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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Дослідження процесів автоматизації керування мережевими пристроями**

Виконав(ла): курсу 6, груп и СНм-61
студент(ка) спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

Шоцький М.І.
(підпис) (прізвище та ініціали)

Керівник Марценко С.В.
(підпис) (прізвище та ініціали)

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

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

Рецензент Жаровський Р.О.
(підпис) (прізвище та ініціали)

Тернопіль
2021

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

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

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня МАГІСТР
(назва освітнього ступеня)

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

студенту Шоцькому Максиму Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи **Дослідження процесів автоматизації керування мережевими пристроями**

Керівник роботи **Марценко Сергій Володимирович, к.т.н., доц.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « » 20___ року № .

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічне завдання на дослідження процесів автоматизації керування мережевими пристроями

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ. 1 Аналіз предметної області; 1.1 Аналіз автоматизації керування мережевими пристроями на основі командної стрічки; 1.2 Аналіз автоматизації мережевого налаштування через графічні інтерфейси; 1.3 Аналіз засобів автоматизації мережевих налаштувань; 1.4 Висновки до першого розділу; 2 Розробка та впровадження методів та засобів автоматизації керування мережевими пристроями; 2.1 Автоматизація управління мережею через використання сценаріїв; 2.2 Автоматизація управління на основі RedHat Ansible для Cisco пристроїв; 2.3 Автоматизація керування мережею через використання програмно конфігурованих мереж SDN; 2.4 Автоматизація управління мережею через мережі на основі намірів IBN; 2.5 Висновки до другого розділу; 3 Охорона праці та безпека в надзвичайних ситуаціях; 3.1 Охорона праці; 3.1.1 Безпечні умови праці при монтажі комп'ютерної мережі; 3.2 Безпека в надзвичайних ситуаціях; 3.2.1 Функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуації мирного та воєнного часу; 3.3 Висновки до третього розділу; Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Приймак М.В., проф. каф. КН		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст.викл. каф ОХ		

7. Дата видачі завдання _____

1.1 КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	**1.2** Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.09.21-27.09.21	*Виконано*
2.	Підбір наукових джерел щодо дослідження процесів	28.09.21-04.10.21	*Виконано*
	автоматизації керування мережевими пристроями		
3.	Переклад та опрацювання наукових джерел щодо	05.10.21-11.10.21	*Виконано*
	автоматизації керування мережевими пристроями		
4.	Виконання дослідження щодо процесів	12.10.21-18.10.21	*Виконано*
	автоматизації керування мережевими пристроями		
5.	Оформлення розділу «Аналіз предметної області»	19.10.21-25.10.21	*Виконано*
6.	Оформлення розділу «Розробка та впровадження	26.10.21-01.11.21	*Виконано*
	методів та засобів автоматизації керування мережевими		
	пристроями»		
7.	Виконання завдання до підрозділу «Охорона праці»	09.11.21-15.11.21	*Виконано*
8.	Виконання завдання до підрозділу «Безпека в	16.11.21-22.11.21	*Виконано*
	надзвичайних ситуаціях»		
9.	Оформлення кваліфікаційної роботи	23.11.21-29.11.21	*Виконано*
10.	Нормоконтроль	30.11.21-05.12.21	*Виконано*
11.	Перевірка на плагіат	30.11.21	*Виконано*
12.	Попередній захист кваліфікаційної роботи	14.12.21	*Виконано*
13.	Захист кваліфікаційної роботи	21.12.2021	

Студент _____ Шоцький М.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження процесів автоматизації керування мережевими пристроями // Кваліфікаційна робота // Шоцький Максим Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм–61 // Тернопіль, 2021 // С. 69 , рис. – 12 , табл. – 1 , кресл. – , додат. – 4 , бібліогр. – 54 .

Ключові слова: АВТОМАТИЗАЦІЯ, КЕРУВАННЯ, КОНФІГУРУВАННЯ, ПРОГРАМНО КОНФІГУРОВАНІ МЕРЕЖІ, МЕРЕЖІ НА ОСНОВІ НАМІРІВ.

У роботі виконано дослідження процесів автоматизації керування мережевими пристроями, що дало змогу розробити рекомендації щодо впровадження відповідних методів та засобів автоматизації для мереж різної складності та розмірів.

В першому розділі кваліфікаційної роботи вісвітлено питання аналізу автоматизації налаштування мережевих пристроїв, що дало змогу класифікувати засоби та методи виконання цієї процедури в мережах різного призначення. Виявлено сильні та слабкі сторони кожного з розглянутих методів автоматизації налаштування мережевих пристроїв.

Другий розділ кваліфікаційної роботи присвячений розробці та можливому впровадженню методів та засобів автоматизації керування мережевими пристроями та функціями.

Метою дослідження є аналіз процесів автоматизації керування мережевими пристроями. Об'єкт дослідження – процес передавання, захисту та віртуалізації потоків інформації в мережах. Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

ANNOTATION

Research of processes of network devices management automation // Diploma thesis Master degree // Shotskyi Maksym I. // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2021 // P. 69 , Tables – 1 , Fig. – 12 , Diagrams – , Annexes. – 4 , References – 54 .

The study of processes of network devices management automation was performed in the work, which allowed to develop recommendations for the implementation of appropriate methods and means of automation for networks of different complexity and size.

The first section of the qualification work covers the analysis of network devices automation, which allowed to classify the means and methods of performing this procedure in networks for various purposes. The strengths and weaknesses of each of the considered methods of the configuration of network devices automating are identified.

The second section of the qualification work is devoted to the development and possible implementation of methods and tools for automating the management of network devices and functions.

The aim of the study is to analyze the processes of network device management automation. The object of research is the process of transmission, protection and virtualization of information flows in networks. Subject of research - the theory of design of telecommunication networks, the theory of data transmission.Key words: AUTOMATION, CONTROL, CONFIGURATION, SOFTWARE DEFINED NETWORKS, INTENT BASED NETWORKS

ЗМІСТ

ВСТУП

Швидкий розвиток мережевих технологій приводить до виникнення ряду питань, що потребують швидкого рішення та гарантування правильності роботи. Навіть у мережах невеликого розміру потреба автоматизації керування мережевими пристроями та функціями стає необхідною умовою їх успішного функціонування, розвитку та забезпечення виконання покладених функцій.

Дослідження показали, що існує цілий ряд методів та засобів для організації автоматизації мережевого управління. Вони відрізняються складністю впровадження та ефективністю роботи. Разом з цим розгортання автоматизації керування мережевими пристроями потребує відповідної кваліфікації мережевих фахівців для побудови та підтримки мереж.

Актуальність теми. Автоматизація процесів керування мережевими пристроями та функціями є важливою та актуальною задачею через все більш складніші мережеві архітектури, що вимагають ефективної, надійної та захищеної роботи.

Мета і завдання дослідження. Метою дослідження є аналіз процесів автоматизації керування мережевими пристроями, що дасть змогу підвищити швидкість впровадження нових послуг, здійснювати моніторинг стану мережі, виконувати захист вразливих елементів. Досягнення поставленої мети передбачає виконання наступних завдань: здійснити аналіз процесів автоматизації керування мережевими пристроями; виявити різні підходи до автоматизації та класифікувати їх застосування; запропонувати дієві засоби та методи автоматизації керування мережевими пристроями та функціями.

Об’єкт дослідження – процес передавання, захисту та віртуалізації потоків інформації в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

Практичне значення одержаних результатів. Висвітлено питання аналізу автоматизації налаштування мережевих пристроїв, що дало змогу класифікувати засоби та методи виконання цієї процедури в мережах різного призначення. Дослідження виконано використовуючи підхід від простішого до складнішого. При цьому результати роботи відображають основні тенденції в розвиткові організації роботи мереж. Наведено приклади використання автоматизації у реальних ситуаціях. Виявлено сильні та слабкі сторони кожного з розглянутих методів автоматизації налаштування мережевих пристроїв. Подано аналіз застосування найбільш відомих програмних продуктів для автоматизації мережевого конфігурування. Досліджено розробку та можливість впровадження методів та засобів автоматизації керування мережевими пристроями та функціями. За результатами роботи виявлено основні тенденцій в автоматизації сучасних мереж. Автоматизації на основі використання сценаріїв має перевагу гнучкості свого застосування та можливості масштабування у різних випадках та розмірах мережі. Проте, даний тип автоматизації потребує знань програмування, що ускладнює його розгортання для мереж невеликого розміру з обмеженеми фінансовими ресурсами. Наступним популярним рішенням автоматизації є Red Hat Ansible, що надає широкий спектр дій, але потребує спеціалізованих знань, що уможливлює його використання за умови виконання зазначених умов. Останнім часом широкого розповсюдження набуло використання концепції та рішень на основі неї яка називаєть програно конфігуровані мережі SDN. При цьому автоматизація керування пристроями є дуже високою через використання спеціалізованого контролера та протоколу Open Flow. Даний підхід до автоматизації є з багатовендорною підтримкою, що дає змогу використовувати його в гетерогенних мережах і навіть при наявності не самого нового обладнання. Основими складнощами його впровадження можна вважати необхідність спеціалізованого контролера для управління мережею, що збільшує витрати, а також знань та вмінь з

програмування для створення програмних додатків. Як надбудова над SDN розглядається наступний виток еволюції мереж у вигляді мереж на основі намірів IBN. Це дає змогу ще більше пришвидшити розгортання нових послуг у мережі, проводити аудит та відслідковувати стан мережевих пристроїв та додатків.

Наукова новизна розробки: здійснено аналіз та класифікацію сучасних підходів автоматизації керування мережевими пристроями; проведено дослідження методів та засобів організації автоматизації управління мережею; запропоновано сучасні підходи до розв’язання задач автоматизації упрвління мережевими пристроями та функціями.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз автоматизації керування мережевими пристроями на основі командної стрічки

Більшість мережевих пристроїв для роботи в малому офісі чи корпоративній мережі підтримують налаштування через командну стрічку. Незважаючи на те, що даний процес є затратним в часі та має високу схильність до виникнення помилки налаштування, він залишається найбільш повноцінним за функціоналом налаштування і у деяких випадках є просто єдиним способом організувати всі інші процеси [1-54].

Автоматизація керування мережевими пристроями з використанням командної стрічки CLI (Command Line Interface) може бути організована через збереження резервних копій налаштувань на сервері і в подальшому їх завантаження на пристрій у випадку його виходу з ладу чи технічних несправностей.

Основним недоліком такого способу організації автоматизації є жорстка прив’язка операційних систем пристроїв до виробника та конкретної моделі. Зміна моделі на більш новішу чи заміна операційної системи може потребувати повної заміни команд для досягнення очікуваного результату. При такому підході потрібно відзначити, що використання резервування конфігураційних файлів прийнятний з формулюванням певних застережень. Хороший результат може бути досягнутий у невеликих мережах, при використанні однотипного обладнання та його централізованій плановій заміні, де рівень підготовки мережевого персоналу не є високим і впровадження додаткових процесів автоматизації може привести до створення більших складнощів ніж очікуваний результат.

Автоматизація при використанні командної стрічки досягається через можливість реплікації готових конфігурацій з незначними змінами

початкового коду. При цьому можна використовувати текстові редактори для копіювання блоків команд і вносити потрібні зміни з подальшим завантаженням на мережеві пристрої.

Іншим варіантом автоматизації налаштування є використання команд, що забезпечують конфігурацію визначеного діапазону елементів мережевих пристроїв. Наприклад, використання команди interface range на Cisco комутаторах дає змогу провести налаштування параметрів діапазону інтерфейсів заміст заходити в налаштування окремого інтерфейсу. Це пришвидшує процес введення однотипних параметрів. На рисунку 1.1 показано налаштування параметрів безпеки для портів комутатора

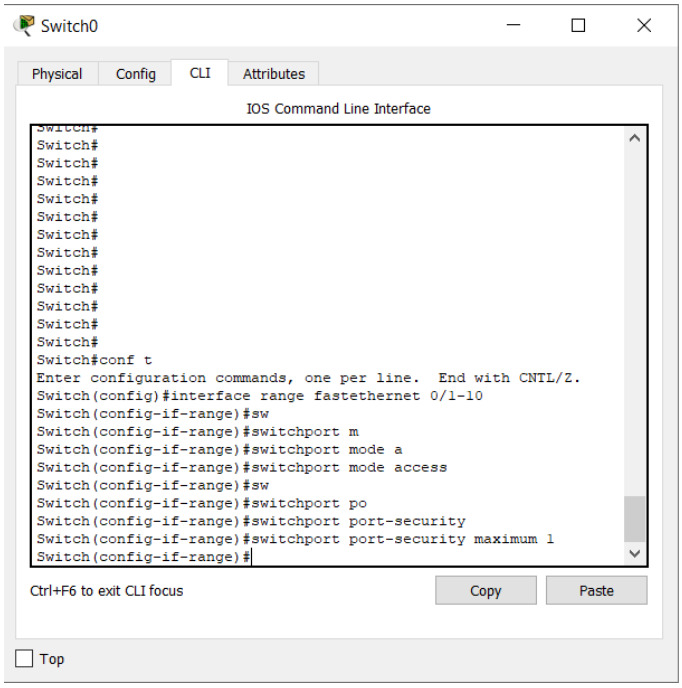

Рисунок 1.1 – Приклад автоматизації налаштування комутатора через використання групових команд

В даному прикладі показано налаштування обмеження динамічного вивчення MAC адрес для порта з вказанням, що тільки одна адреса може бути збереженою для портів в діапазоні з першого по десятий Fastethernet 0/1-10.

Використання функцій автоматизації через командну стрічку є доволі обмеженим, проте заслуговує на увагу через широку доступність для адміністратора.

1.2 Аналіз автоматизації мережевого налаштування через графічні інтерфейси

Велика частина користувачів мережевого устаткування не має бажання вивчати операційні системи різних виробників. Дуже часто буває, що і в межах одного виробника існує декілька операційних систем чи їх версій, що суттєво ускладнює процес налаштування мережевих функцій.

Для спрощення роботи з функціоналом пристроїв виробники все частіше вдаються до розробок графічних оболонок, що є більш зрозумілими для широкого загалу людей. Зникає необхідність розуміти в яких режимах повинна вводитись яка команда, знання синтаксису та послідовності виконання дій. Користувач на основі графічних закладок та заданих опцій вибирає потрібні дії, а машина перетворює це в програмний код і виконує.

Мережевий графічний інтерфейс часто був запізнілою думкою для мережевих постачальників. Інтерфейс командного рядка (CLI) був основним методом конфігурації та керування, а GUI був другорядним. Таким чином, якщо порівнювати CLI і GUI, ранні графічні інтерфейси були несерйозними спробами, які пропонували лише невелику частину загальних параметрів конфігурації для мережевих маршрутизаторів, комутаторів і брандмауерів.

Іншою важливою перевагою CLI є те, що з практикою конфігурація може бути набагато швидшою в порівнянні з графічним інтерфейсом. За допомогою кількох текстових команд користувач може налаштувати інтерфейси, протоколи маршрутизації та списки доступу. Ці елементи потребують кількох клацань мишею та пошуку відповідних сторінок і вкладок у графічному інтерфейсі.

Крім того, командний рядок можна створювати і легко впроваджувати за допомогою простих функцій копіювання та вставки, а також за допомогою інструмента для створення сценаріїв і клієнта безпечної оболонки. Таким чином, керувати мережевими пристроями, які потребують індивідуального, поетапного керування, набагато легше за допомогою CLI.

З точки зору підтримки та усунення несправностей, CLI можна використовувати для швидкого пошуку інформації за допомогою різних ярликів команд. Це включає деталізацію статистики інтерфейсу, створення сценаріїв для поширеної інформації та використання пошуку за ключовими словами або шаблонами. Ці методи показують справжню силу CLI над новішими графічними методами.

Незважаючи на переваги CLI, веб-інтерфейс GUI (Graphical User Interface) – у поєднанні з централізованою, хмарною архітектурою – обганяє CLI як інтерфейс переходу. Насправді, графічні інтерфейси починають функціонуват так добре, що керування CLI може здаватися застарілим.

З сучасними мережевими платформами графічний інтерфейс у багатьох випадках більше не відходить від CLI. Таким чином, більше часу та зусиль було вкладено в простоту використання, можливість централізованого надсилання оновлень конфігурації на кілька пристроїв і створення адміністрування користувача, що забезпечує баланс між простотою та глибиною конфігураційних можливостей.

GUI, як правило, більш зручний для користувачів. За допомогою командних рядків у вас є більш тривалий час навчання, перш ніж оволодіти необхідністю належної конфігурації та усунення несправностей. Однак завдяки добре розробленому графічному інтерфейсу ця сама крива навчання різко скорочується.

Крім того, можливість перегляду різноманітних мережевих інтерфейсів і перевірки стану пристрою у візуальному форматі в графічному інтерфейсі

може допомогти виявити проблеми, а не переглядати ту саму інформацію в текстовому форматі.

На рисунку 1.2 показано приклад графічного інтерфейсу для налаштування бездротового маршрутизатора Linksys WRT 300N.

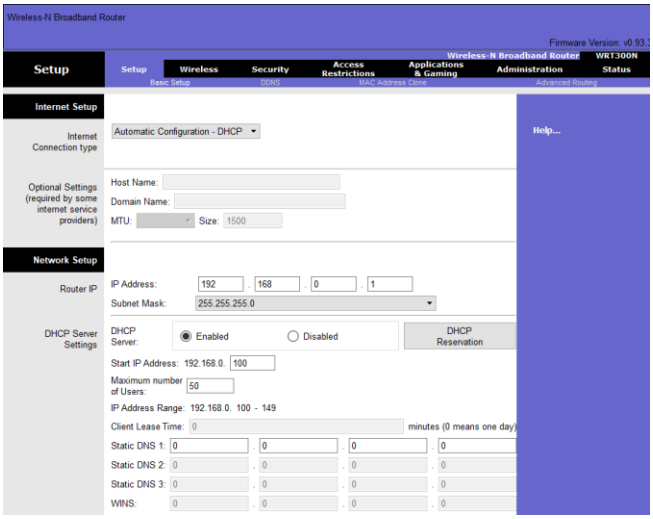

Рисунок 1.2 – Грфічний інтерфейс бездротового маршрутизатора

Для даного пристрою є можливість ввести параметри вручну або під’єднати його до серверів автоматизованого налаштування. При цьому рівень автоматизації налаштувань є доволі мінімальним, оскільки більшість значень потібно вводити. З іншої сторони можливість створення помилки конфігрування також зменшується через візуальне спостереження за результатом та необхідність вибору правильної закладки, що відповідає підрежиму введення. Одним з важливих аспектів такого підходу є зменшення навантаження на адміністратора мережі і відсутність потреби в спеціалізованих знаннях кожної конфігурації.

1.3 Аналіз засобів автоматизації мережевих налаштувань

Автоматизація мережі – це чудовий спосіб для організацій прискорити свою роботу та швидко масштабувати аспекти своїх мережевих процесів,

конфігурацій та тестування. Однак при неправильному виконанні мережева автоматизація також може поширювати серйозні проблеми у великих масштабах; уявіть, що машина виконує завдання знову і знову без нагляду, поширюючи помилку по всій організації. Автоматизація мережі може бути шляхом до покращення швидкості, стійкості, якості та інтелекту мереж, але важливо робити це правильно з самого початку, інакше є ризик створити більший головний біль, ніж очікуваний результат від впровадження прийнятих рішень.

Високоякісні інструменти для автоматизації мережі є ключем до того, щоб мережеві процеси не збивалися. Існує безліч програмних рішень, для організації автоматизації конфігурування мережевих пристроїв та процесів. Наприклад, одним з популярних є SolarWinds® Network Configuration Manager (NCM), добре відомий, стабільний і добре підтримуваний інструмент. Він забезпечує високоякісну автоматизацію мережі та конфігурації, що особливо корисно, оскільки відстеження конфігурацій вручну, як правило, є трудомістким і схильним до помилок.

Автоматизація мережі – це процес налаштування програмного забезпечення для автоматичного керування, налаштування, тестування, розгортання та керування мережевими пристроями (незалежно від того, чи є вони фізичними чи віртуальними). Це покращує ефективність на великих підприємствах і часто може зменшити експлуатаційні витрати та людські помилки, пов’язані з ручним керуванням. Ручні підходи стають все більш неможливими зі зростанням кількості пристроїв на підприємствах. Підвищення автоматизації IT стає важливим для багатьох підприємств.

Деякі засоби автоматизації мережі дозволяють відображати мережеві пристрої та виявляти пристрої, тоді як інші забезпечують керування конфігурацією мережі, надання мережевих ресурсів або планування потужності. Автоматизація мережі може в основному керуватися сценаріями (тобто використовувати мови сценаріїв і програмування для виконання

завдань, коли з’являється тригер) або програмною (також відома як інтелектуальна мережева автоматизація).

Метою засобів автоматизації мережі є підвищення ефективності, зменшення людських помилок і, як наслідок, зменшення операційних витрат. Існує багато типів інструментів для автоматизації мережі. Для інструментів автоматизації мережі на основі сценаріїв і програмного забезпечення існує кілька видів платформ та інтерфейсів.

В таблиці 1.1 наведено аналіз декількох популярних засобів автоматизації з вазанням можливості їх пробного використання. Потрібно відмітити, що більшість засобів є платними, проте мають підтримку у вигляді оновлень, що забезпечує адаптивність до нових трендів.

Таблиця 1.1 – Порівняльний аналіз засобів автоматизації

Назва засобу автоматизації	Період безкоштовного використання	Опис
SolarWinds Network Configuration Manager	30 – днів	Програмне забезпечення корпоративного рівня для автоматизації конфігурування мережі
Kiwi CatTools	14 – днів	Потужний і простий засіб автоматизації для малого бізнесу
ManageEngine Network Configuration Manager	30 – днів	Програмне забезпечення для конфігурування мережі, що базується на сценаріях з використанням шаблонів Configlets

Продовження таблиці 1.1

LAN-Secure Configuration Center	30 – днів	Базовий засіб конфігурування мережі з певною автоматизацією
BMC Truesight Network Automation	немає	Повноцінний засіб автоматизації для досвідчених користувачів

Існує також багато інструментів автоматизації мережі з відкритим кодом, включаючи Ansible, Puppet і Chef. Це гідні та широко використовувані інструменти для певних випадків використання, але вони не мають стандартних можливостей, простих у використанні інтерфейсів і підтримки постачальників інструментів, розроблених спеціально для корпоративного використання.

Одним з кращих представників програмного забезпечення для автоматизації мережі є SolarWinds Network Configuration Manager (NCM). NCM легко встановити, використовувати та налаштувати, а інтерфейс є зручним для користувача. Це означає, що розпочати роботу просто, а повна система автоматизації конфігурації мережі у вас під рукою.

NCM дозволяє виконувати швидкі та широкі зміни конфігурації, використовуючи автоматизацію мережі для масового внесення цих змін. Масове коригування заощаджує час і може зменшити людські помилки, пов’язані з спробами виконати цей процес вручну. NCM також дозволяє розробляти шаблони змін і конфігурації, що означає, що ви можете автоматично розгортати їх і застосовувати до нових пристроїв або передавати нові конфігурації на сотні чи тисячі пристроїв за потребою. Приклад NCM подано на рисунку 1.3

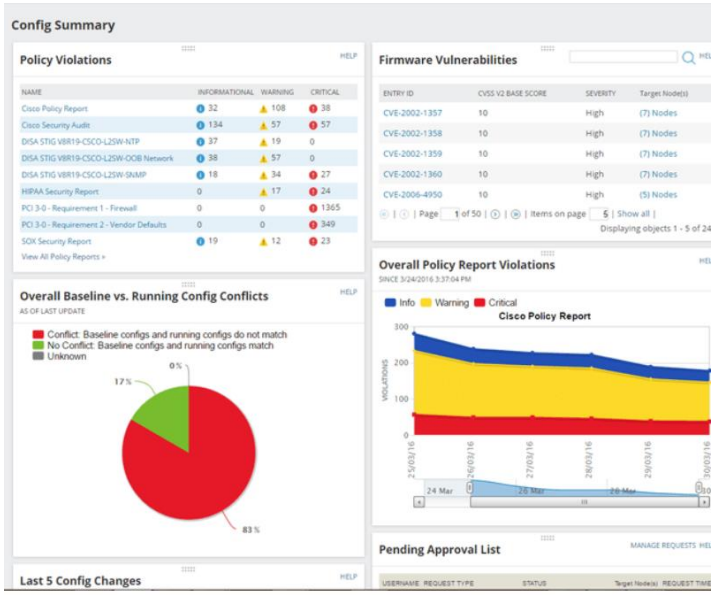

Рисунок 1.3 – Вікно NCM

Крім того, NCM відстежує та записує конфігурації пристрою та попереджає, якщо були внесені зміни. Якщо зміна призведе до проблем, є можливість негайно скасувати зміни або швидко усунути неполадки. В даному програмному продукті також можна побачити, чи було внесено несанкціоновану зміну конфігурації. Це відстеження (поряд із використанням внутрішніх політик і стандартів безпеки) дозволяє організації підтримувати відповідність правилам. NCM також може перевіряти відповідність конфігурації пристрою, щоб переконатися, що вони оновлені, і попередити про будь-які вразливості. Він також інтегрується з Національною базою даних уразливостей, що дає можливість отримувати саму актуальну інформацію та бути повідомленим, коли у вашій системі буде виявлено відому вразливість. Після цього NCM може запровадити масову зміну, щоб виправити вразливість.

Нарешті, конфігурації пристрою можна створювати, керувати та відновлювати через платформу, що означає, що є можливість швидко повернутися до старої конфігурації, якщо сталася помилка, або відновити з резервної копії, якщо є збій або помилка. NCM надає найважливіші функції автоматизації мережі, і це високоякісний інструмент із готовими

конфігураціями та звітами про відповідність, які допоможуть швидко розпочати роботу.

Kiwi CatTools® - це простий, але потужний інструмент для автоматизації мережі та управління змінами, створений з урахуванням потреб мереж малого бізнесу. Спрощуючи планування автоматичного резервного копіювання конфігурацій пристроїв для маршрутизаторів, брандмауерів тощо, Kiwi розроблено, щоб допомогти уникнути необхідності переписувати вбудований код, якщо виникають проблеми з конфігурацією мережевого пристрою. Приклад вікна Kiwi показано на рисунку 1.4.

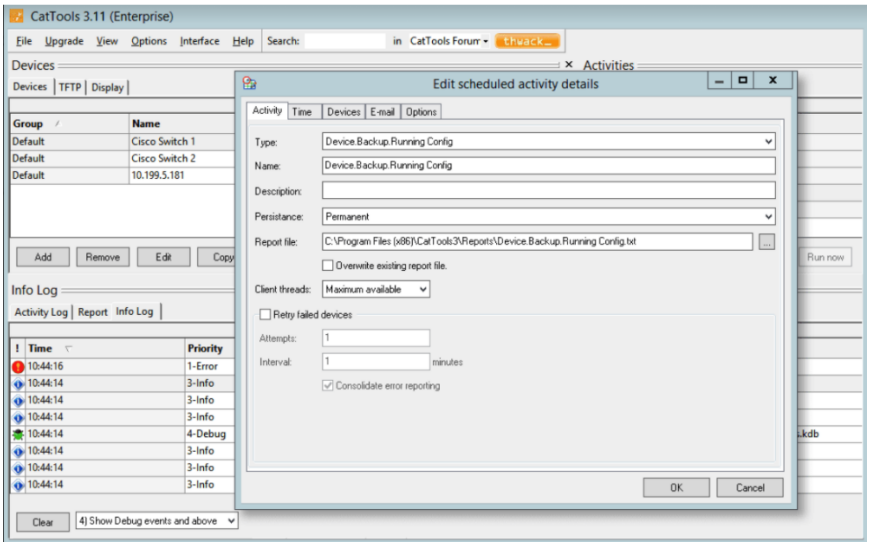

Рисунок 1.4 – Вікно Kiwi CatTools

Kiwi CatTools підтримує резервне копіювання через TFTP за допомогою вбудованого TFTP-сервера, що полегшує резервне копіювання файлів конфігурації, покращує ефективність і контроль під час масового розгортання змін конфігурації, а також спрощує відкат до попередніх хороших конфігурацій. Ці автоматичні резервні копії також можна налаштувати через індивідуальні проміжки часу, щоб не порушувати основні робочі години. Kiwi CatTools включає вбудовану підтримку пристроїв для десятків виробників пристроїв IPv4 і IPv6, включаючи, але не обмежуючись цим, Cisco, HP, 3Com, Enterasys, F5, Huawei і Juniper.

Kiwi CatTools також може автоматизувати мережеві сповіщення для надсилання звітів електронною поштою, коли виявляє зміни конфігурації на пристроях, щоб ви могли відстежувати несанкціоновані зміни конфігурації пристрою та можливі ризики безпеки. Є можливість використовувати Kiwi для перегляду та аналізу змін між конфігураціями, як-от порівняння початкових конфігурацій запуску та діючої конфігурації або поточної конфігурації пристрою та останнього резервного копіювання, на консолі або у звіті, щоб інформувати про зусилля з усунення несправностей.

ManageEngine Network Configuration Manager – це ще один чудовий вибір програмного забезпечення для автоматизації мережі. Він працює на основі сценарію, використовуючи шаблони під назвою Configlets. Configlets допомагають користувачеві виконувати команди для зміни паролів або ввімкнення SNMP, команд списку контролю доступу або інших змін конфігурації. Шаблони Configlets вже є частиною Менеджера конфігурації мережі ManageEngine, коли його встановлюється, але також можна додати їх вручну, якщо потрібно щось налаштувати.

Усі сценарії зміни конфігурації можна автоматизувати за допомогою так званого “Режим виконання сценарію”. Сюди входять команди, які потребують підтвердження користувача, і їх можна автоматизувати, навіть якщо після виконання команди є затримка відповіді або якщо необхідно змінити порядок виконання сценаріїв. Можна запланувати всі види завдань конфігурації, як буде вибрано, а Configlets можна налаштувати, щоб запобігти повторенню роботи. Можна запланувати виконання завдань щогодини, щодня, щотижня, щомісяця або за потребою. Коли Configlets буде виконано, відбувається отримання сповіщення електронною поштою.

Він також включає інструменти для управління змінами в реальному часі, відстеження активності користувачів та аудиту відповідності.

Lan-Secure Configuration Center – це інструмент керування мережею, призначений для автоматизації розгортання конфігурації, створення

резервних копій, моніторингу історії конфігурацій та відновлення старих конфігурацій. Це неспецифічний інструмент виробника і спеціально розроблений для використання в середовищі пристроїв кількох виробників. Він працює за допомогою Telnet, протоколів оболонки SSH і протоколів SNMP. Приклад даного програмного продукту показано на рисунку 1.5.

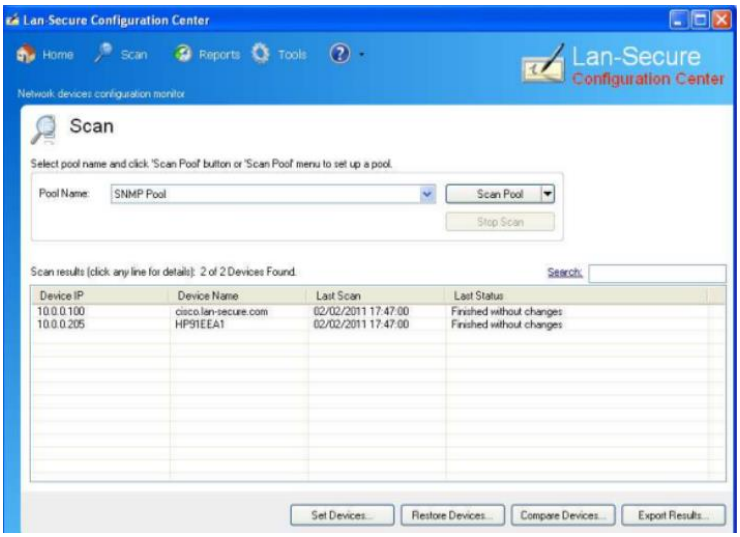

Рисунок 1.5 – Вікно налаштування Lan-Secure Configuration Center

Його можна запускати вручну або автоматично, і можна налаштувати його на певні дати або час. Lan-Secure Configuration Center включає автоматичні аукціони, такі як виконання команд, надсилання пасток SNMP або сповіщення електронною поштою про зміни конфігурації. Завдяки можливостям звітності, реєстрації та експорту це хороший базовий інструмент.

BMC надає численні інструменти моніторингу мережі та керування операціями, але TrueSight Automation for Networks спеціально розроблений для керування конфігурацією мережі та її автоматизації. Можна використовувати цей інструмент, щоб запровадити широкі зміни конфігурації та відновити їх або відстежити зміни, коли це необхідно. Він працює з використанням підходу, заснованого на політиці, із шаблонами, налаштованими наборами правил та інтегрованим керуванням змінами.

Завдяки попередньо налаштованим політикам, розробленим відповідно до нормативних вимог, можна забезпечити відповідність вимогам. Приклад вікна TrueSight Automation показано на рисунку 1.6.

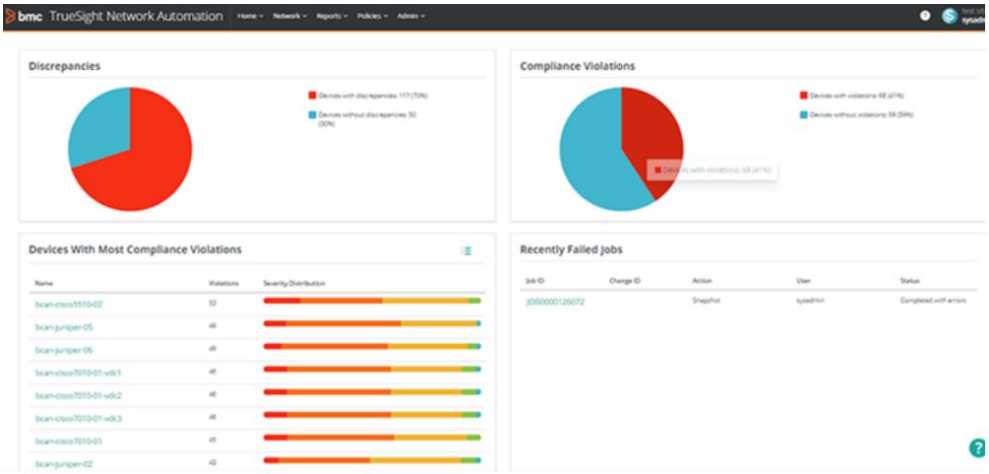

Рисунок 1.6 – Вікно TrueSight Automation

TrueSight Automation for Networks включає інструменти усунення загроз, такі як автоматичне керування вразливими місцями та реагування на них, і використовує національну базу даних NIST для виявлення вразливостей та оновлення пристроїв.

TrueSight Automation for Networks – це високоякісний інструмент із багатьма функціями, але він не настільки зручний, як міг би бути. Немає способу перевести всю систему в автономний режим чи пробні конфігурації, що може призвести до складного процесу розгортання та відкату. Зв’язати з корпоративними системами набагато легше, ніж з такими інструментами, як Chef і Puppet, але, безумовно, потрібен певний досвід написання сценаріїв.

1.4 Висновки до першого розділу

Перший розділ кваліфікаційної роботи висвітлює питання аналізу автоматизації налаштування мережевих пристроїв, що дало змогу класифікувати засоби та методи виконання цієї процедури в мережах різного

призначення. Дослідження виконано використовуючи підхід від простішого до складнішого. При цьому результати роботи відображають основні тенденції в розвиткові організації роботи мереж. Наведено приклади використання автоматизації у реальних ситуаціях. Виявлено сильні та слабкі сторони кожного з розглянутих методів автоматизації налаштування мережевих пристроїв. Подано аналіз застосування найбільш відомих програмних продуктів для автоматизації мережевого конфігурування.

2 РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ АВТОМАТИЗАЦІЇ КЕРУВАННЯ МЕРЕЖЕВИМИ ПРИСТРОЯМИ

2.1 Автоматизація управління мережею через використання сценаріїв

Протягом останніх кількох років мережева автоматизація набула широкої популярності. Як результат, здається, що сучасному інженеру доступний постійно зростаючий запас інструментів, які допомагають реалізувати автоматичну конфігурацію мережі та керування змінами. Хоча наявність такого широкого й різноманітного набору інструментів, безсумнівно, є великою перевагою для спільноти, це, безсумнівно, може здатися трохи приголомшливим і навіть лякаючим.

Існує багато реалізацій автоматизації, що базуються на мові програмування Python. Netmiko – це виняткова бібліотека Python, розроблена Кірком Байерсом, призначена для роботи як рівень абстракції над реалізацією протоколу SSHv2 Paramiko Python. По суті, Netmiko – це переосмислений Paramiko і адаптований для взаємодії саме з мережевими пристроями. Насправді, Netmiko було запрограмовано на усвідомлення особливостей мережевих пристроїв, що згодом приховує ці деталі нижнього рівня від інженера з автоматизації.

Наприклад, Netmiko розуміє, що під час зміни конфігурації пристрою Cisco всі надіслані команди повинні спочатку починатися з підвищення до режиму глобальної конфігурації і, таким чином, автоматично видаватимуть “налаштування терміналу” від вашого імені. Ці, здавалося б, дрібні деталі в кінцевому підсумку призводять до різкого зниження складності сценаріїв автоматизації.

NAPALM – це бібліотека Python, розроблена Девідом Баррозу, ретельно написана для спрощення автоматизованої взаємодії з мережевими

пристроями незалежно від операційної системи за допомогою уніфікованого API.

Наприклад, існує потреба отримати інформацію BGP Neighbor зі своєї мережі. Тепер, якщо всі пристрої є Cisco IOS, можна просто використовувати Netmiko, щоб задати “show ip bgp neighbor” і легко отримати цю інформацію. Але що, якщо мережа була 1/3rd Cisco, 1/3rd Juniper і 1/3rd Arista?

Використовуючи NAPALM Getters, можна отримати всю цю інформацію, просто ввівши команду “get_bgp_neighbors”, яка не залежить від постачальника. Сутність NAPALM видаватиме відповідні команди показу для кожної платформи, для кожного пристрою та надає цей результат у стандартизованому форматі, структурованому в JSON.

Крім того, Netmiko тісно інтегрується з рішеннями для синтаксичного аналізу, такими як TextFSM і Genie, надаючи можливість повертати вихідні дані команд show у вигляді структурованих даних.

Genie – це бібліотека Python, розроблена та призначена для автоматизованого тестування мережі. Він простий у використанні і відразу дає інженеру неймовірний рівень уявлення про стан їхньої мережі. Використовуючи Genie CLI, інженери, по суті, можуть фіксувати та порівнювати різні знімки стану мережі та запускати автоматичне порівняння, щоб точно визначити, що змінилося.

Уявімо, що використовується OSPF у мережі. Видаючи команду Genie CLI “genie learn ospf”, Genie автоматично запускатиме величезний обсяг різних специфічних для OSPF команд відображення та збиратиме інформацію, щоб задокументувати всю інформацію про OSPF. Тепер, якщо припустимо, що згодом зв’язок по низхідній лінії в якійсь частині мережі раптово втрачено. Завдяки повторному введенню команди “genie learn ospf” поточний стан OSPF буде пізнано заново, що дасть Genie можливість порівняти поточний непрацюючий стан з вихідним.

Згодом Genie визначить усі відповідні зміни та поверне інженеру чітко спрямований підсумок елементів, щоб почати усунення несправностей. Це функція, яку будь-який інженер, навіть той, хто не має досвіду програмування, може навчитися використовувати протягом одного дня навчання, і ця функція буде постійно оптимізувати та спрощувати усунення несправностей у мережі.

NCClient – це бібліотека Python, написана для спрощення сценаріїв та автоматизації за протоколом NETCONF. Сучасна автоматизація спрямована на взаємодію з мережевими пристроями за допомогою API, а не інтерфейсу командного рядка. NETCONF має багато функцій і пропонує можливість точного детального контролю над мережею завдяки своїй здатності блокувати сховище конфігурацій пристрою, проводити повну заміну конфігурації та багато іншого.

Протокол на основі XML може бути дещо складним у використанні, особливо для початківців. Однак NCClient та його функція “Менеджер” спрощують це, вмикаючи API для операцій RPC як викликів методів з підтримкою фільтрації Subtree і Xpath. Таким чином, NCClient став стандартним способом взаємодії з протоколом NETCONF і важливою бібліотекою Python для сучасного інженера з автоматизації мережі.

RESTCONF – це легкий протокол на основі HTTP без збереження стану, який вийшов на сцену як новіший і простіший двоюрідний брат NETCONF. Оскільки присутність RESTCONF поступово збільшується, існує ймовірінсть, що буде чути все більше і більше про бібліотеку запитів Python. Бібліотека Requests абстрагує багато складнощів створення HTTP-запитів за простим API і пропонує кілька вбудованих методів для отримання або надсилання даних до API на основі REST, наприклад запити GET або POST.

Для кожного методу Requests повертає об’єкт “відповідь” для перевірки. У цей об’єкт включено багато надзвичайно корисних атрибутів, таких як повернутий код стану та можливість легкого виклику винятків у разі

збою за допомогою об’єкта raise_for_status(). Якщо ви збираєтеся писати сценарії Python для автоматизації своєї мережі через RESTCONF, ви збираєтеся імпортувати бібліотеку запитів.

2.2 Автоматизація управління на основі RedHat Ansible для Cisco пристроїв

Підприємства переживають безпрецедентні зміни і потребують гнучких, масштабованих і орієнтованих на безпеку продуктів, щоб допомогти їм у цифровій трансформації. Оскільки операційна складність зростає, загальні витрати необхідно керувати та зменшувати. Багато збільшення складності експлуатації можна швидко відновити за допомогою автоматизації та за допомогою таких інструментів, як Ansible®. Наприклад, автоматизація мережі дозволяє командам мережевих операцій налаштовувати, масштабувати, захищати та інтегрувати мережеву інфраструктуру та послуги програм набагато швидше та ефективніше.

IT-організації шукають рішення, які відповідають їхнім експлуатаційним вимогам, одночасно спрощуючи управління та забезпечуючи оркестрацію. Автоматизація мережі є ключем до керування цими новими, складними та потенційно незнайомими хмарними середовищами. Всесвітній піврічний трекінг програмного забезпечення IDC, опублікований на початку 2019 року, показує, що світовий ринок програмного забезпечення для автоматизації та конфігурації IT буде становити до 11,5 мільярдів доларів у 2025 році, а в 2020 році – 7,9 мільярда доларів.

Існує тенденція збільшення керування мережею тримаючи витрати під контролем за допомогою автоматизації мережі. Щоб прискорити розробку та розгортання додатків, а також скоротити час отримання вартості, підприємства застосовують методології NetDevOps. Оскільки цифрові

шаблони підприємств розширюються, а їхні мережі стають все більш комплексними, керування цими середовищами стає дедалі складнішим.

Багато організацій досі керують своїми мережами, ввійшовши на кожен мережевий пристрій вручну, вносячи необхідні зміни практично без відстеження чи перевірки. Тільки в Cisco доступні десятки середовищ і платформ для керування всім, починаючи від комутації мережі, маршрутизації та конфігурації брандмауера. Ця складність робить керування й організацію автоматизації в цих середовищах надзвичайно складною.

Автоматизація цих процесів – планування, розробка, тестування, розгортання та обслуговування – є трансформаційним підходом до спрощення IT-операцій. Тим не менш, впровадження рішень з автоматизації відбувалося набагато повільніше серед мережевих команд, ніж очікувалося, тому що:

– інструменти автоматизації є власністю та специфічними для окремої функції або платформи;

– прийняття нових методологій, які впливають на повсякденні процеси та процедури, може бути складним завданням, що вимагає від користувачів навчання новим технологіям;

– щоб успішно робити більше з меншими витратами, потрібно, щоб вся IT-організація ухвалила, створила та виконала план дій, який включає автоматизацію як частину корпоративної та IT-культури.

Гнучкість важлива як для операторів мережі, так і для системних адміністраторів. Red Hat® Ansible® Automation Platform дозволяє вибрати процеси та процедури для автоматизації. Це дозволяє починати з малого, а потім розширюватися відповідно до стратегії, цілей і навичок, щоб принести найбільшу користь організації. Отримується гнучкість, щоб швидко автоматизувати те, що потрібно і коли це потрібно.

Red Hat Ansible Automation Platform дозволяє додати управління та створити міст між мережевими операціями та іншими частинами IT-

організації. Він допомагає командам керувати складними мережевими розгортаннями, додаючи контроль, знання та делегування в середовища на базі Ansible. Інтеграція Ansible із Cisco IOS® надає переваги автоматизації. Коли розгортається модель Network DevOps для прискорення розгортання додатків, щоб швидко реагувати на потреби бізнесу, Red Hat Ansible Automation Platform допомагає досягти дійсно гнучкої операційної моделі, покращуючи автоматизацію, інновації та узгодженість у IT-середовищі, підтримуючи безпеку. зосереджене послідовне робоче середовище.

Red Hat Ansible Automation Platform забезпечує підтримку автоматизації для широкого спектру програмно-визначених мережевих продуктів і платформ Cisco.

Для сучасних користувачів Cisco немає дефіциту в опціях автоматизації, але багато рішень або спеціально створені для конкретного продукту, або вимагають глибокого знання складних мов програмування. Red Hat Ansible Automation Platform мінімізує потребу в розумінні специфічних для платформи конструкцій, а також командних рядків, реалізацій та інтерфейсів прикладного програмування (API), що стосуються виробника. На рисунку 2.1 показано архітектуру Red Hat Ansible.

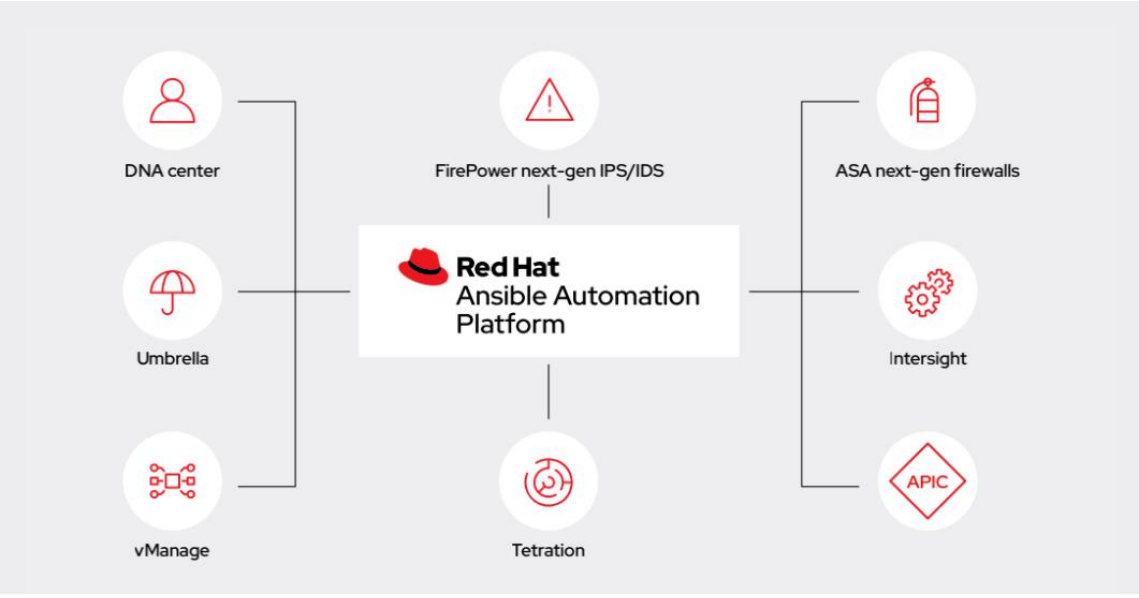

Рисунок 2.1 – Архітектура Red Hat Ansible для Cisco продуктів

Red Hat Ansible Automation Platform є основою для створення та роботи служб автоматизації в масштабі, надаючи підприємствам інструменти та операційну структуру, у спільному та надійному середовищі виконання. Він пропонує новий підхід до автоматизації мереж та управління інфраструктурою на базі Cisco, використовуючи давні відносини Red Hat з Cisco, піонером у сфері мереж, підтримуючи широкий спектр популярних продуктів і рішень. На рисунку 2.2 показано роботу Red Hat Ansible з Cisco ACI.

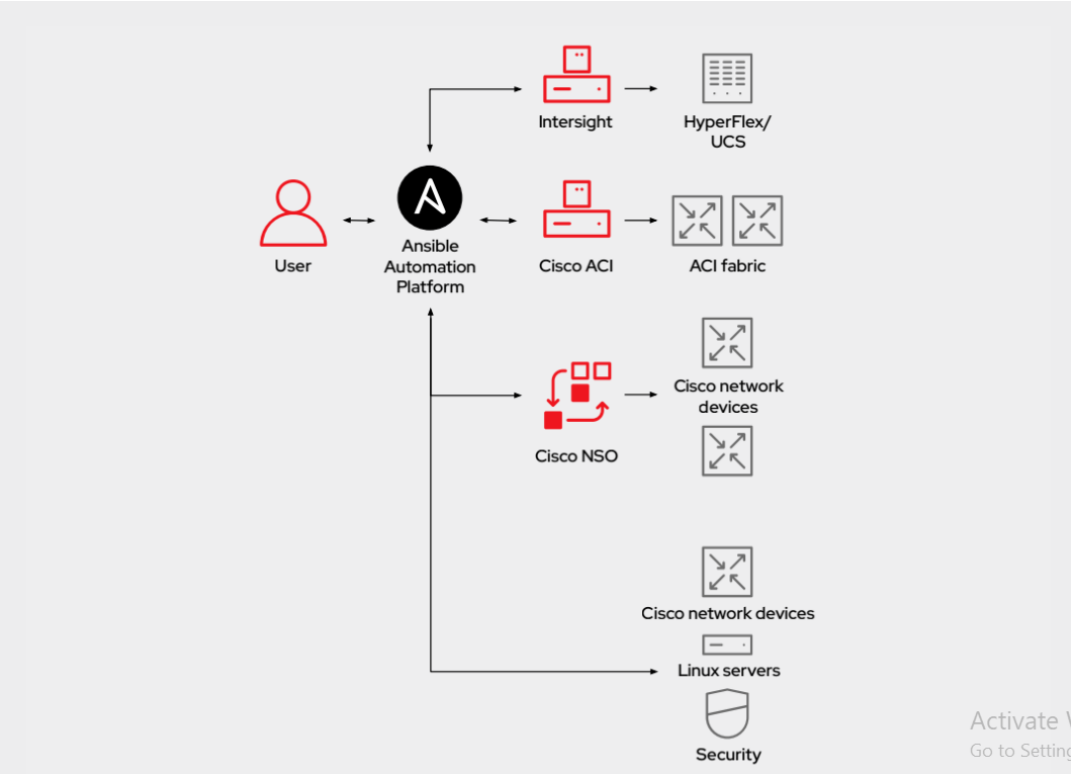

Рисунок 2.2 – Архітектура роботи Red Hat з Cisco ACI

Red Hat Ansible Automation Platform дозволяє виконати три прості дії, щоб прискорити процес автоматизації підприємства:

– створення: почніть швидше, об’єднавши потужність величезної спільноти Ansible з відкритим кодом і попередньо створених сертифікованих колекцій вмісту з найбільш часто використовуваних ролей і модулів Ansible.

Кодифікуйте свою інфраструктуру та поділіться між командами, локально або в хмарі;

– масштаб: передайте свою автоматизацію в кілька доменів і в різні варіанти використання. Зацікавлені сторони з розробників, операцій та бізнес-команд можуть використовувати Ansible способами, які найкраще підходять для них окремо, не сповільнюючи час розробки;

– залучайте: розширте свою автоматизацію за допомогою аналітики, політики та управління, а також керування вмістом. Ці інструменти в Red Hat Ansible Automation Platform роблять управління операціями більш ефективним, дозволяючи одноразово вирішувати проблеми та ділитися результатами з усіма.

Окрім економії часу та енергії, цей унікальний підхід забезпечує більшу віддачу від наявних інвестицій. Багато організацій інвестували значні ресурси в інструменти точкової автоматизації для керування конкретними пристроями або робочими процесами, але ця автоматизація не масштабується. Red Hat Ansible Automation Platform сприяє автоматизації між командами й пристроями, надаючи різним групам, у тому числі NetOps, ITOps та SecOPs, загальний рівень і мову в єдиній панелі для автоматизації практично кожного пристрою, контролера іншого виробника чи контролера Cisco.

Поряд із економією часу та ресурсів, автоматизація конфігурації та керування інфраструктурою Cisco має додаткову перевагу для бізнесу: підвищення безпеки критично важливих систем і даних. Red Hat Ansible Automation Platform надає всі інструменти та функції, необхідні для впровадження автоматизації безпеки та підходів DevSecOps. Він поєднує просту, зручну для читання мову автоматизації та надійне середовище виконання, яке можна компонувати, із можливостями спільного використання та спільної роботи, орієнтованих на безпеку.

Автоматизація може допомогти швидше та масштабніше виявляти загрози безпеці та реагувати на них. Існує можливість захистити свій бізнес, об’єднуючи свої команди, інструменти та процеси за допомогою послідовної, спільної платформи автоматизації.

Щоб отримати гнучкість та узгодженість мережевих адміністраторів, які необхідні для підтримки максимальної продуктивності інфраструктури, важливо автоматизувати кожен компонент центру обробки даних – маршрутизатори, комутатори, брандмауери, IPAM, контролери, сервери та контейнери. Але робити це за допомогою окремих точкових продуктів або специфічних для платформи інструментів не є ефективним підходом до масштабування управління інфраструктурою.

Red Hat Ansible Automation Platform інтегрується з платформами Cisco, забезпечуючи автоматизацію у більшому масштабі та швидкості, щоб існувала можливість:

– використання перевірених проектів Cisco, щоб спростити впровадження, скоротити час розгортання та підвищити загальну вартість володіння.

– зменшення кількості ручних завдань, щоб забезпечити безпомилкові, повторювані конфігурації.

– постійна перевірка зміни, щоб забезпечити відповідність.

Red Hat Ansible Automation Platform є одним із найпопулярніших інструментів для спрощення рутинних завдань конфігурації мережі. Він забезпечує автоматизацію конфігурації після встановлення, що прискорює трансформацію IT для більшої швидкості та можливості швидкого впровадження високоефективної операційної моделі, яка краще відповідає потребам вашого бізнесу.

2.3 Автоматизація керування мережею через використання програмно конфігурованих мереж SDN

Традиційні мережні архітектури погано відповідають вимогам сучасних підприємств, операторів і кінцевих користувачів. Завдяки широким галузевим зусиллям, які очолює Open Networking Foundation (ONF), програмно-конфігурована мережа (SDN) перетворює мережеву архітектуру.

В архітектурі SDN рівні управління та даних роз'єднані, мережний інтелект і стан логічно централізовані, а базова мережева інфраструктура абстрагується від додатків. В результаті підприємства та оператори отримують безпрецедентну програмованість, автоматизацію та контроль мережі, що дає їм змогу будувати високомасштабовані та гнучкі мережі, які легко адаптуються до мінливих потреб бізнесу.

ONF – це неприбутковий галузевий консорціум, який керує розвитком SDN і стандартизує критичні елементи архітектури SDN, такі як протокол OpenFlow®, який структурує зв'язок між рівнями керування та даних підтримуваних мережевих пристроїв. OpenFlow® – це перший стандартний інтерфейс, розроблений спеціально для SDN, що забезпечує високопродуктивний детальний контроль трафіку на мережевих пристроях кількох постачальників.

Наразі SDN на основі OpenFlow впроваджується в різноманітні мережеві пристрої та програмне забезпечення, надаючи значні переваги як підприємствам, так і операторам, зокрема:

– централізоване управління та контроль мережевих пристроїв від кількох постачальників;

– покращена автоматизація й керування за допомогою використання загальних API для абстрагування основних мережевих деталей із систем і програм оркестровки та забезпечення;

– швидкі інновації завдяки змозі надавати нові мережеві можливості та послуги без необхідності налаштовувати окремі пристрої або чекати випуску постачальника;

– можливість програмування операторами, підприємствами, незалежними постачальниками програмного забезпечення та користувачами (не тільки виробниками обладнання) з використанням загальних середовищ програмування, що дає всім сторонам нові можливості для збільшення доходу та диференціації;

– підвищена надійність і безпека мережі в результаті централізованого й автоматизованого керування мережевими пристроями, уніфікованого застосування політики та меншої кількості помилок конфігурації;

– більш детальний контроль мережі з можливістю застосування комплексних і широкомасштабних політик на рівнях сеансу, користувача, пристрою та програми;

– кращий досвід роботи для кінцевих користувачів, оскільки програми використовують централізовану інформацію про стан мережі, щоб легко адаптувати поведінку мережі до потреб користувачів.

SDN – це динамічна і гнучка мережева архітектура, яка захищає наявні інвестиції, одночасно забезпечуючи мережу в майбутньому. Завдяки SDN сучасна статична мережа може перетворитися на розширювану платформу надання послуг, здатну швидко реагувати на зміни бізнесу, кінцевих користувачів і потреб ринку.

Зростання мобільних пристроїв і вмісту, віртуалізація серверів і поява хмарних сервісів є одними з тенденцій, які спонукають мережеву індустрію переглянути традиційні архітектури мереж. Багато звичайних мереж є ієрархічними, побудованими з рівнями комутаторів Ethernet, розташованих у вигляді дерева. Цей дизайн мав сенс, коли домінуючими були обчислення клієнт-сервер, але така статична архітектура погано підходить для

динамічних обчислень і потреб у сховищі сучасних корпоративних центрів обробки даних, кампусів і середовищ оператора. Деякі з ключових обчислювальних тенденцій, що викликають потребу в новій мережевій парадигмі, включають:

– зміна шаблонів трафіку: у корпоративному центрі обробки даних характер трафіку значно змінився. На відміну від клієнт-серверних додатків, де основна частина комунікації відбувається між одним клієнтом і одним сервером, сучасні програми мають доступ до різних баз даних і серверів, створюючи шквал трафіку “схід-захід” між машинами, перш ніж повертати дані до кінцевого пристрою користувача в класичній моделі руху “північ-південь”. У той же час користувачі змінюють шаблони мережевого трафіку, прагнучи отримати доступ до корпоративного вмісту та додатків з будь-якого типу пристроїв (включаючи власний), підключаючись звідусіль і в будь-який час. Нарешті, багато керівників корпоративних центрів обробки даних розглядають модель корисних обчислень, яка може включати приватну хмару, загальнодоступну хмару або деяку комбінацію обох, що призведе до додаткового трафіку через глобальну мережу;

– “наближення IT до споживача”: користувачі все частіше використовують мобільні персональні пристрої, такі як смартфони, планшети та ноутбуки, для доступу до корпоративної мережі. IT-компанії перебувають під тиском, щоб узгодити ці персональні пристрої в тонкодисперсний спосіб, одночасно захищаючи корпоративні дані та інтелектуальну власність та відповідаючи вимогам;

– збільшення кількості хмарних сервісів: підприємства прийняли з великим ентузіазмом як загальнодоступні, так і приватні хмарні послуги, що як наслідок призвело до величезного зростання цих послуг. Підрозділи підприємства тепер хочуть мати гнучкість доступу до додатків, інфраструктури та інших IT-ресурсів на вимогу та à la carte. Щоб ускладнити, IT-планування хмарних служб має здійснюватися в середовищі підвищених

вимог безпеки, відповідності та аудиту, а також реорганізації бізнесу, об’єднання та злиття. Створення можливості самообслуговування, як у приватній, так і в загальнодоступній хмарі, вимагає гнучкого масштабування обчислювальних, сховищ і мережевих ресурсів, в ідеалі використовуючи підхід спільної точки зору та спільного набору інструментів;

– “великі дані” означають більшу пропускну здатність: для роботи з сьогоднішніми “великими даними” або меганаборами даних потрібна масивна паралельна обробка на тисячах серверів, кожен з яких потребує прямого підключення один до одного. Зростання меганаборів даних викликає постійний попит на додаткову пропускну здатність мережі в центрі обробки даних. Оператори гіпермасштабованих мереж центрів обробки даних стикаються з непростим завданням масштабування мережі до раніше немислимого розміру, підтримуючи зв’язок “будь-кого-до-будь-кого” без втрати під’єднання.

Задовольнити поточні вимоги ринку практично неможливо з традиційними мережевими архітектурами. Зіткнувшись із обмеженими або скороченими бюджетами, IT-відділи підприємства намагаються витягти максимум із своїх мереж, використовуючи інструменти керування на рівні пристроїв та ручні процеси. Провайдери стикаються з подібними проблемами, оскільки попит на мобільність і пропускну здатність різко зростає; прибуток знижується через зростання витрат на капітальне обладнання та постійний або зменшуючийся дохід. Існуючі архітектури мережі не були розроблені для задоволення вимог сучасних користувачів, підприємств і операторів; скоріше, розробники мереж лімітовані обмеженнями поточних мереж, які включають:

– складність, яка призводить до застою: на сьогоднішній день мережеві технології складалися в основному з дискретних наборів протоколів, призначених для надійного з’єднання хостів на будь-яких відстанях, швидкостях і топологіях. Щоб задовольнити ділові та технічні

потреби протягом останніх кількох десятиліть, галузь розробила мережеві протоколи, щоб забезпечити більш високу продуктивність і надійність, ширші можливості підключення та суворішу безпеку. Проте, як правило, протоколи визначають ізольовано, кожен з яких вирішує конкретну проблему і без будь-яких фундаментальних абстракцій. Це призвело до одного з основних обмежень сучасних мереж: складності. Наприклад, щоб додати або перемістити будь-який пристрій, IT фахівець повинен торкнутися кількох комутаторів, маршрутизаторів, брандмауерів, порталів веб-аутентифікації тощо, а також оновити списки керування доступом, мережі VLAN, якість послуг (QoS) та інші механізми на основі протоколів, використовуючи керування на рівні пристрою. інструменти. Крім того, слід враховувати топологію мережі, модель комутатора постачальника та версію програмного забезпечення. Через таку складність сучасні мережі є відносно статичними, оскільки IT прагне мінімізувати ризик порушення роботи служби. Статична природа мереж різко контрастує з динамічною природою сучасного серверного середовища, де віртуалізація серверів значно збільшила кількість хостів, які потребують підключення до мережі, і фундаментально змінила припущення про фізичне розташування хостів. До віртуалізації програми перебували на одному сервері і переважно обмінювалися трафіком з вибраними клієнтами. Сьогодні програми розподілені між кількома віртуальними машинами (VM), які обмінюються потоками трафіку один з одним. ВМ переміщуються для оптимізації та перебалансування робочих навантажень сервера, через що фізичні кінцеві точки існуючих потоків змінюються (іноді швидко) з часом. Міграція ВМ кидає виклик багатьом аспектам традиційної мережі, від схем адресації та просторів імен до базового поняття сегментованого дизайну на основі маршрутизації. На додаток до впровадження технологій віртуалізації, сьогодні багато підприємств використовують конвергентну IP-мережу для голосового, даних і відеотрафіку. Хоча існуючі мережі можуть надавати диференційовані рівні

QoS для різних програм, надання цих ресурсів дуже ручне. IT має налаштувати обладнання кожного постачальника окремо та налаштувати такі параметри, як пропускна здатність мережі та QoS, для кожного сеансу та програми. Через свою статичну природу мережа не може динамічно адаптуватися до змін трафіку, додатків і запитів користувачів;

– непослідовна політика: щоб запровадити політику всієї мережі, IT-спеціалістам, можливо, доведеться налаштувати тисячі пристроїв і механізмів. Наприклад, щоразу, коли створюється нова віртуальна машина, можуть знадобитися години, а в деяких випадках і дні, щоб IT переналаштувати списки керування доступом у всій мережі. Складність сучасних мереж дуже ускладнює для IT застосування послідовного набору доступу, безпеки, QoS та інших політик до все більш мобільних користувачів, що робить підприємство вразливим до порушень безпеки, недотримання правил та інших негативних наслідків;

– неможливість масштабування: оскільки вимоги до центру обробки даних швидко зростають, має рости і мережа. Однак мережа стає значно складнішою з додаванням сотень або тисяч мережевих пристроїв, які необхідно налаштовувати та керувати. IT також покладався на надмірну підписку на посилання для масштабування мережі на основі передбачуваних моделей трафіку; однак у сучасних віртуалізованих центрах обробки даних моделі трафіку неймовірно динамічні і тому непередбачувані. Мегаоператори, такі як Google, Yahoo! і Facebook, стикаються з ще більш складними проблемами масштабованості. Ці постачальники послуг використовують широкомасштабні алгоритми паралельної обробки та пов’язані з ними набори даних у всьому своєму обчислювальному пулі. Зі збільшенням обсягу програм кінцевих користувачів (наприклад, сканування та індексація всієї всесвітньої мережі, щоб миттєво повертати результати пошуку користувачам), кількість обчислювальних елементів різко зростає, а обмін наборами даних між обчислювальними вузлами може досягати

петабайт. Цим компаніям потрібні так звані гіпермасштабні мережі, які можуть забезпечити високопродуктивне недороге підключення сотень тисяч – потенційно мільйонів – фізичних серверів. Таке масштабування неможливо виконати за допомогою ручного налаштування. Щоб залишатися конкурентоспроможними, провайдери повинні надавати клієнтам дедалі вищу цінність, краще диференційовані послуги. Багатоарендність ще більше ускладнює їх завдання, оскільки мережа повинна обслуговувати групи користувачів із різними додатками та різними потребами в продуктивності. Ключові операції, які здаються відносно простими, такі як керування потоками трафіку клієнта для забезпечення індивідуального контролю продуктивності або доставки на вимогу, дуже складні для реалізації в існуючих мережах, особливо в масштабі оператора. Вони потребують спеціалізованих пристроїв на межі мережі, що збільшує капітальні та операційні витрати, а також час виходу на ринок для впровадження нових послуг.

– залежність від постачальника: оператори та підприємства прагнуть розгорнути нові можливості та послуги, щоб швидко реагувати на мінливі потреби бізнесу або запити користувачів. Однак їх здатність реагувати заважає циклам виробництва обладнання постачальників, які можуть становити три роки і більше. Відсутність стандартних відкритих інтерфейсів обмежує можливість мережевих операторів адаптувати мережу до їх індивідуальних середовищ. Ця невідповідність між вимогами ринку та можливостями мережі привела галузь до переломного моменту. У відповідь на це промисловість створила архітектуру програмно-визначеної мережі (SDN) і розробляє відповідні стандарти.

Програмно-конфігурована мережа (SDN) – це нова архітектура мережі, де управління мережею відокремлено від пересилання та програмується безпосередньо через програмні додатки. Ця міграція контролю, раніше тісно пов’язаного з окремими мережевими пристроями, на

доступні обчислювальні пристрої дозволяє абстрагувати базову інфраструктуру для додатків і мережевих служб, які можуть розглядати мережу як логічну або віртуальну сутність.

На рисунку 2.3 зображено логічний вигляд архітектури SDN. Мережевий інтелект (логічно) централізований у програмних контролерах SDN, які підтримують глобальне уявлення про мережу. В результаті мережа виглядає для програм і механізмів політики як єдиний логічний комутатор. Завдяки SDN підприємства та оператори отримують незалежний від постачальника контроль над усією мережею з однієї логічної точки, що значно спрощує проектування та роботу мережі. SDN також значно спрощує самі мережеві пристрої, оскільки їм більше не потрібно розуміти й обробляти тисячі стандартів протоколів, а лише приймати інструкції від контролерів SDN.

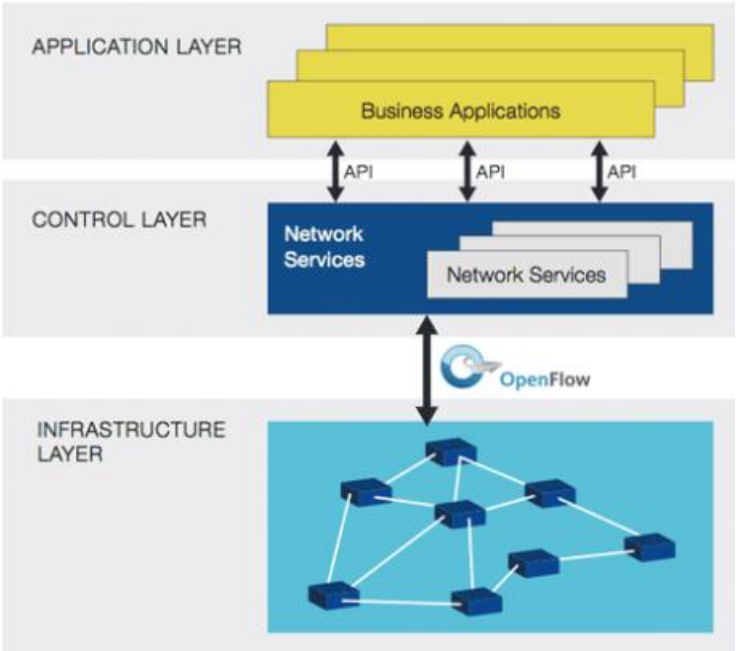

Рисунок 2.3 – Архітектура SDN

Можливо, найважливіше те, що оператори та адміністратори мережі можуть програмно налаштувати цю спрощену мережеву абстракцію замість того, щоб вручну кодувати десятки тисяч рядків конфігурації, розкиданих

серед тисяч пристроїв. Крім того, використовуючи централізований інтелект контролера SDN, IT може змінити поведінку мережі в режимі реального часу та розгорнути нові програми та мережеві послуги за лічені години чи дні, а не за тижні чи місяці, які потрібні сьогодні. Завдяки централізації стану мережі на рівні керування, SDN надає мережевим менеджерам гнучкість для налаштування, керування, захисту та оптимізації мережевих ресурсів за допомогою динамічних автоматизованих програм SDN. Більше того, вони можуть самостійно писати ці програми і не чекати, поки функції будуть вбудовані в власне та закрите програмне середовище постачальників у середині мережі.

На додаток до абстрагування мережі, архітектури SDN підтримують набір API, які дозволяють реалізувати загальні мережеві послуги, включаючи маршрутизацію, багатоадресну передачу, безпеку, контроль доступу, управління пропускною здатністю, інженерію трафіку, якість обслуговування, оптимізацію процесора та сховища, енергію використання та всі форми управління політикою, спеціально розроблені для досягнення бізнес-цілей. Наприклад, архітектура SDN дозволяє легко визначати та застосовувати послідовні політики як у дротових, так і в бездротових з’єднаннях у кампусі.

Аналогічно, SDN дає змогу керувати всією мережею за допомогою інтелектуальних систем оркестрування та надання. Open Networking Foundation вивчає відкриті API для просування управління кількома постачальниками, що відкриває двері для розподілу ресурсів на вимогу, надання самообслуговування, справді віртуалізованої мережі та безпечних хмарних послуг.

Таким чином, за допомогою відкритих API між рівнем керування SDN і прикладними рівнями бізнес-додатки можуть працювати на абстракції мережі, використовуючи мережеві послуги та можливості, не прив’язуючись до деталей їх реалізації. SDN робить мережу не стільки “обізнаною з

додатками”, скільки “налаштованою для додатків”, а програми не стільки “обізнаними про мережу”, скільки “з урахуванням можливостей мережі”. В результаті можна оптимізувати обчислення, сховище та мережеві ресурси.

ONF керується відомими підприємствами та постачальниками послуг, розробниками систем і додатків, компаніями з програмного забезпечення та комп’ютерів, а також постачальниками напівпровідників і мереж. Цей різноманітний перетин комунікаційної та обчислювальної індустрії допомагає гарантувати, що SDN та пов’язані з ним стандарти ефективно задовольняють потреби мережевих операторів у кожному сегменті ринку, зокрема:

Campus SDN – централізована автоматизована модель керування та надання SDN підтримує конвергенцію даних, голосу та відео, а також доступ у будь-який час і з будь-якого місця, дозволяючи IT постійно застосовувати політику як у дротовій, так і в бездротовій інфраструктурі. Аналогічно, SDN підтримує автоматичне надання та керування мережевими ресурсами, що визначаються окремими профілями користувачів і вимогами додатків, щоб забезпечити оптимальну роботу користувача в рамках обмежень підприємства.

SDN центру обробки даних. Архітектура SDN сприяє віртуалізації мережі, що забезпечує гіпермасштабування в центрі обробки даних, автоматизовану міграцію віртуальної машини, тіснішу інтеграцію зі сховищем, кращу завантаження сервера, менше споживання енергії та оптимізацію пропускної здатності.

SDN для хмари. Незалежно від того, чи використовується для підтримки приватного чи гібридного хмарного середовища, SDN дозволяє розподіляти мережеві ресурси надзвичайно еластичним способом, забезпечуючи швидке надання хмарних послуг і більш гнучку передачу зовнішньому хмарному провайдеру. Завдяки інструментам для безпечного

керування своїми віртуальними мережами підприємства та бізнес-підрозділи все більше довірятимуть хмарним сервісам.

SDN пропонує операторам зв’язку, операторам загальнодоступної хмари та іншим постачальникам послуг масштабованість та автоматизацію, необхідні для впровадження моделі корисних обчислень для IT-як-Сервіс, шляхом спрощення розгортання користувацьких послуг і послуг на вимогу, а також перехід на парадигма самообслуговування. Централізована, автоматизована модель керування та надання SDN значно полегшує підтримку мульти-арендаторів; забезпечити оптимальне розгортання мережевих ресурсів; зменшити як капітальні витрати, так і операційні витрати; і збільшити швидкість і вартість обслуговування.

OpenFlow® – це перший стандартний комунікаційний інтерфейс, визначений між рівнями керування та пересилання в архітектурі SDN. OpenFlow® забезпечує прямий доступ і маніпулювання площиною пересилання мережевих пристроїв, таких як комутатори та маршрутизатори, як фізичних, так і віртуальних (на основі гіпервізора). Саме відсутність відкритого інтерфейсу до площини пересилання призвело до характеристики сучасних мережевих пристроїв як монолітних, закритих і схожих на мейнфрейм. Жоден інший стандартний протокол не робить те, що робить OpenFlow®, і такий протокол, як OpenFlow®, потрібен, щоб перенести керування мережею з мережевих комутаторів на логічно централізоване програмне забезпечення.

OpenFlow® можна порівняти з набором інструкцій ЦП. Як показано на рисунку 2.4, протокол визначає основні примітиви, які можуть використовуватися зовнішньою програмною програмою для програмування площини пересилання мережевих пристроїв, подібно до того, як набір інструкцій центрального процесора програмує комп’ютерну систему.

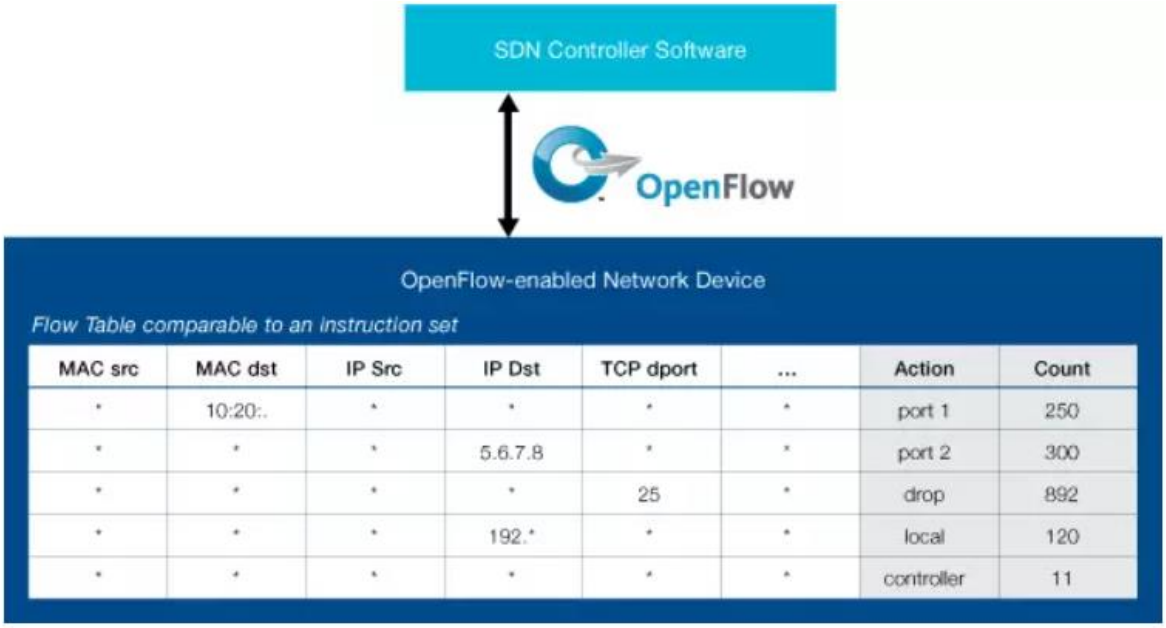

Рисунок 2.4 – Приклад набору інструкцій OpenFlow

Протокол OpenFlow® реалізований по обидва боки інтерфейсу між пристроями мережевої інфраструктури та програмним забезпеченням керування SDN. OpenFlow® використовує концепцію потоків для ідентифікації мережевого трафіку на основі попередньо визначених правил відповідності, які можна статично або динамічно програмувати програмним забезпеченням керування SDN. Це також дозволяє IT визначати, як трафік повинен проходити через мережеві пристрої на основі таких параметрів, як моделі використання, програми та хмарні ресурси. Оскільки OpenFlow® дозволяє програмувати мережу на основі кожного потоку, архітектура SDN на основі OpenFlow забезпечує надзвичайно детальний контроль, що дозволяє мережі реагувати на зміни в режимі реального часу на рівні програми, користувача та сеансу. Поточна IP-маршрутизація не забезпечує такого рівня контролю, оскільки всі потоки між двома кінцевими точками повинні йти по одному шляху через мережу, незалежно від їхніх різних вимог.

Протокол OpenFlow® є ключовим інструментом для програмно-конфігурованих мереж і наразі є єдиним стандартизованим протоколом SDN,

який дозволяє безпосередньо маніпулювати площиною пересилання мережевих пристроїв. Хоча спочатку застосовувалося до мереж на основі Ethernet, перемикання OpenFlow® може поширюватися на набагато ширший набір випадків використання. SDN на основі OpenFlow можна розгорнути в існуючих мережах, як фізичних, так і віртуальних. Мережеві пристрої можуть підтримувати переадресацію на основі OpenFlow, а також традиційну переадресацію, що дозволяє підприємствам і операторам поступово впроваджувати технології SDN на основі OpenFlow навіть у мережевих середовищах кількох виробників.

Open Networking Foundation створено для стандартизації OpenFlow® і робить це через технічні робочі групи, відповідальні за протокол, конфігурацію, тестування сумісності та інші види діяльності, допомагаючи забезпечити взаємодію між мережевими пристроями та програмним забезпеченням для керування різними постачальниками. OpenFlow® широко використовується постачальниками інфраструктури, які зазвичай впроваджують його шляхом простого оновлення мікропрограми або програмного забезпечення. Архітектура SDN на основі OpenFlow може легко інтегруватися з існуючою інфраструктурою підприємства або оператора та забезпечити простий шлях міграції для тих сегментів мережі, які найбільше потребують функціональності SDN.

Як для підприємств, так і для провайдерів, SDN дає можливість мережі бути конкурентоспроможною відмінністю, а не просто неминучим центром витрат. Технології SDN на основі OpenFlow дають змогу IT вирішувати проблеми з високою пропускною здатністю та динамічністю сучасних додатків, адаптувати мережу до постійно мінливих бізнес-потреб і значно зменшити складність операцій та управління.

Переваги, які підприємства та оператори можуть отримати завдяки архітектурі SDN на основі OpenFlow, включають:

– централізоване керування середовищами кількох виробників: програмне забезпечення для керування SDN може керувати будь-яким мережевим пристроєм із підтримкою OpenFlow від будь-якого постачальника, включаючи комутатори, маршрутизатори та віртуальні комутатори. Замість того, щоб керувати групами пристроїв від окремих постачальників, IT-спеціалісти можуть використовувати інструменти оркестрування та керування на основі SDN для швидкого розгортання, налаштування та оновлення пристроїв у всій мережі;

– зменшення складності завдяки автоматизації: SDN на базі OpenFlow пропонує гнучку мережу для автоматизації та управління, що дає змогу розробляти інструменти, які автоматизують багато завдань керування, які сьогодні виконуються вручну. Ці інструменти автоматизації зменшать операційні витрати, зменшать нестабільність мережі, викликану помилками оператора, і підтримають нові моделі IT як послуги та самообслуговування. Крім того, за допомогою SDN хмарними додатками можна керувати за допомогою інтелектуальних систем оркестровки та надання, що ще більше зменшує операційні витрати, одночасно підвищуючи гнучкість бізнесу;

– вищий рівень інновацій: впровадження SDN прискорює бізнес-інновації, дозволяючи операторам IT-мереж буквально програмувати — і перепрограмувати — мережу в реальному часі, щоб задовольнити конкретні потреби бізнесу та вимоги користувачів у міру їх виникнення. Віртуалізуючи мережеву інфраструктуру та абстрагуючи її від окремих мережевих служб, наприклад, SDN і OpenFlow® дають IT — і, можливо, навіть користувачам — можливість адаптувати поведінку мережі та вводити нові послуги та можливості мережі за лічені години;

– підвищена надійність і безпека мережі: SDN дає можливість IT визначати високорівневі конфігурації та політики, які потім транслюються в інфраструктуру через OpenFlow. Архітектура SDN на основі OpenFlow усуває необхідність окремо налаштовувати мережеві пристрої щоразу, коли

кінцеву точку, службу або програму додають або переміщують, або змінюють політику, що зменшує ймовірність збоїв мережі через невідповідність конфігурації або політики.

Оскільки контролери SDN забезпечують повну видимість і контроль над мережею, вони можуть гарантувати, що контроль доступу, інженерія трафіку, якість обслуговування, безпека та інші політики постійно застосовуються в дротових і бездротових мережевих інфраструктурах, включаючи філії, кампуси та дані. центрів. Підприємства та перевізники отримують вигоду від зниження операційних витрат, більш динамічних можливостей конфігурації, меншої кількості помилок та послідовного конфігурації та застосування політики.

Більш детальний контроль мережі: модель керування на основі потоків OpenFlow дозволяє IT застосовувати політику на дуже детальному рівні, включаючи рівні сеансу, користувача, пристрою та програми, дуже абстрактно, автоматизовано. Цей контроль дає змогу хмарним операторам підтримувати багатоквартирну оренду, зберігаючи ізоляцію трафіку, безпеку та еластичне керування ресурсами, коли клієнти використовують одну інфраструктуру.

Кращий досвід роботи з користувачами: завдяки централізації управління мережею та надання інформації про стан для програм вищого рівня, інфраструктура SDN може краще адаптуватися до динамічних потреб користувачів. Наприклад, оператор може запровадити відеосервіс, який пропонує абонентам преміум-класу найвищу можливу роздільну здатність в автоматизований та прозорий спосіб. Сьогодні користувачі повинні явно вибирати налаштування роздільної здатності, яке мережа може підтримувати або не підтримувати, що призводить до затримок і перебоїв, які погіршують роботу користувача. Завдяки SDN на основі OpenFlow відеододаток зможе визначити пропускну здатність мережі в режимі реального часу та автоматично налаштувати відповідним чином роздільну здатність відео.

Такі тенденції, як мобільність користувачів, віртуалізація серверів, IT-як-послуга та потреба швидко реагувати на зміну умов бізнесу висувають значні вимоги до мережі – вимоги, з якими сучасні звичайні мережеві архітектури не можуть впоратися. Програмно-конфігурована мережа забезпечує нову, динамічну архітектуру мережі, яка перетворює традиційні магістралі мережі в багаті платформи надання послуг.

Роз'єднуючи плани керування мережею та даними, архітектура SDN на основі OpenFlow абстрагує базову інфраструктуру від програм, які її використовують, дозволяючи мережі стати таким же програмованим і керованим у масштабі, як і комп'ютерна інфраструктура, на яку вона все більше нагадує. Підхід SDN сприяє віртуалізації мережі, дозволяючи IT-персоналу керувати своїми серверами, додатками, сховищем і мережами за допомогою загального підходу та набору інструментів. Незалежно від того, чи є в середовищі оператора або корпоративного центру обробки даних чи кампусу, впровадження SDN може покращити керованість, масштабованість та гнучкість мережі.

Open Networking Foundation створив живу екосистему навколо SDN, яка охоплює великих і малих постачальників інфраструктури, включаючи розробників додатків, компанії програмного забезпечення, виробників систем і напівпровідників, а також комп'ютерні компанії, а також різних типів кінцевих користувачів. Перемикання OpenFlow® вже впроваджується в ряд проектів інфраструктури, як фізичних, так і віртуальних, а також програмне забезпечення контролера SDN. Мережеві служби та бізнес-додатки вже взаємодіють із контролерами SDN, забезпечуючи кращу інтеграцію та координацію між ними.

Майбутнє мереж все більше залежатиме від програмного забезпечення, яке прискорить темпи інновацій у мережах, як це відбувається в області обчислень і зберігання даних. SDN обіцяє перетворити сучасні статичні мережі в гнучкі, програмовані платформи з інтелектуальними

можливостями для динамічного розподілу ресурсів, масштабом підтримки величезних центрів обробки даних і віртуалізації, необхідною для підтримки динамічних, високоавтоматизованих і безпечних хмарних середовищ. Завдяки багатьом перевагам і вражаючому розвитку галузі, SDN на шляху до того, щоб стати новою нормою для мереж.

2.4 Автоматизація управління мережею через мережі на основі намірів IBN

Мережа на основі намірів (IBN) – це нова технологічна концепція, яка має на меті застосувати більш глибокий рівень інтелекту та передбачуваного стану уявлень про мережу. В ідеалі ці ідеї замінюють ручні процеси налаштування мереж та реагування на проблеми мережі. Простіше кажучи, адміністратори можуть надіслати запит, щоб повідомити мережі, який результат вони хочуть (свої наміри), замість того, щоб кодувати та виконувати окремі завдання вручну.

Мережеві компанії, засновані на намірах, варіюються від стартапів до відомих мережевих постачальників, і всі вони пропонують дещо різні варіанти. Але метою є створення мережі, яка використовує машинне навчання та когнітивні обчислення, щоб забезпечити більше автоматизації та менше часу, витраченого на ручне налаштування й керування. Вони надають програмне забезпечення, яке може перевести намір у конфігурацію мережі. За допомогою створення мережі на основі намірів адміністратори мережі визначають результат або бізнес-ціль – намір і програмне забезпечення мережі визначає, як досягти цієї мети завдяки штучному інтелекту та машинному навчанню.

Мережеві системи на основі намірів не тільки автоматизують виконання трудомістких завдань і забезпечують у реальному часі видимість діяльності мережі для підтвердження певного наміру, вони також

прогнозують потенційні відхилення від цього наміру та призначають дії, необхідні для забезпечення цього наміру. Цей більший інтелект робить мережу швидшою та спритнішою та зменшує кількість помилок. Ця здатність до самоконтролю та самокоригування є основним компонентом мережі на основі намірів.

IBN розроблено для усунення обмежень SDN. Ці рішення забезпечують підключення до мережевих пристроїв із програмними інтерфейсами (API). В результаті мережеві інженери можуть легше розгортати мережеве обладнання, керувати ним і усувати несправності. IBN спрощує мережеве програмування, покращуючи автоматизацію мережі та покращуючи абстракцію. Такий підхід допомагає компаніям створювати, впроваджувати та покращувати маневреність мережі. IBN містить чотири елементи: переклад і підтвердження; автоматизована реалізація; усвідомлення стану мережі; а також забезпечення та динамічна оптимізація/виправлення. Основними завданнями IBN є:

- бере дані від мережевого інженера;
- налаштовує дизайн мережі на основі намірів підприємства;
- перевіряє дизайн на правильність;
- розгортає конфігурацію мережі;
- постійно забезпечує досягнення мети системи;
- за потреби вносить зміни.

Програмована мережа полегшує IT тягар виконання багатьох щоденних мережевих завдань: виділення пропускної здатності, маршрутизації трафіку, налаштування політики безпеки та виявлення аномалій. Компанії заощаджують час, усувають людські помилки та спрощують усунення несправностей та їх усунення – все частіше в реальному часі.

Іншими перевагами IBN є портативність та підхід, що не залежить від постачальника. Програми, розроблені для одного SDN, можна легко перенести в інше середовище.

Замість того, щоб конкурувати одна з одною, технології SDN та IBN найкраще працюють у поєднанні один з одним. Cisco розробила популярне рішення IBN, Cisco Digital Network Architecture (Cisco DNA) Center. Ці інструменти масово налаштовують пристрої за допомогою централізованої консолі керування в автоматизований спосіб, але встановлюють політики безпеки на детальному рівні. Аналітика надає в режимі реального часу інформацію про продуктивність мережі та загрози безпеці, а також надає автоматичні шляхи усунення.

Підприємства набувають гнучкості. Експерти кажуть, що нові підходи дають змогу IT-фахівцям керувати мережею як єдиною сутністю та легше створювати нові можливості поверх неї. Мережа стає централізованою платформою, яка послідовно та легко керує інфраструктурою та додатками. Завдяки DNA Cisco один роздрібний продавець скоротив час розгортання філіальної мережі з кількох років до місяців. Раніше, при ручному налаштуванні, для налаштування кожної мережі філій потрібно було близько 250 кліків. Завдяки можливості програмування та автоматизації мережі кількість зменшилася до чотирьох.

Крім того, мережі можна програмувати новими способами. IT-спеціалісти отримують сповіщення або керують конфігураціями політики з iPhone. Ця зміна звільняє мережевих інженерів контролювати мережу з будь-якого місця, залишаючись при цьому інформованими та здатними виконувати дії в режимі реального часу. Інша зміна полягає в тому, що користувач або адміністратор може надіслати простий запит використовуючи природну мову до фізичної мережі. Наприклад, IT-адміністратор може запитати покращення якості голосу для своєї програми передачі голосу через IP, і мережа відповідає.

Автоматизація мережевих конфігурацій приносить менше помилок. Така узгодженість особливо важлива для компаній, таких як фінансові установи, які повинні довести аудиторам, що вони мають однакову політику брандмауера в усіх своїх місцях.

Більшість поточних мереж керується вручну, а адміністратори створюють сценарії, які детально описують усе, що необхідно для виконання певного завдання через інтерфейс командного рядка (CLI). Навпаки, у мережах на основі намірів намір автоматично інтерпретується на різних пристроях, не вимагаючи від інженерів змінювати кожен пристрій у мережі окремо. За допомогою IBN введення можна надавати через зручний графічний інтерфейс користувача (GUI) або за допомогою API.

Аналогією з IBN може бути автономний транспортний засіб. Бажаний результат буде ідентифікований як адреса призначення та введення в систему. З цього моменту транспортний засіб визначатиме наступні завдання, які необхідно виконати для досягнення цього результату, такі як маневрування дорожнього руху та моніторинг GPS. По суті, функціонуюча система на основі намірів відповідала б автоматично або за запитом на системну подію без участі людини.

Більшість інструментів і програмного забезпечення IBN пропонуються як модель “Мережа як послуга” (NaaS), що означає, що ним можна керувати на кількох пристроях за допомогою одного інтерфейсу. Поширеними постачальниками продуктів IBN є Apstra, Cisco, Forward Networks, Juniper Networks і Veriflow Systems.

Хоча IBN все ще є сферою технологій, що розвиваються, Gartner прогнозує, що IBN буде повністю функціонувати в корпоративних мережах до 2020 року. На думку багатьох галузевих аналітиків, IBN буде необхідним для управління мережами майбутніх центрів обробки даних, загальнодоступних хмар та Інтернету речей (IoT).

На рисунку 2.5 показано архітектуру IBN мережі.

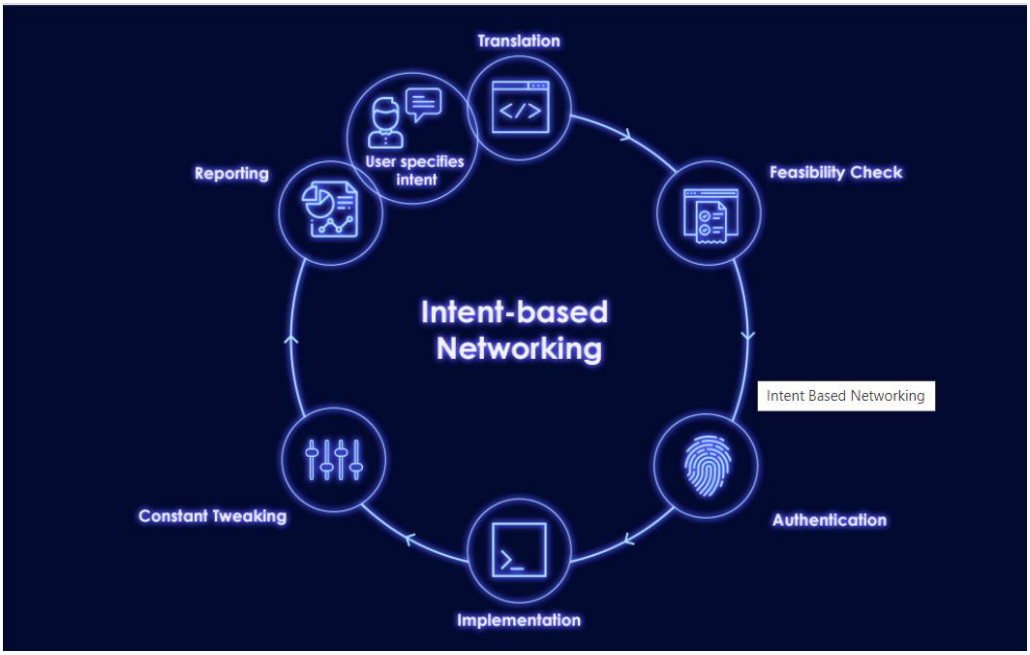

Рисунок 2.5 – Архітектура IBN мережі

Станом на 2020 рік IBN не є основним. Він все ще знаходиться на ранній стадії розвитку. Однак, починаючи з сьогоднішнього дня, можна зробити свою IT-інфраструктуру більш оперативною за допомогою ManageEngine OpManager.

ManageEngine OpManager – це комплексна система моніторингу мережі, яка проактивно відстежує сервери, комутатори, маршрутизатори, брандмауери та все, що має IP і підключено до мережі. Існує можливість забезпечити 360° видимість мережі за допомогою повного:

– моніторингу фізичних та віртуальних пристроїв;
– аналізу мережевого трафіку;
– управління конфігурацією мережі;
– аналізу журналу та керування брандмауером;
– перемикання керування портами та IP-адресами.

Функція автоматизації робочого процесу OpManager без коду допомагає ефективно керувати IT-інфраструктурою, роблячи її більш гнучкою для запитів на обслуговування. За допомогою надбудови Network

Configuration Manager наведений вище приклад можна виконати в OpManager за допомогою конструктора робочих процесів перетягуванням.

Багато рішень, що виходять на ринок, використовують у своїх маркетингових матеріалах “на основі намірів”, але не відповідають можливостям. Рішення діляться на три основні категорії:

Рішення для перевірки рівня даних і управління. Вони аналізують поточний стан мережі за допомогою конфігурації пристрою та визначають робочий стан або витягують таблиці станів, такі як база інформації пересилання (FIB), база інформації про маршрутизацію (RIB) та інші. Використовуючи цю інформацію, рішення для перевірки можуть передбачити поведінку пересилання мережі та виконувати різні сценарії “що буде, якщо” для перевірки змін перед впровадженням у мережу. Більшість рішень цієї категорії є “лише для читання” і фактично не впроваджують автоматизовані зміни в мережі.

Мережні системи на основі намірів Greenfield, як правило, вузькі за обсягом, як рішення для конкретного центру обробки даних або рішення SD-WAN, і є дуже директивними. Незважаючи на те, що вони відповідають критеріям IBN, практичність впровадження обмежена через вузьку спрямованість і необхідність розірвати та замінити існуючу мережу або повністю переписати конфігурацію на кожному мережевому пристрої, що є дуже шкідливим.

Інтелектуальні мережеві системи на основі намірів, наприклад, Gluware надає можливість приймати інформацію про поточний мережевий пристрій, налаштовані функції разом із політиками. Здатність автоматизувати мережу “закритого виробництва” має вирішальне значення для великих підприємств, які підтримують багатоплатформні мережі багатьох постачальників, які розвиваються з часом. Gluware надає можливість абстрагувати інформацію про конфігурацію, автоматизувати впровадження, розуміти поточний стан конфігурації та застосовувати лише необхідні зміни

та перевіряти конфігурацію та робочий стан. Приклад платформи запропонованої Gluware показано на рисунку 2.6.

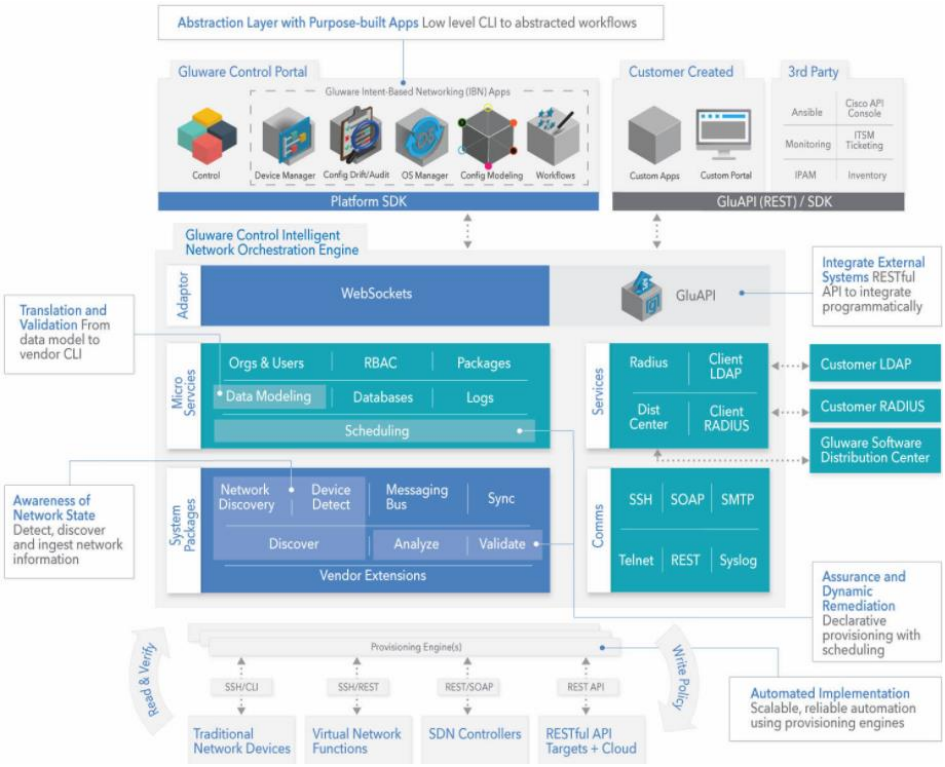

Рисунок 2.6 – Платформа реалізації IBN від Gluware

Gluware може абстрагуватися до вимог будь-якого випадку використання, від ділових намірів до низькорівневої змінної конфігурації. Gluware приймає вхідні дані від користувача та може перевіряти отриману функцію/зміну та після надання динамічно генерує потрібний CLI/API для досягнення бажаного стану конфігурації мережі.

Gluware використовує потужний механізм оркестровки для виявлення (поточний стан), аналізу, перевірки та надання функції/рішення на всіх мережевих вузлах (багатьох постачальників, кількох доменів). Gluware може підтримувати змінні та умови для автоматизації складних сценаріїв.

Gluware має дві функції для фіксації стану мережі в режимі реального часу: механізм Discovery запускається для кожного вузла мережі перед ініціалізацією, щоб визначити поточний стан конфігурації та виконати

декларативне надання та узгодити конфігурацію під час виконання з потрібним станом; і додаткова оцінка стану, яка може запускати будь-яку команду “показати”, щоб перевірити стан пристрою, протоколу чи інтерфейсу.

Gluware не залежить від постачальників і може моделювати будь-яку мережеву функцію, включаючи функції контролю трафіку та інші, які реалізують гарантію, що динамічне виправлення досягається на рівні мережі. Gluware Config Modeling можна запустити, щоб відновити мережу до потрібного стану в будь-який момент, і запустити Config Drift and Audit на постійній основі, щоб переконатися, що мережа відповідає очікуванням і відповідає політиці.

2.5 Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений розробці та можливому впровадженню методів та засобів автоматизації керування мережевими пристроями та функціями. За результатами роботи виявлено основні тенденцій в автоматизації сучасних мереж. Автоматизації на основі використання сценаріїв має перевагу гнучкості свого застосування та можливості масштабування у різних випадках та розмірах мережі. Проте, даний тип автоматизації потребує знань програмування, що ускладнює його розгортання для мереж невеликого розміру з обмеженеми фінансовими ресурсами. Наступним популярним рішенням автоматизації є Red Hat Ansible, що надає широкий спектр дій, але потребує спеціалізованих знань, що уможливлює його використання за умови виконання зазначених умов. Останнім часом широкого розповсюдження набуло використання концепції та рішень на основі неї яка називаєть програно конфігуровані мережі SDN. При цьому автоматизація керування пристроями є дуже високою через використання спеціалізованого контролера та протоколу Open Flow. Даний

підхід до автоматизації є з багатовендорною підтримкою, що дає змогу використовувати його в гетерогенних мережах і навіть при наявності не самого нового обладнання. Основними складнощами його впровадження можна вважати необхідність спеціалізованого контролера для управління мережею, що збільшує витрати, а також знань та вмінь з програмування для створення програмних додатків. Як надбудова над SDN розглядається наступний виток еволюції мереж у вигляді мереж на основі намірів IBN. Це дає змогу ще більше пришвидшити розгортання нових послуг у мережі, проводити аудит та відслідковувати стан мережевих пристроїв та додатків.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Безпечні умови праці при монтажі комп'ютерної мережі

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: "Про охорону праці", "Про охорону здоров'я", "Про пожежну безпеку".

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Особи з простудними і хронічними захворюваннями верхніх дихальних шляхів до роботи з монтажу комп'ютерних мережі та заготовки і монтажу пластмасових труб не допускаються.

Роботи на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів.

Вимоги безпеки перед початком роботи передбачають, що до початку робіт з монтажу комп'ютерної мережі керівник зобов'язаний:

– перевірити ступінь готовності будівельних робіт;

– оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду; можливість безпечного застосування піротехнічного інструменту, безпечної подачі електричних конструкцій, електротехнічних апаратів та інших блоків;

– узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

– ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Керівник робіт повинен здійснити первинний інструктаж, який стосується:

– характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

– наявності небезпечних зон та відкритих каналів і траншей, відкритих прорізів, отворів у перекриттях та стінах;

– порядку розвантаження та складування матеріалів, устаткування та конструкцій;

– місць та порядку трансформаторів безпеки, електрифікованого інструменту, засобів електроосвітлення, випробувальних апаратів;

– порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

– надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежобезпеки, посвідчень на право виконання спеціальних видів робіт (зварювання, монтаж кабельної арматури).

Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов’язкові.

Попередити працюючих, що з’єднання та від’єднання від мережі обладнання, механізмів, інструменту, інвентарних шаф тощо (крім

оперативного вмикання і вимикання) в умовах будівельного майданчика виконуються тільки службою експлуатації власника мережі, якщо не існує іншої письмової домовленості з власником.

Вимоги безпеки під час виконання роботи:

– прокладання кабелів слід виконувати тільки в рукавицях.

– працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

– переносити чи перевозити інструмент з гострими кутами треба лише в чохлах.

– не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї.

– перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана.

– переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше .

Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку. Перед розмотуванням барабан встановити на домкрати (чи інший підіймальний пристрій). Барабан встановити так, щоб кабель розмотувався з його верхньої частини. Розмотувати кабель з барабана слід тільки за наявності гальмівного пристрою.

Прокладання кабелів і монтаж мережевого обладнання слід виконувати у захисному одязі з можливістю використання електростатичних браслетів.

Дотримання вимог безпечної роботи є необхідною умовою для успішного завершення побудови комп’ютерних мереж.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуації мирного та воєнного часу

Моніторинг довкілля – це система спостереження, збирання та аналізу інформації про ситуацію, що може скластись під час надзвичайних ситуацій мирного та воєнного часу. Також це система спостереження за визначеними об’єктами, явищами та процесами з метою оперативного оцінювання їх стану, виявлення результатів впливу на них зовнішніх чинників та прийняття відповідних управлінських рішень (ДСТУ 3891:2013) (див. ДСТУ 7295:2013).

Моніторинг потенційно небезпечних об’єктів це спостереження, контролювання за зміною параметрів технологічних режимів з метою збирання, збереження, передавання та аналізування інформації щодо поточного стану потенційно небезпечних об’єктів, наявності та кількості порушень вимог безпеки, відпрацювання рекомендацій щодо проведення робіт із запобігання та ліквідування техногенних надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг джерел надзвичайних ситуацій це система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації стосовно стану об’єктів моніторингу та розроблення науково-обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування надзвичайних ситуацій (ДСТУ 7295:2013).

Моніторинг довкілля це систематичні спостереження і контролювання, які проводять регулярно, за єдиною програмою для оцінювання стану довкілля, аналізування процесів, які відбуваються в ньому і своєчасне виявлення тенденцій його змінювання (ДСТУ 7295:2013).

Моніторинг надзвичайних ситуацій (НС) – система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації щодо об’єктів моніторингу та розроблення науково обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування НС.

Моніторинг небезпечних явищ та процесів це система спостереження та контролювання за розвитком небезпечних та стихійних природних явищ і процесів, чинниками, які спричинюють їх формування та розвиток, аналізування, збереження та передавання інформації щодо виявлення тенденцій їх змінювання, розроблення комплексу заходів щодо запобігання природним надзвичайним ситуаціям та ліквідування їх наслідків. Небезпечні природні явища і процеси підрозділяють на геофізичні, геологічні, гідрологічні, метеорологічні, медико-біологічні та пожежі в природних екосистемах (ДСТУ 7295:2013).

Моніторинг пожеж в екосистемах це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо пожежної небезпеки в природних екосистемах (умов погоди, стану горючих матеріалів, інших пожежонебезпечних чинників), з метою своєчасного планування та здійснення заходів щодо запобігання виникненню і ліквідування пожеж та їх наслідків (ДСТУ 7295:2013).

Моніторинг радіаційної безпеки це спостереження і контролювання рівня радіоактивного забруднення місцевості, повітря, води, продовольства, об’єктів господарювання, дозових навантажень на населення з метою прийняття оперативних рішень щодо запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг хімічної небезпеки це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо визначення ступеня і характеру хімічного забруднення довкілля, санітарно-

гігієнічний нагляд за дотриманням установлених нормативів з метою виявлення джерела надходження небезпечних хімічних речовин, запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013)

Збір та аналіз інформації про стан довкілля під час мирного та воєнного стану дає можливість приймати оперативні рішння для адекватного реагування на ситуацію.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі. В безпеці в надзвичайних ситуаціях висвітлено питання функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу.

ВИСНОВКИ

В кваліфікаційній роботі виконано дослідження процесів автоматизації керування мережевими пристроями. За результатами цього отримано наступні результати:

– висвітлено питання аналізу автоматизації налаштування мережевих пристроїв, що дало змогу класифікувати засоби та методи виконання цієї процедури в мережах різного призначення;

– наведено приклади використання автоматизації у реальних ситуаціях. Виявлено сильні та слабкі сторони кожного з розглянутих методів автоматизації налаштування мережевих пристроїв;

– подано аналіз застосування найбільш відомих програмних продуктів для автоматизації мережевого конфігурування;

– досліджено розробку та можливість впровадження методів та засобів автоматизації керування мережевими пристроями та функціями. За результатами роботи виявлено основні тенденцій в автоматизації сучасних мереж;

– досліджено автоматизації на основі використання сценаріїв і виявлено, що такий підхід має перевагу гнучкості свого застосування та можливості масштабування у різних випадках та розмірах мережі. Проте, даний тип автоматизації потребує знань програмування, що ускладнює його розгортання для мереж невеликого розміру з обмеженеми фінансовими ресурсами;

– висвітлено, що останнім часом широкого розповсюдження набуло використання концепції та рішень на основі неї, яка називаєть програно конфігуровані мережі SDN. При цьому автоматизація керування пристроями є дуже високою через використання спеціалізованого контролера та протоколу Open Flow. Даний підхід до автоматизації є з багатовендорною

підтримкою, що дає змогу використовувати його в гетерогенних мережах і навіть при наявності не самого нового обладнання;

– як надбудова над SDN розглядається наступний виток еволюції мереж у вигляді мереж на основі намірів IBN. Це дає змогу ще більше пришвидшити розгортання нових послуг у мережі, проводити аудит та відслідковувати стан мережевих пристроїв та додатків.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання безпечних умов праці при монтажі комп'ютерної мережі та функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002, ISBN: 978-1-931836-56-2

2. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

3. V. Olifer and N. Olifer, Novye tekhnologii i oborudovanie IP-setei [New technologies and equipment of IP-networks]. St.-Peterburg, Russia: Bhv, 2000, ISBN: 5-8206-0053-3

4. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

5. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 4.11.2021.

6. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

7. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14.11.2021

8. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний

ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 15.11.2021

9. Приїхав до Польщі – користуйся Інтернетом! [Електронний ресурс] – Режим доступу: http://naszwybir.pl/internet/. – Назва з екрану. – Дата звернення: 15.11.2021

10. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

11. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

12. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

13. Cisco Systems Руководство по технологиям объединенных сетей / Cisco Systems - 3-е издание. СПб: “Вильямс”, 2002. – 1040 с.

14. Дебра Литтлджон Шиндер Основы компьютерных сетей / Дебра Литтлджон Шиндер - СПб: "Вильямс", 2002. – 656 с.

15. Коротыгин С. Стандарт IEEE 802.11 и его расширения / С. Коротыгин, А. Нежуренко - Сети и телекоммуникации, вып. 6(25), 2002 г.

16. Марк А. Спортак Компьютерные сети. Книга 1. High-Perfomance Networking. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

17. Марк А. Спортак Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

18. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

19. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

20. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

21. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

22. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

23. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв'язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

24. Френк Г. Сети, связь и потоки / Г. Френк, И. Фриш ; пер. с англ. под ред. Д. А. Поспелова. – Москва : Связь, 1978. – 448 с.

25. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

26. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

27. Шерстнева О. Г. Подходы к оценке качества управления связью / О. Г. Шестернева // Сети и системи связи. – 2008. – №11. – С. 35-41.

28. Стеклов В. К. Проектування телекомунікаційних мереж / В. К. Стеклов, Л. Н. Беркман. ; під ред. В. К. Стеклова – Київ : Техніка, 2002. – 792 с.

29. Кульгин М. Технология корпоративных сетей / М. Кульгин. – Санкт- Петербург : Питер, 1999. – 704 с.

30. Шварц М. Сети связи: протоколы, моделирование и анализ / М. Шварц. – ч.2. – Москва : Наука, 1992. – 272 с.

31. What is SD-WAN (Software-Defined Wide Area Network)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ – Назва з екрану. – Дата звернення: 12.11.2021.

32. SD-WAN vs MPLS: The Pros and Cons of Both Technologies)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/ – Назва з екрану. – Дата звернення: 18.11.2021.

33. Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html?dtid=osscdc000283 – Назва з екрану. – Дата звернення: 18.11.2021.

34. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 20.11.2021.

35. Draft-ietf-nvo3-geneve-08 [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/draft-ietf-nvo3-geneve-08 – Назва з екрану. – Дата звернення: 22.11.2021.

36. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 22.11.2021.

37. Best Network Automation Tools [Електронний ресурс]. – Режим доступу: https://www.dnsstuff.com/network-automation-tools – Назва з екрану. – Дата звернення: 22.11.2021

38. What is network automation? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/automation/network-automation.html – Назва з екрану. – Дата звернення: 23.11.2021.

39. Network automation and orchestration tools review and ratings [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/network-automation – Назва з екрану. – Дата звернення: 23.11.2021.

40. Network automation tools [Електронний ресурс]. – Режим доступу: https://www.pcwdld.com/network-automation-tools-and-software#wbounce-modal – Назва з екрану. – Дата звернення: 23.11.2021.

41. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 23.11.2021.

42. Arregoces, Mauricio, and Maurizio Portolani. Data center fundamentals. Cisco Press, 2003

43. Long, James. Storage Networking Protocol Fundamentals. Pearson Education India, 2006.

44. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

45. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

46. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

47. Membrey, Peter, Eelco Plugge, and David Hows. Practical Load Balancing: Ride the Performance Tiger. Apress, 2012.

48. Odom, Ccie Routing And Switching Exam Certi cation Guide, 4/E. Cisco press, 2004.

49. Kenyon, Tony. Data networks: routing, security, and performance optimization. Digital Press, 2002.

50. R. Froom, B. Sivasubramanian, and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Cisco press.

51. Popovic, Miroslav. Communication protocol engineering. CRC press, 2016. 277

52. J. Appl. Environ. Biol. Sci., 7(3)268-278, 2017

53. S. Tim, Cisco Telepresence Fundamentals. Pearson Education India, 2010.

54. Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization, 2013.

Додатки

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том І

X Міжнародної науково-практичної конференції молодих учених та студентів

24-25 листопада 2021 року

УКРАЇНА
ТЕРНОПІЛЬ – 2021

Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль 24-25 листопада 2021 року

УДК 004.72

М.І. Шоцький, В.В. Федина, С.В. Марценко, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ КЕРУВАННЯ МЕРЕЖЕВИМИ ПРИСТРОЯМИ

M.I.Shotskyi, V.V. Fedyna, S.V. Martsenko, Ph.D., Assoc.

RESEARCH OF PROCESSES OF NETWORK DEVICES CONFIGURATION AUTOMATION

Сучасні мережі змінились у своїх розмірах та складності архітектури. Кількість пристроїв та їх різноманіття приводять до ускладнення процесів налаштування та контролю правильності роботи. Ручне управління стає все більш утрудненим та, у деяких випадках, практично неможливим для мережевого інженера. В таких випадках автоматизація процесів управління та конфігурації мережевими пристроями стає єдиним рішенням для повноцінної та ефективної роботи.

Дослідження процесів автоматизації налаштування та керування мережевими пристроями показує, що є декілька підходів до вирішення цих задач:

- забезпечення налаштування мережевого обладнання через використання бібліотек готових наборів команд для визначених типів обладнання;
- використання графічних інтерфейсів для виконання конфігурування пристроїв;
- здійснення керування пристроями за допомогою стандартизованих протоколів та спеціалізованого програмного забезпечення;
- повна віртуалізація мережевих функцій.

Набори готових командних шаблонів є хорошим підходом у невеликих мережах, де обладнання у більшості своїй однакове. Такий варіант автоматизації дає змогу швидко відновитись у випадку виходу з ладу пристрою за умови наявності аналогічного. Іншим варіантом використання може бути реплікація коду з незначною зміною. До найбільшого недоліку цього методу можна віднести схильність до помилки у коді, оскільки немає функцій перевірки на адекватність налаштування реальній мережі. Уся відповідальність лягає на мережевого фахівця, що ускладнює масштабування цього підходу у великих мережах.

Графічні інтерфейси дають змогу проводити налаштування обладнання для фахівців без необхідності вникнення в архітектуру операційних систем різних виробників і вивчення їх команд. Проте, автоматизація у цьому випадку дуже складна, оскільки вигляд графічних інтерфейсів може змінюватись і написання шаблонних сценаріїв роботи практично неможливе.

Використання стандартизованих протоколів дає змогу проводити налаштування та управління великою кількістю пристроїв, що загалом вирішує задачу автоматизації цих процесів. Проте, більшість програмних продуктів, що забезпечують функціонал керування мережевими вузлами є платними. Реалізація специфічних, для певної мережі, сценаріїв налаштування ускладнене відсутністю доступу до модифікації шаблонів, якщо це не передбачено розробником.

Багато сучасних мереж організовані у гібридному форматі, коли частина ресурсів є фізичними пристроями, а частина віртуальними, що розміщені у хмарі. При такому підході зручним є використання сучасного методу управління інфраструктура як код. Готовими рішеннями які популярні є AWS CoudFormation, Terraform, Ansible, Chef, Puppet, Vagrant, Azure Resource Manager, Google Cloud Resource Manager, Serverless Framework. Програмування є невід'ємною частиною їх роботи.

Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль 24-25 листопада 2021 року

УДК 004.72

М.І. Шоцький, В.В. Федина
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСУ ОРГАНІЗАЦІЇ ЗОНОВОЇ БЕЗПЕКИ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

M.I.Shotskyi, V.V. Fedyna

RESEARCH OF THE PROCESS OF ZONE SECURITY ORGANIZATION IN A COMPUTER NETWORK

Захист інформації та інформаційних ресурсів набуває все більш вагомого значення при проектуванні нових мереж та модернізації роботи існуючих. Таким чином, актуальною задачею є дослідження організації зонової безпеки для ефективної та безпечної роботи мереж різного призначення. При дослідженні проектування безпеки в мережах потрібно враховувати низку факторів, що визначають особливості роботи організації, наборів обладнання та потоків трафіку, що мають бути захищені.

Аналіз літературних джерел дав змогу сформувати ряд задач, що потребують вирішення при організації зонової безпеки, а саме:

- дослідити розмір мережі для визначення правильного підходу до організації мережевої безпеки;
- визначити набори обладнання, їх тип та можливості для впровадження спроектованих рішень;
- провести аналіз потоків даних з визначенням рівнів важливості для забезпечення роботи організації;
- провести зонування мережі з використанням зон безпеки другого рівня, третього рівня або їх поєднання.

Дослідження розмірів мережі дасть змогу визначити чи створення зональної безпеки не буде приводити до ускладнення її роботи та подальшого обслуговування адмініструючим персоналом. В маленьких мережах, в багатьох випадках, достатнім рішенням є використання списків контролю доступу для організації контролю трафіку. При невеликих кількостях типів потоків даних процес написання таких списків не потребує особливих затрат часу та в подальшому спрощує керування мережею при зміні адміністратора. У мережах з динамічними потоками даних такий підхід працювати не буде або його робота буде неефективною.

Аналіз наборів обладнання дасть змогу провести аудит мережевих ресурсів з визначенням версій операційних систем, апаратних можливостей нести додаткові навантаження щодо аналізу потоків даних, сумісності різного обладнання між собою при розгортанні єдиної політики безпеки мережі.

Для різних мереж не всі потоки даних є однаковими. Створення правильної політики безпеки мережевих ресурсів організації вимагає чіткого розуміння точок входу та виходу трафіку, переходів трафіку між різними сегментами мережі, класифікації наборів даних та ін. Створення зональної безпеки базується на створенні правил роботи з даними чітко визначеними у політиці безпеки мережі організації.

Створення зонування потребує визначення на яких рівнях у мережі буде застосовуватись дана технологія. Використання зон безпеки другого рівня буде акцентувати увагу на інтерфейсах другого рівня і включатиме списки інтерфейсів в зоні, активні політики безпеки, що будуть застосовувати правила до трафіку який проходитиме через інтерфейс. Зональна безпека, що базується на третьому рівні використовує для організації інтерфейси третього рівня.