УДК 004

О.Бондаренко, магістр гр. КІ-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІРТУАЛІЗАЦІЇ МЕРЕЖІ NUAGE NETWORKS ДЛЯ АВТОМАТИЗАЦІЇ SDN І SD-WAN

У статті розроблено програмне забезпечення, яке призначено для системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN. Метою розробки є дослідження та програмна реалізація системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN. Об'єктом дослідження є процес віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN. Предметом дослідження є методи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN. Методи дослідження базуються на методах віртуалізації комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Питання побудови й експлуатації сучасної віртуалізованої мережі є найважливішими для фахівців в області центрів обробки даних. Значна увага приділена актуальним тенденціям галузі: віртуалізації й програмно визначаємим мережам (SDN), продуктам для побудови мережної інфраструктури центрів обробки даних – LAN і SAN, а також організації комунікацій між віддаленими площадками й створенню розподілених центрів даних.

Віртуалізація серверів дозволяє декільком серверам працювати одночасно на єдиному фізичному вузлі; при цьому зазначені сервери залишаються взаємно ізольованими. По суті, кожна віртуальна машина працює як єдиний сервер на даному фізичному комп'ютері. Віртуалізація мереж забезпечує аналогічну можливість, при якій кілька віртуальних мережних інфраструктур функціонують в одній фізичній мережі (з потенційним перекриттям IP-адрес), і кожна віртуальна мережна інфраструктура працює як єдина віртуальна мережа в загальній мережній інфраструктурі. .

У термінах віртуалізації мережі (HNV) клієнт визначається як "власник" групи віртуальних машин, розгорнутих у центрі обробки даних. Клієнтом може бути корпорація або підприємство в багатоклієнтському суспільному центрі реєстрації й обробки даних, або підрозділ або філія компанії в приватному центрі реєстрації й обробки даних. Кожний клієнт може мати в центрі обробки даних одну або кілька мереж віртуальних машин, а кожна мережа віртуальних машин містить у собі одну або декілька віртуальних підмереж.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віртуалізації мережі nuage networks для автоматизації SDN і SD-WAN.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

– Дослідження системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

– Програмна реалізація системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Об'єктом дослідження є процес віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Предметом дослідження є методи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Методи дослідження базуються на методах віртуалізації комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Маршрутизація при віртуалізації мережі

Як і у випадку фізичних мереж, маршрутизація є важливою частиною HNV. Існують два ключових аспекти, важливих для розуміння: маршрутизація пакетів між віртуальними підмережами й маршрутизація пакетів за межами віртуальної мережі.

Маршрутизація між віртуальними підмережами

У фізичній мережі підмережа є доменом рівня 2, у якому комп'ютери (віртуальні і фізичні) можуть зв'язуватися один з одним прямо без маршрутизації. В Windows при статичній конфігурації мережного адаптера для правильної маршрутизації трафіка можна встановити "шлюз за замовчуванням", що буде являти собою IP-адреса для відправлення всього трафіка, що виходить із конкретної підмережі. По суті це маршрутизатор для фізичної мережі. HNV використовує убудований маршрутизатор, що є частиною вузла, для формування розподіленого маршрутизатора віртуальної мережі. Це значить, що кожний вузол, зокрема віртуальний комутатор, діє як шлюз за замовчуванням для всього трафіка між віртуальними підмережами, що є частиною однієї мережі віртуальних машин. В Windows Server 2025 і Windows Server 2025 R2 використовуваний як шлюз за замовчуванням адреса – самий нижній запис для підмережі (наприклад, буде використовуватися адресу ".1" для префікса підмережі /24). Ця адреса резервується в кожної підмережі для шлюзу за замовчуванням, і віртуальні машини не можуть використовувати його у віртуальної підмережі.

HNV, що діє як розподілений маршрутизатор, забезпечує досить ефективний спосіб правильної маршрутизації всього трафіка в рамках мережі віртуальних машин, тому що кожний вузол може прямо направляти трафік у відповідний вузол без посередників. Це тим більше вірно, якщо дві віртуальні машини з однієї мережі, але з різних віртуальних підмереж віртуальних машин перебувають на одному фізичному вузлі. Як ви довідаєтеся пізніше в цьому розділі, пакету немає необхідності залишати фізичний вузол.

Маршрутизація за межами віртуальної мережі

Розгортання більшості клієнтських мереж вимагає, щоб середовище віртуалізації мережі була пов'язана з ресурсами, не включеними в середовище віртуалізації мережі. Шлюзи віртуалізації мереж необхідні для забезпечення можливості зв'язку між цими двома середовищами. Сценарії, що вимагають використання шлюзу віртуалізації мережі, включають приватна хмара й гібридна хмара. В основному шлюзи віртуалізації мережі необхідні для віртуальної приватної мережі (VPN) і маршрутизації.

Шлюзи можуть мати різні фізичні конструктивні параметри. Вони можуть будуватися на Windows Server 2025 R2, вбудовуватися в стійковий комутатор верхнього рівня (TOR) або підсистему балансування навантаження, включатися в інші існуючі мережні пристрої або бути новим автономним мережним пристроєм.

Приватна хмара (маршрутизація)

Великі підприємства можуть або не вирішуватися, або, з міркувань дотримання вимог, бути не в змозі перемістити деякі зі своїх служб і даних у загальнодоступну хмару постачальника послуг розміщення. Разом з тим підприємства хочуть за рахунок об'єднання ресурсів своїх центрів обробки даних у приватній хмарі одержувати переваги хмарних технологій, надавані віртуалізацією мережі. При розгортанні приватної хмари перекриття IP-адрес може не знадобитися, оскільки компанії, як правило, мають у своєму розпорядженні достатній внутрішній простір немаршрутизуємих адрес (наприклад, 10.x.x.x або 192.x.x.x).

Відзначимо в даному прикладі, що адреси клієнта у віртуальних підмережах представлені у вигляді 157.x, при тому що IP-адреси в немережевій віртуалізованій частини мережі (Corp Net) також представлені у вигляді 157.x. У цьому випадку адреси типу АП для віртуальних підмереж у центрі реєстрації й обробки даних є IP-адресами виду 10.x.Таке розгортання дозволяє підприємству скористатися перевагами віртуалізації мережі для забезпечення гнучкості як при розміщенні віртуальних машин, так і перекрестно-підмережній динамічної міграції в структурі центра обробки даних. Це збільшує ефективність центра реєстрації й обробки даних, тим самим знижуючи як поточні витрати (OpEx), так і капітальні витрати (CapEx). У даному сценарії шлюз віртуалізації мережі забезпечує маршрутизацію між IP-адресами виду 10.x і 157.1.

Гібридна хмара (VPN типу " мережа-мережа")

Ключова перевага віртуалізації мережі – те, що вона дозволяє досить легко розширити локальний центр обробки даних до центра обробки даних із застосуванням хмарних технологій на основі Windows Server 2025. Це називається моделлю гібридної хмари.

У даному сценарії внутрішня підмережа, наприклад підмережа, що містить веб-сервери, переміщається з мережі підприємства в центр реєстрації й обробки даних постачальника послуг розміщення хмари. Скориставшись перевагою *Використовуйте власну IP-адресу*, запропонованою постачальником послуг розміщення, підприємство позбулося від необхідності зміни параметрів мережі віртуальної машини веб-сервера або будь-якої іншої кінцевої точки мережі, прив'язаної до веб-серверу. Постачальник послуг розміщення забезпечує безпечний канал зв'язку за рахунок застосування шлюзу віртуалізації мережі. Адміністраторам підприємства потрібно лише настроїти свою локальну VPN з використанням необхідних IP-адрес. Для віртуальної машини веб-сервера її переміщення в хмару залишається непоміченим. Вона залишається в складі домену за рахунок застосування Active Directory (AD) і продовжує використовувати DNS-сервер підприємства. Віртуальна машина веб-сервера також продовжує взаємодіяти з іншими серверами підприємства, наприклад сервером SQL Server.

Шлюз віртуалізації мережі може підтримувати кілька тунелів VPN типу " мережа-мережа" (S2S). Відзначимо, що диспетчер віртуальних машин на схемі не показаний, але він необхідний для розгортання віртуалізації мережі.

Інкапсуляція пакета

У віртуалізації мережі кожний віртуальний мережний адаптер пов'язаний із двома IP-адресами:

– Адреса клієнта (АК) – IP-адреса, призначувана клієнтом на основі інфраструктури своєї інтрамережі. Дана адреса дозволяє клієнтові обмінюватися мережним трафіком з віртуальною машиною безвідносно факту її переміщення в хмару загального користування або частка хмара. АК є видимим для віртуальної машини й доступним для клієнта.

– Адреса провайдеру (АП) – IP-адреса, призначувана адміністратором постачальника послуг або центра реєстрації й обробки даних на основі інфраструктури своєї фізичної мережі. АП з'являється в мережі у вигляді пакетів. Обмін ними виробляється із сервером, на якому розміщається віртуальна машина. АП є видимим у фізичній мережі, але не для віртуальної машини.

АК обслуговують топологію клієнтської мережі, що віртуалізується й втрачає прив'язки до фактичних адрес і топології базової фізичної мережі, як це реалізовано для АП.

На даній схемі віртуальні машини клієнта відправляють пакети даних у просторі АК, які переглядають інфраструктуру фізичної мережі через власні віртуальні мережі, або "тунелі". У наведеному вище прикладі дані тунелі можна зрівняти з "конвертами" навколо пакетів даних А и Б із зеленими індексами (адресами типу АП), які доставляються з вузла-джерела в лівій частині схеми на кінцевий вузол у правій частині схеми. Ключовим тут є те, яким образом дані вузли визначають "адреси відправлення" (АП), що відповідають АК А и Б, яким образом навколо пакетів формується "конверт" і як вузли призначення розвертають пакети й роблять правильну доставку вмісту на кінцеві віртуальні машини А и Б.

Ключові аспекти віртуалізації мереж пояснюються за допомогою простої аналогії:

– АК кожної віртуальної машини зіставляється з АП фізичного вузла. З одним АП може бути зв'язане декілька АК.

– Віртуальні машини відправляють пакети даних у просторах АК, які полягають в "конверт" і забезпечуються парою АП джерела й призначення на основі зробленого зіставлення.

– Зіставлення АК – АП повинні дозволяти вузлам робити диференціацію пакетів для різних клієнтських віртуальних машин.

У результаті механізм віртуалізації мереж зводиться до віртуалізації мережних адрес, використовуваних віртуальними машинами. У наступному розділі описується властиво механізм віртуалізації адрес.

Віртуалізація мереж за допомогою віртуалізації адрес

Як механізм віртуалізації IP-адреси віртуалізація мережі підтримує Generic Routing Encapsulation (NVGRE).

– Generic Routing Encapsulation Цей механізм віртуалізації мережі використовує Generic Routing Encapsulation (NVGRE) як частина заголовка тунелю. У механізмі NVGRE пакет віртуальної машини инкапсулюєся в інший пакет. Заголовок цього нового пакета забезпечується необхідними IP-адресами джерела й призначення типу АП на додаток до ID віртуального підмережі, що зберігається в ключовому полі заголовка GRE.

ID віртуальної підмережі дозволяє вузлам ідентифікувати клієнтську віртуальну машину для кожного окремого пакета навіть у випадку можливого перекриття АП і АК на пакетах. Це дозволяє всім віртуальним машинам одного вузла спільно використовувати єдиний АП.

Спільне використання АП впливає на масштабованість мережі. Кількість IP- і MAC-адрес, що вимагають запам'ятовування мережною інфраструктурою, може бути істотно знижено. Наприклад, якщо на кожному кінцевому вузлі є в середньому 30 віртуальних машин, кількість IP- і MAC-адрес, що вимагають запам'ятовування мережною інфраструктурою, знижується на коефіцієнт 30. ID віртуальної підмережі, включені в пакети, також дозволяють робити просту кореляцію пакетів під фактичних клієнтів.

В Windows Server 2025 і більше пізніх версіях віртуалізація мережі повністю підтримує NVGRE; вона НЕ вимагає відновлення наявного або придбання нового мережного обладнання, наприклад мережних карт (мережних адаптерів), комутаторів або маршрутизаторів. Це досягається за рахунок того, що пакет NVGRE при провідній передачі є звичайним IP-пакетом у просторі АП, сумісному із сучасною мережною інфраструктурою.

В Windows Server 2025 високий пріоритет відданий роботі зі стандартами. Разом із ключовими партнерами галузі (Arista, Broadcom, Dell, Emulex, Hewlett Packard і Intel) корпорація Майкрософт опублікувала проект RFC, що містить опис використання загальної інкапсуляції маршрутів (GRE), що є існуючим стандартом IETF як протокол інкапсуляції для віртуалізації мереж з абревіатурою GRE. Додаткові відомості див. у наступному проекті в мережі Інтернет: Віртуалізація мереж з використанням загальної інкапсуляції маршрутів (Network Virtualization using Generic Routing Encapsulation). У міру комерційного впровадження NVGRE вигода від реалізації даного методу ще більше зросте.

Приклад архітектури обслуговування одним екземпляром додатка декількох розгортань

Представлено приклад розгортання двох клієнтів, що переміщаються в хмарі центра обробки даних з використанням взаємин адрес АК-АП, обумовлених політикою віртуалізації мережі.

До переходу до розміщення в службі IaaS, забезпеченої провайдером:

– Компанія A задіяла SQL Server (з ім'ям SQL) за IP-адресою 10.1.1.11 і веб-сервер (з ім'ям Web) за IP-адресою 10.1.1.12, що використовує свій SQL Server для транзакцій бази даних.

– Компанія Б задіяла SQL Server, що також має ім'я SQL і призначений IP-адреса 10.1.1.11, і веб-сервер, теж іменований Web і що має IP-адреса 10.1.1.12, що використовує свій SQL Server для транзакцій бази даних.

– Компанії А и Б перемістили свої сервери SQL Server і відповідні веб-сервери в те саме розміщення в службі IaaS, забезпеченої постачальником, де, по випадковому збігу, вони задіяли віртуальні машини SQL на вузлі 1 (Host 1) і віртуальні машини Web (IIS7) на вузлі 2 (Host 2). Всі віртуальні машини зберігають свої вихідні внутрімережні IP-адреси (свої АК).

Обом компаніям при виділенні віртуальних машин провайдером розміщення призначаються наступні ID віртуальної підмережі (VSID) і адреси типу АП:

– АП віртуальних машин компанії А: VSID – 5001, SQL – 192.168.1.10, Web – 192.168.2.20.

– АП віртуальних машин компанії Б: VSID – 6001, SQL – 192.168.1.10, Web – 192.168.2.20.

Постачальник розміщення створює параметри політики, що складаються із клієнтської віртуальної підмережі для компанії Б, що встановлює відповідність АК віртуальних машин компанії Б призначеним АП і VSID, і окремої клієнтської віртуальної підмережі для компанії А, що встановлює відповідність АК віртуальних машин компанії А призначеним АП і VSID. Далі провайдер застосовує дані параметри політики до Вузла 1 і Вузлу 2.

Коли віртуальна машина Web компанії А запитує на Вузлі 2 свій SQL Server за адресою 10.1.1.11, відбувається наступне:

Вузол 2, ґрунтуючись на своїх параметрах політики, переводить адреси у вигляді пакета по маршруті:

– Джерело: 10.1.1.12 (АК компанії А Web).

– Призначення: 10.1.1.11 (АК компанії А SQL).

Інкапсульований пакет містить:

– Заголовок GRE (OIM) з VSID: 5001.

– Зовнішнє джерело: 192.168.2.20 (АП компанії А Web).

– Зовнішнє призначення: 192.168.1.10 (АП компанії А SQL).

При одержанні пакета Вузол 1, ґрунтуючись на своїх параметрах політики, декапсулює пакет NVGRE:

– Зовнішнє джерело: 192.168.2.20 (АП компанії А Web).

– Зовнішнє призначення: 192.168.1.10 (АП компанії А SQL).

– Заголовок GRE (OIM) з VSID: 5001.

– Декапсульований пакет (вихідний пакет, відправлений з віртуальної машини Web компанії А) доставляється на віртуальну машину SQL компанії А:

– Джерело: 10.1.1.12 (АК компанії А Web).

– Призначення: 10.1.1.11 (АК компанії А SQL).

– Коли віртуальна машина SQL компанії А на Вузлі 1 відповідає на запит, відбувається наступне:

Вузол 1, ґрунтуючись на своїх параметрах політики, переводить адреси у вигляді пакета по маршруті:

– Джерело: 10.1.1.11 (АК компанії А SQL).

– Призначення: 10.1.1.12 (АК компанії А Web).

Інкапсульований пакет містить:

– Заголовок GRE (OIM) з VSID: 5001.

– Зовнішнє джерело: 192.168.1.10 (АП компанії А SQL).

– Зовнішнє призначення: 192.168.2.20 (АП компанії А Web).

При одержанні пакета Вузол 2, ґрунтуючись на своїх параметрах політики, декапсулює даний пакет:

– Джерело: 192.168.1.10 (АП компанії А SQL).

– Призначення: 192.168.2.20 (АП компанії А Web).

– Заголовок GRE (OIM) з VSID: 5001.
– Декапсульований пакет доставляється на віртуальну машину Web компанії А:
– Джерело: 10.1.1.11 (АК компанії А SQL).
– Призначення: 10.1.1.12 (АК компанії А Web).
– Аналогічний процес для трафіка між Б Web і віртуальними машинами SQL використовує параметри політики HNV для корпорації Б. У результаті при використанні HNV віртуальні машини компанії Б и А взаємодіють так, ніби перебували у своїх інтрамережах компаній. При цьому вони не можуть взаємодіяти один з одним, навіть незважаючи на те, що використовують однакові IP-адреси.

– Роздільні адреси (АК і АП), параметри політики вузлів, а також перетворення адрес із АК в АП і назад для вхідні й вихідного трафіка віртуальних машин ізолюють ці комплекти серверів. Більше того, зіставлення віртуалізації й перетворення позбавляють архітектуру віртуальної мережі прив'язки до інфраструктури фізичної мережі. Хоча SQL і Web компанії А и SQL і Web компанії Б розташовуються в їх власних підмережах IP АК (10.1.1/24), їхнє фізичне розгортання відбувається на двох вузлах у різних підмережах АП: 192.168.1/24 і 192.168.2/24 відповідно. Суть у тім, що перекрестно-підмережне виділення віртуальних машин і динамічна міграція стають можливими із застосуванням віртуалізації мережі.

Архітектура віртуалізації мереж

В Windows Server 2025 застосування політики віртуалізації мережі й віртуалізація IP виконувалися фільтром полегшеного доступу (LWF) специфікації інтерфейсу мережного драйвера (NDIS), що називається мережний віртуалізацією Windows (WNV). Фільтр WNV розташовувався нижче комутатора. У такої архітектури був побічний ефект: розширення комутатора могли бачити тільки трафік простору АК, але не простору АП.

В Windows Server 2025 R2 HNV є частиною віртуального комутатора, завдяки чому розширення можуть бачити обоє простору адрес: і АК, і АП.

Кожний мережний адаптер віртуальної машини при налаштуванні забезпечується IPv 4- або IPv 6-адресою. Існують АК, використовувані для зв'язку віртуальних машин один з одним, вони надходять в IP-пакетах із цих віртуальних машин. Віртуалізація мережі віртуалізує такі АК в АП, ґрунтуючись на політиках мережний віртуалізації.

Віртуальна машина відправляє пакет з адресою джерела АК1, що віртуалізується на основі політики у фільтрі HNV у комутаторі. Особливий список керування доступом до віртуалізації мереж на основі VSID ізолює віртуальну машину від інших віртуальних машин, не включених у ту ж віртуальну підмережа або в той же домен маршрутизації.

Керування політикою віртуалізації мереж

Платформа Windows надає API загального користування для керуючого ПЗ центрів обробки даних для керування віртуалізацією мережі. Диспетчер віртуальних машин є одним з таких продуктів для керування центром обробки даних. Керуюче ПЗ містить усе політики віртуалізації мережі. Оскільки диспетчер віртуальних машин повинен розпізнавати віртуальні машини й, що важливіше, забезпечувати віртуальні машини й у цілому клієнтські віртуальні мережі в центрі обробки даних, а також підтримувати архітектуру багатотенантного обслуговування, керування політикою віртуалізації мережі є природним розширенням організації мереж на основі політики.

Зведення

Центри реєстрації й обробки даних на основі технології хмари можуть забезпечувати безліч переваг, наприклад поліпшену масштабованість і більше ефективне використання ресурсів. Реалізація цих потенційних переваг вимагає застосування технології, присвяченої принциповому рішенню проблем багатоклієнтської масштабованості в динамічному середовищі. Віртуалізація мережі створена для рішення цих проблем і підвищення робочої ефективності центрів обробки даних за рахунок поділу топологій віртуальної й фізичної мереж. Побудована на основі існуючого стандарту, віртуалізація мережі працює в середовищі сучасного центра обробки даних, а в міру впровадження встаткування, сумісного

з NVGRE, кількість переваг, що здобуваються, буде збільшуватися. Із застосуванням віртуалізації мережі клієнти одержують можливість поєднувати свої центри обробки даних у приватна хмара або за допомогою технології гібридної хмари відносно легко розширювати свої центри обробки даних до середовища постачальника послуг розміщення.

Розробка структурної схеми

Віртуалізація від Nuage

Мережні інфраструктури стають вузьким місцем при «переході» до віртуалізованих IT і хмарної моделі одержання IT-сервісів. Динамічне середовище віртуальних машин (ВМ) дуже погано співвідноситься зі статичними мережами, у яких використовуються протоколи (наприклад, VLAN і STP), що застосовувалися в них і п'ять, і десять років тому.

Розглянемо типове завдання по розгортанню нового додатка або впровадженню нового сервісу, що складає з декількох функціональних компонентів, розміщених у різних підмережах. Раніше для цього була потрібна установка нових серверів, що займало кілька тижнів. Сучасні системи віртуалізації серверних ресурсів дозволяють виділити необхідні новому додатку або сервісу віртуальні машини з потрібною продуктивністю за лічені мінути.

Однак відповідна підготовка мережі займає набагато більше часу. Конфігурування різних типів мережних пристроїв часто відбувається вручну й вимагає залучення великої кількості фахівців: один займається локальною мережею, іншої – територіально розподіленої, третій – налаштуванням VLAN, четвертий – конфігуруванням міжмережних екранів і т.д. Як результат, всі переваги віртуалізації серверів у частині прискорення впровадження додатків зводяться на ні «повільністю» традиційних процедур налаштування мережі.

Вирішити проблему дозволяють нові технології віртуалізації мережі, які зараз активно розробляють і виводять на ринок багато виробників. Одне з найбільш зрілих рішень, що вже розгорнули у своїх мережах кілька закордонних компаній, пропонує Nuage Networks. Воно підтримує більшість основних гіпервізорів (KVM, Xen, ESXi), систем оркестрації (включаючи VMware, OpenStack, CloudStack) і працює поверх мережної інфраструктури, побудованої на встаткуванні будь-якого виробника.

Рішення Nuage Networks Virtualized Services Platform (VSP) складається із трьох основних елементів:

– каталогу віртуалізованих сервісів (Virtualized Services Directory, VSD);
– агентів віртуальної маршрутизації/комутації (Virtual Routing & Switching, VRS);
– контролерів віртуалізованих сервісів (Virtualized Services Controller, VSC).

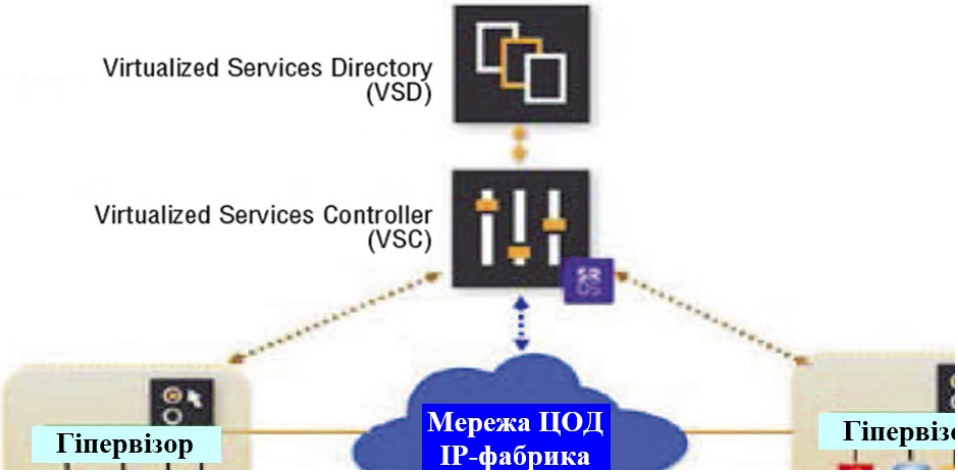

Рисунок 1 – Структурна схема системи

Каталог VSD забезпечує високий рівень абстракції. Він дозволяє описати мережні структури користувачів хмарної мережі й надати можливість адміністраторам самостійно управляти мережними ресурсами в заданих границях. Найважливішою функцією VSD є

створення шаблонів мережних політик, не зв'язаних зі специфікою апаратного пристрою мережі. Надалі, при запуску конкретного екземпляра віртуалізованого додатка, на основі заданого шаблона створюється опис конфігурації його мережі. Наприклад, окремий шаблон можна створити для додатків (віртуальних машин), що поміщаються в «демілітаризовану» зону, доступ у яку може здійснюватися тільки по TCP і тільки через протокольний порт 80.

Агенти VRS відповідають за керування віртуальними мережними інтерфейсами відповідно до заданих шаблонів (політиками) і працюють під керуванням найпоширеніших гіпервізорів. Вони інкапсулюють генеруємий віртуальними машинами трафік і передають його між кінцевими точками (гіпервізорами) по тунелях. Таким чином, поверх фізичної інфраструктури мережі формується накладена мережа типу «фабрика».

Агенти VRS одержують інструкції щодо того, що робити з конкретним трафіком, від контролера VSC, відповідального за цілісну роботу й подання загальної топології багатокористувальницької мережі. Оскільки цей контролер використовує ту ж операційну систему SROS, що й лінійка сервісних маршрутизаторів Alcatel-Lucent 7x50, на базі якої працюють ряд найбільших у світі IP-мереж, він здатний управляти повнофункціональною маршрутизацією (на рівнях L 2-L4) для тисяч користувальницьких підмереж.

При запуску віртуальної машини, що виконує роль одного з функціональних компонентів віртуалізованого додатка, контролер VSC за запитом від VRS одержує з бази даних VSD екземпляр шаблона (instance). Потім цей шаблон завантажується в контролер, що автоматично набудовує всі мережні елементи, які можуть бути задіяні в обслуговуванні даного додатка. Ручне переконфігурування окремих мережних пристроїв виключається.

Шаблон, у якому визначені мережна конфігурація й правила обробки трафіка конкретного додатка, залишається прив'язаний до відповідних віртуальних машин поза залежністю від їхніх переміщень. Вони можуть розташовуватися в одному ЦОД або в декількох, переміщатися між фізичними серверами й територіально віддаленими площадками – віртуальна мережа буде автоматично підлаштовуватися.

Прискорення інтеграції віртуалізованого додатка/сервісу в мережу, пояснює він, досягається за рахунок створення шаблона, у якому вказуються вимоги до мережі, включаючи конфігурацію підмереж, параметри якості обслуговування (Qo), налаштування безпеки та ін. Пізніше адміністратор може багаторазово тиражувати його при розгортанні екземплярів віртуалізованого додатка/сервісу.

На практичному семінарі фахівці Nuage Networks розгорнули демонстраційну мережу, до складу якої входили хости із двома типами гіпервізорів: ESXi (під керуванням VMware vCenter) і KVM (під керуванням OpenStack Havana). За допомогою засобів VSD було продемонстроване формування структури накладеної мережі (поділ її на зони, підмережі), після чого подібні дії були виконані із застосуванням системи OpenStack – відповідні зміни автоматично з'явилися в каталозі Nuage VSD.

Потім віртуальні машини були запущені на хостах з гіпервізорами KVM і ESXi (в останньому випадку через vCenter). Вони містилися в ті зони (підмережі), які забезпечували необхідні ним параметри обслуговування. Трафік між гіпервізорами різних типів (KVM і ESXi) передавався в режимі L3 – тобто з маршрутизацією.

Найбільш затребуваний сценарій – «живаючи» міграція віртуальних машин з одного хоста на інший. Ця процедура була ініційована із системи керування vCenter, а мережа автоматично перенастроїлася для обслуговування ВМ на новому місці. Шаблон, що визначає правила обробки трафіка додатка, автоматично треба за віртуальною машиною при її переїзді. При цьому ніякого втручання адміністратора не потрібно. Більше того, віртуальну мережу можна розтягти по VPN через територіально розподілену мережу (WAN) до офісної мережі компанії. Ця функціональність теж була продемонстрована фахівцями Nuage Networks.

З огляду на той факт, що не всі підключені до мережі пристрої піддаються віртуалізації, рішення Nuage VSP передбачає механізми інтеграції апаратних компонентів (таких, наприклад, як сервери баз даних, міжмережні екрани, різні шлюзи). Для сценаріїв, що

не вимагають високої продуктивності, пропонується програмний модуль VRS Gateway. Для ситуацій з більшими обсягами трафіка розроблений апаратний шлюз 7850 VSG із продуктивністю більше 1 Тбіт/с, що підтримує інтерфейси 1GE, 10GE і 40GE.

Brocade: віртуалізируя фабрику й мережні функції

З 2008 року в результаті покупки Foundry Networks у лінійці компанії Brocade з'явилися IP-рішення, і зараз у сферу її інтересів входять класичні IP-маршрутизатори L3, а також SDN, NFV і засобу оркестрації хмар (автоматизація виділення ресурсів у хмарі й керування ними). Останні реалізуються Brocade по SAN і LAN у рамках проекту OpenStack. Рішення, орієнтовані на ЦОД, мають стратегічне значення, були представлені як уже успішно експлуатовані в замовників продукти, так і нові розробки.

З появою в лінійці продуктів Ethernet взяли краще з миру FC, об'єднали ці інструменти з технологіями Ethernet і одержали Ethernet-Фабрики – віртуальний розподілений Ethernet-Комутатор. Фактично це новий підхід до побудови мережі передачі даних – з використанням одного логічного комутатора, керування яким здійснюється з єдиної точки, і при цьому забезпечується високий ступінь автоматизації. Зараз поряд з фабриками FC лінійка Brocade містить у собі Ethernet-Фабрики – основні її рішення для ЦОД.

Ethernet-Фабрика Brocade VCS реалізує віртуальний розподілений комутатор рівня доступу й агрегування. Вона практично не вимагає налаштування, підтримуючи «самоформування» і автовизначені пристроїв у будь-якій топології, при цьому керування нею здійснюється як одним віртуальним комутатором. Для запуску фабрики досить задати її домен і ID, а потім можна користуватися єдиною консоллю керування всіма комутаторами.

Для підвищення надійності підтримується топологія Full Mesh, завдяки чому працездатність системи зберігається навіть при виході з ладу одного комутатора. Крім того, фабрика готова до конвергенції (FC 16 / FCo 10 Гбит/с), підтримує три рівні балансування трафіка й здатна агрегувати (без попереднього налаштування) велика кількість каналів. Завдяки покадровому балансуванню забезпечується рівномірний розподіл навантаження між портами комутаторів. За допомогою протоколу ECMP здійснюється балансування між еквівалентними за вартістю шляхами, що з'єднують кінцеві точки (незалежно від числа транзитних вузлів). А балансування навантаження між шлюзами VRRP-E L3 (до чотирьох шлюзів) поліпшує масштабованість і надійність рішення.

Недавно з'явилася в Brocade технологія дає можливість створювати «віртуальні фабрики» усередині VCS. Виділення логічних фабрик для кожного користувача в рамках поділюваної фізичної фабрики на основі TRILL Fine-Grained Labels (IETF draft) дозволяє повторно задіяти VLAN. У рамках кожної фізичної фабрики підтримується до 8000 віртуальних фабрик VCS.

Завдяки інтеграції з VMware vCenter, Ethernet-Фабрика може одержувати інформацію про віртуальні машини, їх MAC- і IP-адресах, групах VLAN. Ця інформація автоматично заноситься в Ethernet-Фабрику, і за замовчуванням створюються «профілі портів», до яких можна застосовувати різні налаштування – наприклад, задавати якість обслуговування Qo. Система настроюється однократно – надалі фабрика сама застосовує задані політики по MAC-адресі, на якому б з портів він не був ідентифікований. Одна фабрика поєднує до 48 комутаторів.

В останніх версіях фабрики Brocade реалізований VXLAN-шлюз VCS (VTEP) для VMware NSX – міст між віртуальними й фізичними ресурсами. Його можна використовувати для інтеграції із класичними мережами, що не підтримують VXLAN. Повна підтримка VCS реалізована в комутаторах Brocade VDX серії 6740 і маршрутизаторах 8770. У серії 6740 (SDN-ready) можна використовувати протокол OpenFlow 1.3. Відповідно до планів Brocade, контролер SDN з'явиться на ринку під кінець року. Він буде сполучати функції контролера й комутатора SDN, продовжуючи лінійку VDX 6740. Протокол OpenFlow підтримується також продуктами Brocade Fibre Channel.

На думку аналітиків, у найближчій перспективі будуть розгортатися переважно гібридні рішення, що сполучають традиційну мережну інфраструктуру й SDN, тому більшість комутаторів SDN допускають програмне перемикання між SDN і комутацією L2/L3. Тим самим знижуються ризики впровадження нової технології. Brocade пропонує своє рішення. На відміну від інших вендорів компанія розробила комутатори й маршрутизатори з «гібридними портами», тобто вони можуть працювати в змішаному режимі, підтримуючи як традиційне керування, так і керування за допомогою контролера SDN. Такий режим зараз реалізується маршрутизаторами Brocade MLXe.

SDN уже знаходить практичне застосування. Так, в одного із замовників подібна система допомагає знизити негативний вплив атак DDo. Погрози виявляються за допомогою sFlow-RT (у режимі реального часу) і відправляються на колектор, де обробляються програмним забезпеченням централізованого керування мережею Brocade Network Advisor, здатним виступати також як контролер sFlow. Колектор сповіщає контролер, що потрібно використовувати правило OpenFlow DDo на маршрутизаторі MLXe (див. Рисунок 5) для протидії атаці DDo.

Поряд з SDN, у мережній галузі набирає популярність технологія NFV. Вона дозволяє за допомогою віртуалізації консолідувати різні мережні пристрої (міжмережне встаткування, комутатори, маршрутизатори, балансувальники навантаження й т.п.) на стандартних серверах x86, що веде до зменшення вартості й збільшенню «живучості» систем. Перераховані пристрої стають віртуальними (функціонують у вигляді ВМ), так що здобувати дороге «залізо» не потрібно.

Тим часом Brocade уже пропонує віртуальний маршрутизатор Vyatta vRouter з функціями концентратора VPN із шифруванням IPSec і міжмережного екрана. Це відносно недороге й гнучке рішення для невеликої мережі Ethernet дає можливість надавати мережні функції «за запитом» і реалізує маршрутизацію, міжмережной екран, VPN. Для розгортання таких ВМ можна використовувати існуючі стандартні сервери x86, здатні успішно заміняти спеціалізовані системи, у тому числі рішення для інфраструктури зв'язку. vRouter інтегрований зі стандартними оркестраторами (OpenStack).

Ще один віртуальний продукт Brocade – повнофункціональний балансувальник трафіка додатків ADX. Будучи ключовим компонентом L 4-L7 в NFV, він динамічно балансує трафік додатків і прискорює запуск сервісів. Для цілей централізованого керування передбачається підтримка OpenStack і API. Віртуальний ADX можна розгортати у вигляді ВМ на сервері з гіпервізорім або без гіпервізора, виділяючи йому весь сервер.

Ці продукти дозволяють гнучко (за запитом) впроваджувати різні сервіси, однак пропускна здатність у них трохи нижче, ніж у фізичних пристроїв, – від 10 Мбіт/с до 3 Гбіт/с (обмеження залежить від ліцензії, а не від швидкодії сервера). Продуктова лінійка Brocade, включаючи віртуальні пристрої, підтримує оркестрацію за протоколом OpenStack (через оркестратори сторонніх вендорів). Компанія бере активну участь у розробці стандартів OpenStack і пропонує розширення Dynamic Network Resource Management (DNRM) у рамках проекту Neutron, щоб спростити побудову мультивендорних мереж.

Зі збільшенням обсягів мережного трафіка й кількості підключених до мережі пристроїв конфігурування мереж і керування ними перетворюється в складне завдання. Щоб неї полегшити, потрібні серйозні зміни в підходах до побудови, експлуатації мереж і керуванню ними. Мережна інфраструктура розвивається й еволюціонує повільно, відстаючи від бурхливого розвитку засобів віртуалізації серверів і систем зберігання, однак саме мережі повинні стати надійною й гнучкою основою для середовища хмарних обчислень. В останні рік-два в цій області намітився явний прогрес, а розробки в області NFV відкривають для замовників перспективи переходу від апаратних до віртуальних мережних рішень зі збереженням всіх функцій, властивим апаратним продуктам.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

– Досліджена система віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

– На основі отриманих результатів досліджень створена програмна реалізація системи віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання віртуалізації мережі Nuage Networks для автоматизації SDN і SD-WAN. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
4. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
5. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
6. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
7. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
8. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
9. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
10. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
11. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
12. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
13. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
14. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
15. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

16. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
17. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
18. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
19. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
20. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
21. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
22. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
23. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
24. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
25. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.