УДК 004

А.Мороз, магістр гр. КІ-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПОБУДОВИ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ SDN

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

Постановка проблеми. За два-три роки SDN пройшла шлях від концепції до конкретних технічних рішень. Як показав наш аналіз, виробники пропонують комплексні рішення SDN, цілком готові до впровадження, при цьому вони передбачають еволюційний шлях розгортання SDN у традиційних мережних інфраструктурах. Інакше кажучи, обіцяні новою технологією переваги цілком можна одержати без революційної заміни всього наявного устаткування. На ринку з'явилося досить велике число продуктів, що вписуються в концепцію SDN, а замовники всерйоз стали вивчати питання доцільності розгортання SDN і поступового переходу до програмувальних мереж – саме так ми пропонуємо йменувати SDN. Настав час проаналізувати конкретні рішення SDN, щоб допомогти замовникам у їхньому виборі. Як нам представляється, найкращий спосіб зробити це – сформулювати типову (якщо, звичайно, поняття «типове» застосовно до такої інноваційної області, як SDN) завдання й запропонувати для нього рішення. Ефектною й одночасно ефективною можливістю багатьох рішень SDN є візуалізація трафіку у фізичній і логічній мережах, що дозволяє спростити експлуатацію, прискорити виявлення й усунення несправностей, спростити моніторинг SLA.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи побудови мережі на основі технології SDN.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи побудови мережі на основі технології SDN.

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

– Огляд існуючих систем побудови мережі на основі технології SDN.
– Дослідження системи побудови мережі на основі технології SDN.
– Програмна реалізація системи побудови мережі на основі технології SDN.

Об'єктом дослідження є процес побудови мережі на основі технології SDN.

Предметом дослідження є методи побудови мережі на основі технології SDN.

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

Виклад основного матеріалу. Головним елементом будь-якого рішення SDN, безумовно, є контролер. З мережною інфраструктурою контролер взаємодіє через «південні»

інтерфейси, основний з них – OpenFlow. Шість із семи представлених контролерів підтримують зазначений протокол. Виключення становить тільки контролер APIC-EM компанії Cisco. На момент підготовки матеріалу в якості «південного» API на цьому контролері був доступний тільки Cisco CLI (відповідно, і працювати він міг тільки з комутаторами й маршрутизаторами Cisco). Однак уже в наступних версіях ПЗ APIC-EM запланована підтримка устаткування інших виробників або комутаторів без передвстановленої ОС (bare-metal switch) за рахунок використання OpenFlow і Cisco OnePK.

Загальний підхід Cisco складається в поділі мережі замовника на логічні домени (ЦОД, WAN, кампус, сервісна інфраструктура й т.д.) і використанні для кожного домену (або груп доменів) спеціалізованого SDN-контролера, що найбільше ефективно вирішує стандартні для обраного домену завдання. Для забезпечення наскрізного сервісу, що вимагає взаємодії декількох інфраструктурних доменів, Cisco поставляє рішення по оркестрації (Network Service Orchestrator, NSO). Для поставленого завдання Cisco запропонувала контролер APIC-EM (Application Policy Infrastructure Controller – Enterprise Module), спеціально розроблений для корпоративних кампусних і розподілених (WAN) мереж. Це ідеологічний і технологічний спадкоємець контролера APIC, використовуваного в рамках архітектури Cisco Application Centric Infrastructure (ACI) для керування інфраструктурою ЦОДу.

Контролер APIC-EM реалізує функціональність керування мережними елементами, залишаючи всі інші завдання зовнішнім системам керування й сторонніх додатків, взаємодіючим з APIC-EM через «північний» програмний інтерфейс REST.

На відміну від Cisco, компанія NEC є затятим прихильником стандартизованого підходу на основі OpenFlow. Представники NEC називають свій контролер «лідером по відповідності стандартам OpenFlow і сумісності з комутаторами інших виробників», що щорічно підтверджується більшим числом тестів. На «північній» стороні контролер NEC підтримує JSON, XML і SOAP.

Саме собою що розуміє вважають підтримку протоколу OpenFlow і в компанії Huawei. При цьому Huawei створила розширення стандарту OpenFlow – технологію Protocol Oblivious Forwarding (POF), назад сумісну з OpenFlow. Цей підхід забезпечує можливість використовувати як OpenFlow, так і традиційні механізми маршрутизації для передачі й керування трафіком. Таким чином, замовник може здійснити плавний перехід до SDN. Подібну міграцію пропонують і інші компанії (див. нижче).

Для керування SDN-Устаткуванням контролер HP VAN SDN Controller, крім OpenFlow 1.0 і 1.3.1, також підтримує SNMP і NetConf. На «північній» стороні він надає відкриті програмні інтерфейси на Java і REST API для запуску додатків SDN і їхньої інтеграції із зовнішніми системами (наприклад, із системами керування й оркестрації). Крім того, рішення HP підтримує динамічне завантаження й запуск додатків SDN безпосередньо на самому контролері за рахунок використання відкритої архітектури на базі OSGi.

Компанії Brocade і Extreme Neworks запропонували замовникові контролери на базі систем з відкритим вихідним кодом OpenDaylight. Як відзначають у компанії Extreme Neworks, у своєму рішенні One Controller вони поліпшили захист і розширили функціональність платформи OpenDaylight. На «південному» інтерфейсі використовується стандартний протокол OpenFlow v.1.3. ПЗ OneFabric Control Center і OneFabric Connect забезпечують API на «північному» інтерфейсі для підтримки додаткової, розширеної функціональності, зокрема, з використанням компонентів керування мережею – Netsight, уніфікованого доступу до мережі – NAC, моніторингу роботи додатків у мережі – Purview.

Комерційна версія контролера OpenDayLight від компанії Brocade – Brocade SDN Controller (BSC) – на «південній» стороні, крім OpenFlow 1.0/1.3, підтримує NETCONF, OVSDB, BGP-LS, PCEP. На «північному» інтерфейсі BSC має веб-сервісний RESTful API, для роботи з яким можуть використовуватися високорівневі мови програмування Python, Ruby, Perl.

Замовник одержав і рішення на основі контролера Runos, відмінними рисами якого, за твердженням представників ЦПІКС, є висока продуктивність (пропускна здатність 8 млн подій у секунду, затримка на обробку одного запиту 30 мкс) і зручність розробки. Проект Runos перебуває у відкритому доступі (http://arccn.github.io/runos/) на умовах ліцензії Apache 2.0, що повинне сприяти широкому поширенню контролера, його розвитку й доробці сторонніми розроблювачами. У відкритому доступі перебувають ядро контролера, базовий набір сервісів і додатків (визначення топології, побудова маршруту, статистика й моніторинг, інтерфейс REST, графічний інтерфейс). У комерційній версії контролер Runos має механізми резервування, масштабованості й розподіленого керування.

Важливим моментом є резервування контролера. Не зрячи у своєму завданні замовник особливо обмовило необхідність відказостійкої схеми. І всі постачальники забезпечили її – подробиці нижче в розділах, присвячених конкретним рішенням.

Вибір комутаторів

Незважаючи на те що замовник наполегливо цікавився можливістю використання в проекті комутаторів без передвстановленої ОС (так звані bare metal switch або white box), більшість постачальників зволіли традиційні мережні пристрої, але з підтримкою SDN.

Пояснюючи причину того, що Huawei не пропонує у своїх рішеннях комутатори класу bare metal, тому що при впровадженні SDN важливо забезпечити наступність архітектури й зберегти працездатність наявних додатків, а існуючі сервіси й протоколи орієнтовані на традиційні мережні засоби.

Представляючи свої SDN-рішення в цілому, компанія HP відзначила можливість побудови мережної інфраструктури з комутаторами на базі відкритої платформи (white box), але рекомендувала їхнє використання в ЦОДух більших масштабів – від 200 To-комутаторів або від 10 000 портів. Такі інфраструктури можна реалізовувати на базі комутаторів HP серії Altoline. На думку фахівців HP, вони найбільш ефективні для ЦОДів, у яких в основному використовуються додатки Open Source, хмарні платформи OpenStack/CloudStack, рішення HPC на базі Hadoop, бази даних NoSQL (Cassandra/HBase) і т.п. Очевидно, що це не випадок нашого замовника.

Хоча більшість постачальників рекомендували замовникові свої ж комутатори, дві компанії, Extreme Networks і NEC, не стали обмежувати його вибір, указавши можливості установки комутаторів інших виробників – головне, щоб вони підтримували стандарти OpenFlow.

У частині вибору комутаторів на тлі інших виділяється пропозиція ЦПІКС. Фахівці цієї компанії рекомендували доповнити свій контролер Runos комутаторами класу white box або комутаторами, побудованими на основі серверів x86. У першому випадку на комутатори встановлюється система Open Networking Linux з розробленим у ЦПІКС агентом OpenFlow 1.3. Такі пристрої підтримують до 48 портів 1Gb, а також чотири порти 10Gb. У другому випадку використовуються традиційні сервери Intel з більшим числом мережних інтерфейсів. Комутація здійснюється спеціальним ПЗ за рахунок ресурсів центрального процесора. Такі комутатори здатні підтримувати до 24 портів 1Gb і до 12 портів 10 Gb с сумарною гарантованою пропускною здатністю 60 Gb на пристрій.

Як відзначають фахівці ЦПІКС, важливою відмінністю комутаторів на базі серверів x86 від комутаторів white box є повна підтримка можливостей протоколу OpenFlow 1.3. У комутаторах white box, як правило, використовуються стандартні набори мікросхем від Broadcom, які на апаратному рівні не підтримують найчастіше необхідну функціональність OpenFlow, наприклад перезапис IP-адрес.

Додатки SDN

Одне з важливих переваг SDN – можливість використання широкого набору додатків, що реалізують різні мережні сервіси й функції. Такі додатки створюються в тому числі сторонніми розроблювачами й найчастіше надаються замовникам безкоштовно.

Більшість компаній для просування рішень SDN прагнуть сформувати екосистему SDN, важливою частиною якої є розроблювачі додатка. Відзначимо пропонований HP

онлайн-магазин SDN-додатків HP SDN App Store (див. урізання «SDN-додатка з магазина»). Як затверджують в HP, користувачі можуть буквально одним кличем мишки завантажувати SDN-додатка з магазина на контролер, відразу ж їх запускати й використовувати.

SDN-додатки з магазина:

– Hyperglance – додаток 3D-візуалізації мережної топології. Воно дозволяє робити моніторинг потоків трафіку в режимі реального часу, а також гнучко маніпулювати ними (перенаправляти, фільтрувати, оптимізувати утилізацію каналів і т.п.) зі зручного графічного інтерфейсу.

– SDN Privatizer – безкоштовний додаток, що реалізує функціональність Private VLAN у масштабах всієї мережі, що дозволяє ізолювати друг від друга різні групи користувачів, у тому числі, підключених до різних комутаторів або навіть розташовуються в різних сегментах мережі.

– BlueCat DNS Director – безкоштовний додаток, що перехоплює DNS-запит користувача й, яка би IP-адреса сервера в ньому не був зазначений, заміняє його на заданий адміністратором адреса корпоративного DNS, тим самим забезпечуючи додатковий рівень безпеки IT-інфраструктури.

В NEC також підкреслюють наявність широкого спектра SDN-додатків від компаній-партнерів. Ці додатки вирішують питання оптимізації мережі (балансування навантаження, WAN-Оптимізація), аналізу її продуктивності, фільтрації й керування правами доступу (DPI), безпеки (MCE, захист від DDoS і злобливого ПЗ), оптимізації трафіку й т.д. Зі списком інтегрованих з SDN-контролером NEC додатків P-Flow можна ознайомитися, зареєструвавшись в екосистемі NEC SDN Partner Space. У рамках даної ініціативи також здійснюються перевірка на сумісність і тестування комутаторів OpenFlow інших виробників, які надалі можуть використовуватися в мережах SDN під управлінням контролера NEC.

Фахівці NEC звертають увагу на переваги концепції сервісних ланцюжків (Service Chaining), коли різні необхідні користувачеві функції можуть вибиратися й комбінуватися із загального пула для конкретної віртуальної мережі VTN. Це можуть бути класичні для IP-мереж L2/L3 функції контролю доступу, пріоритизації трафіку, керування політиками QoS і т.д., а реалізовані вони можуть бути як у вигляді окремого SDN-додатка, так і на базі апаратного компонента. Такий підхід дозволяє власникові мережі SDN створити набір VTN, архітектурно й функціонально оптимізованих відповідно до вимог користувачів, а також динамічно реагувати на штатні й позаштатні ситуації. Наприклад, система захисту від DDoS-атаки або пристрій фільтрації трафіку можуть включатися в структуру мережі й задіятися тільки у випадку виявлення погрози.

Розробка структурної схеми
ЦПІКС

Проект ЦПІКС, як уже говорилося, виділяється вибором комутаторів (пристрою white box або на основі серверів x86), у плані ж архітектури він більш-менш типовий. У центральному офісі кінцеві користувачі підключаються до шести граничних комутаторів, кожний з яких з метою резервування приєднується до двох центральних комутаторів 10G. На серверній фабриці функціонують необхідні замовникові мережні сервіси, включаючи контролер Runos. Останній запускається у двох екземплярах у режимі Active/Standby: у випадку «падіння» першого екземпляра керування передається на резервний контролер.

На відміну від центрального офісу, у філіях не потрібно великої кількості кінцевих портів, тому там досить двох комутаторів. Замість серверної фабрики розгортається один сервер віртуальних машин, на якому й будуть працювати необхідні мережні сервіси.

Додаток SDEnterprise для контролера Runos забезпечить необхідну функціональність, включаючи взаємодію із сервісами VPN, MCE й DPI, з інтернет-провайдером (BGP, MPLS), керування списками контролю доступу ACL і ін.

У центральному офісі й філіях працюють свої екземпляри контролерів SDN. У випадку втрати каналу до центрального офісу мережа філії продовжить функціонувати автономно.

Серед додаткових можливостей, які надає рішення ЦПІКС, – інтеграція з контролером Wi-Fi для безшовного роумінгу й можливість роботи із протоколу dot1x для автентифікації користувачів без твердої прив'язки до порту комутатора. Остання функція дозволяє користувачам мігрувати між мережними пристроями (включаючи точки доступу Wi-Fi), при цьому мережа буде автоматично підбудовуватися під нове розташування користувача.

Brocade

Для рішення завдання фахівці Brocade запропонували використовувати L 3-комутатори сімейства ICX 7000, програмний маршрутизатор Brocade vRouter 5600 і контролер Brocade SDN Controller (далі BSC). У великому офісі передбачається розгорнути дворівневу мережу, у ядрі якої встановити пари високопродуктивних комутаторів ICX 7750 (вони ж можуть використовуватися для підключення серверів), зв'язаних твінаксіальними кабелями на швидкості nx40G. Рівень доступу реалізується на базі ICX 7250. Засоби керування всією мережею (включаючи порти доступу) консолідовані на рівні ядра (архітектура SwitchPort Extender) – вся локальна мережа, по суті, являє собою один комутатор («розподілене шасі»). На границі мережі встановлюється відказостійка пара маршрутизаторів vRouter 5600, а у філіях – vRouter 5600 і 48-портовий ICX 7250.

Серед переваг комутаторів Brocade ICX з ОС FastIron (у порівнянні з комутаторами white box, а також пристроями ряду інших виробників) фахівці Brocade назвали підтримку вже згаданої архітектури Switch Port Extender і гібридних портів – той самий порт можна використовувати як для традиційної комутації/маршрутизації, так і для передачі трафіку відповідно до обумовленого контролера правилами. Комутатори можна об'єднати в стек за допомогою стандартних інтерфейсів 1/10/40G Ethernet, причому такий стік може бути розподіленим (до 10 км). Використовувана в комутаторах технологія Po+/Po дозволяє дистанційно (по локальній мережі) подавати електроживлення потужністю до 90 Вт.

На базі BSC можна побудувати відказостійкий кластер із трьох територіально розподілених вузлів. Як варіант можливий створення пула контролерів, схованих за однією віртуальним IP-адресою (VIP).

Як опція в проект може бути включений продукт Brocade Flow Optimizer, що разом з BSC використовується для інтелектуального керування потоками даних, виявлення аномалій і захисту від різних атак. У графічному інтерфейсі FlowOptimizer визначаються профілі трафіку й застосовувані до них правила, задані налаштування автоматично трансформуються в правила OpenFlow і за допомогою контролера в динамічному режимі передаються на мережні пристрої.

CISCO

Для комутації в мережах центрального й віддаленого офісів Cisco запропонувала комутатори серії 2960 з підтримкою Po/UPo або серій 3650/3850, що включають також функції контролера бездротового доступу. У центральному офісі варто передбачити від 8 до 20 комутаторів (по 24 або 48 клієнтських портів) – вибір, тип і кількість пристроїв визначаються топологією СКС, наявністю ЦОДу й вимог по підтримці бездротової мережі. У віддалених офісах пропонується встановити два-три комутатори зазначених серій.

Зв’язність центрального й віддаленого офісів забезпечать маршрутизатори серії ISR 4000. У центральному офісі пропонується встановити відказостійку пари маршрутизаторів Cisco ISR 4451, а у віддалених офісах (залежно від вимог відказостійкості й можливостей каналів глобальної мережі) – один або два маршрутизатори ISR 4431.

Для забезпечення відказостійкості Cisco рекомендувала розмістити контролер APIC-EM на декількох віртуальних машинах, причому ті, у свою чергу, повинні виконуватися на територіально рознесених серверних платформах. Будуть потрібні серверні платформи x86 з гіпервізором VMware ESXi.

Для складання правил, керування життєвим циклом елементів і контролю змін пропонується програмний продукт Prime Infrastructure (PI). Для забезпечення ідентифікації й контролю прав доступу – Identity Service Engine (ISE).

Серед додаткових можливостей, надаваних рішенням на базі APIC-EM, представники Cisco виділили автоматичне виявлення й налаштування нових мережних пристроїв (для цього використовуються протоколи CDP/LLDP, а також функціонал Pn-сервера з боку APIC-EM і PnP-клієнта з боку комутатора або маршрутизатора), взаємодія із системами уніфікованих комунікацій (телефонія, відео, конференції), автоматизоване забезпечення Call Admission Control (CAC), автоматизацію мережної безпеки (при інтеграції із зовнішніми системами). Рішення Cisco забезпечує візуалізацію топології й сервісів, а також застосування й візуалізацію налаштувань QoS, ACL, індивідуальних правил для кожного клієнта.

Cisco планує поставляти APIC-EM безкоштовно з набором убудованих мережних додатків (за нові спеціалізовані додатки буде, імовірно, стягуватися додаткова плата).

Extreme networks

Запропонований Extreme Neworks SDN-контролер One Controller, як уже говорилося, побудований на базі платформи з відкритим вихідним кодом OpenDaylight. Компанія не конкретизувала моделі комутаторів, рекомендувавши лише свої продукти сімейств Summit і Black Diamond, які використовують мережну ОС EXOS з підтримкою OpenFlow v.1.3. Крім того, у запропонованому рішенні можливе використання будь-яких комутаторів з підтримкою протоколу OpenFlow v.1.0 і вище, що, природно, розширює «волю маневру» замовника.

Фахівці компанії відзначають широкі можливості платформи SDN на базі контролера OneController, зокрема, підтримку відкритого й стандартизованого механізму групових політик, а також інтеграцію OpenDaylight із платформою уніфікованих комунікацій Microsoft Skype for Business.

Крім запитаного замовником функціонала, запропоноване рішення дозволяє реалізувати ряд додаткових SDN-додатків і сервісів, включаючи автоматизацію створення віртуальних мереж, графічний інтерфейс керування трафіком, інжиніринг трафіку для бізнес-додатків, роботу систем безпеки на терабітних швидкостях і ін. Динамічному впровадженню нових сервісів допоможе можливість гнучкого перенапрямку трафіку (вибіркових потоків) на різні компоненти мережної інфраструктури, такі як система аналітики й моніторингу додатків Purview, Captive-портали бездротових мереж Wi-Fi, системи запису IP-Телефонії. Крім того, Extreme пропонує «SDN для Wireless»: повна підтримка концепції SDN і інтеграції сторонніх додатків з бездротовими мережами Wi-Fi від Extreme Networks – IdentiFi (у тому числі пріоритизація трафіку VoIP, інтеграція з рішеннями MDM, BYOD).

HP

Компанія надіслала найдетальнішу відповідь, де була описана її загальна стратегія в частині SDN, представлений весь портфель продуктів SDN і, звичайно, деталізоване рішення конкретного завдання. Відповідно до пропозиції HP, ядро регіонального офісу складуть два модульних комутатори HP 5406R zl2, які забезпечать підключення комутаторів доступу (по 10G), а також комутаторів ЦОДу, граничних маршрутизаторів і опціонального Wi-Fi-контролера HP Aruba. Для рівня доступу – підключення кінцевих пристроїв (ПК, ноутбуків, телефонів, опціональних Wi-Fi-точок HP Aruba) – призначаються сім 48-портових комутаторів HP 3800 з підтримкою Po+, а для ЦОДу – підключення серверів і СХД (по 10Gb/FCo/iSCSI або 4/8G FC) – двох конвергентних комутатора HP 5900CP.

Для філій на базі HP проробили два варіанти. Перший передбачає установку стека із двох 48-портових комутаторів HP 2920, другий – двох модульних комутаторів HP 5406R zl2. У другому випадку в комутатори встановлюється сервісний модуль HP Advanced Services v2 zl Module із системою віртуалізації VMware vSphere, а локальний контролер SDN у вигляді віртуальної машини з ПЗ HP VAN SDN Controller інсталюється безпосередньо на цей модуль.

Для формування територіально розподіленої мережі запропоновано використовувати маршрутизатори HP MSR3044 (у регіональному офісі) і HP MSR3012 (у філіях). Вони забезпечують контроль доступу й фільтрацію трафіку на границі мережі за допомогою

убудованого міжмережного екрана. Для організації VPN-підключення рекомендована технологія HP ADVPN.

Відказостійкий кластер SDN-контролерів HP VAN SDN Controller у центрі HP запропонувала реалізувати на базі серверів HP ProLiant DL360/380 Gen9 – поверх ОС Linux (Ubuntu або RHEL) або на платформі віртуалізації VMware. Можна використовувати й сторонні сервери, однак у цьому випадку HP не може гарантувати заявлені характеристики продуктивності контролера SDN, які були протестовані на серверах HP ProLiant. Кластер контролерів забезпечить резервне керування SDN-інфраструктурою філій у випадку відмови локальних контролерів у філії.

У якості основних HP запропонувала три SDN-додатки: HP Network Protector забезпечує безпека в локальній мережі; HP Network Optimizer – керування QoS у ЛОМ; HP Network Visualizer – моніторинг і діагностику ЛОМ. Крім перерахованих, можна використовувати додаткові додатки з HP SDN App Store.

HUAWEI

Ядром мережі регіонального офісу замовника, за задумом архітекторів Huawei, повинен стати модульний комутатор S7706 із установленими інтерфейсними платами з портами 10 Гбіт/с (для підключення серверів і комутаторів доступу) і 1 Гбіт/с (для підключення робочих місць). Для рівня доступу запропоновані комутатори S 5700-X-LI. Мережі філій будуть будуватися на базі комутаторів S 5720-HI.

Важливим програмним компонентом рішення є Super Virtual Fabric (SVF). SVF – це технологія віртуалізації мережної інфраструктури й уніфікованого керування мережними елементами, користувачами й додатками. Завдяки SVF мережна інфраструктура буде представлена у вигляді єдиного віртуального комутатора із централізованим керуванням конфігураціями, QoS, правилами контролю доступу й автентифікацією користувачів (причому як для головного офісу, так і філій). Крім провідної інфраструктури, SVF дозволяє віртуалізувати і бездротову мережу, при цьому обробка трафіку й автентифікація будуть вироблятися відповідно до загальних правил. Комутатор S7706 виступає в якості головного керуючого комутатора SVF-Parent, а комутатори S 5700-X-LI і S 5720-HI – у якості керованих SVF-Client, тому для останніх не потрібні індивідуальні конфігурація й керування.

Для підключення до територіально розподіленої мережі, побудови тунелів і шифрування трафіку, забезпечення безпеки й надання голосових сервісів у регіональному офісі встановлюються маршрутизатори AR2240, а у філіях – AR1220E. Найближчим часом, відповідно до концепції Agile Branch, маршрутизаторами віддалених офісів також стане можливо управляти із централізованого контролера (споконвічно заявлена робота через контролер Open Daylight, поряд із власним), так що їх не потрібно буде конфігурувати окремо.

Розробляючи свій контролер SDN, Huawei передбачила підтримку кластеризації й модульну структуру ПЗ для забезпечення відказостійкості й високої доступності. Agile Controller має ієрархічну структуру з декількома компонентами (Management Center (MC), Service Manager (SM), Service Controller (SC)) плюс зовнішні бази даних. Кожний з компонентів може бути зарезервований, а розподілений дизайн дозволяє розмістити частина компонентів безпосередньо у філіях.

Крім забезпечення запитаних замовником базових функцій, Huawei запропонувала ряд додаткових можливостей. Так, завдяки функції Free Mobility користувач одержить єдині політики безпеки, обслуговування й виділення ресурсів, а також сервісні політики, тобто обслуговування буде однаковим поза залежністю від місця, часу, типу термінала або порту доступу. А технологія iPCA дозволить забезпечити наскрізний контроль якості на реальних потоках трафіку й визначити оптимальні шляхи передачі трафіку.

NEC

Для побудови запропонованого SDN-рішення, на базі NEC пропонується платформу NEC ProgrammableFlow, що включає контролер NEC PF6800 і лінійку комутаторів P-Flow. Відказостійкий контролер PF6800 являє собою ПЗ, що виконується на кластері, що

організований на базі двох окремих фізичних серверів або віртуальних машин. Як відзначають в NEC, її платформа SDN інтегрована з відкритими платформами SDN/NFV, що розвиваються в рамках проектів OpenStack і OpenDayLight.

Для побудови мережі SDN під управлінням контролера NEC PF6800 можуть використовуватися комутатори NEC або інших виробників, що відповідають стандартам OpenFlow 1.0 і/або OpenFlow 1.3 (для побудови комерційних рішень фахівці NEC рекомендують комутатори з підтримкою OpenFlow 1.3). У лінійку комутаторів NEC P-Flow входять пристрою серій PF52xx, PF53xx і PF54xx різній ємності й продуктивності. Крім того, слід зазначити, що NEC регулярно проводить тестування свого контролера на сумісність із комутаторами інших виробників.

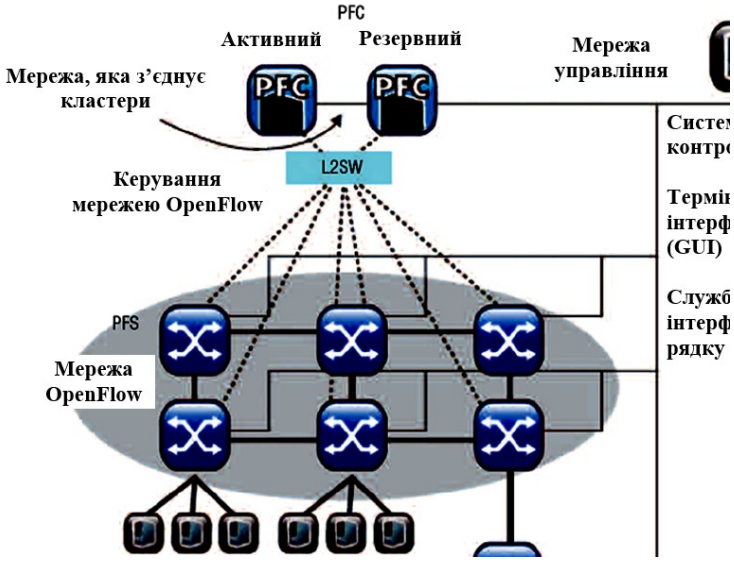

Рисунок 1 – Структурна схема системи

Основою запропонованого SDN-рішення, на базі NEC, є віртуалізація мережі VTN: у хмарі комутаторів OpenFlow створюється безліч незалежних мереж L2/L3 IPv4/IPv6, робота яких підтримується автоматично при змінах у фізичній мережі. Користувач може створювати VTN, динамічно змінювати конфігурацію VTN у процесі експлуатації й застосовувати мережні політики незалежно від інших VTN. При цьому для створення своїх VTN він може як скористатися пулом мережних ресурсів, пропонованих оператором мережі SDN і вже інтегрованих з контролером SDN, так і задіяти свої унікальні фізичні пристрої або віртуалізованні (VNF) компоненти.

Серед переваг запропонованого SDN-рішення, на базі NEC є підвищення продуктивності мережі (стабільна робота забезпечується навіть при 100-процентному завантаженні каналів), можливість перебудови фізичної мережі без переривання обслуговування у віртуальних мережах, підвищення безпеки за рахунок повної ізоляції віртуальних мереж другові від друга, збільшення надійності мережі завдяки самовідновленню й автоматичному перерозподілу потоків трафіку відповідно до правил. Ефектної й одночасно ефективної є візуалізація трафіку у фізичній і логічній мережах, що дозволяє спростити експлуатацію, прискорити виявлення й усунення несправностей, спростити моніторинг SLA.

Міграція (гібридні мережі)

Жоден постачальник не пропонує одним махом замінити традиційну мережу на інфраструктуру SDN. Усі підготували сценарії поступової міграції й/або побудови гібридний мереж.

Впровадження SDN не вимагає повної заміни існуючої IP-інфраструктури, а більшість переваг SDN стають доступні при повній або навіть частковій заміні ядра мережі або рівня агрегації. Запропоноване NEC рішення SDN може інтегруватися з IP-мережами на рівнях L2

(MCLAG) і L3 (VRRP/HSRP). При цьому один сегмент SDN може мати кілька підключень рівня L2 і/або L3 до мереж IP, і для всіх підключень може використовуватися єдиний пул мережних сервісів (MCE, балансувальник, DPI, Proxy і ін.), що значно спрощує завдання адміністрування. Для інтеграції декількох сегментів SDN фахівець NEC рекомендує організувати L2 VPN в існуючих мережах передачі даних.

Як зазначено у компанії Huawei, негайний перехід до SDN може привести до втрати інвестицій, частина наявних функцій може бути втрачена або істотно спрощена (наприклад, функції балансувальника або оптимізатора трафіку). Тому її комутатори Agile надають можливість саме міграції на SDN, а не радикального переходу до цієї технології. Вони здатні паралельно підтримувати два режими роботи: традиційна комутація/маршрутизація й SDN.

Фахівці Huawei особливо відзначають те, що в її комутаторах Agile використовуються мережні процесори власної розробки (Ethernet Network Processor, ENP). Традиційні ASIC обробляють дані тільки визначених протоколів, а впровадження нових сервісів (наприклад, з нестандартною інкапсуляцією) тягне апаратні зміни (редизайн мікросхем). На відміну від ASIC, процесори ENP повністю програмувальні, тому замовники можуть уже зараз почати фрагментарно впроваджувати «готові до SDN» пристрою в існуючу інфраструктуру й надалі, просто обновивши прошивання, підтримувати майбутні нові протоколи й сервіси.

По даним Cisco, у випадку вибору її рішення інтеграція із традиційною мережею здійснюється прозоро й без застосування яких-небудь додаткових технологій. Підключення до існуючої мережі рекомендується робити через два опорних маршрутизатори Cisco ISR 4451, розташованих у центральному офісі. Незважаючи на те що ці маршрутизатори перебувають під контролем APIC-EM, для взаємодії із традиційною частиною мережі використовуються стандартні механізми – протоколи канального рівня (залежно від типу ліній зв'язку) і протоколи комутації/маршрутизації відповідно до корпоративного стандарту.

У рішенні HP для реалізації гібридної інфраструктури SDN використовується стандартна функціональність протоколу OpenFlow, а саме інструкції NORMAL і FLOOD, які дозволяють після аналізу трафіку в таблицях OpenFlow на мережному пристрої передати його для наступної обробки в традиційний мережний стек протоколів, настроєних на цьому ж пристрої.

У цілому, завдяки гібридній архітектурі, можна поетапно впроваджувати рішення SDN в існуючих мережах, при цьому дані рішення будуть тісно інтегруватися й взаємодіяти з устаткуванням, що не підтримує SDN і протокол OpenFlow. Це, зокрема, дозволяє використовувати переваги, які надають SDN-додатка, без необхідності повної заміни всього устаткування в мережі.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів побудови мережі на основі технології SDN.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем побудови мережі на основі технології SDN.

– Досліджена система побудови мережі на основі технології SDN.

– На основі отриманих результатів досліджень створена програмна реалізація системи побудови мережі на основі технології SDN.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання побудови мережі на основі технології SDN. 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. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of

Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.