовувати в рамках гібридної реалізації програмно-визначуваної мережі.

При реалізації запропонованого методу практично використовувалося:

- Устаткування Cisco Systems Inc.
- Програмні компоненти Cisco Systems Inc., які складаються з операційної системи для мережевого обладнання з встановленими API, а також програмних бібліотек, сумісних із зазначеними API (Cisco IOS 15.4.2, ONE Platform Kit (onePK)).

Cisco® Open Network Environment (ONE) є комплексним рішенням, яке дозволяє впровадити в існуючу мережну інфраструктуру елементи програмно-визначеної мережі, зокрема, елементи гібридної моделі програмно-визначуваної мережі. По суті, це рішення включає набір взаємопов'язаних технологій і механізмів:

- API для різноманітних платформ Cisco Systems Inc;
- контролер;
- додатки агенти для взаємодії з контролером.

Можливості onePK є реалізацією гібридної моделі SDN. Однак, за допомогою цих можливостей також може бути реалізована класична модель SDN, зокрема, за допомогою onePK на мережевих пристроях можуть бути впроваджені OpenFlow-агенти, кожен з яких є частиною архітектури класичної моделі SDN.

Пакет розробки onePK сумісний з усіма основними платформами Cisco. Гнучке середовище розробки, включене до складу onePK, надає програмний рівень представлення мережевих елементів за допомогою API, що підтримуються об'єктно-орієнтованими мовами програмування [12, 13].

Центральним елементом архітектури onePK є єдиний набір бібліотек API для всіх основних платформ Cisco.

По суті, цей рівень інфраструктури (платформи зі встановленими бібліотеками API) надає рівень абстракції для специфічних платформенних рішень. Така реалізація дозволяє розробникам додатків не концентруватися на специфічних особливостях окремих платформ чи всієї інфраструктури, що значно спрощує розробку та збільшує масштабованість додатків. Розробники можуть використовувати ті самі бібліотеки API у всій інфраструктурі, навіть якщо окремі мережеві пристрої працюють під управлінням різних операційних систем. Між рівнем уявлень та рівнем мережевої інфраструктури будується канал для забезпечення їхньої взаємодії, як правило, у рамках клієнт-серверної моделі взаємодії. Вся описана вище архітектура onePK представлена на рисунку 5.

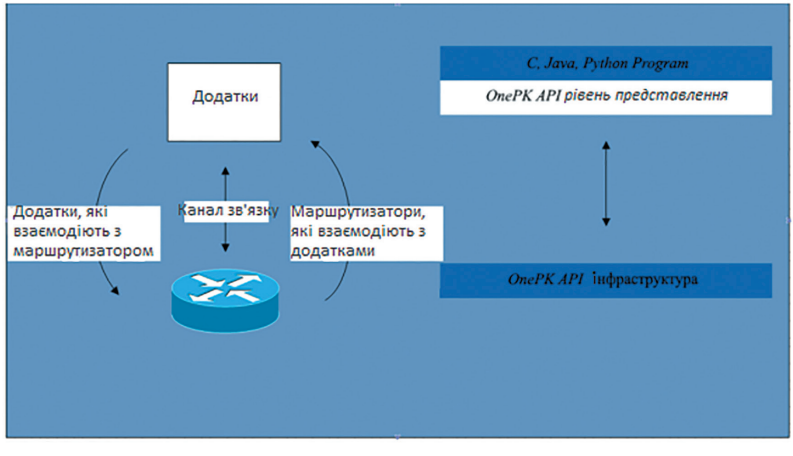

Рис. 5. Архітектура onePK

Існує кілька моделей розгортання onePK додатків. Додатки onePK можуть бути розгорнуті:

- на пристроях Cisco (комутаторах, маршрутизаторах);
- на інтегрованих у пристрої Cisco обчислювальних елементів;
- на зовнішніх серверах.

При реалізації механізму було обрано модель розгортання додатків на зовнішньому сервері програми onePK, оскільки запускаються на зовнішніх серверах, пов'язаних з IP з мережевими пристроями. Принцип роботи цієї моделі розгортання проілюстровано на рисунку 6.

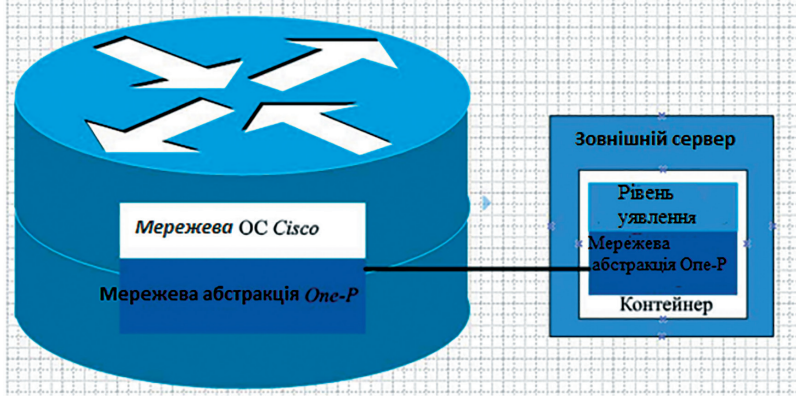

Рис. 6. Модель розгортання додатків на зовнішньому сервері

Ця модель дозволяє розробникам та адміністраторам мережевої інфраструктури вибирати платформу для роботи за власними критеріями. Платформи (серверні) можуть бути використані:

- сервери під управлінням операційної системи GNU/Linux;
- сервери під керуванням операційної системи Windows;
- мобільні пристрої під керуванням операційних систем Android або iOS (Apple).

Ці платформи можуть запускати виконання onePK або в окремих програмних контейнерах, або в просторі операційної системи сервера. Такий підхід забезпечує найбільший рівень ізоляції onePK додатків.

Розглянемо реалізацію механізму перерахунку навантаження. Програма, що реалізує запропонований алгоритм обліку навантаження, написана об'єктно-орієнтованою мовою програмування Java. Вибір в якості мови програмування Java обумовлений його багатоплатформністю [12], а також великою кількістю матеріалів і готових бібліотек. При цьому використані спеціальні бібліотеки API для onePK, створені спеціально для мови Java. Програма складається з трьох основних компонентів:

- DeviceSetup модуль, що власне реалізує з'єднання до API onePK пристрою;
- PinningHandler – модуль верифікації TLS сесії;

Recalculation – модуль зчитує параметри вхідного та передаючого навантаження, а так само здійснює її перерахунок за формулою (3) і передає нове значення на пристрій.

Висновки та пропозиції. Розглянуте рішення пропонується у рамках концепції програмно-визначуваної мережі. Ця концепція виносить площину управління мережею на новий архітектурний рівень, що дозволяє приймати рішення на основі великої кількості параметрів, що належать до мережі в цілому, що значно збільшує можливості застосування алгоритму, а також підвищує якість та доцільність його рішень. Таким чином, представлене рішення має такі характеристики:

- здатність отримувати дані від мережевих пристроїв про навантаження в мережі та її зміні;
- централізований аналіз та обробка отриманих даних на контролері;
- застосування адаптивних алгоритмів для прийняття рішень, відповідно зі змінами в навантаженні;
- концентрація процесорного навантаження на контролері.

Застосування описаного в статті методу дозволяє, по-перше, стабілізувати роботу EIGRP, і, по-друге, забезпечити більший контроль над IP-мережею передачі даних, що, в сукупності, дозволяє запобігти відмовам у обслуговуванні та забезпечити властивість доступність..

ЛІТЕРАТУРА

1. Боброва О., Колесник М. Програмно-визначені мережі: архітектура, технології, засоби управління // *Наукові праці Української інженерно-педагогічної академії. Серія: Технічні науки*. 2019. № 4. С. 7 – 13.

2. Клименко М., Шмарда О. Програмно-визначені мережі: переваги, недоліки, можливості // *Інформаційні технології та комп'ютерна інженерія*. 2017. Вип. 5. С. 5 – 10.

3. Маринченко І., Нікітін А. Управління трафіком в програмно-визначених мережах // *Науковий вісник Миколаївського національного університету імені В.О. Сухомлинського*. 2018. № 3(137). ч. 1. С. 117 – 120.

4. Міньков О., Курінний О., Мінькова Ю. Аналіз можливостей мережі Cisco ONE в програмно-визначеній мережі // *Системні технології*. 2018. № 3(96). С. 43 – 50.

5. Шевчук С., Мелешко В. Програмно-визначені мережі: аналіз стану розробки // *Комп'ютерні науки та інформаційні технології*. 2017. Вип. 163. С. 101 – 108.

6. Арлов О. І., Селезньов Д. Є. Основні напрями розвитку програмно-визначених мереж // *Науковий вісник Національного гірничого університету*. 2019. № 4. С. 32 – 37.

7. Твердохліб А.О., Коротін Д.С. Ефективність функціонування комп'ютерних систем при використанні технології блокчейн і баз данних. *Таврійський науковий вісник. Серія: Технічні науки*. 2022 (6).

8. Цвик О.С. Аналіз і особливості програмного забезпечення для контролю трафіку. *Вісник Хмельницького національного університету. Серія: Технічні науки*. 2023. (1).

9. Новіченко Є.О. Актуальні засади створення алгоритмів обробки інформації для логістичних центрів. *Таврійський науковий вісни*к. Серія: *Технічні науки*. 2023 (1).

10. Зайцев Є.О. Smart засоби визначення аварійних станів у розподільних електричних мережах міст. *Таврійський науковий вісник. Серія: Технічні науки*. 2022 (5).

11. Karmakar N., Zhou J., Liu H. *A Survey of Traffic Engineering Techniques in Software Defined Networks* // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. Issue 3. P. 2911.

12. Летенко І. Д. Нечітка керування трафіком модель динамічного у програмованих мережах // *Системи управління та інформаційні технології*. 2015. Т. 62. No 4.1. 3. 179 – 184.

13. Красов А. В., Левін М. В. Можливості управління трафіком у рамках концепції SDN // IV Міжнародна науково-технічна та науково-методична конференція «Актуаль-2015. С. 350 – 354.

14. Doyle D., Carroll J. Routing TCP/IP Vol. 1. Cisco Press. 2005. 936p.

15. Doyle D., Carroll J. Routing TCP/IP Vol. 2. Cisco Press. 2001. 976p.

16. White R., Slice D., Retana A. Optimal Routing Design. Cisco press, 2005, 504 p.

17. Pepelnjak I. EIGRP network design solutions. Cisco press. 2000. 384 p.

18. Zinin A. Cisco IP Routing: пакет forwarding and Intra-domain routing. Addison Wesley Professional. 2001. 656 p.

19. Weisfeld M. Object-Oriented thought process. Addison Wesley, 2009. 309 p.

20. Scratch S. R. Object-Oriented and classical software engineering. McGraw Hill. 2007. 654 p.

REFERENCES

1. Bobrova O., Kolesnyk M. Software-defined networks: architecture, technologies, management tools // *Scientific works of the Ukrainian Engineering and Pedagogical Academy. Series: Technical sciences.* 2019. No 4. P. 7 – 13 [in Ukrainian].

2. Klymenko M., Shmarda O. Software-defined networks: advantages, disadvantages, opportunities // *Information technologies and computer engineering*. 2017. Issue 5. Pp. 5 – 10 [in Ukrainian].

3. Marinchenko I., Nikitin A. Traffic management in software-defined networks // *Scientific Bulletin of V.O. Mykolaiv National University. Sukhomlynskyi*. 2018. No. 3(137), part 1. P. 117 – 120 [in Ukrainian].

4. Minkov O., Kurinnyi O., Minkova Yu. Analysis of capabilities of the Cisco ONE network in a software-defined network // *System technologies.* 2018. No. 3(96). P. 43 – 50 [in Ukrainian].

5. Shevchuk S., Meleshko V. Software-defined networks: analysis of the state of development // *Computer sciences and information technologies.* – 2017. Issue 163. Pp. 101 – 108 [in Ukrainian].

6. Arlov O.I., Seleznyov D.E. Main directions of development of software-defined networks // *Scientific Bulletin of the National Mining University.* 2019. No. 4. P. 32 – 37 [in English].

7. Tverdokhlib A.O., Korotin D.S. Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz dannykh. T*avriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky*. 2022. (6) [in Ukrainian].

8. Tsvyk O.S. Analiz i osoblyvosti prohramnoho zabezpechennia dlia kontroliu trafiku. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ceriia: Tekhnichni nauky*. 2023. (1) [in Ukrainian].

9. Novichenko Ye.O. Aktualni zasady stvorennia alhorytmiv obrobky informatsii dlia lohistychnykh tsentriv. T*avriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky*. 2023 (1) [in Ukrainian].

10. Zaitsev Ye.O. Smart zasoby vyznachennia avariinykh staniv u rozpodilnykh elektrychnykh merezhakh mist. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky*. 2022. (5) [in Ukrainian].

11. Karmakar N., Zhou J., Liu H. *A Survey of Traffic Engineering Techniques in Software Defined Networks* // IEEE Communications Surveys & Tutorials. 2019. Vol. 21, Issue 3. P. 2911 [in English].

12. Letenko I. D. Fuzzy traffic management model of dynamic in programmable networks // *Management systems and information technologies*. 2015. T. 62. No. 4.1. Q. 179 – 184 [in Ukrainian].

13. Krasov A.V., Levin M.V. Possibilities of traffic management within the SDN concept // IV International scientific-technical and scientific-methodical conference Aktual-2015. C. 350-354 [in Ukrainian].

14. Doyle D., Carroll J. Routing TCP/IP Vol. 1. Cisco Press. 2005. Pp. 936 [in English].

15. Doyle D., Carroll J. Routing TCP/IP Vol. 2. Cisco Press. 2001. Pp. 976 [in English].

16. White R., Slice D., Retana A. Optimal Routing Design. Cisco press. 2005. Pp. 504 [in English].

17. Pepelnjak I. EIGRP network design solutions. Cisco press. 2000. Pp. 384 [in English].

18. Zinin A. Cisco IP Routing: forwarding and Intra-domain routing. Addison Wesley Professional. 2001. Pp. 656 [in English].

19. Weisfeld M. Object-Oriented thought process. Addison Wesley. 2009. Pp. 309 [in English].

20. Scratch S. R. Object-Oriented and classical software engineering. McGraw Hill. 2007. Pp. 654 [in English].

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 03.12.2023