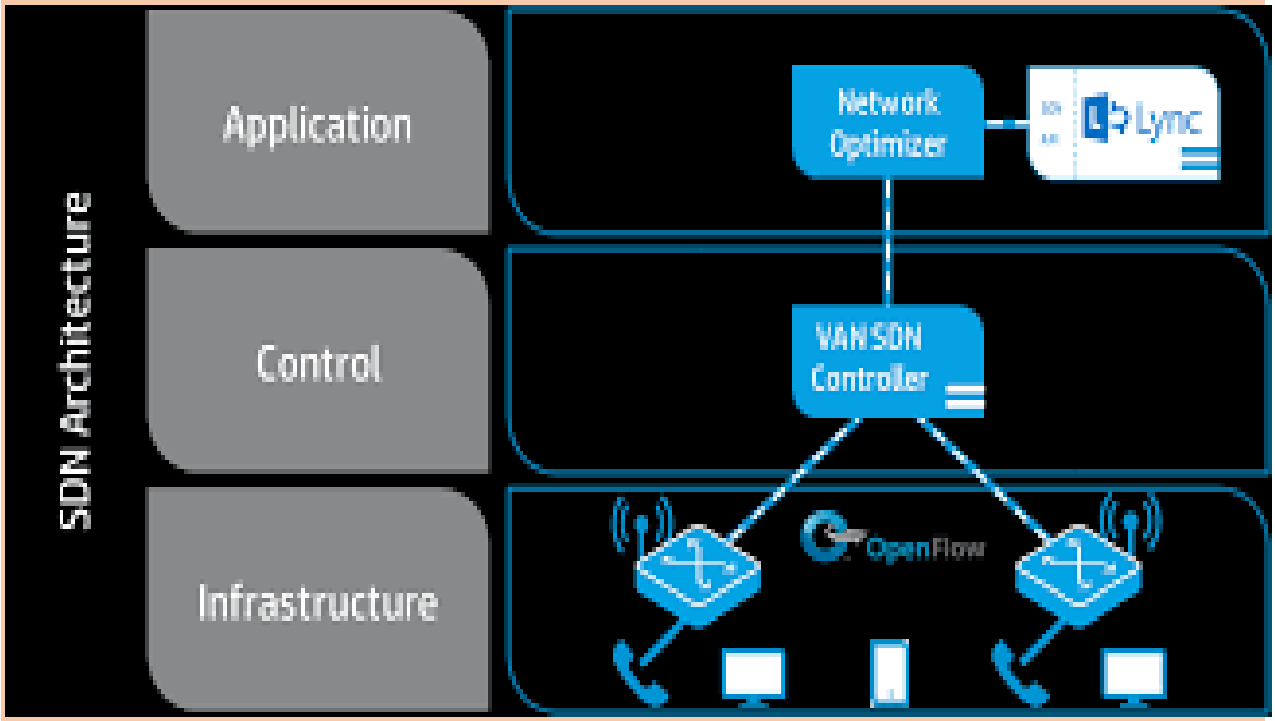
Міністерство освіти і науки України
Державний університет телекомунікацій

Гніденко М.П., Вишнівськтй В.В., Ільїн О.О.

Побудова SDN мереж

Навчальний посібник



Київ – 2019

Міністерство освіти і науки України
Державний університет телекомунікацій

Гніденко М.П., Вишнівський В.В., Ільїн О.О.

Побудова SDN мереж

Навчальний посібник

Київ – 2019

УДК 004.7(075)

Гриф надано Державним університетом телекомунікацій

Рецензенти: **Левківський К.М.,** кандидат технічних наук, доцент, головний спеціаліст Інституту модернізації змісту освіти.
Приходько Ю.І., кандидат технічних наук, доцент, головний науковий співробітник Науково-методичного центру Національного університета оборони України

Гніденко М.П., Вишнівський В.В., Ільїн О.О.
Побудова SDN мереж. – Навчальний посібник. – Київ: ДУТ, 2019. – 190 с.

У навчальному посібнику системно викладено теоретико-методичні та практичні аспекти побудови программно-конфігуровних мереж SDN (Software-Defined Networks). Значна увага приділяється розгляду порядку розгортання, налаштування та використання основних елементів мереж SDN: контролера HP VAN SDN,

Навчальний посібник призначено для студентоа, аспірантів і викладачів, які планують підготуватися до міжнародної сертифікації рівня HP Accredited Technical Associate (HP ATA) – Creating HPE Software-defined Networks.

Зміст

Введення

У зв'язку з постійним розвитком інформаційних технологій і появою нових технологій (таких як хмарні обчислення та Big Data), вимоги до комп'ютерних мереж зростають, а реалізація ускладнюється. Мережі потребують більшої швидкості передачі даних та вдосконалення інструментів, що використовуються для мережевого управління і моніторингу. Така ситуація призводить до появи нових функціональних і технологічних мереж, з ускладненою інфроструктурою. Старі методи моніторингу і управління не відповідають новим вимогам.

Тому останнім часом зростає популярність программно-конфігуровних мереж SDN (Software-Defined Networks). Самій ідеї мереж SDN вже більше десяти років, але в останні декілька років відомі компанії пропонують нові реалізації, які відкривають більше можливостей. Одною з найпопулярніших є організація мережі SDN зі спільним застосуванням протоколу OpenFlow.

Головна перевага представленої технології в тому, що вона працює окремо від мережевих пристроїв і її контроль може здійснюватися операторами за допомогою стандартного сервера.

Головна мета SDN є відокремлення рівня додатків від рівня управління і рівня управління від рівня передачі даних. Таким чином, можна значно спростити сладність фізичних пристроїв, оскільки виконування логічних функції повністю переноситься на вищий рівень. Це не тільки здешевлює фізичні пристрої, а й покращує надійність і спрощує управління мережі в цілому. Тепер, замість маршрутизаторів можна використовувати звичайні комутатори. Для адміністратора мережі буде значно легше контролювати мережу в цілому. Також, це дозволяє абстрагуватися від реалізації кожного конкретного пристрою, оскільки рівень управління зв'язується з рівнем даних через стандартний інтерфейс. А це, в свою чергу, значно спрощує взаємодію між пристроями різних виробників, і зменшує час налаштування і підготовки або ремонту всієї мережі.

Окрім того, така побудова мережі значно прискорює створення нових мережевих додатків. Оскільки для взаємодії рівнів додатків і управління також використовується стандартний інтерфейс, програмісту більше не потрібно думати про те, яким саме чином можна передавати команди і запити до мережі. Головне реалізувати основний функціонал додатку, а додаток буде взаємодіяти з рівнем контролю через попередньо виділені інтерфейси.

Навчальний посібник пропонує матеріал по программно-конфігуровних мережам SDN (Software-Defined Networks) як з точки зору теоретичних основ мережевих технологій і мережевого устаткування, так і практичних рекомедацій по їх використанню. Такий підхід може бути корисний як початківців освоювати новий вид діяльности, так і фахівцям, яким необхідно освіжити знання і підвищити кваліфікацію.

Розділ І. Введення до програмно-визначених мереж (SDN)

SDN стала популярною темою на мережевих веб-сайтах та в різних журналах. Ви не можете переглянути такі публікації без того, щоб не знайти принаймні декілька статей про SDN.

Крім того, розробники мережевих технологій (вендори) часто проводять веб-семінари, які присвячені SDN та перевагам, які вони можуть надати у майбутньому.

Як це часто буває з новими технологіями, вендори розходяться у поглядах на те, що таке SDN. Деякі із них зосереджуються лише на одному аспекті SDN, що не забезпечує бачення повної "великої картини" SDN.

Цей розділ вводить у світ SDN та надає пояснення, чому це необхідно і окреслює, наскільки принципово SDN змінює мережеві технології. У цьому розділі можна дізнаєтися, як SDN дозволяє різним організаціям швидше реагувати на зміни та забезпечення роботи мереж. Можна також побачити, як це дозволяє розробникам впроваджувати нові програмні додатки, дізнатися про рішення SDN, які впроваджує компанія HP.

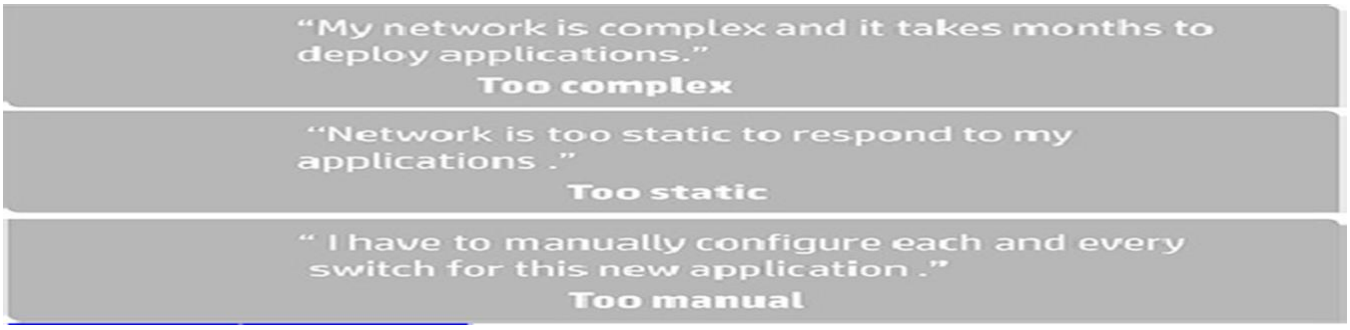
1.1 Основи Software-defined Networking (SDN) та OpenFlow

Архітектури серверів і та систем зберігання інформації були модернізовані, щоб йти в ногу з постійно зростаючими очікуваннями сучасного світу, але відносно мереж, які лежать в основі їх роботи, цього не відбулося.

Мережа Центрів обробки даних (ЦОД) , яка напевно збільшилася в обсязі і забезпечує значну більшу швидкодію, в основному залишилась побудованою таким же чином, як і протягом двох останніх десятиліть. Еволюція мереж кампусу була повільною, не дивлячись на революцію мобільності.

Як на рівні Центру обробки даних (ЦОД) так і на рівні кампусу, коли застарілі мережі зазнають обмежень у своєму розвитку, вони поступово втрачають надійність, стають важкими в управлінні, вразливими та дорогими в обслуговуванні.

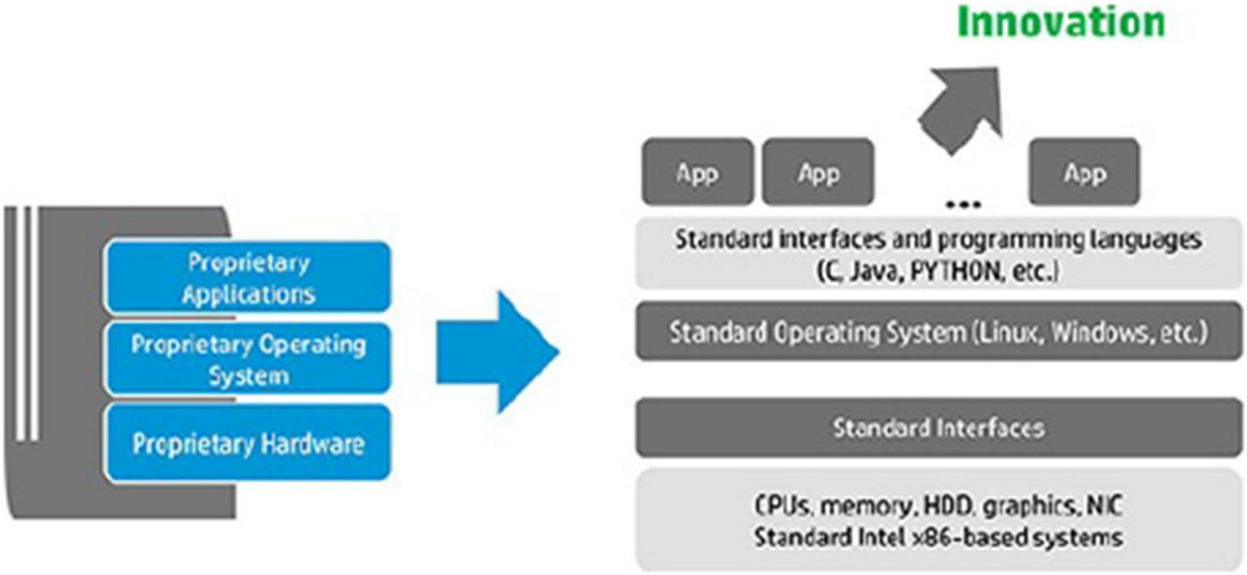
На малюнку показані деякі проблеми, з якими стикаються компанії при використанні цих мереж.



Ручна конфігурація та керування мережами просто не дають можливості наблизитись до вимог сучасних програм, користувачів та бізнесу. Бізнес підприємства, чиї мережі залишаються на тому ж рівні розвитку, ризикують втратити наступну хвилю можливостей. Застарілі мережі не можуть забезпечити вимоги з боку хмарності, безпеки, мобільності та великих даних.

Лише SDN надає інтелектуальний, адаптований, програмований та централізований дизайн мережі. SDN легко керувати і воно йде в ногу з сучасними різноманітними зростаючими навантаженнями. HP SDN забезпечує програмування мережі, яка адаптується до програмних додатках в інтересах бізнеса та базується на основі відкритих стандартів. Для підримки, створений перший промисловий портал HP SDN App Store, який забезпечує ринок для SDN додатків і платформи для обміну інноваціями.

Перш ніж вийти за межі технічних деталей, слід розуміти тенденції розвитку галузі, які ведуть переходу до SDN, як показано на малюнку, на прикладі віртуалізації та інновації серверів.



У серверному средовищі такі технології віртуалізації, як VMware, зробили революцію в процесі розгортання та налаштування сервера. Адміністратори серверів більше не повинні витрачати багато днів, а то і тижнів на пошук фізичного сервера, використовуючи компакт-диски або DVD-диски для встановлення операційних систем, завантаження драйверів та встановлення різних програмних компонентів, таких як Exchange або SQL-сервер. Вони можуть просто підготувати сервер за лічені хвилини або секунди за допомогою віртуальних машин VMware.

Такого роду швидкі інновації та швидке розгортання все ще відсутні в мережах сьогодні. Мережеві адміністратори часто все ще налаштовують мережі трудомістким способом за допомогою CLI. Інтерфейс CLI використовується для налаштування VLAN, маршрутизації, IP-адресацію і реалізації політики розгортання. Опції керування, такі як протокол SNMP, допомагають в управлінні мережею, але це ще один спосіб налаштування

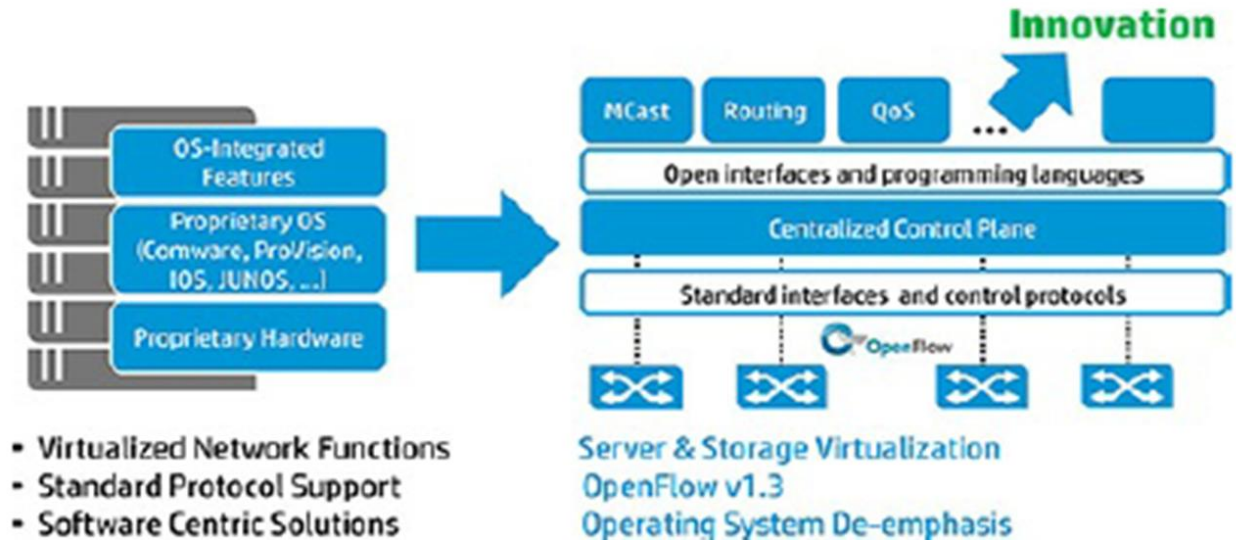
локалізованої контрольної панелі на кожному пристрої, а не зміна способу роботи з мережею.

Серверне середовище піддається все більшій абстракції за допомогою віртуальних серверів. Використання віртуальних серверів дозволяє адміністратору системи здійснювати їх розгортання протягом хвилин і навіть секунд. Крім цього, вони можуть легко переміщати віртуальні сервери з одного фізичного хосту до іншого, використовуючи таку технологію як VMware vMotion.

Віртуальний сервер також може бути переміщений динамічно, на основі використання ресурсів. Тобто, якщо віртуальний сервер потребує більше ресурсів або ресурси на певному сервері перевантажуються, віртуальний сервер автоматично переміщується на серверне обладнання, що має доступні ресурси.

Накопичувач (storage) має аналогічну еволюцію: накопичувач більше не залежить від фізичних дисків на кожному окремому сервері. Накопичувач абстрагується логічним сховищем та компонентами фізичного зберігання. Для забезпечення швидкого і надійного зберігання інформації для обчислень та обробки даних диски тепер розміщені в масивах накопичувачів. Системні адміністратори отримують доступ до логічного сховища незалежно від фізичної структури накопичувача.

Для серверів та накопичувачів, абстракція забезпечила гнучкість і оперативність та відкрила двері для інновацій. На малюнку показано, яким чином замовники мігрують від патентованого (пропрієтарного) обладнання до віртуалізованих систем.



Розмірковуючи про сьогоднішню мережу, необхідно пам'ятати, що сталося на ринку серверів та накопичувачів. Ми починаємо бачити, що подібні типи впливу та інновації виходять і на мережевий ринок. Часто відбувається обговорення того, як швидко або як повільно буде впроваджена SDN. При цьому необхідно пам'ятати, що впровадження технологій віртуалізації можна було спостерігати декілька разів - один раз із серверами і знову з накопичувачами. Тобто, це вже знайома концепція.

А зараз будуть наведені крайні приклади віртуалізованих мереж, що ілюструють бачення SDN.

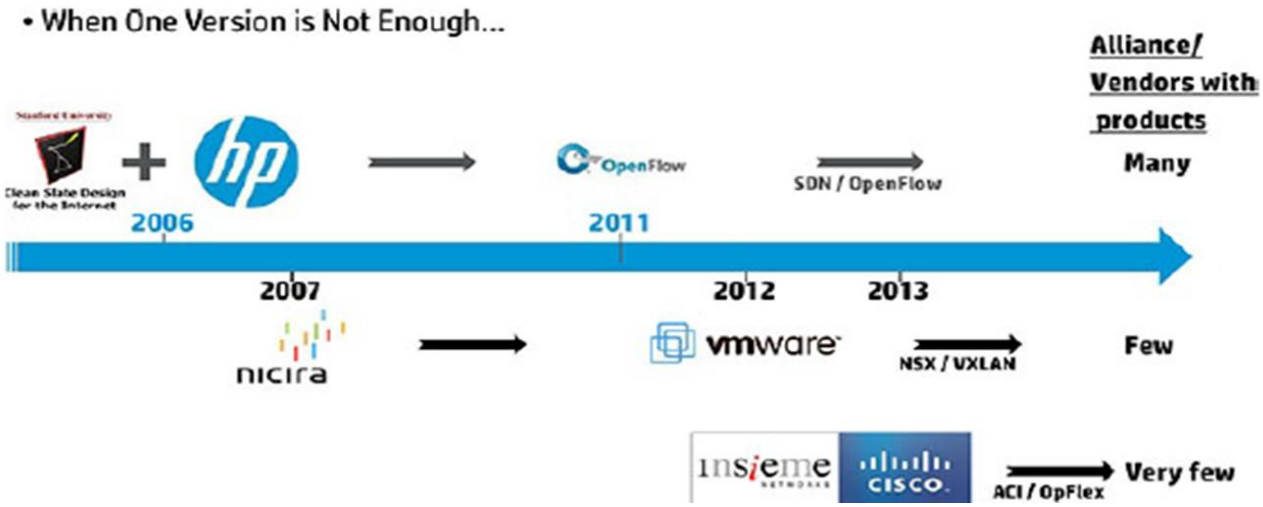
Замість того, щоб зосередитись на операційних системах, таких як Comware, ProVision або IOS, а потім порівняти характеристики та функціональність кожної операційної системи, SDN перекреслює операційну систему і зосереджується на розширенні можливостей мережевих пристроїв за допомогою програмного забезпечення.

Це програмне забезпечення може працювати на платформі x86, написаній на Java, Python або на безлічі інших мов. Функції можуть бути додані до мережевого пристрою програмним шляхом через відкриті API, такі як OpenFlow та інші.

SDN змінює парадигму:

- Відсутня необхідність вкладати якомога більше можливостей в операційну систему, яка працює тільки на конкретному апаратному забезпеченні (ASICS) і має додатковий ризик того, що операційна система та обладнання стануть застарілими протягом кількох років;
- Необхідно покращувати мережеві функції, додаючи їх на зовнішні сервери, а потім програмно розширюючи набори функцій мережевих пристроїв.

Важливо визначити, що SDN представляє собою насправді, оскільки існують конкуруючі точки зору. Є конкуруючі точки зору та визначення, деякі з яких є відкритими стандартами, а деякі - власними. На малюнку відображені ці стандарти.



Ще у 2005 році програма **Clean Slate** поставила запитання: якби ми почати будувати мережі заново - без будь-яких існуючих традиційних методів - як би ми їх будували?

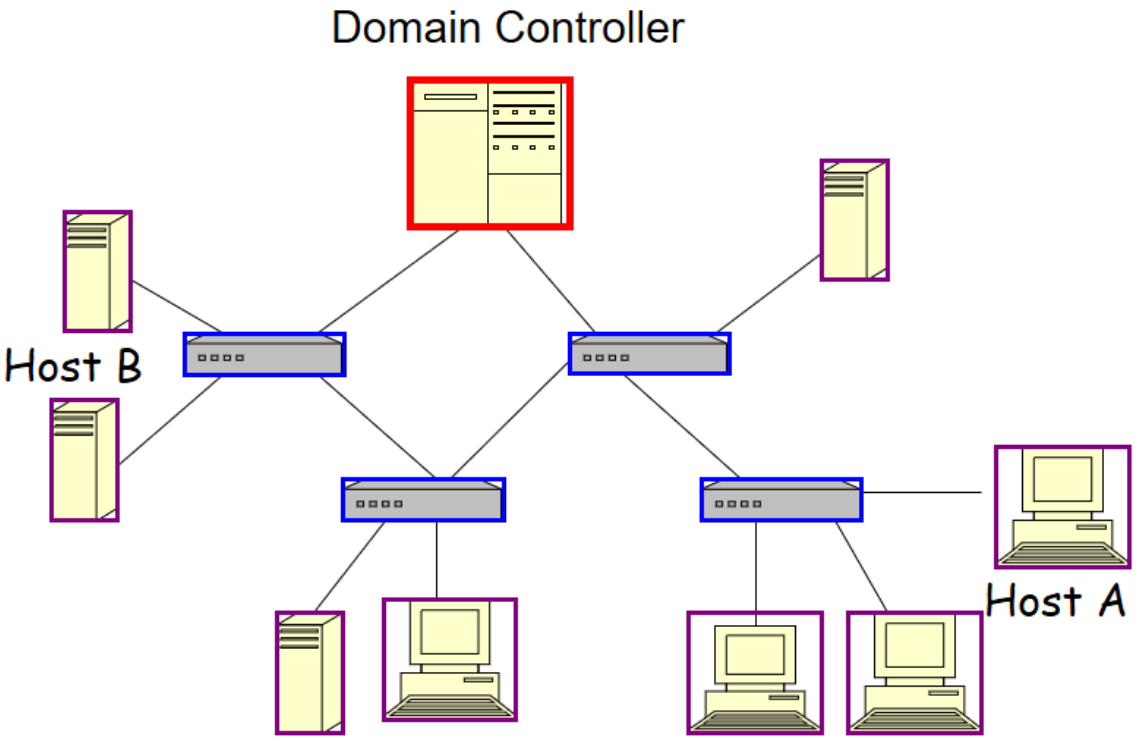
Відповідь, отримана програмою **Clean Slate**, полягає в тому, що повинна існувати система контролю та управління усім процесом. Тобто сама мережа повинна керуватися на рівні мережі (а не розподіленими конфігураціями пристроїв). Більше того, ця централізована система зможе розглядати всю мережу у цілому і приймати оптимальні, розумні та

передбачувані рішення про те, як трафік повинен пересилатися та маршрутизуватися по всій мережі.

Ця центральна система управління - так звана **"Ethane"** - використовує інформацію про політику та базу даних різної інформації (топології, реєстрації та прив'язки) для адміністрування правил щодо доступу до мережі окремими пристроями.

Таким чином, **"Ethane"** є свого роду рішенням контролю доступу до мережі (NAC). Це рішення було досягнуто без спеціального програмного забезпечення пристрою чи додатку - все це було зроблено простими пристроями, які виставляли свої "таблиці потоків" на центральний контролер.

У 2006 році HP та Стенфорд співпрацювали в рамках проекту **"Ethane".** Існував перехресний обмін ідеями між Стенфордськими дослідниками та HP, що дозволило зробити мережі більш програмованими. **"Ethane"** був попередником OpenFlow і він дозволив розробникам отримати доступ до логіки переадресації комутатора, а потім програмно змінювати поведінку переадресації.



Концепція заміни операційної системи комутатора програмним забезпеченням (контролером) виявилась потужною концепцією. Зважаючи на це, деякими Стенфордськими дослідниками була започаткована компанія під назвою Nicira. Метою їхньої компанії було створення програмованого комутатора у виді програмного забезпечення і який міг бути розгорнений на різних апаратних платформах, як то платформа x86.

Тим часом, Pothers в Стенфорді та інші вендори мережевих технологій працювали над OpenFlow і була створена галузева організація для подальшого розвитку OpenFlow. Вона має назву Open Networking Foundation (ONF) і в 2011 році OpenFlow версія 1.0 був випущений.

За цією активністю на ринку спостерігали з великою зацікавленістю багато інших вендорів. У той час на ринку з'явилося і деякі зрушення. VMware (також компанія з розробки програмного забезпечення) запропонувала компанії Nicira 1.26 мільярда доларів. Технологія Nicira отримала ребрендинг VMware NSX.

NSX реалізує версію SDN, де віртуальна мережа накладається (оверлейна мережа) на традиційну фізичну мережу, використовуючи тунелі Virtual Extensible LAN (VXLAN). Це дозволяє адміністратору сервера динамічно створювати віртуальні мережі між серверами ESXi, не вимагаючи від мережевих адміністраторів конфігурувати та дозволяти VLAN. VXLAN також підтримує 16 мільйонів VLAN у порівнянні з 4096 VLAN, які підтримується 802.1Q.

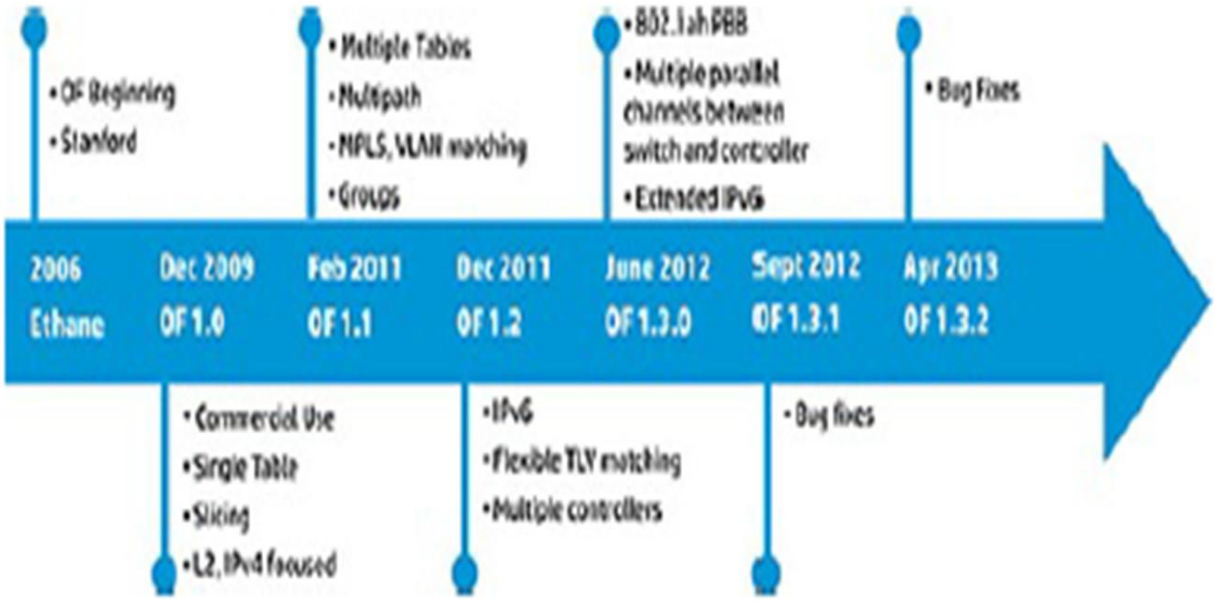
Стартап, що фінансується компанією Cisco, компанія Insieme, спочатку була окремою компанією, яка повністю фінансувалась компанією Cisco. Згодом ця компанія була повністю придбана Cisco в 2013 році.

Співробітники компанії Insieme мали великий досвід у сфері програмного забезпечення для ASIC (спеціальна прикладна інтегральна схема) та створенні програмованих масивів. Insieme вирішила зробити програмне забезпечення для SDN на ASIC.

Ця версія SDN - Application Centric Infrastructure (ACI) - в основному базується на апаратній платформі, розроблена на ASIC для реалізації SDN. Це стало товарною лінією Nexus 9000. Вона використовує власний протокол (OpFlex) замість OpenFlow.

ONF використовує протокол OpenFlow. VMware використовує VXLAN. Cisco використовує OpFlex.

За станом на 2013 рік VMware співпрацювала близько з 19 вендорами. Якщо ви вирішите використовувати NSX, ви обмежуєтесь лише приблизно 19 вендорами. При використанні технології Cisco у вас буде близько 40 вендорів, з якими Cisco підписала стратегічні договори про співробітництво. Якщо ви користуєтесь версією SDN від ONF, ви отримуєте підтримку більше 150 вендорів.

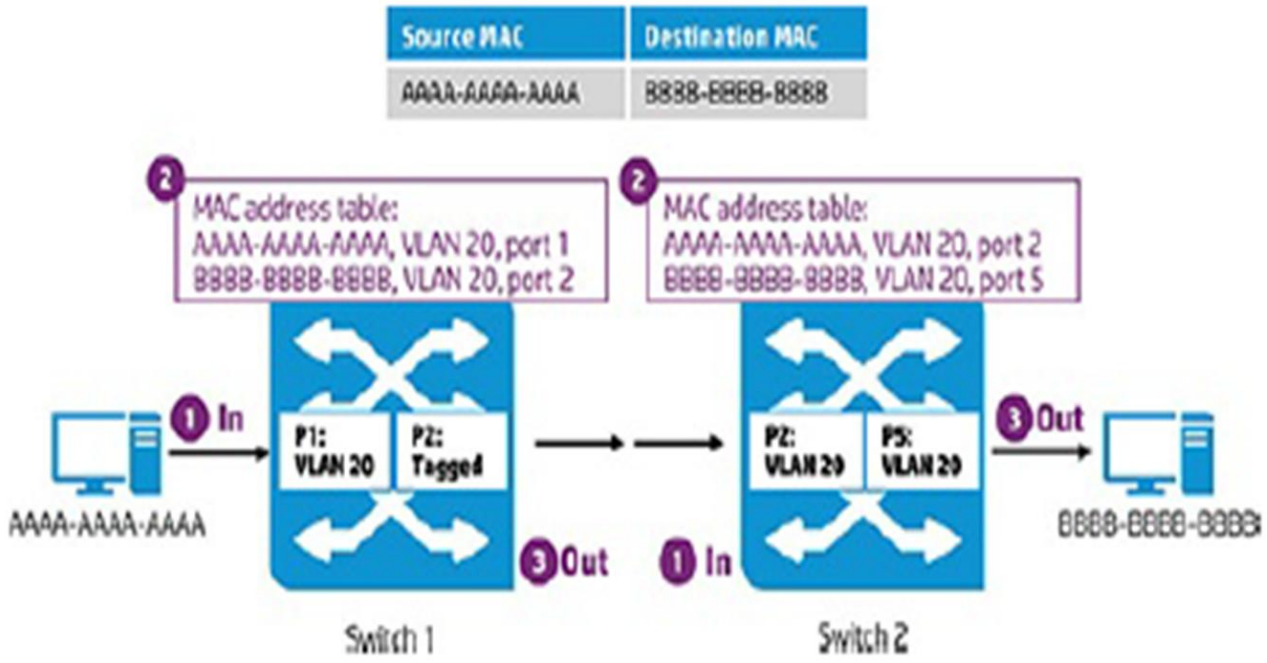


OpenFlow керується ONF. OpenFlow - це стандартний протокол, що підтримує площину централізованого керування в окремому пристрої (контролері).

OpenFlow здійснює апаратну абстракцію, забезпечуючи контролерові спосіб зв'язку з пристроями різних виробників та різноманітними апаратними типами (маршрутизаторами, комутаторами, балансирами навантаження тощо) та використовує стандартний інтерфейс.

Протокол реалізує логіку контролю за виконанням переадресації пакетів за допомогою правил пакетів та вкладає ці правила в апаратну абстракцію, де за ними може слідувати індивідуальний мережевий пристрій.

Традиційна маршрутизація здійснюється наступним чином, як показано на малюнку.



Основна обробка фреймів через мережу полягає в наступному:

1. Фрейм передається на Switch 1 від PC A (MAC = AAAA-AAAA-AAAA) для PC B (MAC = BBBB-BBBB-BBBB).
2. Таблиця MAC-адресів перевіряється на розташування PC B.
3. Адреса знаходиться в таблиці переадресації.
4. Фрейм передається на вихід через порт 2.

Цей процес повторюється при кожній комутації в мережі.

У середовищі OpenFlow пристрої перш за все використовують таблиці потоків (flow tables), а не таблиці маршрутизації або таблиці MAC-адресів. Іншими словами, комутатор має конвеєр OpenFlow для обробки пакетів, а не традиційний процес, що використовує традиційні механізми комутації та маршрутизації.

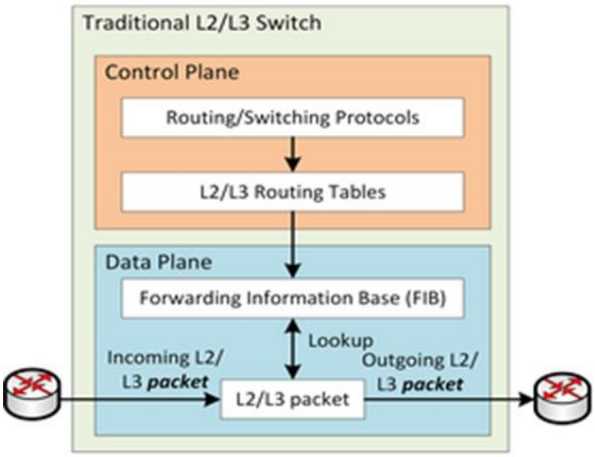


Figure 1 : Abstract view of traditional L2/L3 Switches

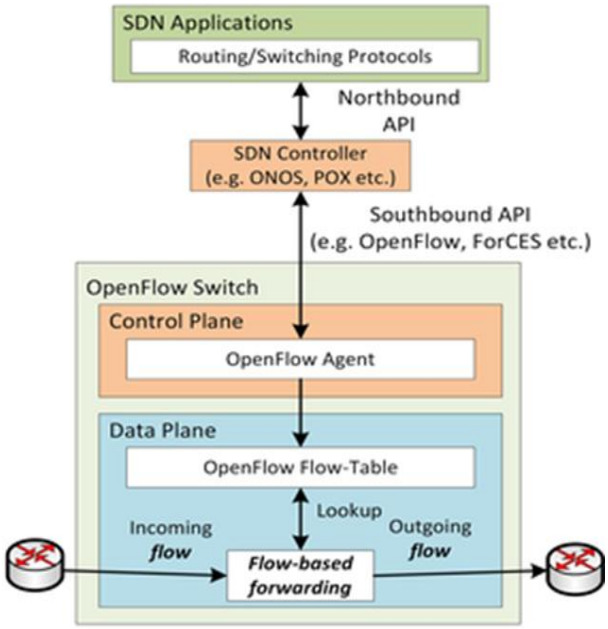


Figure 2 : Abstract view of an OpenFlow-enabled switch

Пристроєм OpenFlow може бути будь яке мережне обладнання, яке підтримує протокол OpenFlow, наприклад комутатор. Кожний пристрій підтримує Таблицю потоку (flow table), яка вказує на обробку, що застосовується до будь якого пакету певного потоку.

Протокол OpenFlow працює як інтерфейс між контролером та комутатором налаштовуючи таблицю потоку.

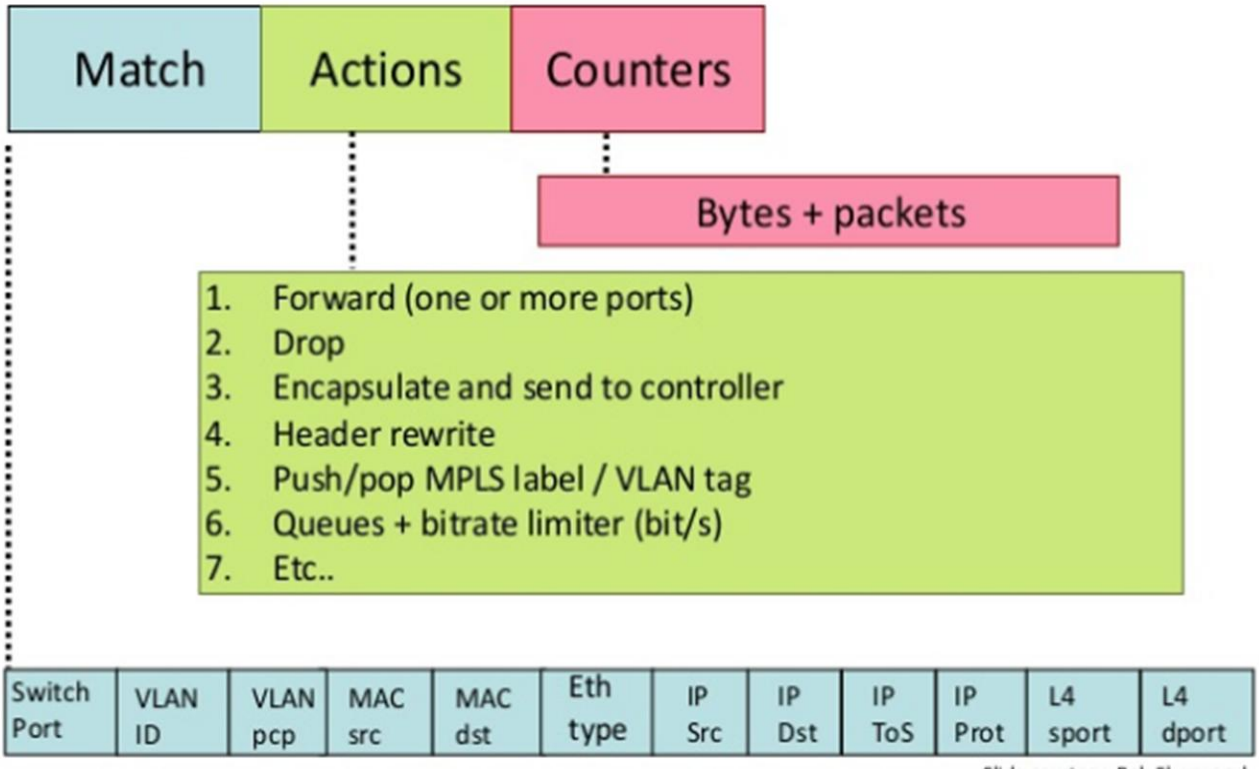
Таблиця потоку (flow Table) оновлюється додаванням або вилученням потокових записів (flow entries) використовуючи протокол OpenFlow. Таблиця потоку (flow table) містить деяку кількість потокових записів (flow entries), які асоціюються з діями для управління комутатором, який застосовує деякі дії (переадресація, відкидання або інкапсуляція) до певного потоку.

Потоковий запис в базовій таблиці потоку містить приймні три поля:

- Header field: використовується для визначення умов точного співпадання з потоком. Співпадання потоку базується на визначених критеріях співпадання (дивись малюнок нижче).
- Action (instruction): дії які визначають, яким чином пакет повинен бути оброблений.
- Counters (statistics) відслідковує кількість пакетів і байтів для кожного потоку (наприклад, 100 пакетів, 8000 байт). Час з моменту останнього співпадання потоку записується для видалення неактивних потоків. Це налаштовується в HP VAN SDN Controller.

Кожний потоковий запис (flow entry) містить певні дії (actions), які з ним асоціюються. Три дії, які повинні підтримуватися усіма виділеними комутаторами OpenFlow, є наступними:

- Forward
- Drop
- Redirect



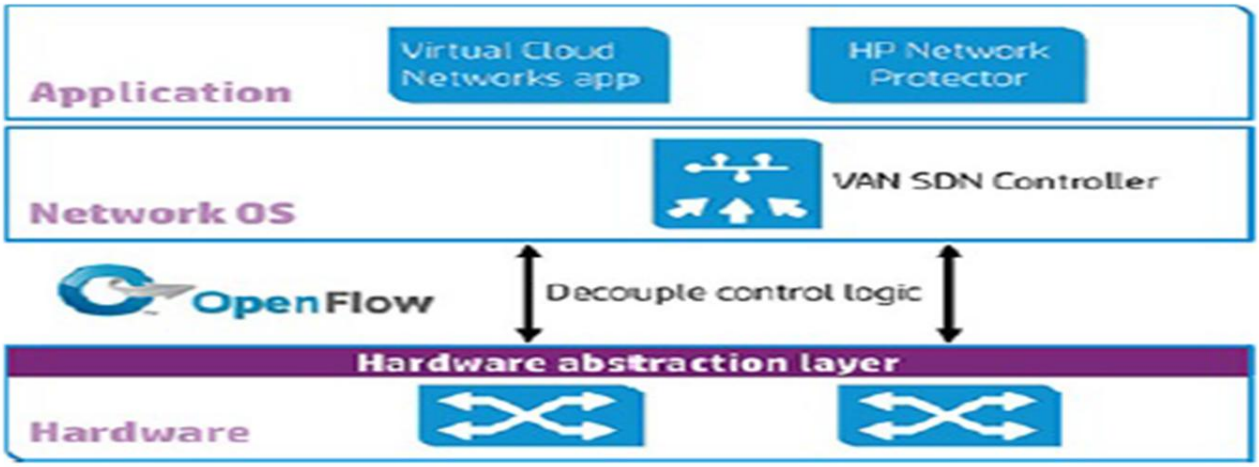
Forward: Перший варіант – переадресація (пересилка) пакетів потоку на заданий порт (або набір портів). Це дозволяє здійснювати комутацію пакетів через мережу. У більшості комутаторів пересилка відбувається зі швидкостями лінії.

Drop: Другий варіант – відкидання пакетів потоку. Це може бути використано з міркувань безпеки, за рахунок чого блокується несанкціонований трафік, зупиняються DOS атаки або зменшується зайвий широкомовний трафік з кінцевих хостів. Зупинка шкідливого трафіку реалізується за допомогою програмного додатку HP Network Protector.

Redirect: Третій варіант – інкапсуляція пакету та переадресація (пересилання) пакетів на контролер SDN. Контролер приймає рішення і пересилає пакет назад до комутатора. Як правило, цей метод використовується тільки для першого пакету нового потоку, завдяки чому контролер може вирішити, чи добавляти цей потік до таблиці потоку. З іншого боку, цей варіант може бути використаний для пересилки усіх пакетів на контролер для обробки, якщо програмний додаток вимагає цієї функціональності.

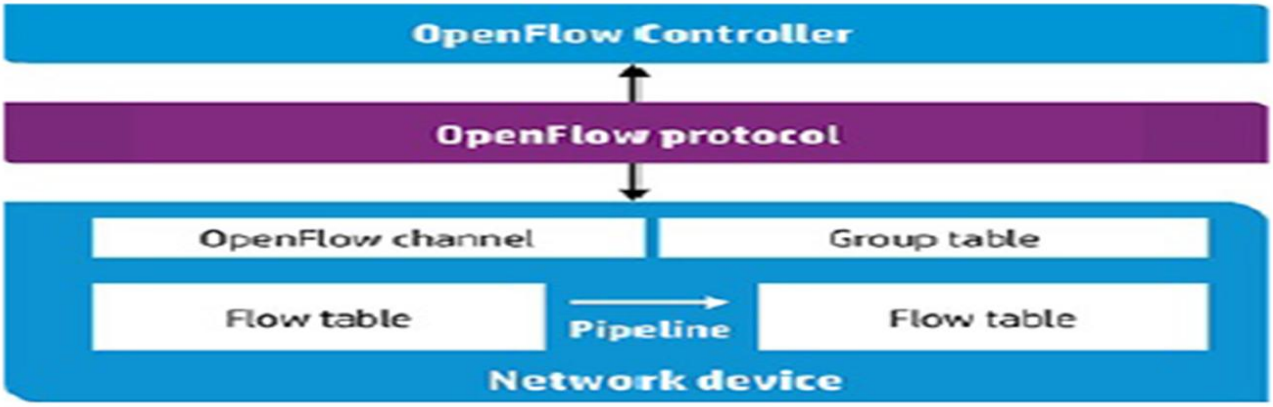
1.2 SDN абстрагує мережну інфраструктуру

Як показано на малюнку, SDN відділяє логіку управління від мережних пристроїв. Логіка пересилки пакетів та правила пакету переміщуються на окремий пристрій (контролер). Комутатори та інші пристрої здійснюють пересилку трафіку відповідно до інструкцій контролера.



Більшість первинних SDN пристроїв є маршрутизатори та комутатори. Однако OpenFlow та SDN здійснюють забезпечення для багатьох типів пристроїв, а не обмежуються лише маршрутизаторами та комутаторами. Інші пристрої, такі як балансири навантаження, брандмауери, пристрої оптимізації WAN зможуть підтримуватися SDN у майбутньому. Також, будь який мережний пристрій для переадресації, який може бути запрограмованим для виконання різних видів діяльності, може бути частиною SDN та OpenFlow у майбутньому.

Як показано на малюнку, комутатор OpenFlow складається із однієї або декількох таблиць потоку (flow tables) та групової таблиці (group table), які здійснюють пошук і пересилку пакету, а також каналу OpenFlow до зовнішнього контролера. Комутатор здійснює комунікацію з контролером, а контролер управляє комутатором через протокол OpenFlow.



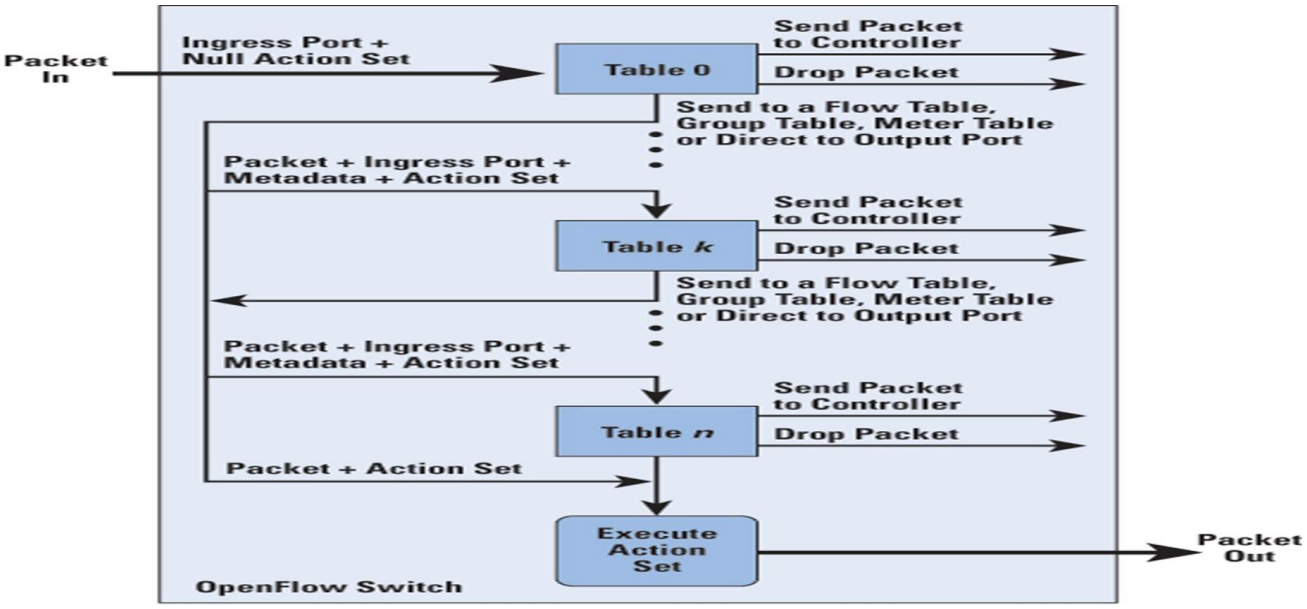
Протокол OpenFlow для захисту передачі використовує Transport Layer Security (TLS), який є попередником Secure Sockets Layer (SSL).

Використовуючи протокол OpenFlow, контролер може додавати, обновляти та видаляти потокові записи в таблиці потоків як реактивно (у відповідь на пакети) так і проактивно. Кожна таблиця потоку комутатора містить набір потокових записів; кожен потоковий запис місить поле співпадання (match fields), лічильники (counters) та набір інструкцій, які необхідно застосувати до співпадаючих пакетів.

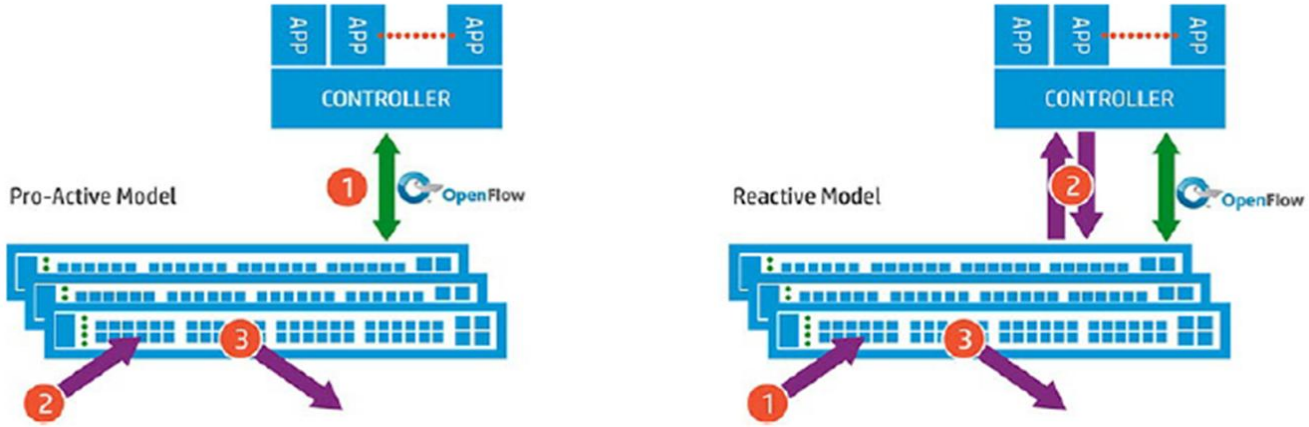
Процес перевірки співпадання розпочинається з першої таблиці потоку і може закінчитись на додаткових таблицях. Потокові записи співставляють пакети у пріоритетному порядку, з першим співпадаючим записом у кожній використаній таблиці.

Якщо знайдено співпадаючий запис, то виконується інструкції, які пов'язані з конкретним потоковим записом.

Якщо в таблиці потоку не знайдено жодного співпадання, то результат залежить від конфігурації потокового запису пропущеної таблиці (table-miss flow entry); наприклад, пакет може бути пересланим на контролер через канал OpenFlow, відкинутим, або може бути продовжена обробка у настуній таблиці потоку.



Як показано на малюнку, OpenFlow підтримує два методи вставлення потоку: проактивний і реактивний.



Реактивна вставка потоку відбувається тоді, коли пакет попадає на комутатор OpenFlow без співпадання потоку. Пакет відправляється контролеру, який його оцінює, додає відповідні потоки і дозволяє комутатору продовжувати переадресацію.

Альтернативно, потоки можуть бути вставлені контролером до комутатора проактивно, до прибуття пакетів.

Не треба забувати, що HP VAN SDN Controller та HP комутатори підтримують гібридний режим. Установки гібридного режиму визначають, які рішення про переадресацію пакетів виконуються керованими комутаторами OpenFlow і які з цих рішень контролер виконує самостійно.

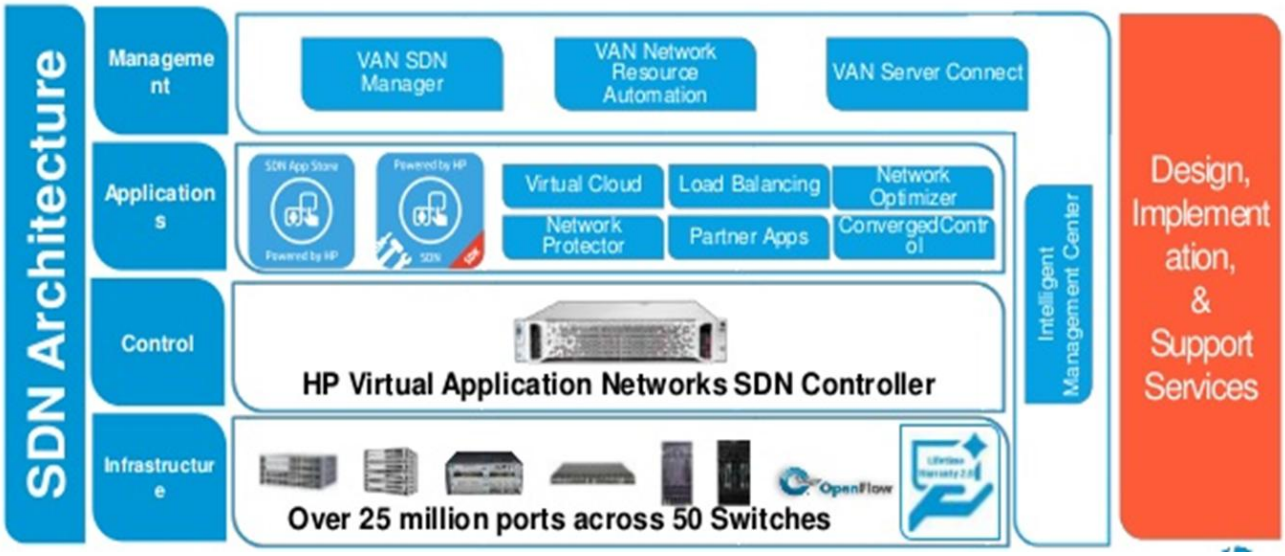
Якщо ввімкнено гібридний режим (за замовчуванням), контролер делегує нормальну переадресацію пакетів до керованих комутаторів, але перекриває ці комутатори для прийняття нестандартних рішень про переадресацію пакетів встановленними програмними додатками для певних типів пакетів. У цьому режимі контролер спирається на керовані комутатори, щоб усунути петлі та визначати шляхи пересилання за допомогою традиційних мережевих механізмів (таких як протокол Spanning Tree Protocol [STP] або протокол Open Shortest Path First [OSPF]).

Якщо гібридний режим відключений, контролер приймає рішення про пересилання для всіх пакетів у мережі, керованої OpenFlow. У цьому стані контролер усуває мережеві петлі та визначає шляхи переадресації.

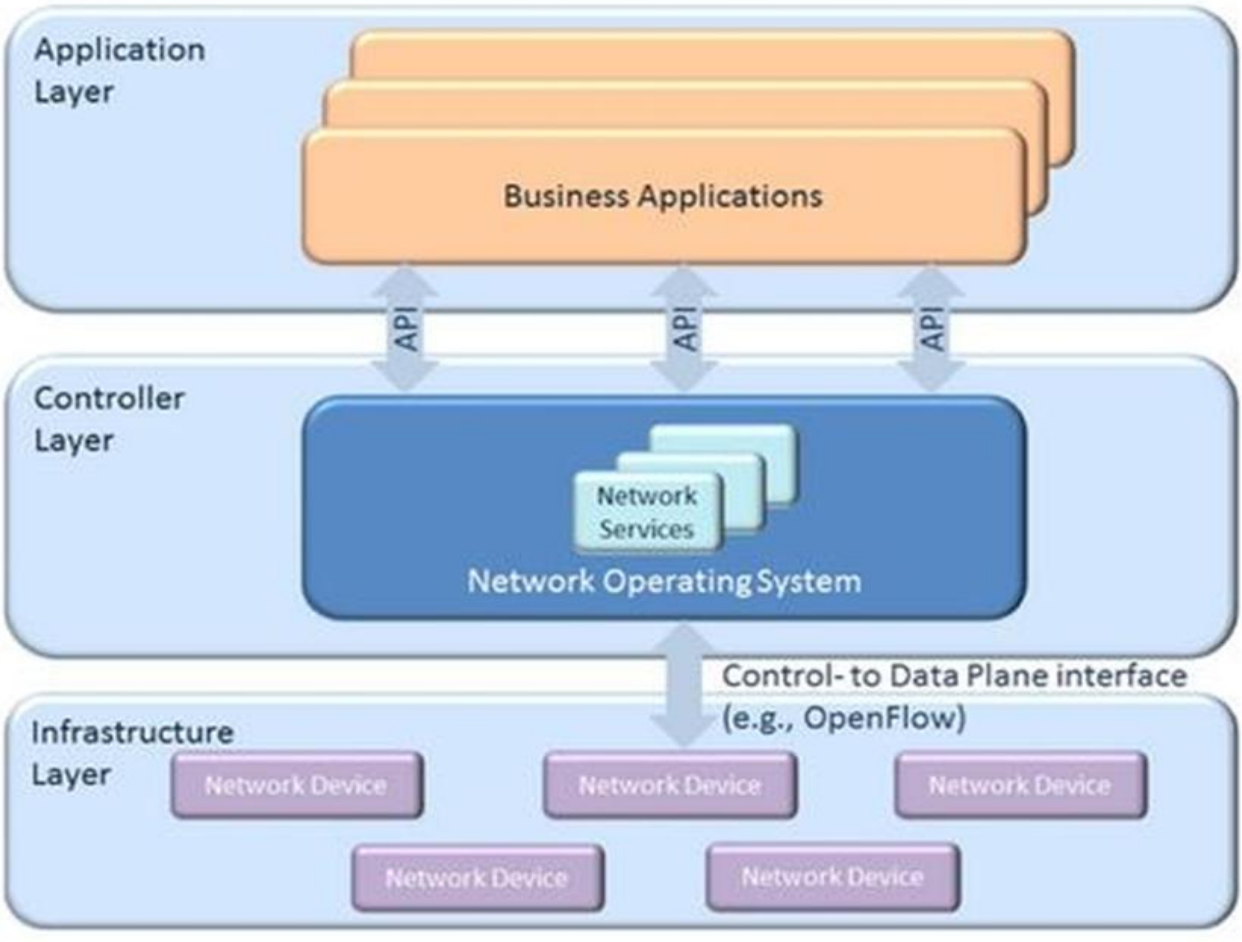
HP надає SDN рішення для автоматизації мереж різного рівня - від центру обробки даних до кампусу та філії. Розширюючи інновації SDN, екосистема HP SDN забезпечує ресурси для розробки та створення ринку для додатків SDN. Екосистема HP SDN забезпечує такі переваги:

- Simple: Розширення простоти програмування мережі за допомогою пристроїв з підтримкою OpenFlow.
- Open: Підвищення цінності SDN з відкритим середовищем, що поставляється SDN Software Development Kit (SDK).
- Enterprise ready: Сприяння інноваціям зі створенням першого ринку SDN App Store для програм SDN.

На малюнку показано архітектуру SDN та рішення, які забезпечує HP на основі цієї архітектури.



На рівні Інфраструктури HP спростила можливість переходу до архітектури SDN, надаючи підтримку OpenFlow більше ніж 50 існуючих моделей комутаторів.



Software-Defined Network Architecture: Image Courtesy of the Open Networking Foundation

Оскільки HP збільшує підтримку OpenFlow для програмного забезпечення існуючих комутаторів, вам не доведеться чекати, поки HP випустить нове обладнання, а потім замінить всю вашу існуючу мережеву інфраструктуру.

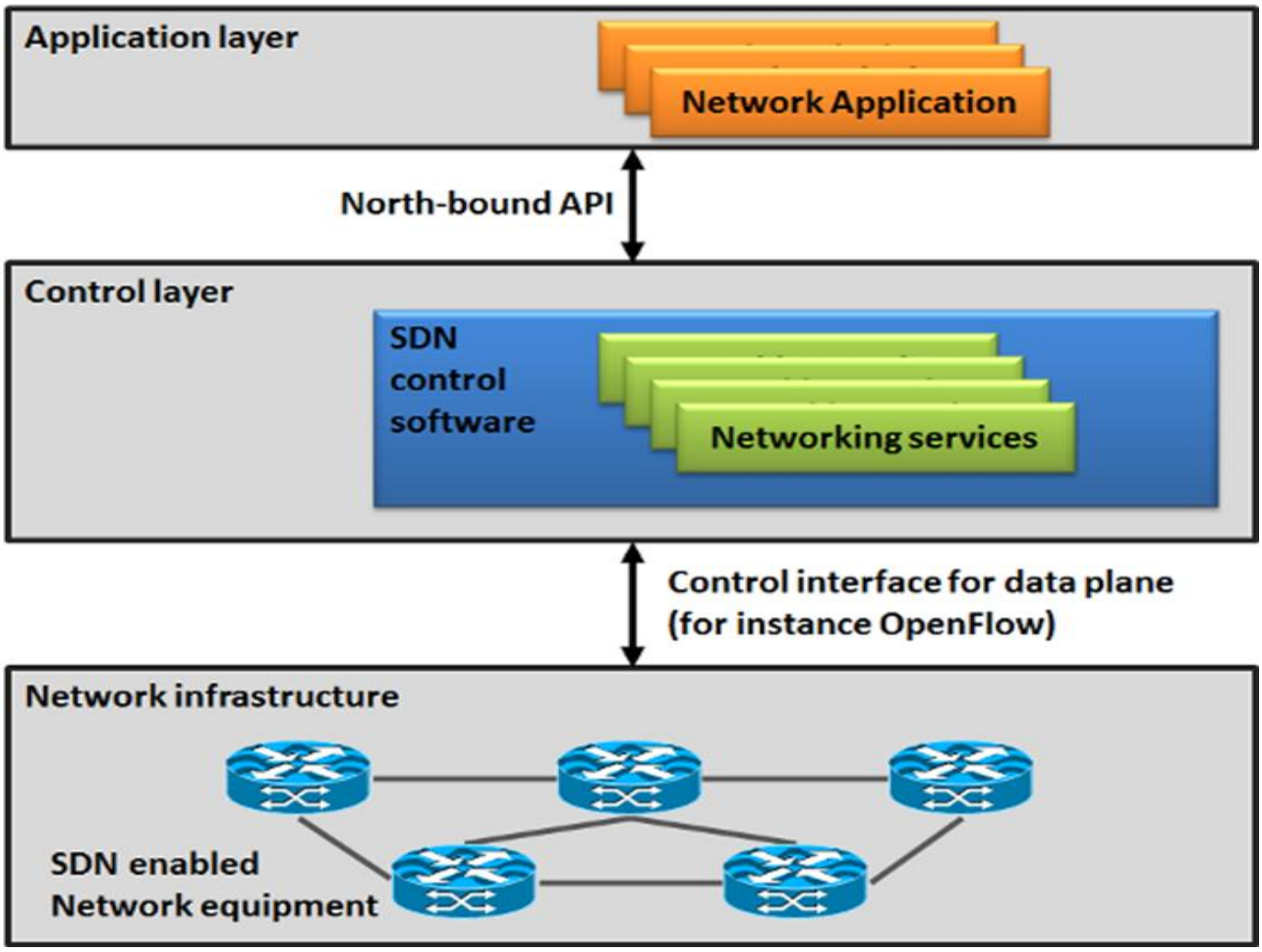
Якщо ваша мережа вже включає ці комутатори, ви можете просто оновити програмне забезпечення для комутаторів. Оскільки SDN Controller побудований за відкритими стандартами, він буде працювати з пристроями інших постачальників, які реалізують специфікацію OpenFlow (наприклад, Open vSwitch).

Рішення HP SDN підтримує гібридні комутатори, які працюють в гібридному режимі. Це дозволяє вам керувати міграцією до SDN, не порушуючи існуючих операцій мережі.

HP також може забезпечити з'єднання із безпроводовими точками доступу (wireless Aps), які підримують OpenFlow.

HP Virtual Services Routers (VSR) та HP Multi-Service Routers (MSR) також підтримують OpenFlow. Існує більше ніж 10 моделей, включаючи маршрутизатори серії HP MSR 2000, 3000 та 4000.

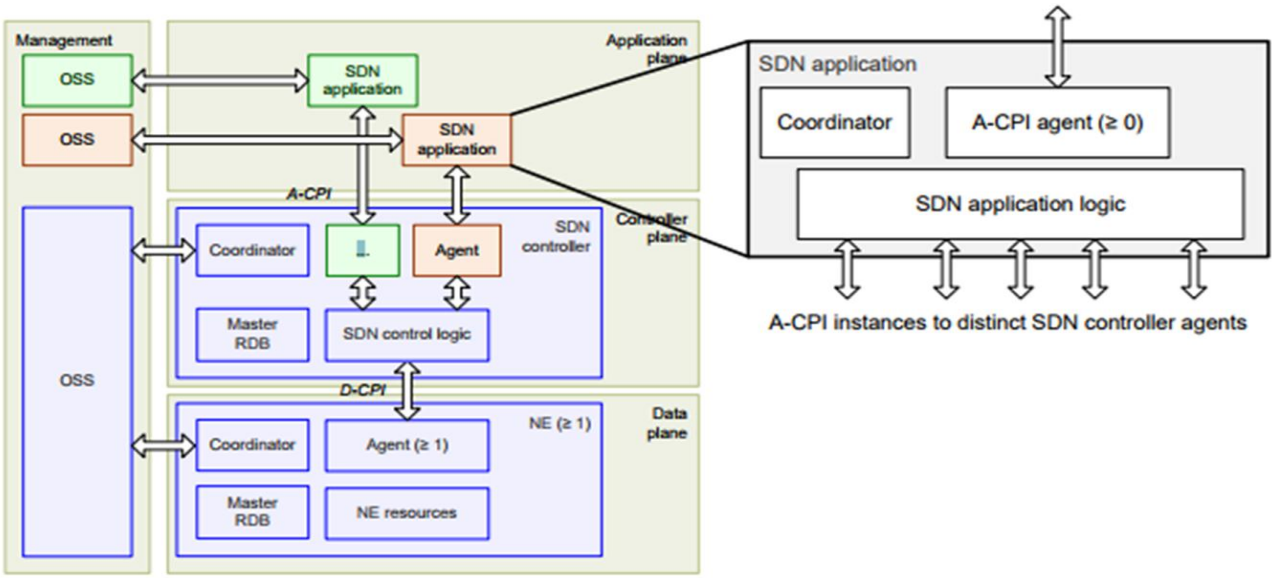
Контрольний рівень забезпечує контролер HP VAN SDN, який є централізованою платформою керування для програмно-визначенних мереж. Він взаємодіє з мережевою інфраструктурою, використовуючи відкриті стандартні інтерфейси та протоколи управління, такі як OpenFlow, NetConf, SNMP та OVSDB. Мережеві пристрої виставляються як абстрактна та централізована контрольна площина для мережевих програм, що дозволяє спростити розроблення програмних додатків.



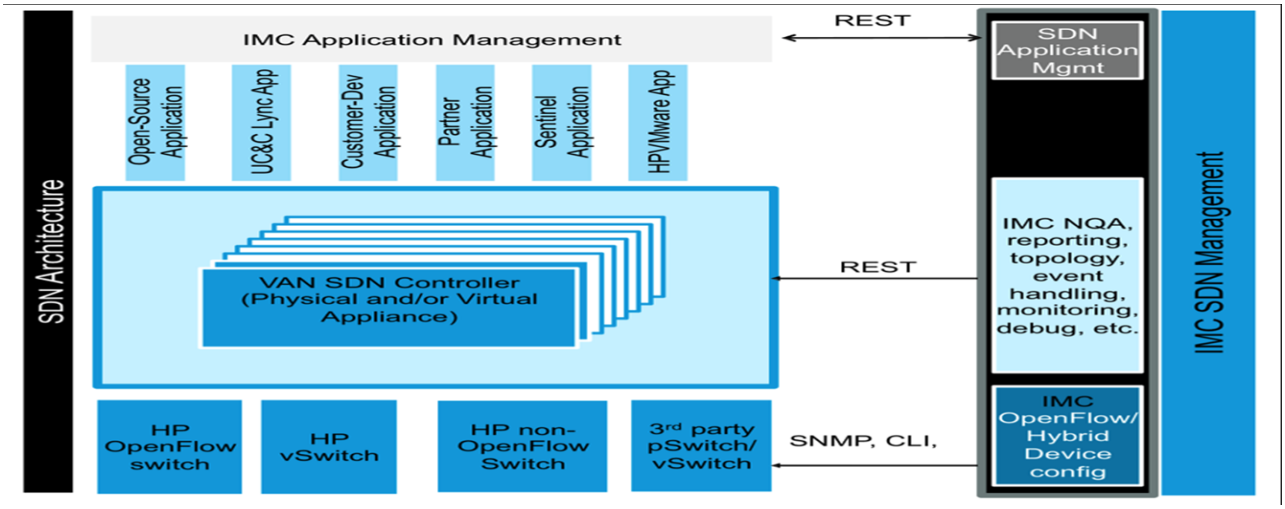
Контролер HP VAN SDN також забезпечує платформу для додатків SDN, які були побудовані та інтегровані в контролер для надання послуг мережі, такі як мережева віртуалізація, безпека, QoS, техніка дорожнього руху тощо.

Контролер HP VAN SDN виступає посередником між цими додатками (які збирають інформацію та приймають рішення) та пристроями інфраструктури (які виконують рішення). HP надає програмовані інтерфейси на площині керування (контролер HP VAN SDN), що дозволяє стороннім розробникам створювати власні програми для їх встановлення як внутрішні програми на контролері. Або вони можуть інтегрувати зовнішні програми з контролером за допомогою API RESTful.

SDN додаток - це програма, яка призначена для виконання завдання в середовищі SDN.



Для управління SDN, HP створив для HP Intelligent Management Center (IMC) новий модуль під назвою SDN Manager (SDNM). IMC забезпечує послідовне управління на основі політики як OpenFlow так і не OpenFlow мереж.



IMC VAN SDN Manager забезпечує функціональність, конфігурацію, облік, продуктивність та управління безпекою для доменів SDN, що підтримують HP.

- Включає розгортання, моніторинг та керування комутаторами, що підтримують HP OpenFlow
- Візуалізує потоки трафіку та моніторинг продуктивності в доменах HP SDN
- Здійснює резервне копіювання та відновлення конфігурацій і програмного забезпечення контролерів HP SDN
- Надає графічний аналіз шляхів усунення несправностей OpenFlow

Використовуючи функції платформи IMC, IMC SDN Manager підсилює моніторинг потоку, топологічне відображення та функції усунення несправностей, щоб забезпечити повні можливості керування SDN в тому ж

інтерфейсі, що і проводова, безпроводова фізична та віртуальна мережі. Ви зможете керувати обома типами - SDN, а також традиційними інтерфейсами - з однієї консолі, що забезпечує оперативну ефективність, необхідну для адміністрування мережі.

1.3 Програмні додатки HP SDN

HP має власний App store для доставки програмних додатків SDN. Програми від партнерів HP AllianceONE та спільноти в цілому доступні в магазині HP SDN App Store. Усі програми можна придбати за допомогою кредитної картки, а вибрані HP та HP Partner програми можна придбати за допомогою традиційних каналів із доставкою через магазин HP SDN App Store.

На малюнку представлено 120 постачальників, які створюють продукти, які підтримують Open Networking Foundation (ONF) software-defined networking (SDN).

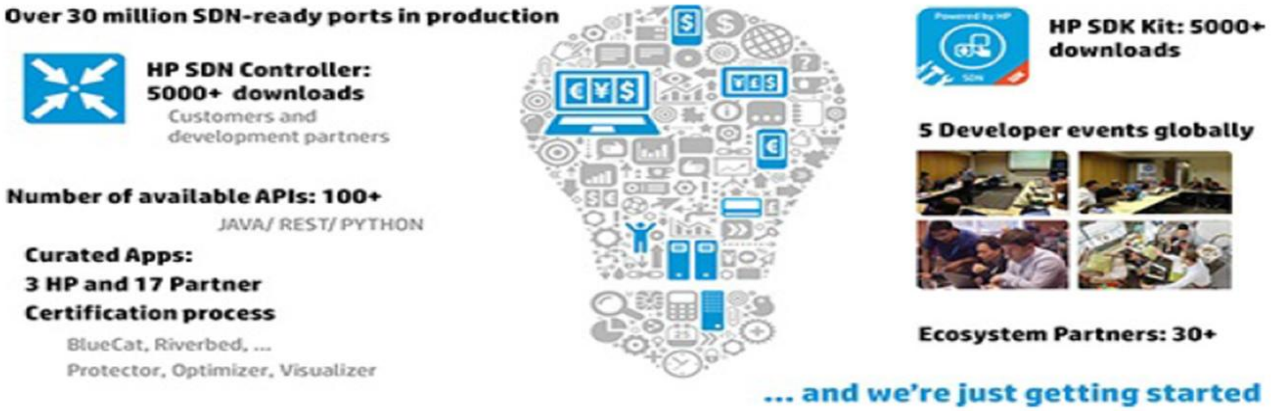
HP випустила комплект розробника програмного забезпечення (Software development kit - SDK), доступний з контролера HP VAN SDN. SDK надає розробникам усі інструменти, необхідні для створення SDN-додатків для контролера HP. Він включає в себе документацію як для Java, так і для REST API, а також всіх файлів jar, необхідних під час складання. Приклади додатків також включені.

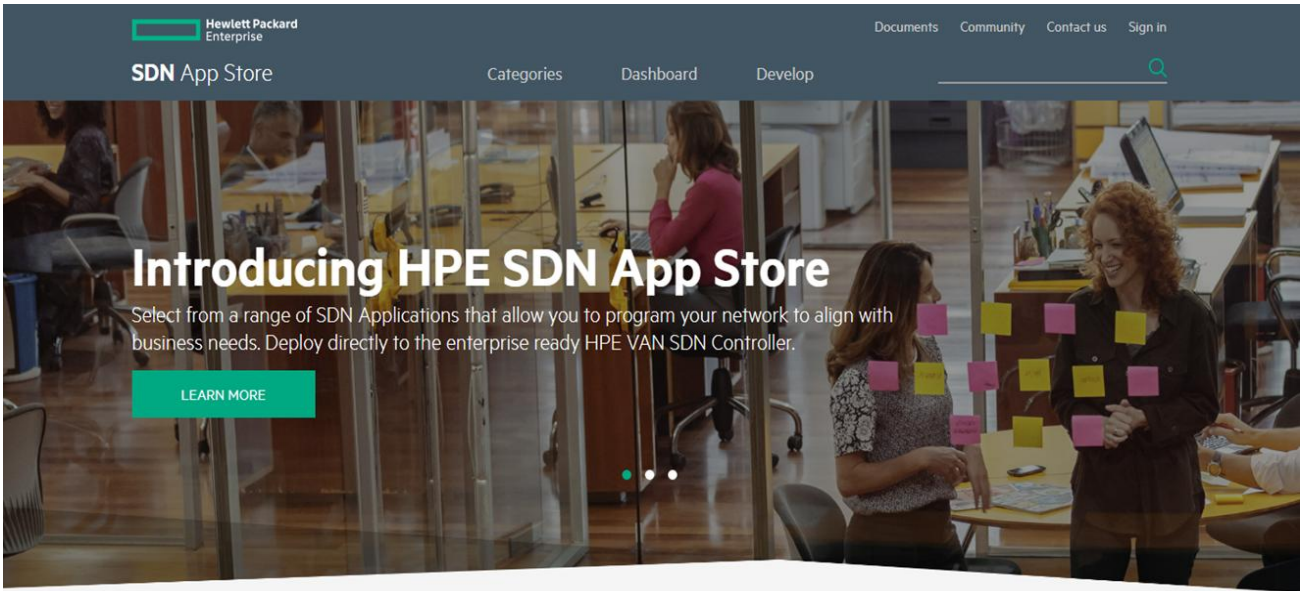
Віддалена лабораторія також доступна партнерам AllianceONE для тестування програм SDN з реальним обладнанням. HP також розміщує та контролює форум розробника, де розробники можуть співпрацювати, щоб отримати відповіді на питання.

HP створює повну екосистему SDN, яка на сьогодні включає в себе наступне:

- Більше 30 мільйонів SDN-готових портів у виробництві, що надає клієнтам швидкий шлях до нового стилю бізнесу, одночасно забезпечуючи розробникам великий ринок
- Більше 5000 завантажень контролера HP VAN SDN

- Більше 100 API-інтерфейсів, а не лише API, але повне спільнота розробників, підтримка, послуги та модель продажів
- Понад 5000 чоловік у сертифікації SDN додатків
- П'ять розробників глобальних подій забезпечують підтримку нашої зростаючої спільноти
- У цілому 5000 завантажень HP SDK Kit
- Більше 30 партнерів в екосистемі



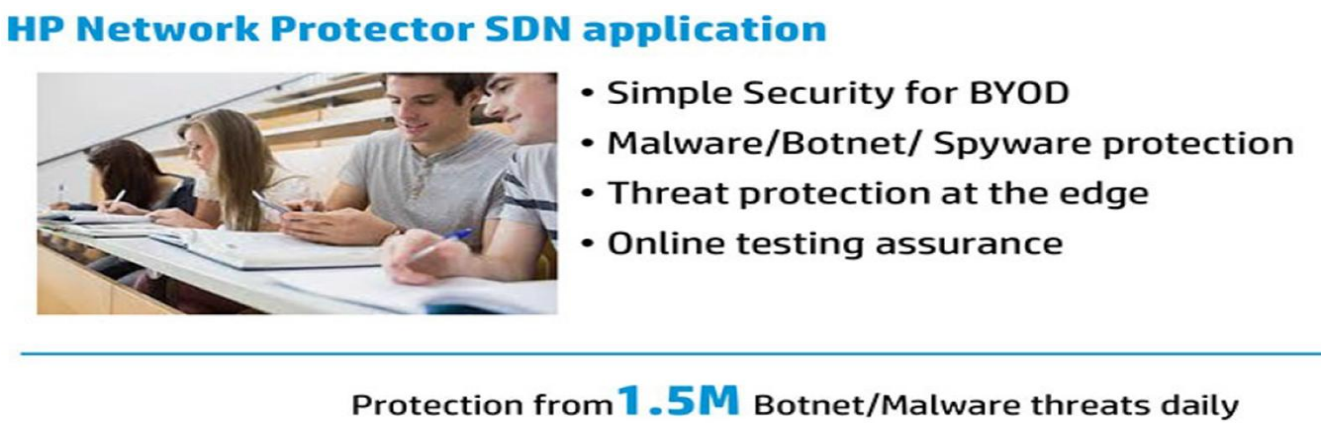


HP має три основні програмні додатки у HP SDN App Store:

- HP Network Protector SDN Application: забезпечує захист від загроз безпеці в реальному часі
- HP Network Optimizer SDN Application: забезпечує керовану додатком якість обслуговування (QoS)
- HP Visualizer SDN Application: забезпечує видимість мережі

1.3.1 HP Network Protector SDN Application

The Network Protector SDN application забезпечує автоматичну оцінку стану мережі та безпеку в режимі реального часу в мережі з підтримкою SDN, забезпечуючи:



Network Protector SDN Application використовує контролер HP VAN SDN для програмування мережевої інфраструктури з інформацією про безпеку з бази даних лабораторії TipupPoint Reputation Digital Vaccine (RepDV).

Це перетворює пристрої мережевої інфраструктури на пристрої забезпечення безпеки, що забезпечує видимість та захист від загрози від більш ніж мільйона шкідливих веб-сайтів, шкідливих програм та програм-шпигунів.

HP Network Protector SDN Application зупиняє загрози на рівні доступу до мережі, перш ніж вони можуть заподіяти шкоду. Network Protector може використовуватися в будь-якому мережевому середовищі, де виникає проблема безпеки.

HP представляє мережу, в якій Network Protector може бути реалізований на будь-якому мережевому пристрої, в будь-якій точці мережі, для безпрецедентної видимості мережі, точності кореляції подій та контролю безпеки.

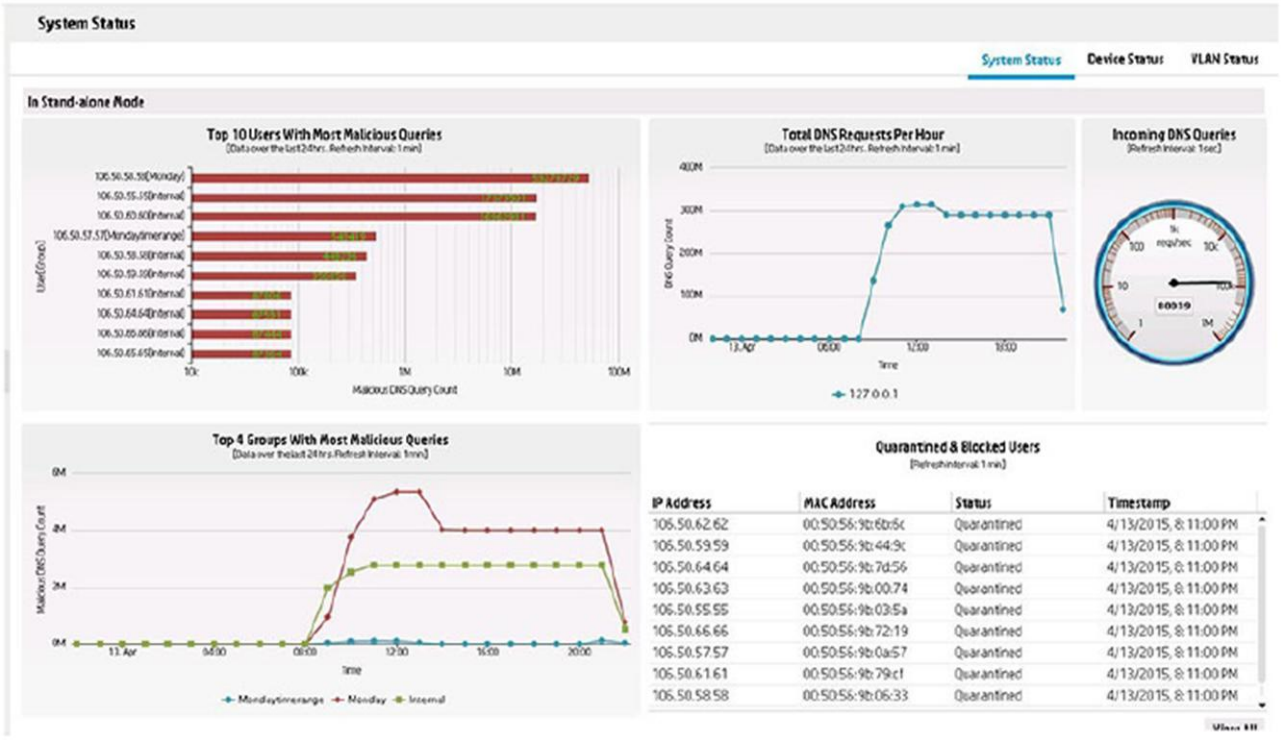
Забезпечує автоматичну оцінку стану мережі. Network Protector SDN application покращує видимість та точність мережі. Програма визначає пріоритет трафіку певної служби доменного імені (DNS) (наприклад, критично для бізнесу) та обмежує некритичний трафік DNS (наприклад, соціальні медіа).

Проактивне IT-управління загрозами. HP Network Protector SDN application дозволяє керувати потоковими динамічними списками керування доступом (ACL), переводячи безпеку на наступний рівень. Програма дозволяє для кожного комутатора та пристрою контроль дроселювання. Програма забезпечує розширену політику маршрутизації користувачів із білого/чорного/сірого списку.

Забезпечує виявлення загрози в режимі реального часу в мережах кампусу підприємства. Network Protector SDN application захищає від понад мільйона зловмисних веб-сайтів, шкідливих програм і програм-шпигунів. Програмний додаток дає характеристику ризику в реальному часі,

використовуючи базу даних хмарних служб HP TippingPoint RepDV. Network Protector SDN application може звертатися до хмарної інформації про загрозу.

Малюнок надає знімок екрана інформаційної панелі HP Network Protector.



Особливості та переваги програми HP Network Protector SDN включають наступне:

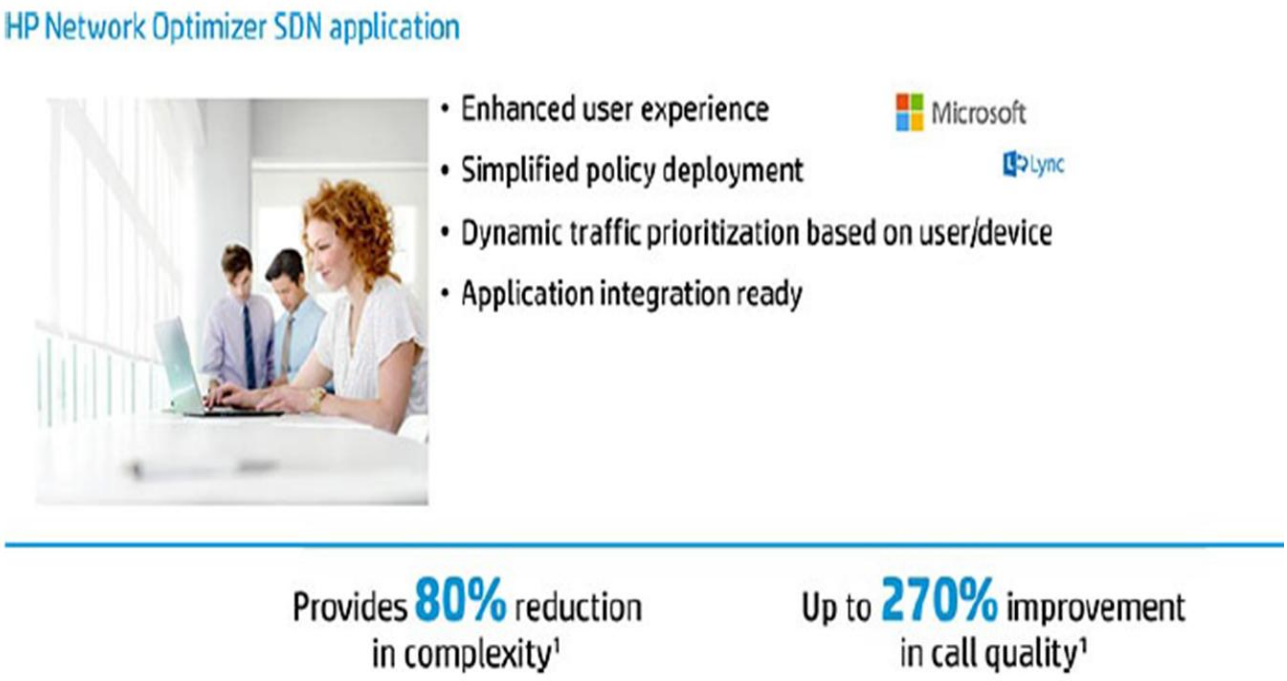
- Гарантовані порогові рівні можуть бути налаштовані на DNS запити кожного клієнта за секунду або на загальну кількість унікальних шкідливих з'єднань для кожного клієнта, що призводить до перенаправлення або скидання всього IP-трафіку клієнта.
- Шкідлива ідентифікація відображає IP-адреси, пов'язані з ізольованими чи заблокованими клієнтами, або відкриває ідентифікатор користувача при інтеграції з IMC.
- Користувальницький білий список дозволяє адміністраторам обходити перевірку репутації для налаштованих доменів.
- Користувальницький чорний список дозволяє адміністратору заблокувати налаштовані домени. Це може бути налаштовано на блокування в певні проміжки часу.
- Високоінфіковані дисплеї VLAN забезпечують видимість відносного здоров'я клієнтів VLAN.
- Високоінфіковані дісплеї кінцевих пристроїв забезпечують видимість джерела шкідливого трафіку.
- Контрольне дроселювання гарантує, що продуктивність мережі не впливає на сплески сильного трафіку.
- Групова політика підтримує рівні індивідуальної репутації для блокування чи ізоляції членів групи.

- Функція оповіщення електронною поштою сповіщає адміністратора ізольованих або шкідливих клієнтів про спроби зловмисного з'єднання.
- Інтеграція з HP ArcSight дозволяє входити в журнал шкідливих активностей у форматі загальних подій (common event format - CEF) (необов'язкова можливість).

Розгортання довіреної та надійної QoS може бути надзвичайно складним і для цього потрібно виконати стомливі та багато часові інтенсивні ручні конфігурації окремо на кожному пристрої. Фактично майже неможливо реалізовувати послідовну політику кінцевого трафіку за допомогою DPI (Deep Packet Inspection) для клієнтів із застарілими мережами. Session Initiation Protocol (SIP) Transport Layer Security (TLS) шифрування та порти динамічних додатків, які використовуються програмами уніфікованого зв'язку (UC), призводять до поганої видимості трафіку додатків.

1.3.2 HP Network Optimizer SDN Application

На малюнку показано, яким чином HP Network Optimizer SDN application зменшує складність і покращує QoS.

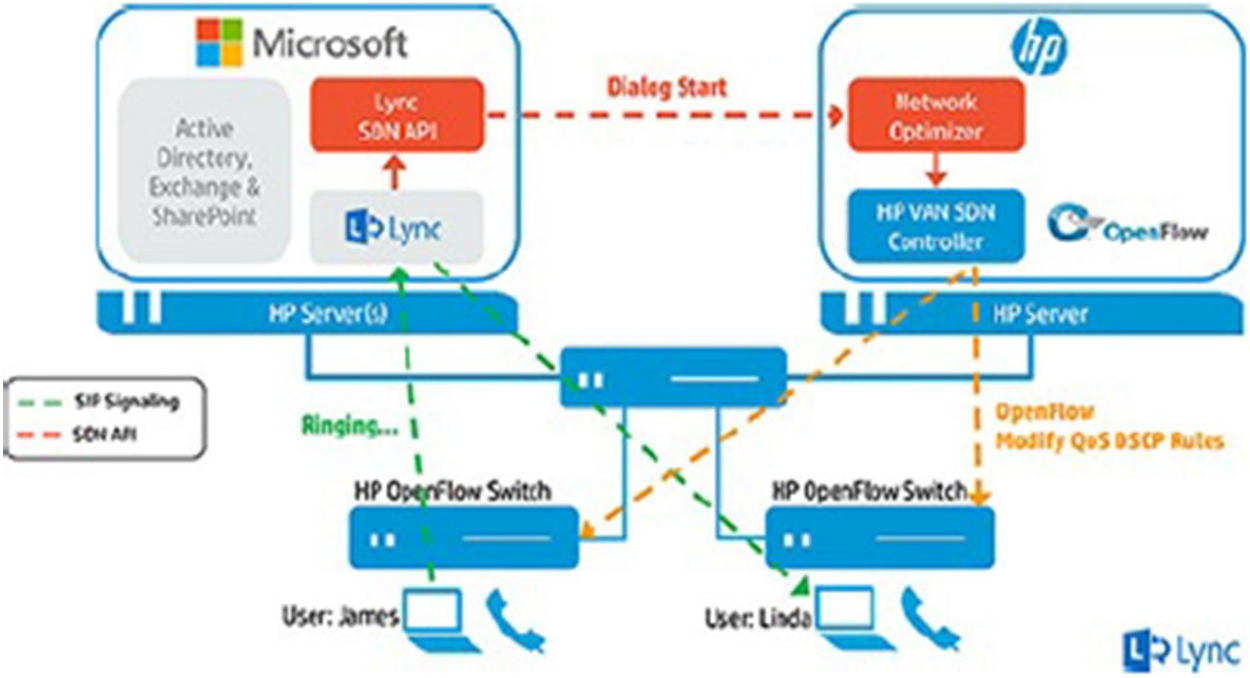


The HP Network Optimizer SDN application використовує OpenFlow для динамічного визначення пріоритету трафіку на краю мережі. Існує чотири традиційних способи ідентифікації уніфікованих комунікацій та встановлення пріоритетів у мережі:

1. Перший спосіб визначає пріоритетність всього трафіку з пристрою. Цей метод використовується з традиційними VoIP-телефонами, поміщаючи телефон у VoIP VLAN і визначаючи пріоритет для всього трафіку у цій VLAN. Це рішення неможливе з використанням Microsoft Lync (коммунікаційна платформа) в оптових розгортаннях, оскільки голосовий

клієнт, як правило, є клієнтом програмного забезпечення Lync, який працює на ПК.

2. Другий спосіб використовує попередньо визначений номер порту для Transport Control Protocol (TCP) чи User Datagram Protocol (UDP) або діапазон, у якому трафік, що відповідає цим порту, може бути визначений як пріоритет. Це не є ідеальним рішенням, оскільки збільшує накладні витрати Lync та мережевого управління, а також підвищує потенціал конфліктів зіставлення портів на клієнтських ПК (дивись малюнок для графічної ілюстрації комунікації Microsoft Lync в мережі.)



The HP Network Optimizer SDN application використовує OpenFlow для динамічного визначення пріоритету трафіку на краю мережі. Існує чотири традиційних способи ідентифікації уніфікованих комунікацій та встановлення пріоритетів у мережі:

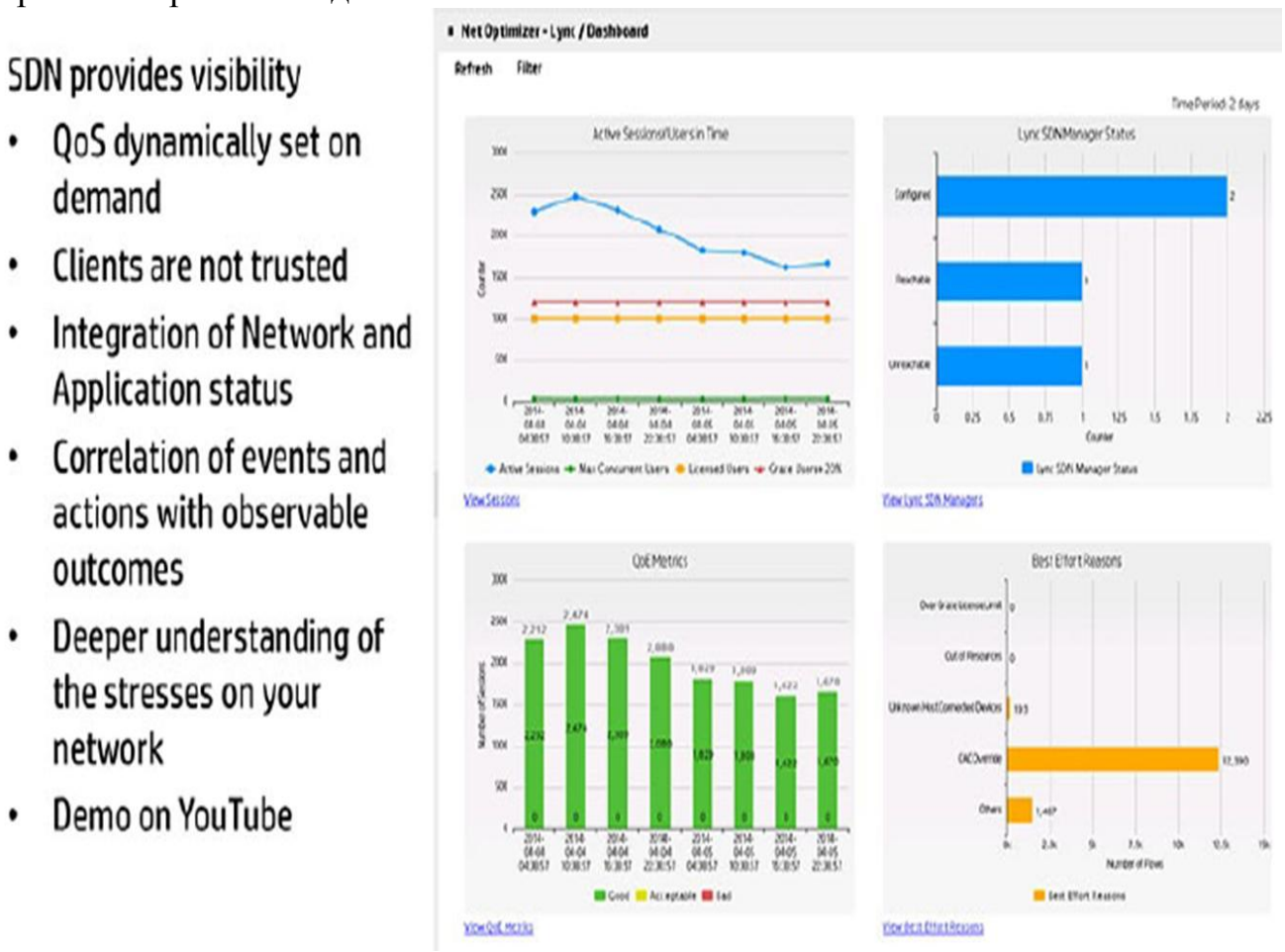
3. Третій спосіб використовує DPI (Deep Packet Inspection) для аналізу та визначення характеру пакета. Однак у випадку з Lync це неможливо, тому що весь керований трафік Lync зашифровується в сеансах TLS. Це робить аналіз DPI неможливим або ненадійним у його здатності ізолювати бізнес-Lync трафік від не-бізнес голосової або відео комунікації.

4. Нарешті, клієнт може відзначити трафік як важливий і налаштувати мережу на довіру до тегів. Хоча це буде працювати і Lync підтримує це, це вимагає рівня довіри від мережевих клієнтів, що не рекомендується. Як тільки мережа довіряє клієнту, з'являться користувачі, які зловживають довірою і намагаються визначити пріоритет усім своїм трафіком. Іншими словами, користувач може використовувати мережу компанії для перегляду фільмів або завантаження файлів BitTorrent з високим пріоритетом.

Вищевказані рішення привели HP і Microsoft до розробки кращого методу для визначення пріоритетного значення важливого трафіку Lync.

Сервер Lync мав детальні знання про інформацію сеансу UC, що відбувається в середовищі, а контролери HP SDN мали детальні знання про фізичну топологію.

Microsoft, у співпраці з HP, розробила API, який встановлюється на сервері Lync, і може робити виклики RESTful API до програми HP Network Optimizer SDN з усіма деталями викликів, включаючи користувачів, тип виклику та вимоги пропускної здатності. HP Network Optimizer може використовувати OpenFlow для динамічного визначення трафіку в мережі протягом тривалості дзвінка.



Performance. Копія HP Network Optimizer може підтримувати інфраструктуру у складі більш ніж 2000 OpenFlow мережевих пристроїв та більш ніж 10,000 користувачів. Ці цифри передбачають мінімальні системні вимоги щодо використання чотирьох ядерного процесора, 8 GB RAM та 64 GB доступного дискового простору. Додаткові копії HP Network Optimizer можуть бути розгорнуті для підтримки значно більшої кількості OpenFlow мережевих пристроїв та користувачів.

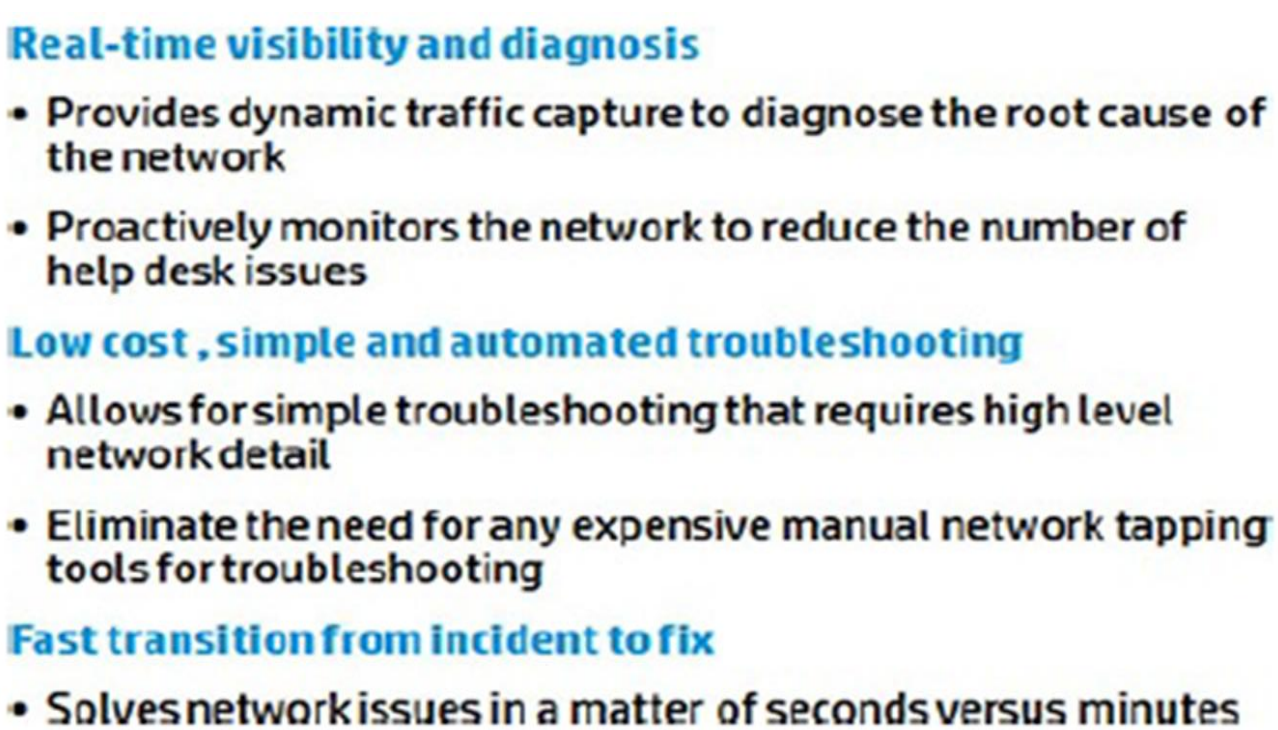
Redundancy. У поточному випуску HP Network Optimizer HA (high availability) не підтримується. Щоб максимально збільшити доступність мережі, пристрої з підтримкою OpenFlow у мережі мають бути налаштовані на відмову в тому випадку, якщо контролер недоступний. HP Network Optimizer розроблений для роботи в гібридному режимі SDN. Це означає, що трафік пересилається мережею за допомогою традиційних методів,

заснованих на MAC-адресі або IP-адресі призначення. Коли комутатор недоступний, ці ж традиційні механізми пересилання продовжують пересилати трафік, як і очікується.

Security. Безпека мережі була дуже важливою проблемою протягом дуже тривалого часу і не змінюється з впровадженням SDN. Методи забезпечення безпеки мережі потребують деякої оцінки. Є кілька механізмів, які допомагають забезпечити безпеку середовища SDN. По-перше, зв'язок між комутатором та контролером має бути переданий до виділеної VLAN управління або, для додаткової безпеки, оброблятись повністю поза межами мережі. Зовнішня мережа, ймовірно, неможлива в локальній мережі, але можлива в центрі обробки даних. По-друге, зв'язок між пристроєм OpenFlow та контролером має бути автентифікований та зашифрований. Контролер HP VAN SDN і комутатори HP підтримують взаємну автентифікацію за допомогою сертифікатів та TLS. Доступ до контролера для цілей управління також зашифрований за допомогою TLS та перевірено за допомогою OpenStack Keystone.

1.3.3 HP Network Visualizer Application

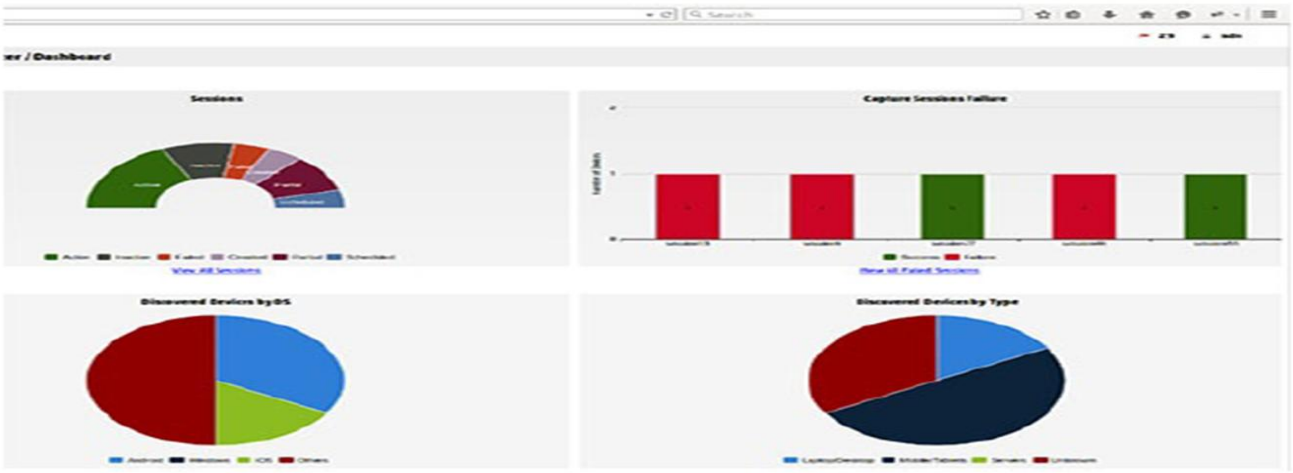
Як видно із малюнку, the **HP Network Visualizer Application** надає видимість мережевого трафіку та пропонує гнучке рішення для отримання копій мережевих пакетів для перевірки, підтвердження та з метою динамічного усунення несправностей.



Ви можете отримати копії мережевих пакетів з декількох вихідних пристроїв і зробити переадресацію захоплених пакетів дляїх збору на пристрої, який може бути розташований практично в будь-якій точці мережі, за допомогою універсального тунелю інкапсуляції маршрутизації (GRE).

Network Visualizer динамічно встановлює правила OpenFlow для контролю мережевого трафіку за критеріями фільтра, визначеними адміністратором мережі через графічний інтерфейс користувача (GUI). Критерії фільтрації визначаються за допомогою атрибутів політики SDN, побудованих на атрибутах відповідності мережевих списків контролю доступу (ACL) та застарілих дій.

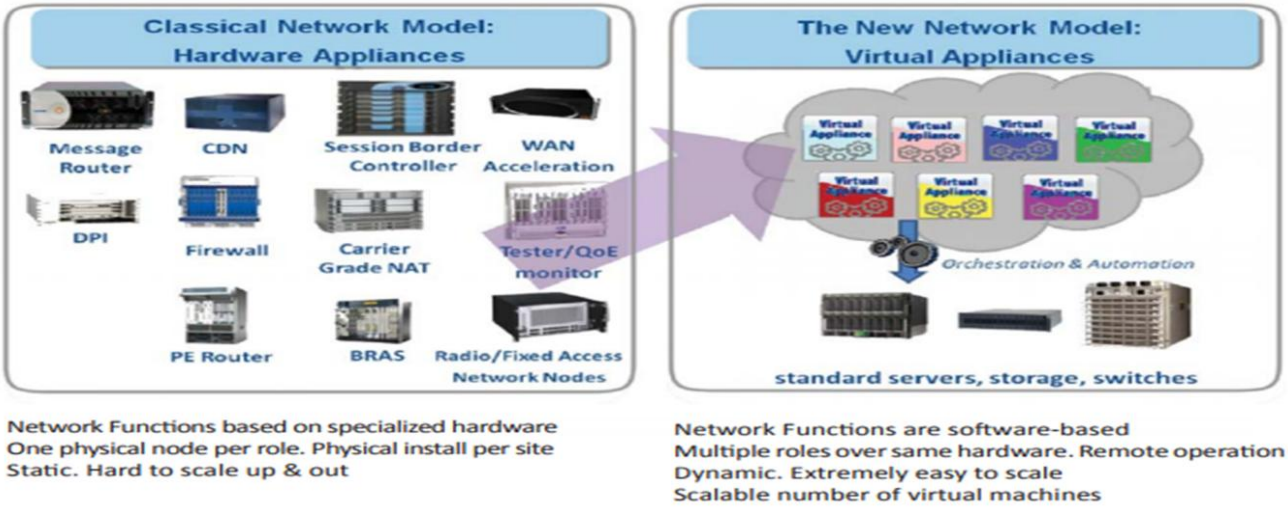
Як показано на малюнку, інформаційна панель (dashboard) Network Visualizer забезпечує графічне представлення захоплення поточної конфігурації сеансу, захоплення сеансу збоїв та виявлених пристроїв за типом та операційною системою (ОС).



1.3.4 Network Functions Virtualization (NFV)

Віртуалізація мережевих функцій (NFV) пропонує новий спосіб розробки, розгортання та управління мережевими службами. NFV відокремлює мережеві функції, такі як трансляція мережевих адрес (NAT), брандмауер, виявлення вторгнень, служба доменних імен (DNS) і кешування, від пропрієтарних апаратних пристроїв, щоб вони могли запускатися в програмному забезпеченні.

Вона призначена для консолідації і доставки мережевих компонентів, необхідних для підтримки повністю віртуалізованої інфраструктури, включаючи віртуальні сервери, сховища і навіть інші мережі. Вона використовує стандартні технології віртуалізації IT, які працюють на високопродуктивних сервісах, комутаторах і пристроях зберігання для віртуалізації втратити зв'язок із мережею. Вона застосовується до будь-якої площини обробки даних або функції площини управління як в проводовій, так і в безпроводовій мережевій інфраструктурі.



Network Functions based on specialized hardware
One physical node per role. Physical install per site
Static. Hard to scale up & out

Network Functions are software-based
Multiple roles over same hardware. Remote operation
Dynamic. Extremely easy to scale
Scalable number of virtual machines

NFV має ряд важливих переваг, зокрема:

- Зменшення потреби у мережному обладнанні
- Зменшення енергоспоживання мережі
- Зниження вартості обслуговування мережі
- Просте та швидке оновлення мережі

NFV не слід плутати з віртуалізованою мережею, оскільки NFV, як технологічна концепція, прагне вилучати лише мережеві функції, а не всю мережу.

NFV доповнює SDN, хоча NFV може бути реалізований без SDN. SDN дозволяє IT та мережевим операціям застосовувати бізнес-логіку безпосередньо до нових програмних мереж і динамічно впроваджувати нові послуги швидше за рахунок менших витрат на управління та меншої складності. SDN розблоковує недостатньо використані та обмежені мережі, щоб підвищити їх цінність.

NFV і SDN можуть бути об'єднані, щоб створити більшу цінність, оскільки SDN поширює динамічність на мережеву інфраструктуру, подібно тому як віртуалізації сервера вносить до обчислювальної інфраструктури. HP передбачає, що сьогодні віртуалізовані функції зрештою стануть віртуалізованими мережевими сервісами в рамках архітектури SDN.

Демонстрація поглибленої інтеграції цих двох технологій є ключовою вимогою, виконаною в рамках архітектури HP.

Network functions virtualization (NFV). Використовуючи стандартну технологію віртуалізації IT для консолідації багатьох типів мережевого обладнання такі як стандартні великогабаритні сервери, комутатори та накопичувачі на базі стандартів, NFV надає модель для вирішення завдань CSP навколо зменшення капітальних видатків (CapEx), покращення керованості, зменшення часу на ринок і заохочення ширшої екосистеми.

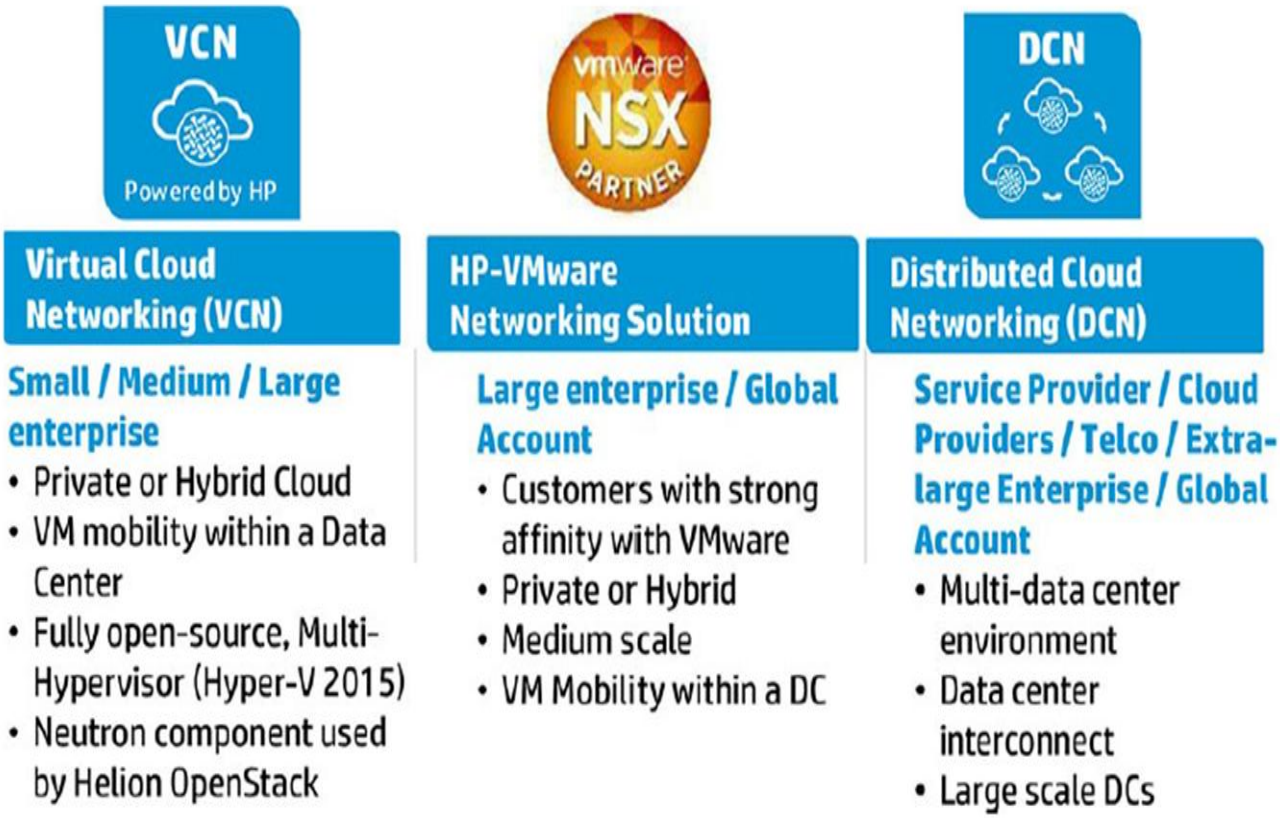
Software-defined networking (SDN). SDN дає змогу новим програмним мережам, що дозволяють IT та мережевим операціям безпосередньо і динамічно застосовувати бізнес-логіку, швидше вводити нові служби, зменшити витрати на управління з меншою складністю та змінювати багато мережевих функцій, зменшуючи CapEx. SDN - це технологія, яка реалізує існуючу практику шляхом відокремлення контрольної площини від механізмів передачі даних.

1.4 Рішення SDN для ЦОД та хмари

Від підприємців до постачальників послуг IT-клієнтам, усім потрібні спеціальні рішення для віртуалізації мереж, що відповідають конкретним бізнес-результатам. Щоб задовольнити цю унікальну вимогу, компанія HP пропонує пакет з трьох частин, який позбавляє вас від застарілих мереж, покращує швидкість обслуговування та знижує вартість.

Будуючись на найповнішому портфоліо мережевої віртуалізації у галузі та спираючись на обслуговування та підтримку світового рівня, HP має унікальну можливість безпечно здійснювати навігацію за допомогою цієї технології та трансформації бізнесу.

Кожне з рішень, які ви бачите на малюнку, забезпечує відкриту і базовану на стандартах основа для клієнтів (за бажанням) перейти до більш широкого розгортання додатків SDN. HP являється відкритою екосистемою SDN, а HP SDN Store App Store допомагає клієнтам швидко та за низьку ціну покращити досвід роботи з кінцевими користувачами.

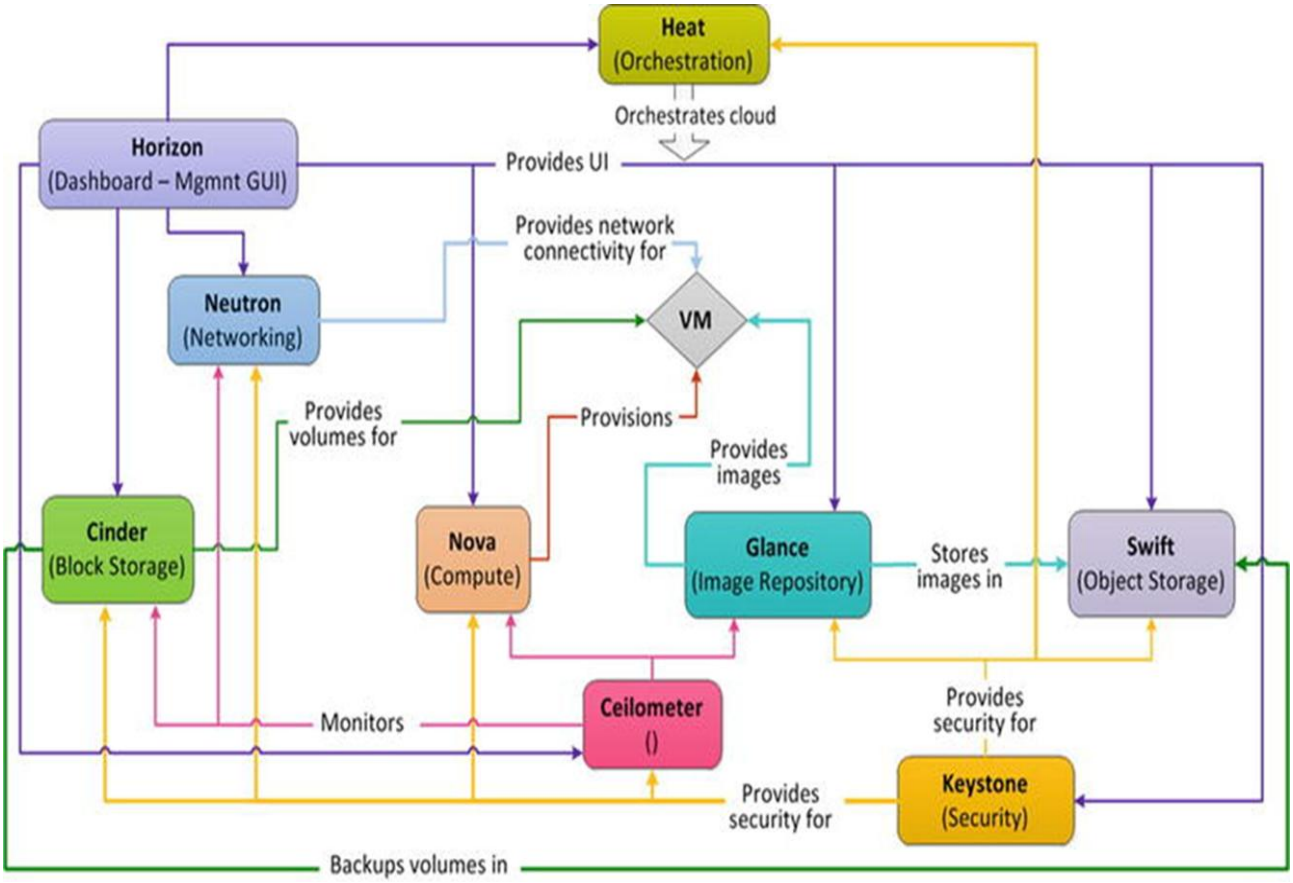


1.4.1 Virtual Cloud Networking (VCN)

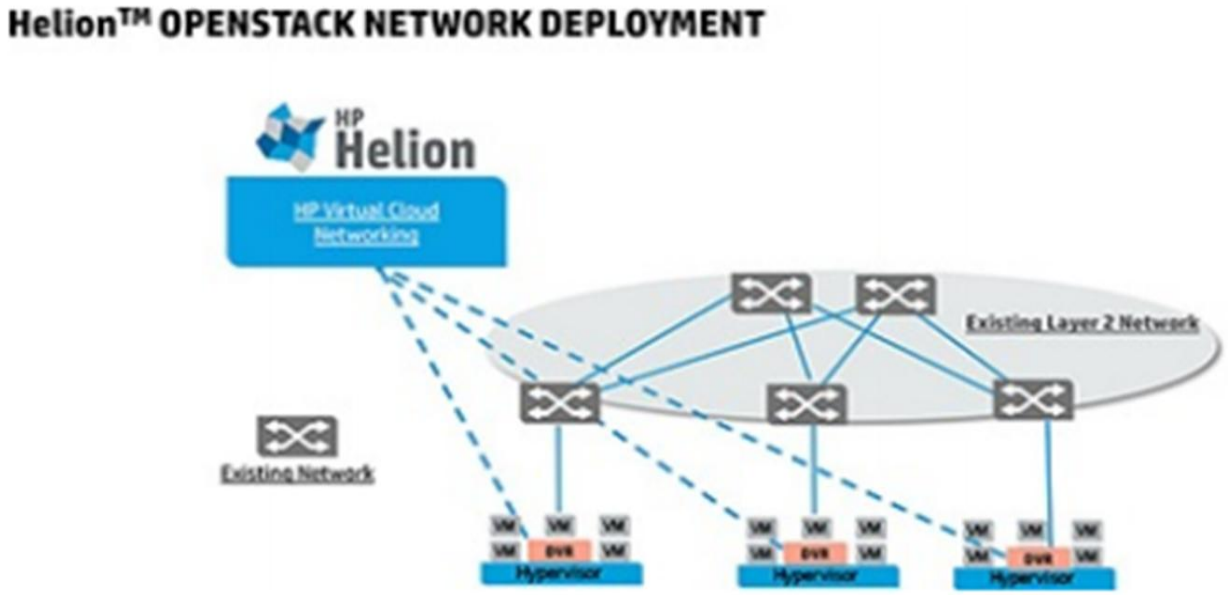
У липні 2014 року, HP оголосила про застосування the Virtual Cloud Networking (VCN) SDN та її інтеграції в HP's Helion OpenStack®. VCN пропонує розширення OpenStack Neutron з унікальним покращенням

підтримки багато гіпервізорної системи, розподіленої віртуальної маршрутизації, high availability (HA), шлюзу Virtual Extensible LAN (VXLAN), VPN as a service (VPNaaS) та вдосконалення груп безпеки. Це також забезпечує поліпшену масштабованість. Багато хто з цих удосконалень було внесено до спільноти з відкритим кодом.

HP в даний час є провідним учасником OpenStack Neutron, плануючи поточну роботу з підтримки додаткових гіпервізорів, які встановлюють на "голий метал", поєднання служб та інтеграції програм SDN для підтримки операцій мережі та безпеки.



Програма HP VCN SDN - це розширений мережевий модуль Neutron HP Helion OpenStack (див. Малюнок), що забезпечує віртуалізацію мережі через SDN та організовує всю інфраструктуру центрів обробки даних.



Програма VCN SDN допомагає провайдеру хмари та підприємства побудувати надійну, мультиорендну мережну інфраструктуру, яка здатна надати готові до використання комп'ютери, накопичувачі та мережі. Це передбачає:

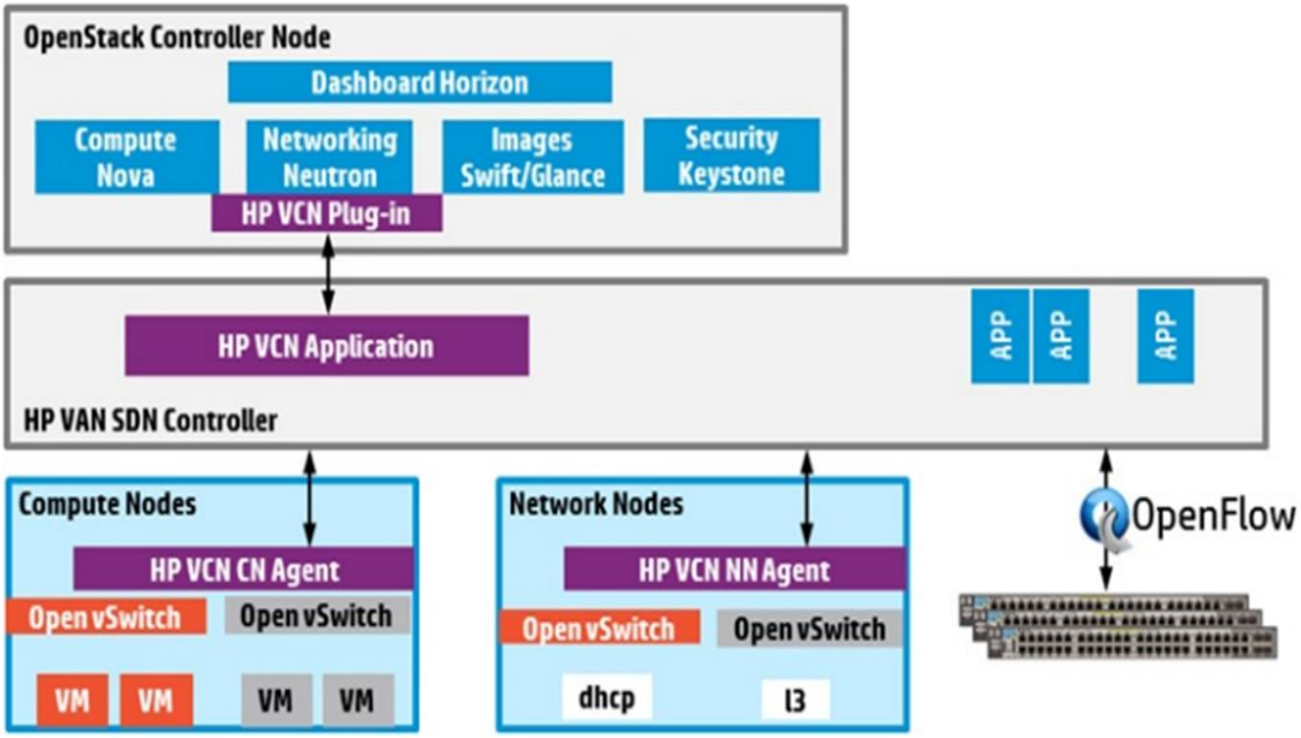
- Масштабована, безпечна та стійка хмарна корпоративна мережа
- Повний доступ до відкритої екосистеми SDN, яка включає додатки SDN, як HP та і сторонніх розробників

Програма HP VCN SDN інтегрується з контролером HP VAN SDN і використовує OpenFlow для створення уніфікованого керування динамічною політикою як у віртуальному (Open vSwitch) так і в фізичному (HP та сторонніх розробників) мережах.

VCN надає мультиорендну мережеву службу віртуалізації для Kernel-based Virtual Machine (KVM) та VMware ESX multi- hypervisor програмних додатків для ЦОД, пропонуючи організаціям як відкриті, так і пропрієтарні рішення. Мультиорендна ізоляція забезпечується централізовано оркестрованими віртуальними мережами VLAN або VXLAN, що працюють по стандартам ЦОД L2 або L3.

Невіртуалізовані, на "голому залізі", сервера та додатки можуть підтримуватися в середовищі VXLAN за допомогою додавання комутаторів HP 5930 для забезпечення кінцевої точки апаратного тунелю. У повністю віртуалізованому розгортанні існуюча інфраструктура комутації центрів обробки даних може бути збережена без необхідності дорогих оновлень. Пристрої з підтримкою OpenFlow 1.3 рекомендуються для реалізації переваг додатків для ЦОД на базі SDN.

Для того, щоб зрозуміти яким чином HP VCN працює, необхідно зрозуміти її компоненти, які показані на малюнку.



Програмний додаток HP VCN вбудований у контролер HP VAN SDN як внутрішня програма. Він може використовувати всі послуги контролера, такі як керування потоком, прослуховування пакетів, обробку бізнес-логіки, перманентність даних та HA.

Програма використовує RESTful API для спілкування з HP VCN Plug-in на контролері OpenStack. HP пропонує корпоративний OpenStack-сумісний контролер, але клієнти можуть встановити HP VCN Plug-in на будь-якому контролері OpenStack, який вони оберуть.

Контролер HP VAN SDN забезпечує Neutron L2 Agent та L3 Agent APIs. Ці API дозволяють HP VCN спілкуватися з агентами VCN, встановленими на віртуальних хостах. Кожен комп'ютерний вузол, що підтримує VM, вимагає VCN Compute Node (CN) агента і кожен мережний вузол, що підтримує віртуальну мережеву, потребує агента VCN Network Node (NN).

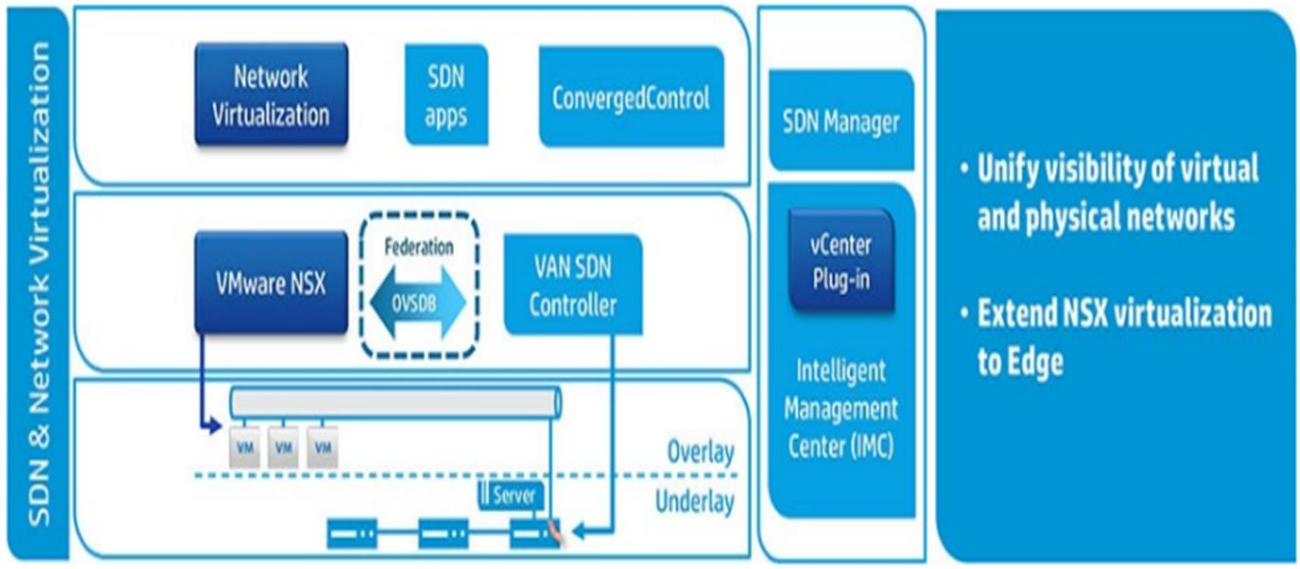
Коли HP VCN отримує запити на надання послуг від контролера OpenStack, HP VCN використовує вбудований бізнес інтелект та знання інфраструктури для побудови плану для виконання запиту. Потім програма встановлює відповідні налаштування, зробивши виклики RESTful API для агентів CN і NN. Він може використовувати служби платформи для зміни транспортних потоків у фізичній інфраструктурі, якщо це необхідно.

1.4.2 HP-VMware networking solution

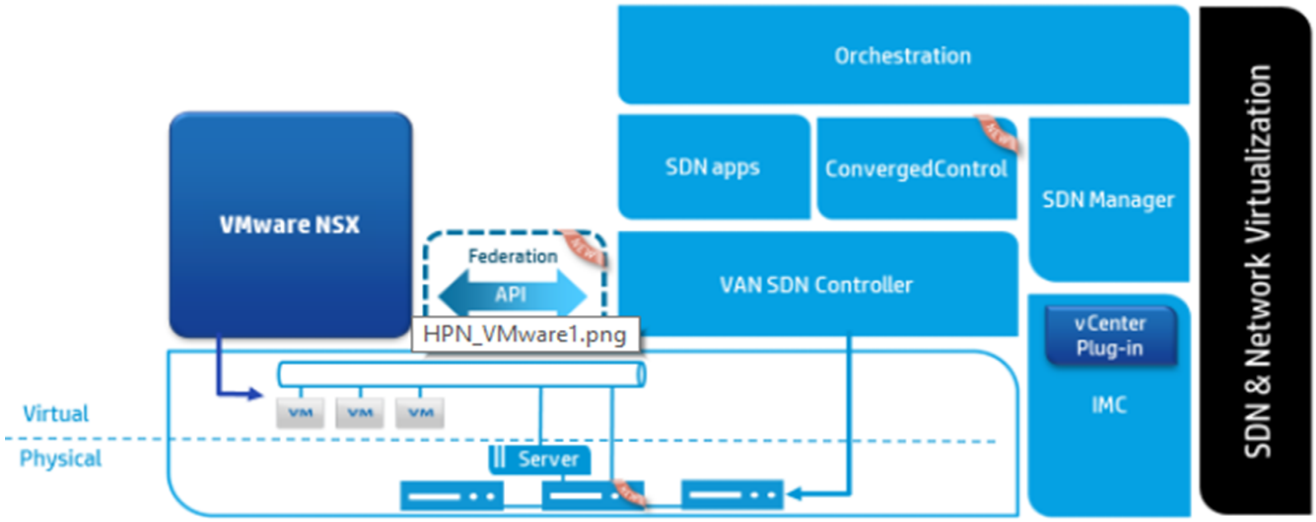
Рішення для мереж HP-VMware networking solution забезпечує сумісне застосування для віртуалізації SDN та мережі, яке реалізує уніфіковану автоматизацію та видимість клієнтів у віртуальних та фізичних мережах для Vmware центрів обробки даних.

Рішення поєднує платформу віртуалізації мережі HP VAN SDN Controller та VMware NSX через спільний API, що забезпечують автоматизацію SDN у фізичних та віртуальних центрах обробки даних.

HP та VMware співпрацюють, щоб забезпечити першим сумісним рішенням SDN в галузі. Як показано на малюнку, рішення об'єднує контролер HP VAN SDN з платформою віртуалізації мережі VMware NSX, щоб забезпечити клієнтів комплексним підходом для автоматизації їх фізичної та віртуальної мережної інфраструктури.



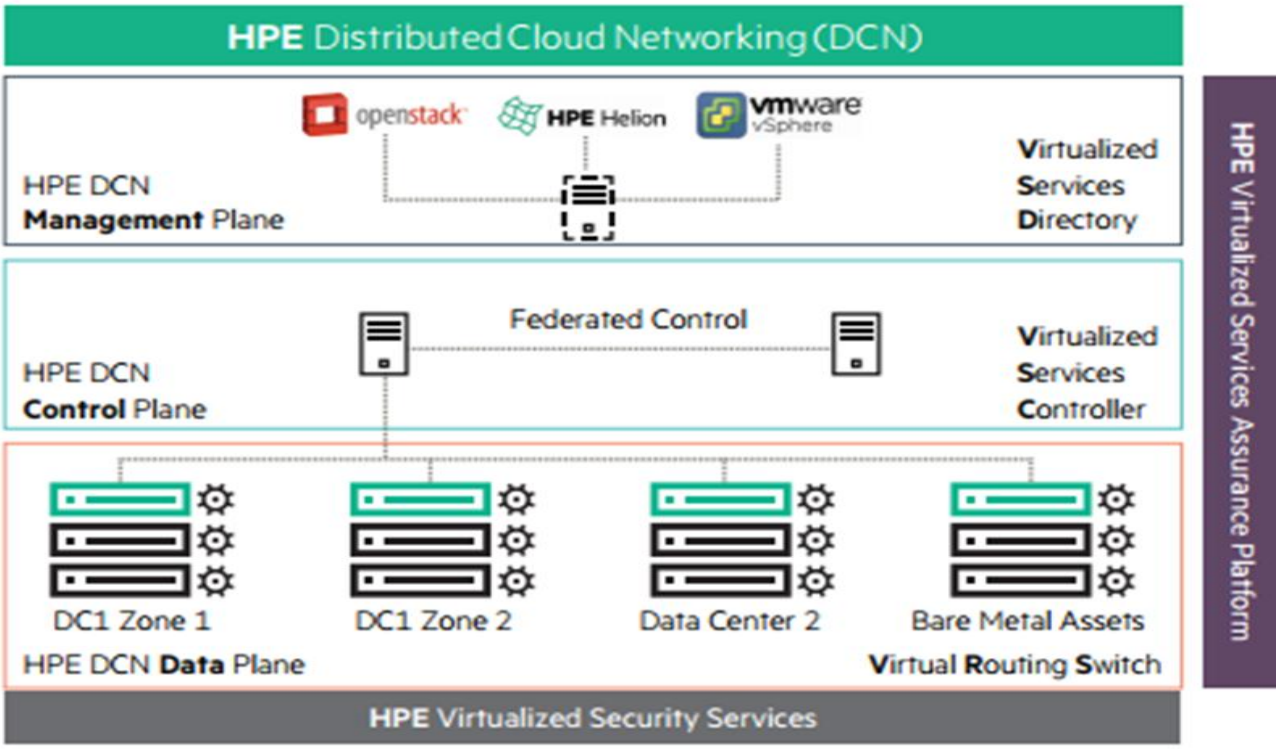
Open, interoperable solution unifying physical and virtual



1.4.3 HP Distributed Cloud Networking (DCN)

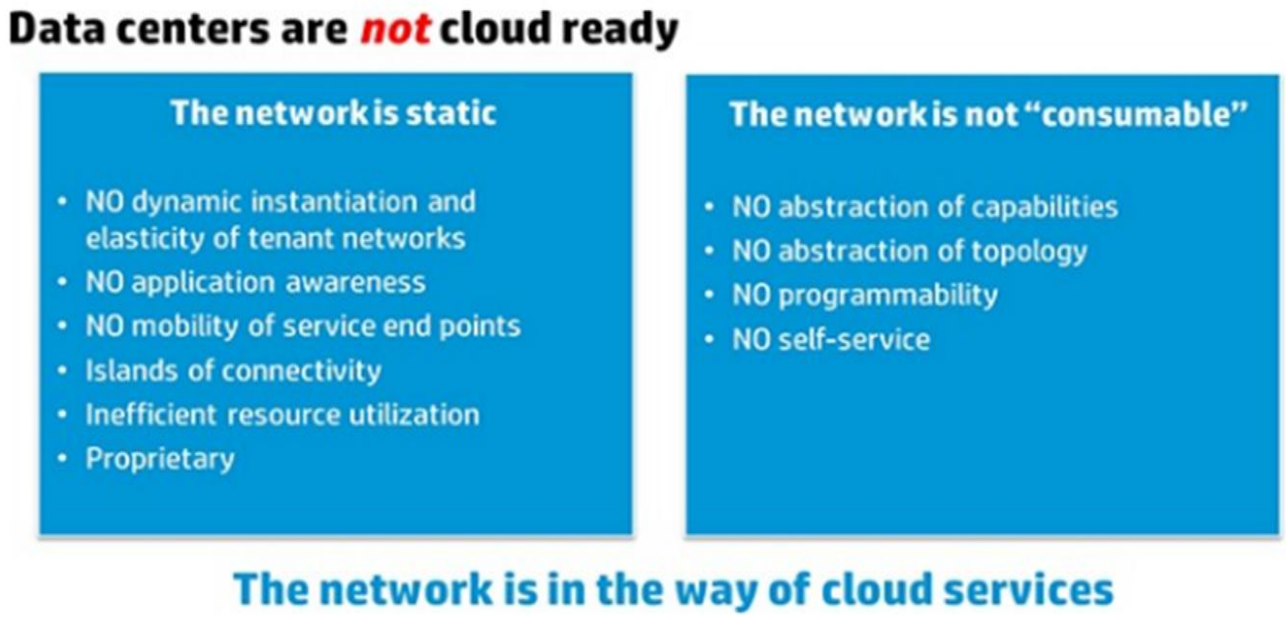
HPE Distributed Cloud Networking - це повне і всеосяжне мережеве рішення, яке об'єднує приватні, публічні та гібридні хмари шляхом віртуалізації існуючих центрів обробки даних і дозволяє легко керувати ресурсами мережі за допомогою таких платформ управління, як Openstack,

Cloudstack або vCenter. Використовуючи програмованість бізнес-логіки та політичного механізму, платформа дозволяє відкрити та реалізовувати рішення, яке масштабується для вирішення обмежених у коштах потреб центрів обробки даних, що розташовані у різних місцях.



HPE Distributed Cloud Networking (DCN) представляє собою SDN рішення, яке віртуалізує будь-яку мережеву інфраструктуру ЦОД та автоматично встановлює зв'язок між обчислюваними ресурсами після їх створення.

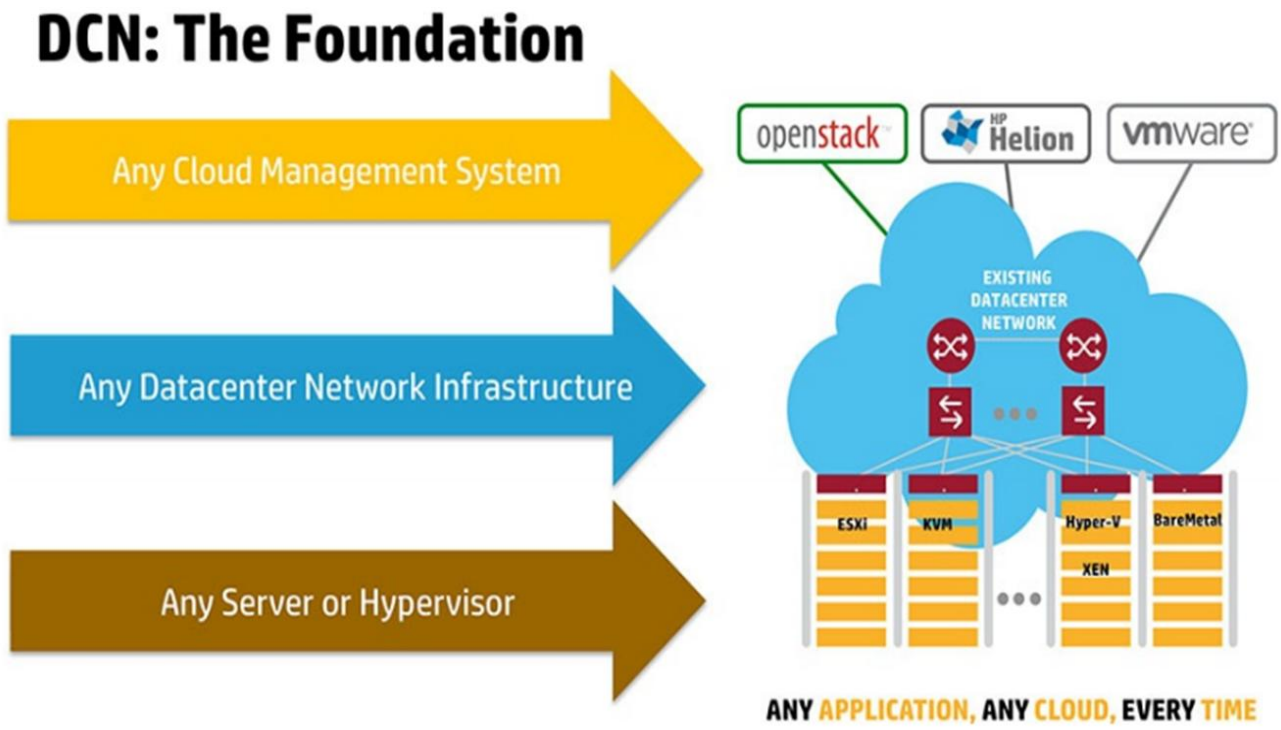
На малюнку ілюструється антитеза про те, що провайдери і великі організації повинні створювати розподілені, масштабні, багатододанні середовища простими, стандартними та гнучкими методами, використовуючи SDN та мережеву віртуалізацію. HP DCN, з іншого боку, саме те, що їм потрібно. Це повне і всеосяжне мережеве рішення, яке віртуалізує існуючі центри обробки даних і дозволяє легко управляти мережевими ресурсами за допомогою платформ керування апаратним забезпеченням, таких як HP CloudSystem, OpenStack, CloudStack або vCenter.



Рішення складається з мережевого рівня, як фізичного, так і віртуального, контрольного рівня з об'єднаними контролерами, які можуть взаємоз'єднувати з використанням протоколу Border Gateway-Multiprotocol (BGP-MP) в центрах обробки даних та між ними, а також рівня службового каталогу з передовими програмованими політиками і аналітикою, де IT-адміністратори можуть визначати, візуалізувати та управляти мережею, не обтяжуючись деталізацією мережевої реалізації. Вони можуть застосовувати безпеку, балансування мережного навантаження та політику доступу користувачів з високим рівнем абстракції замість ручного інтерфейсу командного рядка (CLI) та призначення IP-адреси. Визначені один раз, як ці політики можуть бути використані динамічно для керування поведінкою в мережі в потрібній мірі, викликаної створенням обчислювальної екземпляра, міграцією та видаленням.

Як показано на малюнку нижче, HPDCN являє собою фундамент, який дозволяє провайдерам послуг та великим організаціям керувати розподіленим середовищем з виликою кількістю ЦОД, простим, відкритим та гнучким способом, використовуючи SDN та мережеву віртуалізацію. Завдяки повністю інтегрованим анделейними та оверлейної мережами, ви можете зменшити загальну вартість володіння (TCO) шляхом поєднання інтелектуального управління робочими навантаженнями з автоматизацією політики.

DCN також прискорює перехід провайдерів в послуг до NFV, оптимізуючи ресурси мережі, збільшуючи спритність та прискорюючи час для виходу на ринок через динамічну, керовану службою конфігурацію.



Уніфікація приватних, публічних та гібридних ЦОД за допомогою SDN. Через SDN та мережеву віртуалізацію HP DCN дозволяє мережевим адміністраторам керувати розподіленим мережним середовищем з одного центрального розташування, незалежно від того, чи є організація приватним, публічним або гібридним ЦОД. Це:

- Підтримує політику мережевого забезпечення для автоматизації та швидкості розгортання додатків
- Розгортає розподілені мережі центрів обробки даних за хвилини

Використання декількох центрів обробки даних з єдиної точки управління:

- OHP DCN має плагіни для OpenStack, CloudStack, HP Cloud OS та HP Helion для більшої гнучкості у виборі середовища.
- Відповіді на подання заявки на самостійне встановлення мережевих послуг автоматично відповідають політиці корпоративної безпеки та бізнес-логіці програми.

Забезпечує маневреність бізнесу, контролюючи витрати на інфраструктуру:

- HP DCN - платформа віртуалізації від 2 до 4 рівня, яка оптимізує мережу, вилучаючи неефективність.
- Він автоматично вибирає найшвидший шлях для оптимізації використання пропускної здатності та затримки при зменшенні вузького місця зовнішнього маршрутизатора чи шлюзу.
- Функції політики зближують розгортання мережі з потребами програми в автоматичному режимі, пропонуючи користувачам можливість конфігурувати мережу в дружній спосіб.

Що потрібно для підтримки такої мережевої функції? Як показує малюнок, відповідь така:

Висновки.

Дізналися, як SDN допомагає вдосконалювати мережі. Ви дізналися про потреби, які потребують керування SDN і переглянули деякі випадки початкового використання OpenFlow і SDN.

Дізналися про деякі основи SDN і OpenFlow і дізналися, як SDN абстрагує мережеву інфраструктуру, що дозволяє розробникам програмного забезпечення програмно реалізувати бізнес-політику.

Зозглянули деякі різні точки зору того, що таке SDN, а потім дізнався деякі переваги відкритих стандартів для впровадження мультивендорних SDN на основі протоколу OpenFlow.

Ознайомились з різними програмними додатками HP SDN для облаштування кампусу та ЦОД. Дізналися також про HP SDN App Store та різні програми, які доступні в App Store.

Коротко обговорили наступні програми та рішення:

- HP Network Protector SDN Application
- HP Network Optimizer SDN Application for Microsoft Lync
- HP Visualizer SDN Application
- HP VMware NSX federation
- HP VCN (Virtual Cloud Networking)
- HP DCN (Distributed Cloud Networking)

Розділ ІІ. Контролер HP VAN SDN

У даному розділі розглядається HP Virtual Application Network Software-Defined Networking (VAN SDN) Controller, який розроблений на базі мови програмування Java.

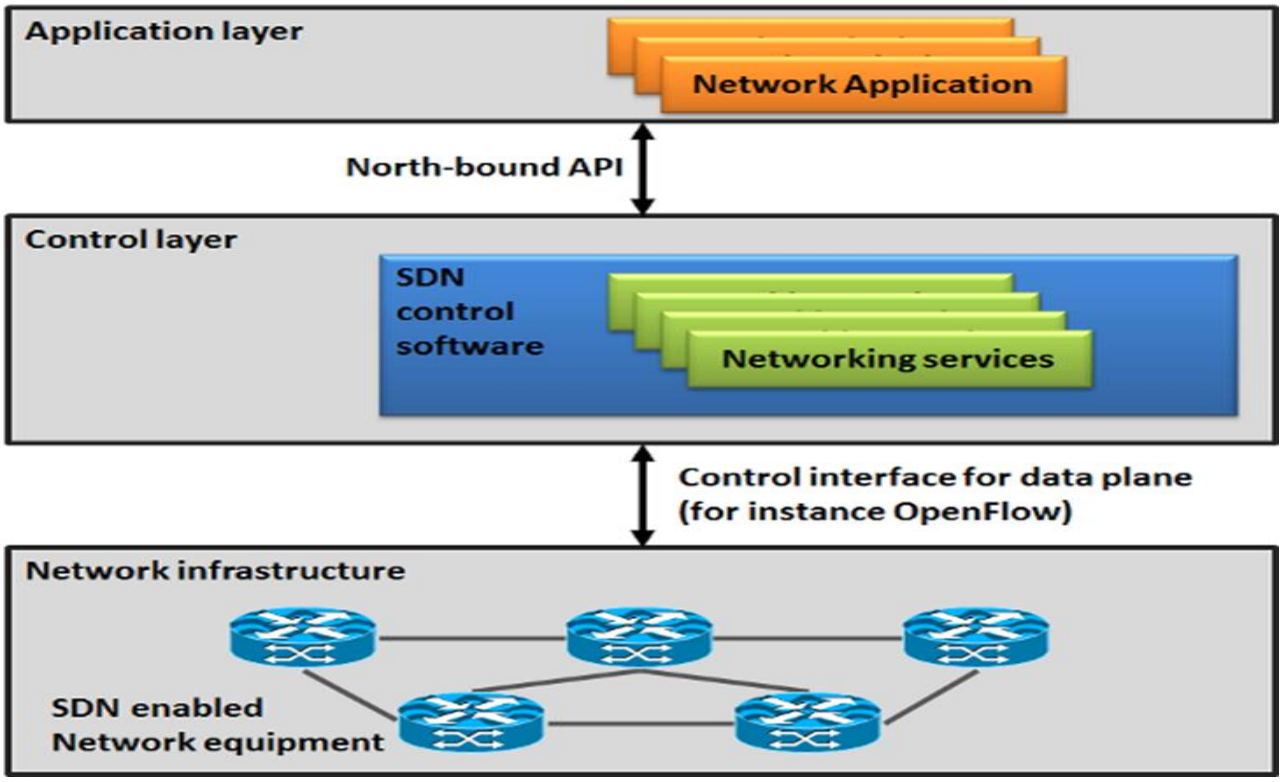
Програмне забезпечення контролера HP VAN SDN працює під керуванням OS Ubuntu версії 12.04 LTS (64-bit) і надає розробникам платформу для створення програмних додатків, які взаємодіють і програмують мережі, які підтримують протокол OpenFlow.

У цьому розділі також розглядається Mininet (мережний симулятор), в якому використовується комутатор Open vSwitch – програмний комутатор з відкритим вихідним кодом та підтримкою протоколу OpenFlow.

2.1 Загальні відомості про контролер HP VAN SDN

У архітектурі Software Defined Networking (SDN) управління мережею та мережевий трафік відокремлені один від одного, централізуючи мережевий інтелект та абстрагуючи базову мережеву інфраструктуру від програм.

HP VAN SDN Controller забезпечує управління фізичними та віртуальними комутаторами через стандартний протокол OpenFlow, а також Netconf та SNMP.



Мережеві порти, зв’язки (links) та топології є безпосередньо видимими, що дозволяє реалізовувати політику централізованого адміністрування та більш ефективного вибору шляху на основі динамічного глобального погляду на мережі. Це значно спрощує оркестровку багатокористувальницького середовища та дотримання мережевої політики як для мобільних клієнтів так і для серверів.

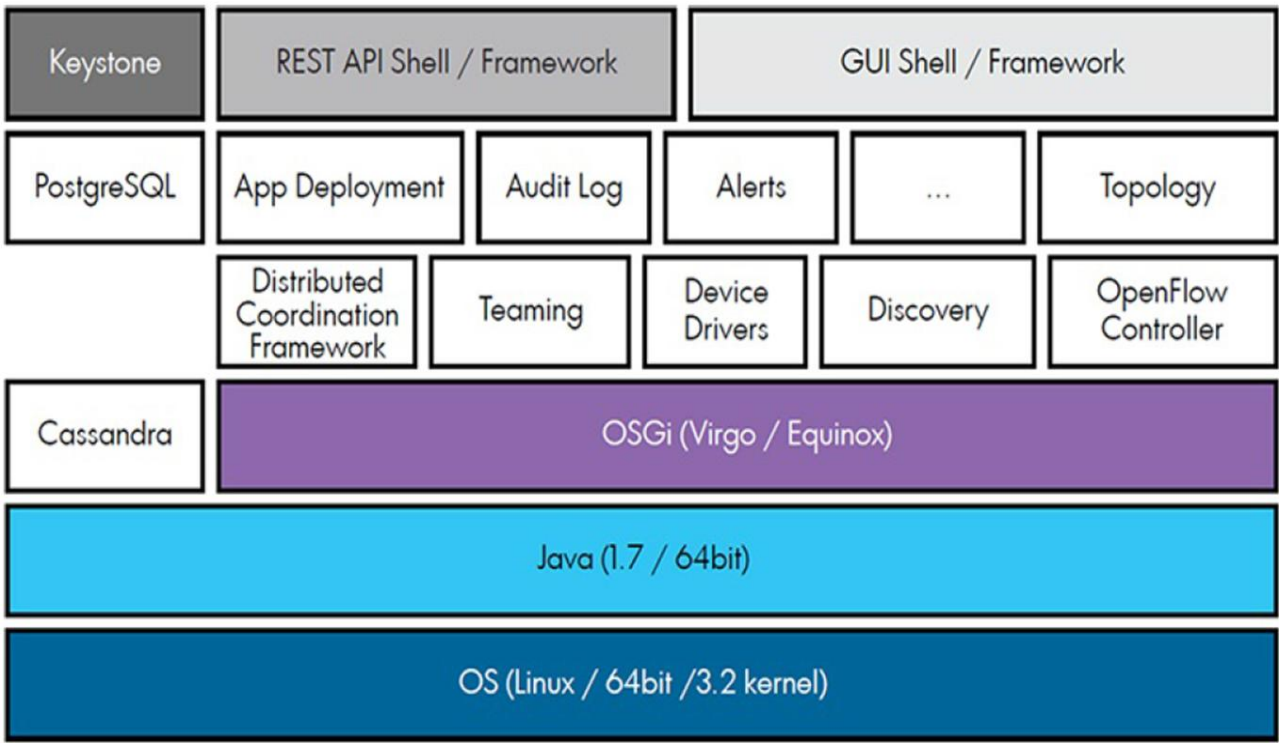
The HP Virtual Application Networks (VAN) SDN Controller забезпечує єдину контрольну точку в мережі з підтримкою SDN, спрощуючи управління та забезпечуючи оркестування (*orchestration*). Це дозволяє надавати нове покоління мережевих послуг на основі додатків. Він також забезпечує відкриті програмні інтерфейси (APIs), що дозволяє розробникам створювати інноваційні рішення для динамічного зв'язку бізнес-вимог до інфраструктури мережі через будь-які користувацькі програми Java або універсальні REST-інтерфейси керування.

Orchestration - автоматизоване аранжування, координація та керування комп'ютерними системами, проміжним програмним забезпеченням та службами.

Характеристики HP VAN SDN Controller:

- Платформа класу підприємства для широкого кола мережевих інновацій;
- Сумістна з протоколами OpenFlow 1.0 and 1.3;
- Підтримка більш ніж 50 моделей комутаторів HP із підтримкою OpenFlow;
- Відкритий APIs, що забезпечує розробку SDN додатків іншими виробниками;
- Розширювана, масштабована та стійка архітектура контролера.

Архітектура контролера HP VAN SDN приведена на малюнку.



Keystone - зовнішня служба, яка забезпечує аутентифікацію та послуги авторизації високого рівня. Вона підтримує аутентифікацію на основі токенів та використовується для захисту RESTful web-послуг (REST APIs) та веб-інтерфейсів користувача.

REST API Shell/Framework - В архітектурному стилі REST дані та функціональність розглядаються як ресурси і ці ресурси є доступними за допомогою уніфікованих ідентифікаторів ресурсів (URI), як правило посилань в Інтернеті. Архітектурний стиль REST умовно складається з клієнтів і серверів, які використовують протокол зв'язку, як правило, HTTP. Клієнти ініціюють запити до серверів; сервери обробляють запити та повертають відповідні відповіді. Запити та відповіді будуються навколо передачі представлень ресурсів. Клієнти та сервери обмінюються представленнями ресурсів, використовуючи стандартизовані інтерфейс і протокол. Ці принципи сприяють тому, що RESTful програми стають простими, легкими і мають високу продуктивність.

GUI Shell/Framework - Контролер HP VAN SDN також пропонує структуру програмної системи для розробки веб-інтерфейсів користувача: SKI Framework. SKI Framework забезпечує платформу, на якій розробники можуть створювати веб-додатки на основі браузера. Це набір інструментів, який надає активи, які програмісти можуть використовувати для побудови веб-інтерфейсу GUI (Graphical User Interface). Система SKI реалізує навігаційну модель, яка складається зі списку категорій вищого рівня, в якій кожна категорія складається зі списку навігаційних елементів. Кожен елемент навігації складається зі списку переглядів, в яких один з переглядів вважається типовим представленням.

PostgreSQL - використовується для збереження даних контролера та додатків.

App Deployment - Application Manager контролера дозволяє встановлювати, модернізувати, вмикати (запускати), відключати (зупиняти) та видаляти SDN додатки на контролері.

Audit Log - Записує події, пов'язані з діями, операціями та змінами конфігурації, ініційовані авторизованим користувачем.The Audit Log керує службою журналу перевірки контролера.

Backup and restore framework (не показано) - Контролер HP VAN SDN забезпечує створення резервної копії та відновлення контролера та стану додатків у файлі резервної копії. Файл резервної копії можна скопіювати та зберігати для подальшого використання. Збережений файл резервної копії можна завантажити до контролера.

Topology - Контролер використовує вбудовані програми Topology Manager і Topology Viewer для збору та відображення інформації про мережу OpenFlow.

Distributed Coordination Framework - Є однією з високодоступних функцій контролера. Це забезпечує інфраструктуру для комунікації контролер-контролер та координації інформації про стан контролерів в команді контролерів.

Teaming - Контролер HP VAN SDN може бути налаштований у команді. Служби спільної роботи (teaming services) контролера зберігають стан виконання кожного контролера в команді (активний, недоступний або призупинений) в актуальному стані та використовується іншими частинами контролера для функцій, пов'язаних з HA (high availability).

Device Drivers - Драйвери пристроїв. Моделюють можливості пристроїв і надають API для взаємодії з різними типами пристроїв.

Discovery - Контролер використовує вбудовані програми *OpenFlow Link Discovery* і *OpenFlow Node Discovery*, щоб відкрити інформацію про мережу OpenFlow.

OpenFlow Controller - Контролер OpenFlow (*також називається як ядро контролера*) обробляє з'єднання з пристроями OpenFlow і забезпечує засоби верхнього рівня програмного забезпечення для взаємодії з цими пристроями.

Apache Cassandra - Високопродуктивний, надзвичайно масштабований, відмовостійкий (немає жодної точки відмови), розподілений пост реляційних баз даних. Cassandra поєднує в собі всі переваги Google Bigtable та Amazon Dynamo для обробки типів потреб керування базами даних, які традиційні постачальники RDBMS не можуть підтримувати. Apache Cassandra використовується для зберігання даних програмних додатків.

OSGi (Virgo/Equinox) - Основний набір програмного забезпечення контролера використовує OSGi framework (Equinox) і контейнер (Virgo) як основу для модульного програмного забезпечення та забезпечує розподіл постачальника/споживача послуг. Програмне забезпечення, що працює в основному контейнері OSGi, може взаємодіяти з іншими компонентами, що працюють як інші процеси на контролері. Virgo, яка базується на Tomcat, є

розділом на основі серверу Java-додатків, призначеним для запуску корпоративних застосунків Java із високою гнучкістю та надійністю.

2.2 Програмні додатки, які вбудовані в контролер

Контролер HP VAN SDN є платформою для розробки та розгортання програмних додатків SDN.

Контролер HP VAN SDN - це розширювана платформа, що підтримує:

- *Власні (внутрішні)* програмні додатки - іноді називаються модулями;
- *Зовнішні* програмні додатки.

Власні (внутрішні) програмні додатки створюються на Java або сумісною мовою і розгортаються на контролері як збірки пакетів OSGi. Внутрішні програмні додатки використовують служби Java, які експортуються та рекламуються платформою контролера та іншими програмами.

Внутрішні програмні додатки можуть динамічно розширювати можливості REST API контролера, розширювати графічний інтерфейс контролера та інтегрувати його з системою авторизації та авторизації контролера. Внутрішні програмні додатки добре підходять, коли програмам потрібні часті взаємодії з низькою затримкою з мережевими пристроями.

Зовнішні програмні додатки можуть бути розроблені будь-якою мовою та розгортаються за межами платформи контролера або на тій же платформі, що й контролер. Зовнішні програмні додатки взаємодіють з контролером, використовуючи служби REST API, які експортуються та рекламуються платформою контролера, а також з власними (внутрішніми) програмними додатками, розгорнутими на контролері.

Оскільки зовнішні програмні додатки розгортаються поза платформою контролера, вони не можуть розширити можливості REST API або GUI контролера. Зовнішні програмні додатки підходять для програм, які мають відносно рідку та високолатентну взаємодію з мережевими пристроями, а також коли потрібне розгортання на різних платформах.

Базова платформа також включає в себе мережні служби (внутрішні програмні додатки), які забезпечують наступне:

- OpenFlow Link Discovery
- OpenFlow Node Discovery
- Path Daemon
- Path Diagnostics
- Topology Manager
- Topology Viewer

2.2.1 OpenFlow Link Discovery

Програма OpenFlow Link Discovery є програмою за замовчуванням, яка встановлюється разом з контролером.

Ця програма реалізує com.hp.sdn.supplier.LinkSuppliersBroker interface, LinksSupplierService, LinkService API для створення та підтримки інформації про зв'язки (links) для каналів передачі даних (datapath) OpenFlow, які реєструються в контролері.

Програма OpenFlow Link Discovery просуває модулі потоку (flow-mods) з пакетами відкриття, інжектує пакети відкриття на усі порти, усіх каналів передачі даних (datapath) і відкриває зв'язки (links) в контрольованій мережі, прослуховуючи повідомлення PACKET_IN.

The HPN SDN Controller інжектує та спостерігає за пакетами в контрольованій мережі, щоб виявити зв'язки між копіями OpenFlow. Виявлені зв'язки можуть бути одним із наступних типів:

- *Direct* - Зв'язки, які з'єднують один порт копії OpenFlow з іншим, без проміжних комутаторів.
- *Multihop* - Зв'язки, які з'єднують один порт копії OpenFlow з іншим, перетинаючи проміжні неконтрольовані комутатори. Неконтрольований комутатор є комутатором, який не має визначеної копії OpenFlow або підключений до контролера, який намагається виявити зв'язки.

The HPN SDN Controller відкриває зв'язки та визначає типи зв'язків шляхом інжектування двох пакетів в кожний порт копії OpenFlow.

Ці пакети мають один і той же тип Ethernet (0x8999), але надсилаються на різні MAC-адреси доставки. Зміст цих пакетів є пропрієтарним, але, як правило, включає в себе ідентифікацію копії OpenFlow та порту, звідки бере початок пакет. Пакети інжектуються негайно, як тільки комутатор підключається до контролера та періодично повторюється.

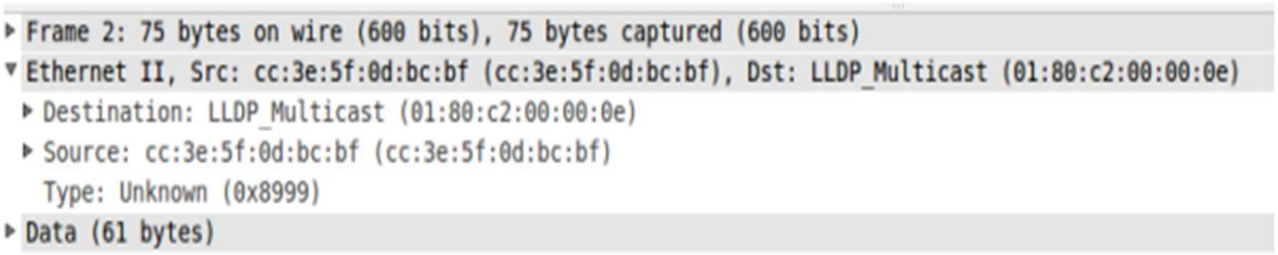
The HPN SDN Controller не має доступу до інформації відносно конфігурації VLAN або порта комутаторів, які розміщують в копії OpenFlow, яку він контролює. Тому ці сформовані пакети не містять заголовка 802.1Q, оскільки конфігурації VLAN і порта копії OpenFlow вимагає створення правильного тега VLAN.

Контролер генерує пакети для відкриття звязків:

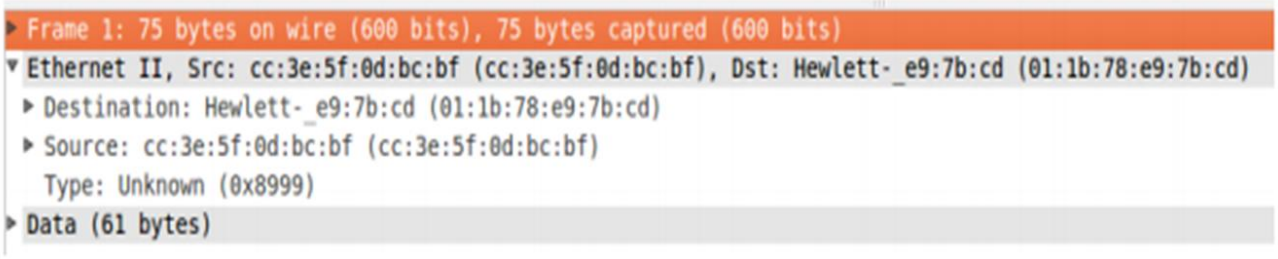
- Використовується нестандартний протокол, BDDP (Broadcast Domain Discovery Protocol), який використовує формат корисного навантаження (payload), подібний до LLDP (Link Layer Discovery Protocol).
- Надсилається або на link-local MAC address (to discover direct links) або multicast MAC address (to discover multihop links).
- The link-local MAC address is: 01:80:c2:00:00:0e.
- The multicast MAC address used for link discovery is: 01:1B:78:E9:7B:CD.
- Містить вихідний пристрій та порт, який ввів пакет в контрольовану мережу.

Нижче наведено приклади пакетів, які інжектуються для відкривання зв'язків:

Direct discovery packet sample:



Multi-hop discovery packet sample:



Програма OpenFlow Link Discovery прослуховує повідомлення PACKET_IN, що містять протокол BDDP. Кожен пакет відкриття (discovery packet) має ідентифікатор вихідного пристрою (source device), вбудований у його корисне навантаження, а цільовий пристрій (destination device) можна визначити із повідомлення PACKET_IN. Ця конструкція дозволяє програмі OpenFlow Link Discovery заповнити таблицю зв'язків (link table) інформацією, яку вона вивчає з таких отриманих пакетів.

Використовуючи інформацію про походження, що міститься в отриманому пакеті, контролер отримує адрес джерела та адрес призначення лінії зв'язку, між якими передається пакет і записує зв'язок між копіями OpenFlow.

Тип зв'язку визначається за допомогою MAC-адреси пакета (direct or multi-hop). Якщо зв'язок є прямим, він буде відкритий (will be discovered) одночасно як “direct” так і “multihop” зв'язок з відповідною копією OpenFlow, але оскільки тип "direct" має пріоритет над типом "multi-hop", тому посилання записується як "direct".

Якщо компонент конфігурації OpenFlow Link Discovery (com.hp.sdn.disco.of.link.impl.OpenflowLinkDiscovery Component) має режим age.multihop.links=true, OpenFlow Link Discovery періодично інжектує пакети відкриття у контрольовану мережу для оновлення “multihop” зв'язків. Будь який “multihop” зв'язок, який не оновлений протягом інтервалу, визначеного для multihop.poll.interval key вважається не дійсним та видаляється із таблиці зв'язків.

Крім того, мережеві події, такі як “падіння” порту або зміна статусу пристрою, призводить до вилучення відповідних зв'язків з таблиці зв'язків і викликає направлення пакетів відкриття до всіх каналів передачі даних (datapaths), які знаходяться в стані готовності.

2.2.2 OpenFlow Node Discovery

Програма OpenFlow Node Discovery є програмою за замовчуванням, яка встановлюється разом з контролером.

Ця програма реалізує com.hp.sdn.supplier.LinkSuppliersBroker, interface uses LinkSupplierService, LinkService APIs для створення та підтримки інформації про вузли (nodes) для каналів передачі даних (datapath) OpenFlow, які реєструються в контролері.

Якщо конфігурація ControllerManager має hybrid.mode=false, всі пакети неявно викрадаються контролером та обробляються програмою OpenFlow Node Discovery. Якщо learn.ip=true, программа відкривання вузлів у цьому випадку використовує ARP, DHCP та IP пакети для відкривання хостів.

Якщо ControllerManager configuration має режим hybrid.mode=true:

Програма OpenFlow Node Discovery просуває модулі потоку (flow-mods) на керовані пристрої, які копіюють пакети ARP або DHCP до контролера для обробки і прослуховує повідомлення PACKET_IN, що містять протоколи ARP або DHCP.

За замовчуванням у гібридному режимі IP-пакети не надсилаються контролеру. На підставі інформації, що поставляється цими скопійованими ARP, DHCP, тільки якщо learn.ip = true, програма OpenFlow Node Discovery надсилає IP-пакети для оновлення таблиці вузлів.

Лише коли learn.ip = true, інші програми також просувають потік, який надсилає IP-пакети до контролера.

Node Manager не оновлює таблицю вузлів для кожного отриманого повідомлення PACKET_IN. Зокрема, повідомлення PACKET_IN ігноруються, якщо підключений порт ідентифікується Topology Manager як частина інфраструктури.

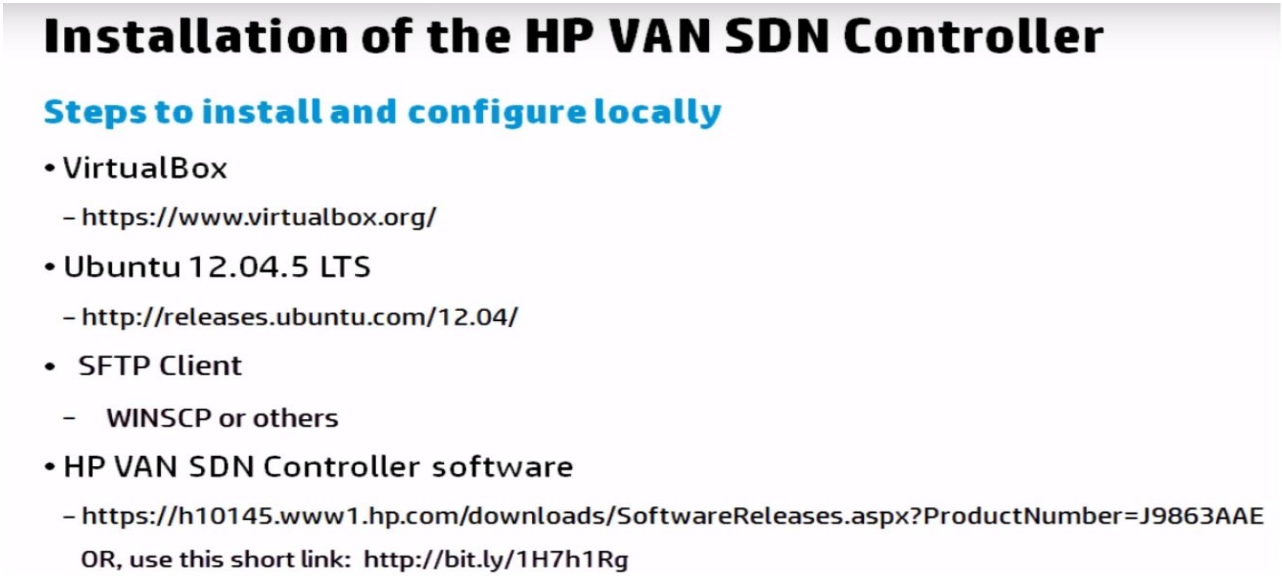
Якщо компонент конфігурації OfIpDiscoveryComponent learn.ip=true, програма OpenFlow NodeDiscovery також прослуховує повідомлення PACKET_IN, що містять IP-протокол, але явно не запускає модулі потоки для керованих пристроїв, які відправляють IP-пакети, оскільки це призведе до суттєвого зниження продуктивності мережі через перевагу контрольної площини.

2.3 Інсталяція контролера HP VAN SDN на сервер

Процес інсталяції контролера HP VAN SDN може значно відрізнятися залежно від версії, яку ви встановлюєте. Перед початком інсталяції перегляньте інструкцію із встановлення.

HP VAN SDN Controller 2.5.20 Installation Guide знаходиться за наступною адресою: http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04647290.

На малюнку наведені кроки, які необхідно виконати для встановлення контролера HP VAN SDN на сервер.



Для допомоги виконання кожного кроку встановлення контролера HP VAN SDN на сервер можна переглянути наступні відео:

1. Download and install Virtual Box and Ubuntu
https://www.youtube.com/watch?v=UbwD1c7R87s
2. Install Ubuntu
https://www.youtube.com/watch?v=P2syT0-wwmI
3. HP Controller software download and unpacking
https://www.youtube.com/watch?v=zwTZ6oYHKUI
4. HP Controller Install and Verify
https://www.youtube.com/watch?v=gaBSHna8v4E

To download the HP VAN SDN Controller software:

1. Go to the HP Networking support site http://bit.ly/1H7h1Rg.
2. Enter the HP VAN SDN base product number J9863AAE in the Auto Search field.
3. Select the check box next to the HP VAN SDN Controller product and then click Display selected.
4. In the lower right quadrant of the product display screen, click Software downloads.
5. On the My Networking Download software screen, select and download the VAN_SDN_Controller_v2.5.X software package (.zip file) to your local computer.
6. Unzip the software package.

sudo service sdnc (*sdna) status* command використовується для перевірки того, що служба ядра контролера стартувала:

- *sdnc* - є головною службою SDN контролера.
- *sdna* - є службою SDN адміністратора, яка використовується для віддаленого адміністрування через REST API (controller stop, start, restart, log download, reboot, and so forth).

```
sdn@sdnctl:~$ sudo service sdnc status
sdnc start/running, process 1629
sdn@sdnctl:~$
```

```
sdn@sdnctl:~$ sudo service sdna status
sdna start/running, process 1624
sdn@sdnctl:~$
```

Після встановлення Контролера та його перевірки за допомогою команд *sudo service sdnc status* and *sudo service sdna status* що його служби запущені, можна здійснити перевірку для підтвердження запуску служб Контролера.

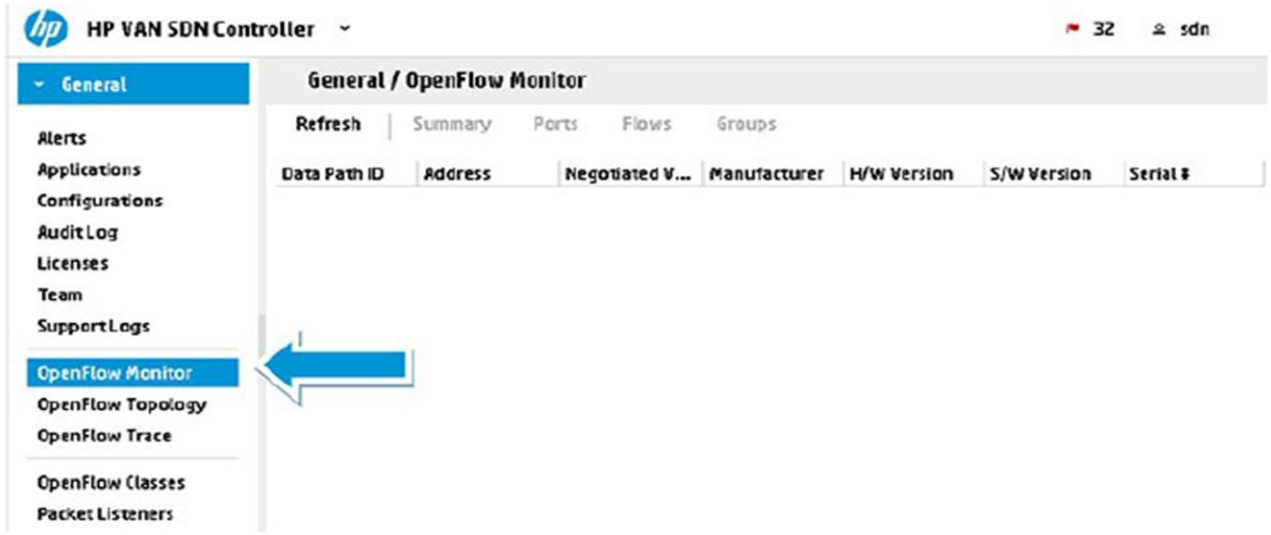
Щоб це зробити, необхідно здійснити навігацію до веб-інтерфейсу Контролера за допомогою браузера Chrome. Необхідно використати IP-адресу Контролеру, номер порту та */sdn/ui*.

Наприклад, якщо IP-адрес 192.168.56.11, можна здійснити навігацію до інтерфейсу, використовуючи наступний адрес: *192.168.56.11/8443/sdn/ui.*

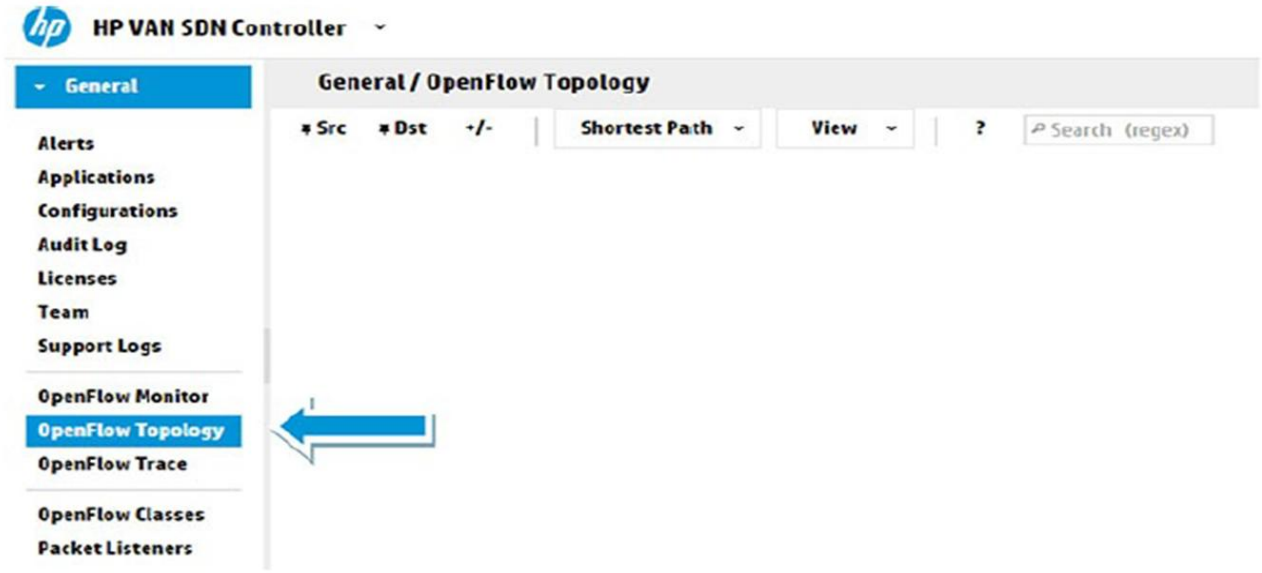
HP VAN SDN Controller за замовчуванням використовує самопідписаний сертифікат. Тому браузер може відображати помилку конфіденційності, якщо сертифікат раніше не був прийнятий. Для прийняття сертифікату, клікніть *Advanced*.

Коли з'явиться запит, увійдіть, використовуючи ім'я користувача та пароль Keystone. У деяких попередніх версіях контролера HP VAN SDN, у Keystone було створено стандартне ім'я користувача *sdn* та пароль *skyline.*

Клікніть *OpenFlow Monitor* (дивись на малюнку). На цей момент, OpenFlow-enabled мережні пристрої не мають з’єднання з HP VAN SDN Controller. У більшості випадків в OpenFlow середовищі, комутатори OpenFlow взаємодіють з Controller, використовуючи заздалегідь визначений порт TCP 6633 для OpenFlow 1.3.2).



Клікніть *OpenFlow Topology* (дивись на малюнку). Як і в попередньому випадку, на цей момент, жодного мережного пристрою не приєднано до HP VAN SDN Controller.

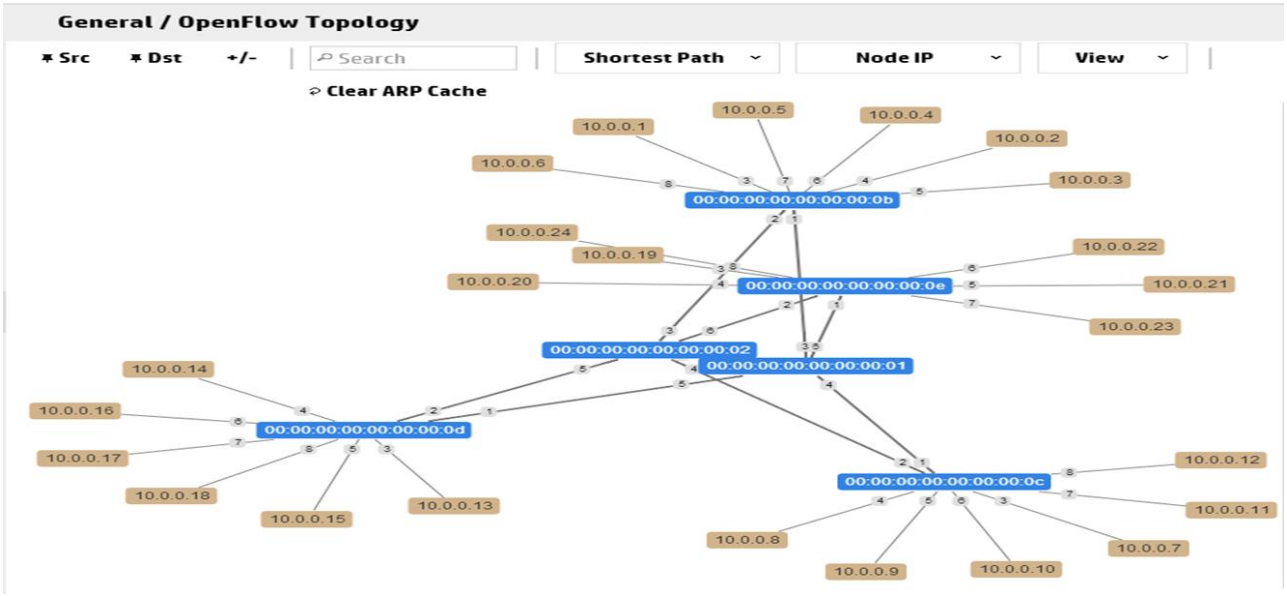


2.4 Інтеграція Mininet з HP VAN SDN Controller та використання Mininet для створення віртуальної комутованої мережі

Mininet - це мережевий емулятор, а не симулятор. Емулятор для цієї дискусії визначається наступним чином: запуск немодифікованого коду в інтерактивному режимі, на віртуальному обладнанні, на звичайному ПК. Це забезпечує зручність та реалізм при низькій вартості (з деякими обмеженнями, такими як швидкість).

Команда sudo mn запускає середовище Mininet. Це віртуалізує мережу пристроїв і хостів, які працюють як реальні пристрої. Ви можете запускати програми на хост-пристроях (наприклад, веб-сервері) або переглядати таблиці OpenFlow на комутаторах. Програми на хостах можуть надсилати пакети через інтерфейси комутатора, які можуть бути налаштовані на різну швидкість і затримку. Пакети обробляються точно так же, як і реальним комутатором Ethernet або маршрутизатором з заданою кількістю черги. Такі програми, як iPerf, також можуть використовуватися для вимірювання продуктивності.

Як показано на малюнку, Mininet емулює різні топології мережі, що складаються з віртуальних хостів (кінцевих хостів), комутаторів, контролерів та зв'язків на одному ядрі Linux.



Mininet підтримує дослідження, розробку, демонстрацію, вивчення, тестування, налагодження та будь-які інші завдання, які можуть мати користь від повної експериментальної мережі на ноутбуці або іншому ПК.

Топології різних розмірів можна створити простими командами, такими як *sudo mn* (один комутатор і два хоста) або *sudo mn --topo linear,4* (чотири комутатори та чотири хоста). Це дозволяє швидко редагувати, запускати та тестувати різні середовища SDN.

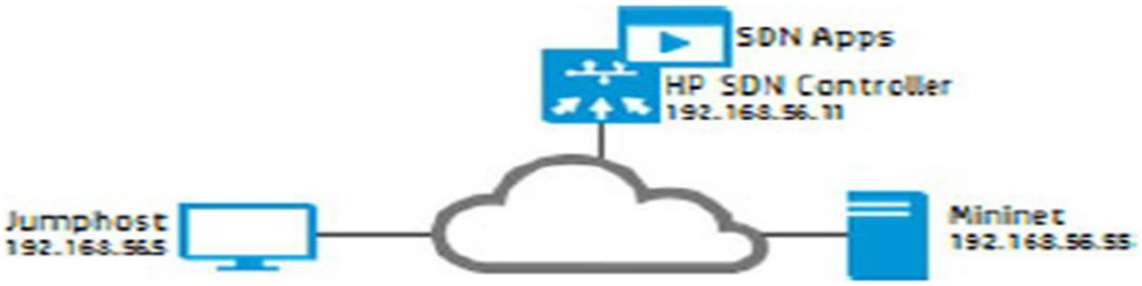
Користувальницькі топології можуть також бути створені для моделювання дуже великих центрів обробки даних або інших великих мереж. За допомогою Mininet було успішно завантажено до 4096 хост-пристроїв.

На хостах Mininet можуть також працювати реальні програми, такі як веб-сервер, DNS-сервер, інструменти моніторингу вікон TCP або Wireshark. Все, що працює на Linux, можна запустити на Mininet.

Комутатори Mininet можна програмувати за допомогою протоколу OpenFlow. Mininet підтримує віддалені (встановлені на іншому сервері) та зовнішні контролери (зовнішні від Mininet). У цьому курсі ми будемо використовувати контролер HP VAN SDN для керування комутаторами Mininet.

Розроблені мережі SDN можна моделювати та тестувати, використовуючи Mininet та програмні додатки SDN, перш ніж вони будуть розгорнуті на апаратних засобах комутаторів OpenFlow.

Як і багато інших мережевих систем віртуалізації, доступних для фізичних маршрутизаторів і комутаторів, таких як HP VSR або Simware, головною перевагою Mininet є те, що складні мережі можуть бути створені для демонстрації, вивчення та тестування. Як показано на малюнку, замість використання фізичних мережевих пристроїв або віртуальних машин, що працюють під керуванням операційних систем, таких як Windows або Linux для хостів, або намагаються підключитися до віддаленої мережі, повну топологію можна швидко і легко створити на одному комп'ютері .



Інтеграція Mininet та HP VAN SDN Controller забезпечує велику кількість переваг, які включають:

- Mininet базується на Open vSwitch. Mininet є не симулятором, а емулятором комутатора. Open vSwitch є продуктивним багаторівневим віртуальним комутатором подібним до VMware's vSwitch, HP VSR або Cisco Nexus 1000V.
- Інтеграція Mininet з HP VAN SDN Controller. Це дозволяє переглядати топології за допомогою додатку Topology Viewer контролера OpenFlow. Потокові записи (flow entries) для комутаторів Mininet також можна переглядати та керувати за допомогою API контролерів.
- Комутатори та топології завантажуються протягом декількох секунд, а не хвилин.
- Може бути створена мережа із сотень хостів і комутаторів.
- Mininet мережі створюються на одному ПК і є більш масштабованими у порівнянні із запуском кожного вузла на окремій VM.
- При демонстрації технологій OpenFlow та SDN не потрібно транспортувати фізичне обладнання або підключатися до віддалених лабораторій.
- Дуже швидко і легко переналаштувати та перезапустити топології.
- Програми SDN можуть бути перевірені на різних топологіях без їх відновлення.

Мережі на основі Mininet не можуть перевантажити процесор або пропускну здатність, які доступні на одному сервері. Mininet також може запускати лише Linux-сумісні OpenFlow-комутатори або програми.

Існують обмеження на Mininet, такі як ресурси, доступні для Mininet та обмеження ресурсів хост-системи. Ресурси на єдиній системі будуть розподілені між хостами Mininet і комутаторами, що працюють в цій системі.

Mininet використовує єдине ядро Linux для всіх віртуальних хостів. Не підтримується програмне забезпечення, яке залежить від інших операційних систем, таких як Microsoft Windows.

Mininet взаємодіє з контролерами OpenFlow. Контролер може бути використаний для оновлення таблиць потоку на комутаторах Mininet. У цьому курсі використовується контролер HP VAN SDN.

Далі наведені інструкції щодо використання Mininet для підключення віртуальних комутаторів OpenFlow до контролера HP VAN SDN. Для цього припустимо, що Mininet OVA завантажено на мережевий сервер і ви

використовуєте PuTTY на віртуальній машині Windows для підключення до сервера Mininet за допомогою SSH. Також припустимо, що ви маєте логін користувача та пароль для Mininet. Якщо ви успішно підключились, то повинні побачити щось подібне до наступного:

```
login as: mininet
mininet@192.168.56.55's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Mon Jun 22 08:29:04 2015 from 192.168.56.5
mininet@mininet-vm:~$
```

Можна використати команду ping –c для перевірки наявності зв'язку між контролером та Mininet:

```
mininet@mininet-vm:~$ ping -c 5 192.168.56.11
PING 192.168.56.11 (192.168.56.11) 56(84) bytes of data.
64 bytes from 192.168.56.11: icmp_seq=1 ttl=64 time=1.62 ms
64 bytes from 192.168.56.11: icmp_seq=2 ttl=64 time=0.351 ms
64 bytes from 192.168.56.11: icmp_seq=3 ttl=64 time=0.471 ms
64 bytes from 192.168.56.11: icmp_seq=4 ttl=64 time=0.533 ms
64 bytes from 192.168.56.11: icmp_seq=5 ttl=64 time=0.423 ms
--- 192.168.56.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.351/0.681/1.629/0.478 ms
mininet@mininet-vm:~$
```

Рекомендовано очистити топології Mininet для видалення будь-яких фантомних процесів за допомогою команди sudo mn -c. Зробіть це, щоб в пам'яті не залишилося колишніх топологій:

```
mininet@mininet-vm:~$ sudo mn -c

*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes

killall controller of protocol of datapath ping nox_core lt-nox_core ovs-openflowd ovs-
controller udpbwtest mnexec ivs 2> /dev/null

...<omitted>...

*** Removing all links of the pattern foo-ethX

ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'

*** Killing stale mininet node processes

pkill -9 -f mininet:

*** Shutting down stale tunnels

pkill -9 -f Tunnel=Ethernet

pkill -9 -f .ssh/mn

rm -f ~/.ssh/mn/*

*** Cleanup complete.

mininet@mininet-vm:~$
```

Список команди Mininet, які ви можете побачити у подальшому у цьому курсі. Команди чутливі до регістру.

Command Value	**Meaning**
sudo	Sudo or “substitute user id do” allows users to run programs with the security privileges of another user—in this case with root privileges.
mn	Mininet application.
--controller=remote	Use a remote OpenFlow controller rather than the local built-in Mininet controller.
ip=192.168.56.11	Example IP address of the HP VAN SDN Controller used in this study guide.
--topo=linear,4	Create a linear topology of four switches. In a linear topology, each switch has a single host attached and is connected back-to-back to other switches in the topology.
exit	Exit Mininet
-c	Clear Mininet processes
--mac	Assigns each host a sequential MAC address
--controller=remote, ip=<controller_ip_address>	Option for using a remote controller
\	Option for splitting commands across multiple lines
--switch=ovsk	Option for using kernel mode Open vSwitch
Protocols=OpenFlow13	Option to negotiate with the controller to use OpenFlow 1.3

Щоб створити топологію з чотирма вимикачами, з'єднаними лінійним способом (зворотний зв'язок), кожен з яких має єдиний хост, підключений до нього, використовуйте команду:

```
sdn@ubuntu:~$ sudo mn --controller=remote,ip=192.168.56.11
--topo=linear,4
```

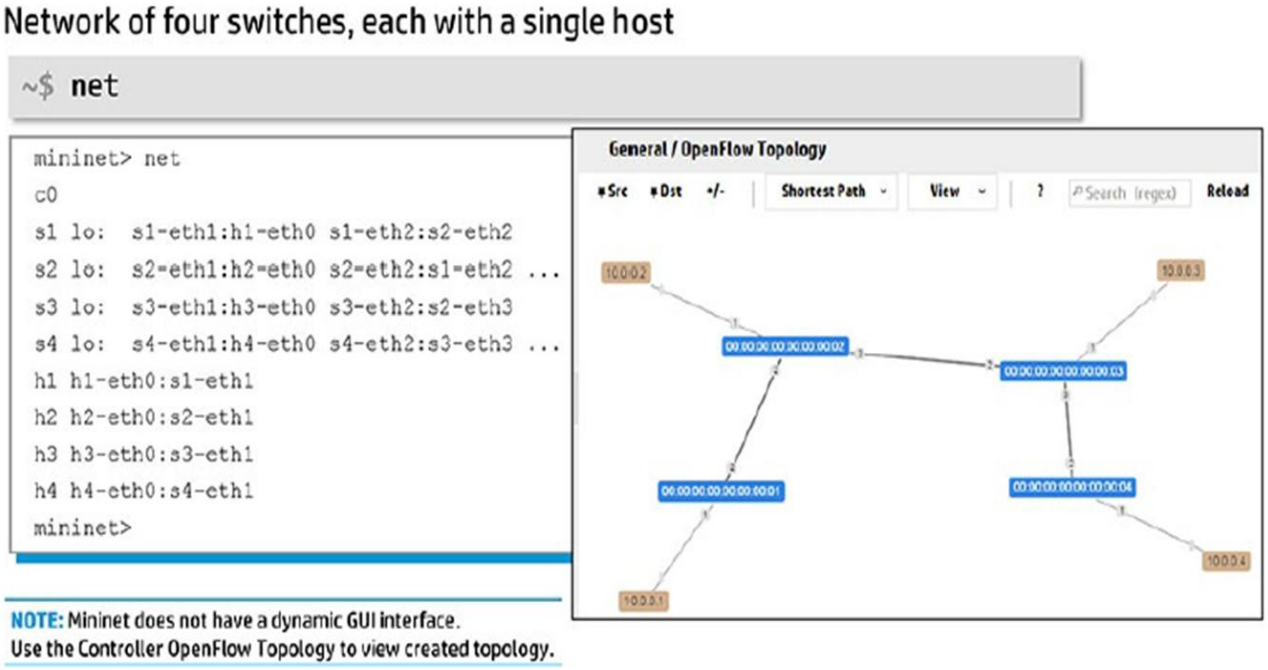
Результатом виконання цієї команди є наступний результат:

```
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2 h3 h4
*** Adding switches:
s1 s2 s3 s4
*** Adding links:
(h1, s1) (h2, s2) (h3, s3) (h4, s4) (s1, s2) (s2, s3) (s3, s4)
*** Configuring hosts
h1 h2 h3 h4
*** Starting controller
*** Starting 4 switches
s1 s2 s3 s4
*** Starting CLI:
mininet>
```

Щоб побачити створену топологію в Mininet, необхідно використати команду *net*:

```
mininet> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s2-eth1
h3 h3-eth0:s3-eth1
h4 h4-eth0:s4-eth1
s1 lo: s1-eth1:h1-eth0 s1-eth2:s2-eth2
s2 lo: s2-eth1:h2-eth0 s2-eth2:s1-eth2 s2-eth3:s3-eth2
s3 lo: s3-eth1:h3-eth0 s3-eth2:s2-eth3 s3-eth3:s4-eth2
s4 lo: s4-eth1:h4-eth0 s4-eth2:s3-eth3
c0
mininet>
```

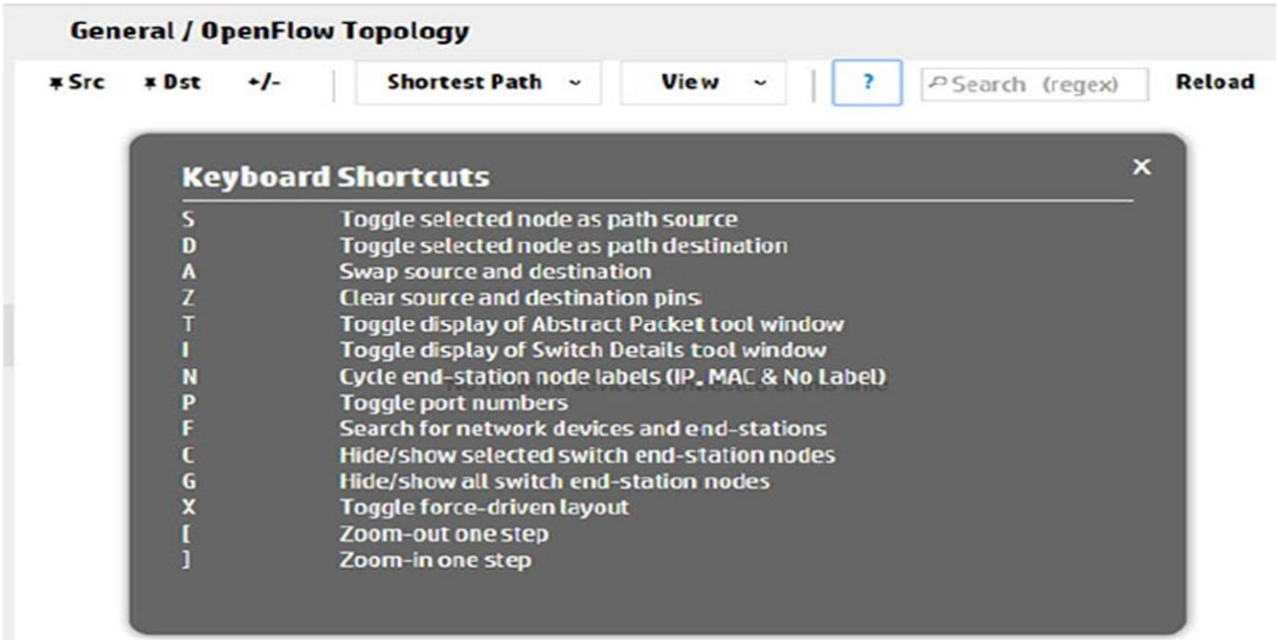
Mininet не має графічного інтерфейсу, який динамічно оновлюється. Необхідно використати HP VAN SDN Controller OpenFlow Topology для того, щоб побачити створену топологію. Малюнок надає знімок екрану цієї сторінки.



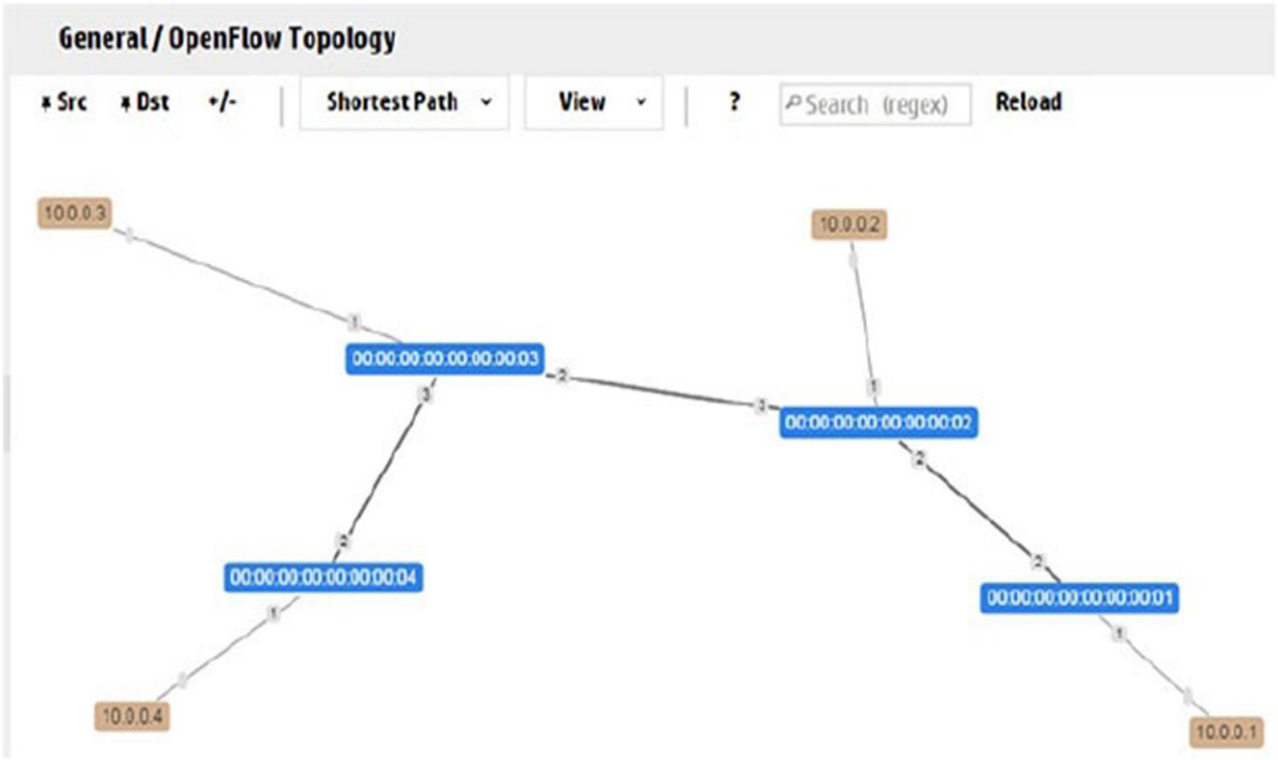
Комутатори Mininet взаємодіють з контролером SDN за допомогою порту OpenFlow за замовчуванням 6633. Таким чином, комутатори автоматично з'являться на діаграмі контролера OpenFlow.

Контролер може виявляти хости лише тоді, коли вони надсилають ARP, DHCP або інший трафік для комутаторів з підтримкою OpenFlow. Хости не появляються на діаграмі OpenFlow Topology, так як Mininet хости не генерують трафік доки не отримають інструкцію. Mininet необхідно чітко надати інструкцію відправляти трафік хоста для того, щоб хости були відкриті.

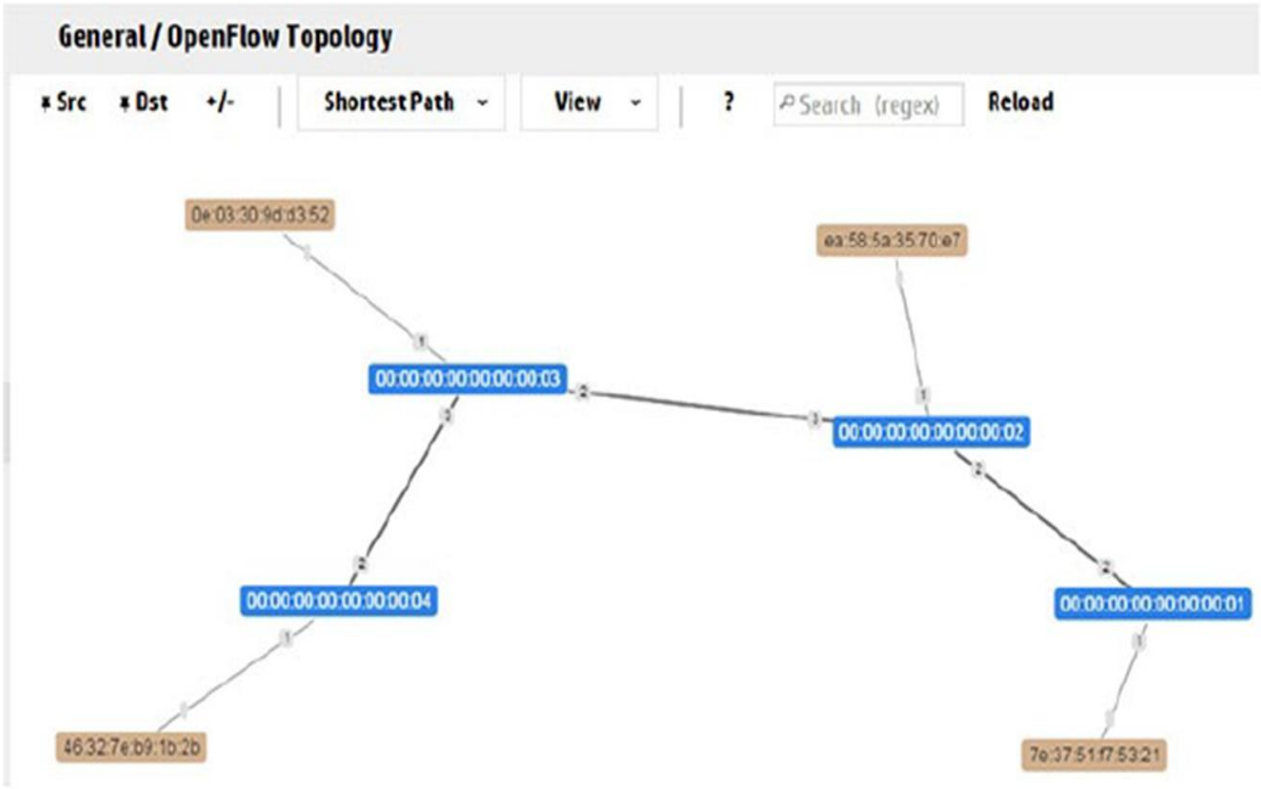
Сторінка HP VAN SDN Controller Topology містить комбінації клавіш, які ви бачите на малюнку, які можна переглянути, натиснувши символ позначки запиту (?) у верхній частині сторінки.



Наприклад, клавіша *n* показує кінцеві вузли як IP-адреси, MAC-адреси або без них. Малюнок ілюструє результат натискання клавіші *n* один раз.



Малюнок показує результат натискання клавіші *n* повторно.



За замовчуванням, хости починають з випадково призначених MAC-адрес. Це може зробити налаштування складним. Як показує малюнок, кожного разу, коли створюється топологія Mininet, MAC-адреси змінюються, тому корелюючий контроль трафіку з конкретними хостами є складним.

Опція *--mac* присвоює кожному хосту послідовну MAC-адресу, що відповідає IP-адресу.

```
$ sudo mn --mac
```

BEFORE

```
sdn@ubuntu:~$ sudo mn
...
mininet> h1 ifconfig
h1-eth0   Link encap:Ethernet  HWaddr ce:be:58:0b:06:75
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
```

AFTER

```
sdn@ubuntu:~$ sudo mn --mac
...
mininet> h1 ifconfig
h1-eth0   Link encap:Ethernet  HWaddr 00:00:00:00:00:01
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
```

Mininet підтримує OpenFlow версії 1.3. На наступних рисунках показані різні параметри, які доступні при створенні топології Mininet.

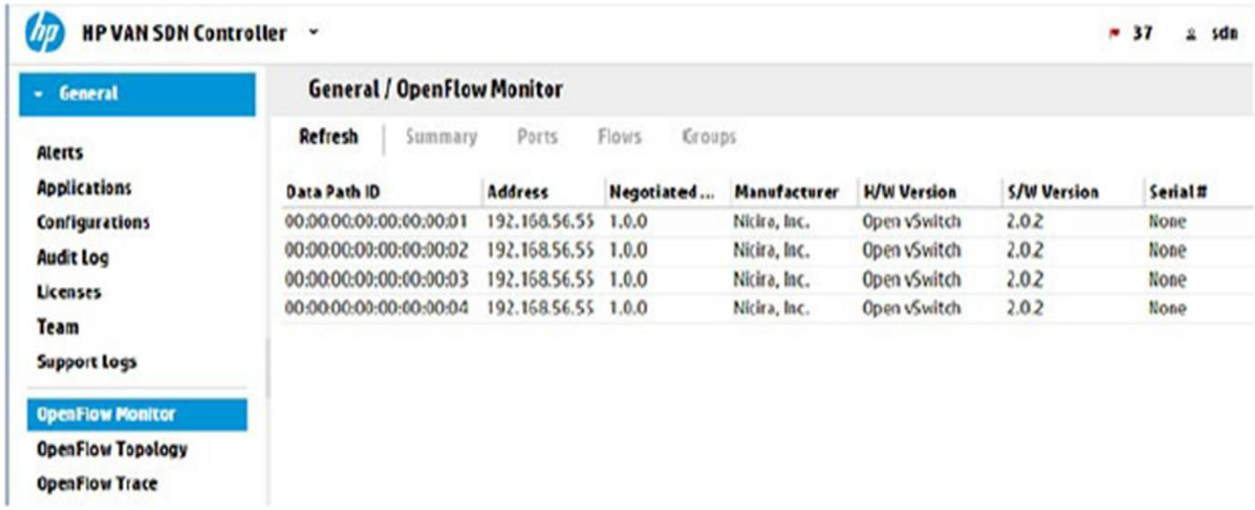
OpenFlow 1.3:

```
~$ sudo mn --controller=remote,ip=192.168.56.11 --topo=linear,4 \
--switch=ovsk,protocols=OpenFlow13 --mac
```

- `--controller=remote,ip=192.168.56.11`: Use a remote controller
- `--topo=linear,4`: Create a lineartopology
- `\`: Split commandacross multiplelines
- `--switch=ovsk`: Use kernel mode Open vSwitch
- `protocols=OpenFlow13`: Negotiate with controllerto use OpenFlow 1.3
- `--mac`: Allocate MAC addressto hosts (easy to read)
- Note:The command is case sensitive

У ілюстрованому прикладі використовується зовнішній контролер з IP-адресою 192.168.56.11, а не вбудований контролер Mininet. Побудовано лінійну топологію з чотирма комутаторами, а комутатори налаштовані на використання OpenFlow 1.3 з контролером.

HP VAN SDN Controller OpenFlow Monitor містить основну інформацію про комутатори OpenFlow, які налаштовані на контролері.



Наприклад, OpenFlow Monitor на малюнку показує, що узгоджена версія OpenFlow - 1.0.0. Контролер HP VAN SDN підтримує версії OpenFlow від 1,0 до 1,3. Комутатори HP ProVision підтримують OpenFlow 1.0 та 1.3. Комутатори HP Comware підтримують лише OpenFlow 1.3. Mininet підтримує OpenFlow 1.0 і 1.3.

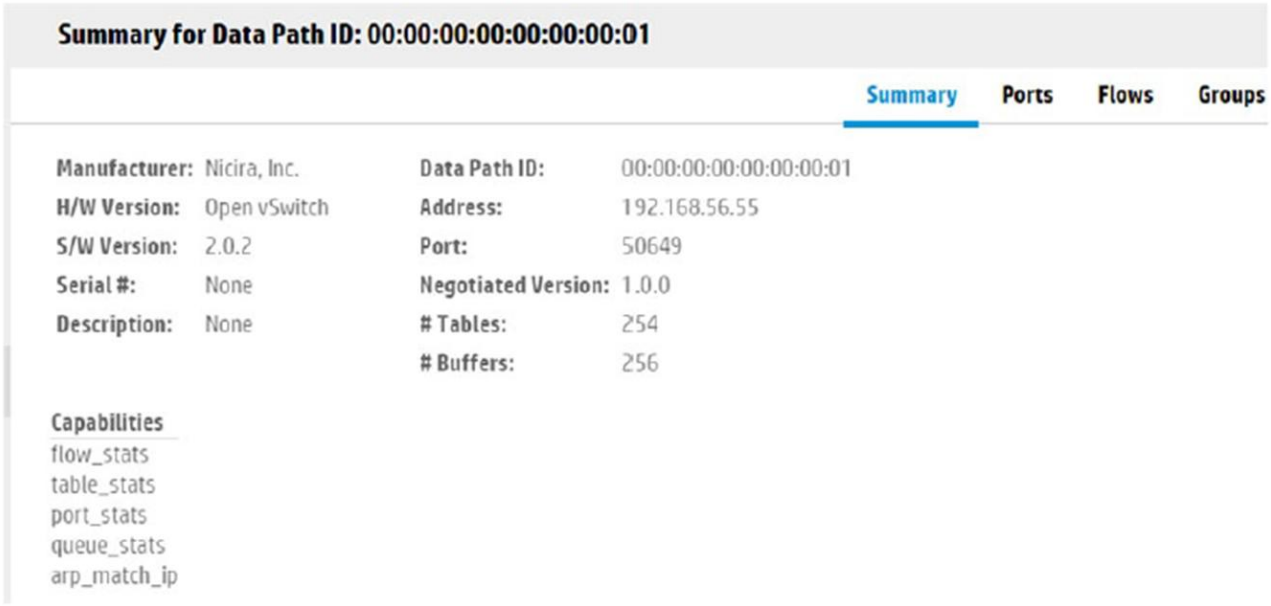
На малюнку також показано, що Nicira Inc. (придбаний компанією VMware) випускає всі комутатори, апаратна версія цих перемикачів - Open vSwitch, а версія ОС 2.0.2.

Комутатори OpenFlow ідентифікуються за допомогою *Data Path IDs (DPIDs)*. Це 64-бітне число, що складається з двох частин:

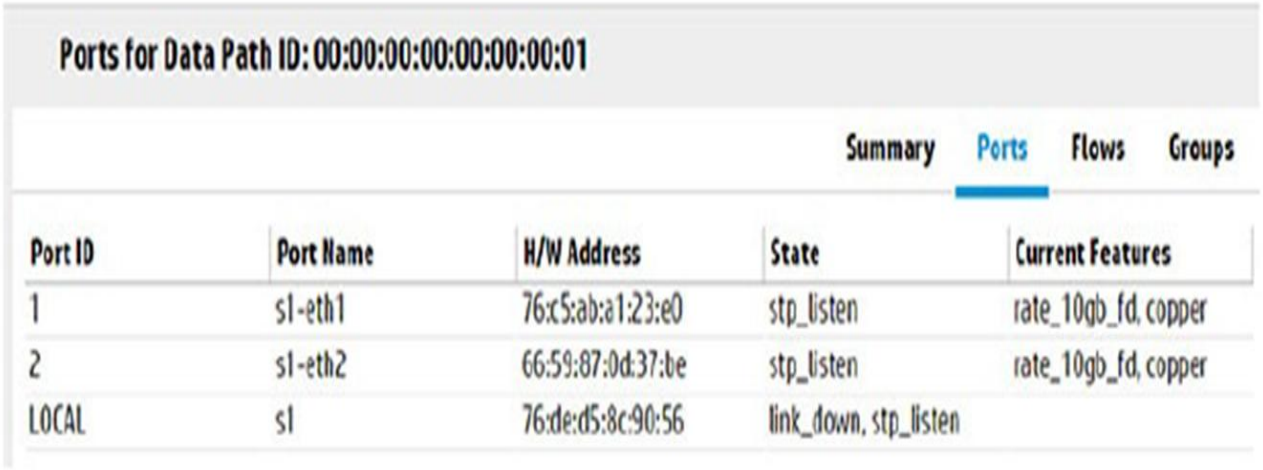
- Most significant 16 bits: визначають специфічного вендора. Комутатори Mininet за замовчуванням мають значення 00:00.
- Least significant 48 bits: MAC-адрес комутатора. Комутатори Mininet використовують значення, яке легко читається - 00:00:00:00:00:01.

Якщо ви хочете вибрати перемикач, який має DPID 00:00:00:00:00:00:00:01 і потім клацнути *Summary*, в режимі перегляду відображатиметься різноманітна інформація про комутатор, включаючи можливості, підтримувана версія OpenFlow та підтримувані дії.

OpenFlow Monitor *Summary* відображає інформацію про Data Path IDs (DPIDs) 00:00:00:00:00:01.

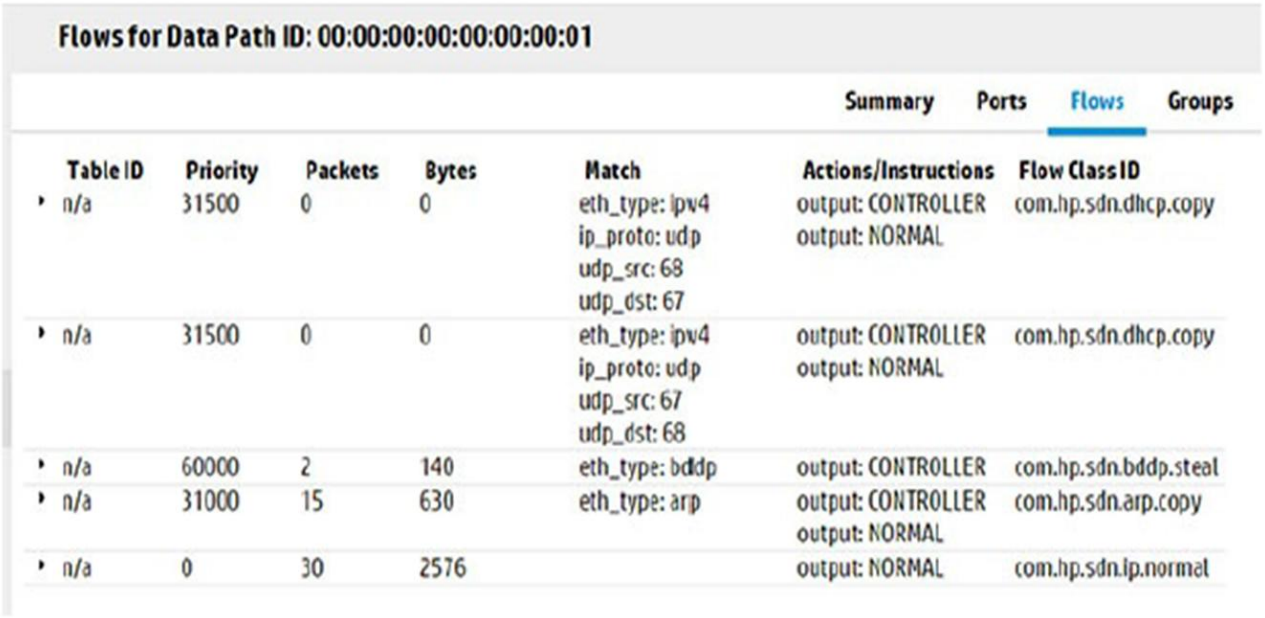


OpenFlow Monitor *Ports* надає інформацію про усі порти, які доступні на комутаторі.



Відповідно до малюнку, три порти доступні на комутаторі. Порти 1 і 2 є портами Ethernet. Це будуть фізичні порти на фізичному комутаторі OpenFlow. Локальний порт - це інтерфейс управління на комутаторі. Наведено також іншу інформацію, таку як стан і швидкість STP. Про це ми детальніше поговоримо далі у цьому курсі.

OpenFlow Monitor *Flows* забезпечує перегляд таблиці потоку OpenFlow.



Flows for Data Path ID: 00:00:00:00:00:00:00:01

Summary | Ports | Flows | Groups

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
n/a	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
n/a	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
n/a	60000	2	140	eth_type: bddp	output: CONTROLLER	com.hp.sdn.bddp.steal
n/a	31000	15	630	eth_type: arp	output: CONTROLLER output: NORMAL	com.hp.sdn.arp.copy
n/a	0	30	2576		output: NORMAL	com.hp.sdn.ip.normal

Table ID у цьому прикладі встановлено n/a, а це означає, що використовується OpenFlow 1.0. У OpenFlow 1.0 комутатор розглядається як такий, що має єдину таблицю потоку (flow table) і контролер не має видимості таблиць потоків у конвеєрі. У наступних версіях OpenFlow в конвеєрі доступні кілька таблиць.

Поле **Priority** визначає порядок потоків. Чим вище пріоритет відповідного потокового запису (flow entry), тим більше імовірність того, що запис може бути співставленим.

Поле **Match** використовується для співставлення вхідного трафіку. Це співставляється з полем у заголовку пакетів, наприклад MAC-адресою джерела, IP-адресою призначення, номером порту джерела та ін., Про це ми будемо обговорювати більш докладно пізніше у навчальному курсі. *Перші два записи* на малюнку співставляються з DHCP трафіком. Третій запис співставляється з Broadcast Domain Discovery Protocol (BDDP), який використовується для відкриття зав'язків між комутаторами. Протокол BDDP у подальшому буде розглянуто детально. *Четвертий запис* співставляється з ARP трафіком і використовується для відкриття хостів (вузлів) у топології. *Останній запис* має назву таблиці пропусків (table miss). Це співставляється з усім (порожнє поле відповідності). У цьому прикладі трафік передається на порт NORMAL, який надсилає трафік на традиційний маршрутизатор та комутаційний конвеєр на комутаторі.

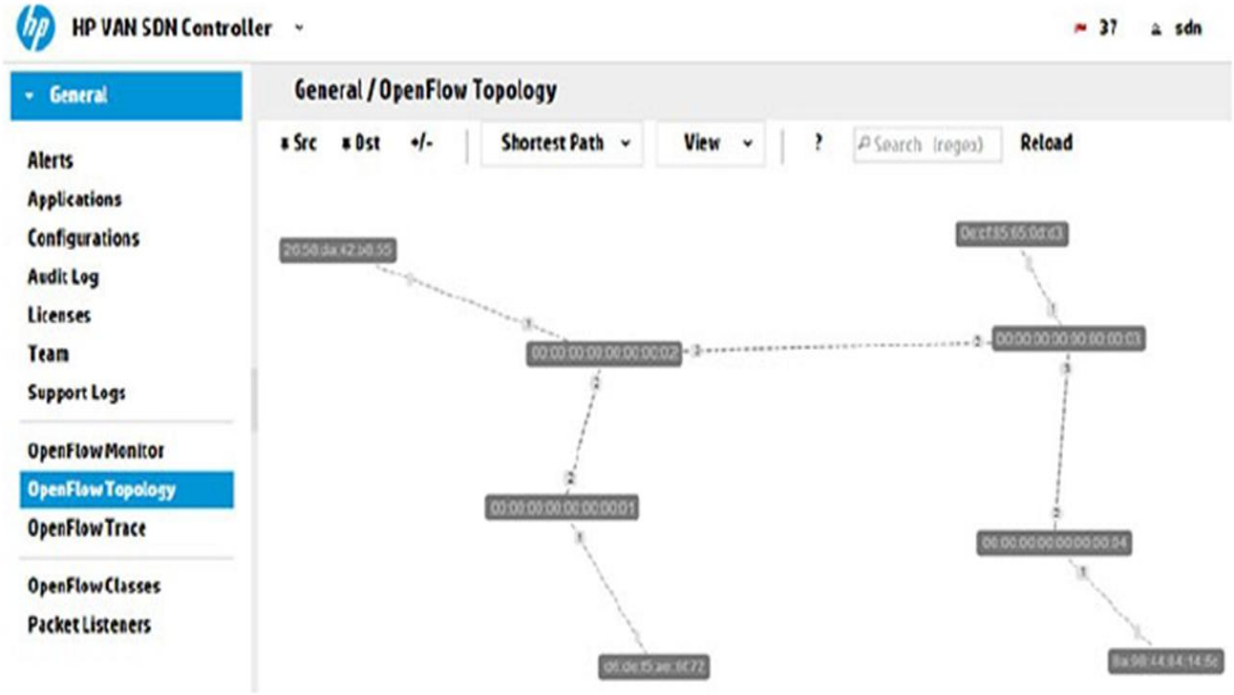
Actions/Instructions. Action (OpenFlow 1.0) або Instruction (OpenFlow 1.3) визначає, що трапиться з трафіком. DHCP трафік у цьому прикладі має вихід на порт NORMAL (відправляє на конвеєр традиційного комутатора) і на контролер. Це відомо як "копія" і дозволяє контролеру вивчати хости (вузли) мережі. Вхід протоколу BDDP відомий як “викрадання” та перенаправляє BDDP трафік на HP VAN SDN Controller. Це дозволяє контролеру HP VAN SDN видаляти трафік BDDP з мережі. Отже, єдиним вихідним портом є CONTROLLER. BDDP використовується для відкриття топології мережі. Це буде розглянуто детально у подальшому. Вхід ARP

також копіюється як на конвеєр традиційного комутатора (NORMAL порт), так і на контролер (порт CONTROLLER).

Використання команди виходу аналогічно вимкненню всіх пристроїв у фізичній мережі.

```
mininet> exit
*** Stopping 1 controllers
c0
*** Stopping 4 switches
s1 ..s2 ...s3 ...s4 ..
*** Stopping 7 links
*** Stopping 4 hosts
h1 h2 h3 h4
*** Done
completed in 3776.970 seconds
mininet@mininet-vm:~$
```

Коли ви вводите цю команду, пристрої на HP VAN SDN Controller OpenFlow Topology спочатку мають бути сірими, як ви бачите на малюнку.



На OpenFlow Topology вони потім зникають, як показано на малюнку.

Flows for Data Path ID: 00:00:00:00:00:00:00:01

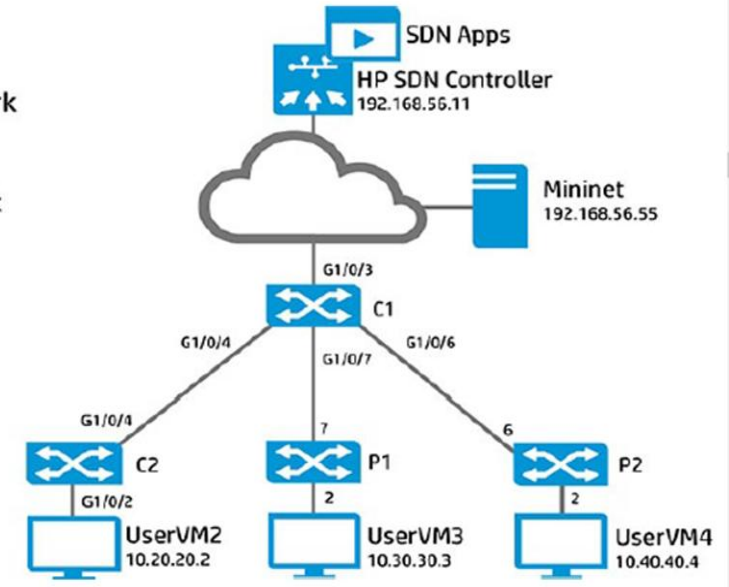
Summary | Ports | Flows | Groups

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
0	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
0	60000	2	140	eth_type: bddp	apply_actions: output: CONTROLLER	com.hp.sdn.bddp.steal
0	31000	15	630	eth_type: arp	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.arp.copy
0	0	38	3252		apply_actions: output: NORMAL	com.hp.sdn.ip.normal

2.5 Інтеграція Mininet з фізичною мережою

Використовуючи топологію, яка показана на малюнку, в цьому розділі будуть надані інструкції та приклади інтеграції мережі Mininet з фізичною мережею. Ця інтеграція показує, як пристрої віртуалізації мережевих функції (NFV) можуть взаємодіяти з фізичними пристроями.

- Integrate Mininet with the physical network
- Test traffic flows
  - Virtual Mininet hosts to physical network



1. Перегляньте інтерфейси на сервері Ubuntu де запущена Mininet:

```
mininet@mininet-vm:~$ ifconfig | more
eth0 Link encap:Ethernet HWaddr 00:0c:29:ba:c2:00
inet addr:192.168.56.55 Bcast:192.168.56.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4576 errors:0 dropped:0 overruns:0 frame:0
TX packets:4150 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:744361 (744.3 KB) TX bytes:556045 (556.0 KB)
eth1 Link encap:Ethernet HWaddr 00:0c:29:ba:c2:0a
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1895 errors:0 dropped:0 overruns:0 frame:0
TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:286481 (286.4 KB) TX bytes:28044 (28.0 KB)
lo Link encap:Local Loopback
... <omitted> ...
mininet@mininet-vm:~$
```

Result: There are two physical Ethernet interfaces on the Ubuntu server.

1. Створіть невелику Mininet топологію у складі двох комутаторів і встановіть для мережі адресу 192.168.56.0/24:

```
sudo mn --controller=remote,ip=192.168.56.11 --topo=linear,2 \
--switch=ovsk,protocols=OpenFlow13 --mac \
--ipbase=192.168.56.0/24
```

Result: A Mininet network will start

3. Яку IP адресу будуть використовувати хости? Використайте команду *ifconfig*, як показано на прикладі:

```
mininet> h1 ifconfig
h1-eth0 Link encap:Ethernet HWaddr 00:00:00:00:00:01
inet addr:192.168.56.1 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::200:ff:fe00:1/64 Scope:Link
...<ommitted>...
mininet>
mininet> h2 ifconfig
h2-eth0 Link encap:Ethernet HWaddr 00:00:00:00:00:02
inet addr:192.168.56.2 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::200:ff:fe00:2/64 Scope:Link
...<ommitted>...
mininet>
```

Answer:
h1 = 192.168.56.1/24,
h2 = 192.168.56.2/24.

4. Чи можна з h1 пінгувати h2 (192.168.56.2)? Використайте команду *ping –c 5 <ip address>* , як показано на прикладі.

```
mininet> h1 ping -c 5 192.168.56.2
PING 192.168.56.2 (192.168.56.2) 56(84) bytes of data.
64 bytes from 192.168.56.2: icmp_seq=1 ttl=64 time=5.40 ms
64 bytes from 192.168.56.2: icmp_seq=2 ttl=64 time=0.136 ms
64 bytes from 192.168.56.2: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 192.168.56.2: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 192.168.56.2: icmp_seq=5 ttl=64 time=0.094 ms
--- 192.168.56.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.094/1.173/5.401/2.114 ms
mininet>
```

Result:
Yes, host 1 can ping host 2.

5. Чи можна з host 1 (h1) пінгувати 192.168.56.11 (The HP VAN SDN Controller)?

```
mininet> h1 ping -c 5 192.168.56.11
PING 192.168.56.11 (192.168.56.11) 56(84) bytes of data.
From 192.168.56.1 icmp_seq=1 Destination Host Unreachable
From 192.168.56.1 icmp_seq=2 Destination Host Unreachable
From 192.168.56.1 icmp_seq=3 Destination Host Unreachable
From 192.168.56.1 icmp_seq=4 Destination Host Unreachable
From 192.168.56.1 icmp_seq=5 Destination Host Unreachable
--- 192.168.56.11 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4009ms
pipe 3
mininet>
```

Answer:
No, pings fail.

6. Використайте PuTTY на Windows VM (Jumphost), щоб відкрити інший SSH сеанс на сервері Mininet:

- IP address: 192.168.56.55
- Port number: 22
- Protocol: SSH

7. Коли з'явиться запит, увійдіть до системи за допомогою наступних облікових даних:

- Username: mininet
- Password: mininet

8. Переглянемо інтерфейси, які в даний час використовуються Open vSwitch за допомогою команди *sudo ovs-vsctl show*, як показано у наступному прикладі:

```
mininet@mininet-vm:~$ sudo ovs-vsctl show
1077578e-f495-46a1-a96b-441223e7cc22
    Bridge "s2"
        Controller "ptcp:6635"
        Controller "tcp:192.168.56.11:6633"
            is_connected: true
        fail_mode: secure
        Port "s2-eth1"
            Interface "s2-eth1"
        Port "s2"
            Interface "s2"
            type: internal
        Port "s2-eth2"
            Interface "s2-eth2"
    Bridge "s1"
        Controller "tcp:192.168.56.11:6633"
            is_connected: true
        Controller "ptcp:6634"
        fail_mode: secure
        Port "s1"
            Interface "s1"
            type: internal
        Port "s1-eth2"
            Interface "s1-eth2"
        Port "s1-eth1"
            Interface "s1-eth1"
    ovs_version: "2.0.2"
mininet@mininet-vm:~$
```

Result: Обидва комутатори S1 і S2 мають порти eth1 і eth2. Обидва комутатори також підключаються через TCP до контролера HP VAN SDN (IP-адреса 192.168.56.11) за допомогою OpenFlow (порт 6633). Це з'єднання використовує традиційну мережу маршрутизації та комутації і відокремлено від віртуалізованої мережі OpenFlow.

9. Підключимо фізичний інтерфейс Ubuntu eth1 до S1, щоб віртуальна мережа була підключена до фізичної мережі, за допомогою команди *sudo ovs-vsctl add*, як показано в наступному прикладі:

```
mininet@mininet-vm:~$ sudo ovs-vsctl add-port s1 eth1
```

10. Повернемося до попередньої сесії SSH, в якій працює Mininet. Чи може хост 1 пінгувати контролер HP VAN SDN зараз?

```
mininet> h1 ping -c 3 192.168.56.11
PING 192.168.56.11 (192.168.56.11) 56(84) bytes of data.
64 bytes from 192.168.56.11: icmp_seq=1 ttl=64 time=0.986 ms
64 bytes from 192.168.56.11: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.56.11: icmp_seq=3 ttl=64 time=0.707 ms
--- 192.168.56.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.707/0.937/1.119/0.173 ms
mininet>
```

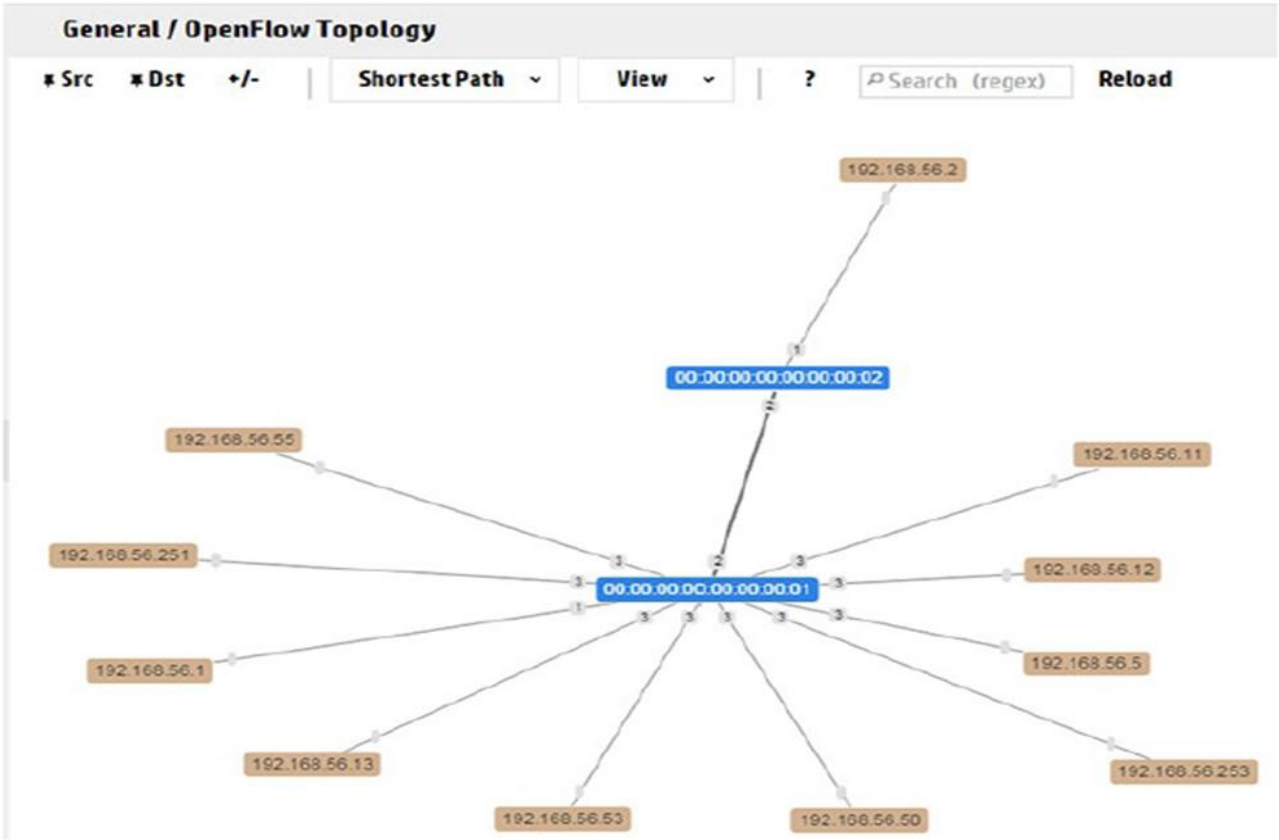
Result: The virtual host can ping the HP VAN SDN Controller.

11. Чи може хост 1 пінгувати фізичний HP комутатор c1 (HP Comware комутатор 1)?

```
mininet> h1 ping -c 3 192.168.56.251
PING 192.168.56.251 (192.168.56.251) 56(84) bytes of data.
64 bytes from 192.168.56.251: icmp_seq=1 ttl=255 time=7.44 ms
64 bytes from 192.168.56.251: icmp_seq=2 ttl=255 time=1.72 ms
64 bytes from 192.168.56.251: icmp_seq=3 ttl=255 time=1.85 ms
--- 192.168.56.251 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.723/3.676/7.447/2.667 ms
mininet>
```

Result: The virtual host can ping physical switches through a virtual OpenFlow enabled network.

12. Переглянемо оновлену топологію OpenFlow у інтерфейсі HP VAN SDN Controller:



Result: Both virtual Mininet hosts (192.168.56.1, 192.168.56.2) and other devices such as physical HP switches (192.168.56.251, 192.168.56.253) and the Windows Jumphost (192.168.56.5) are visible in the topology. The HP switches display as nodes as OpenFlow is not enabled on them yet.

Mininet - це чудовий спосіб перевірити та вивчити OpenFlow за допомогою єдиної віртуальної машини, яка створює мережі різних розмірів. Однак ви, мабуть, хочете побачити технології OpenFlow і SDN в мережі, що складається з реальних комутаторів.

2.6 Налаштування фізичних комутаторів

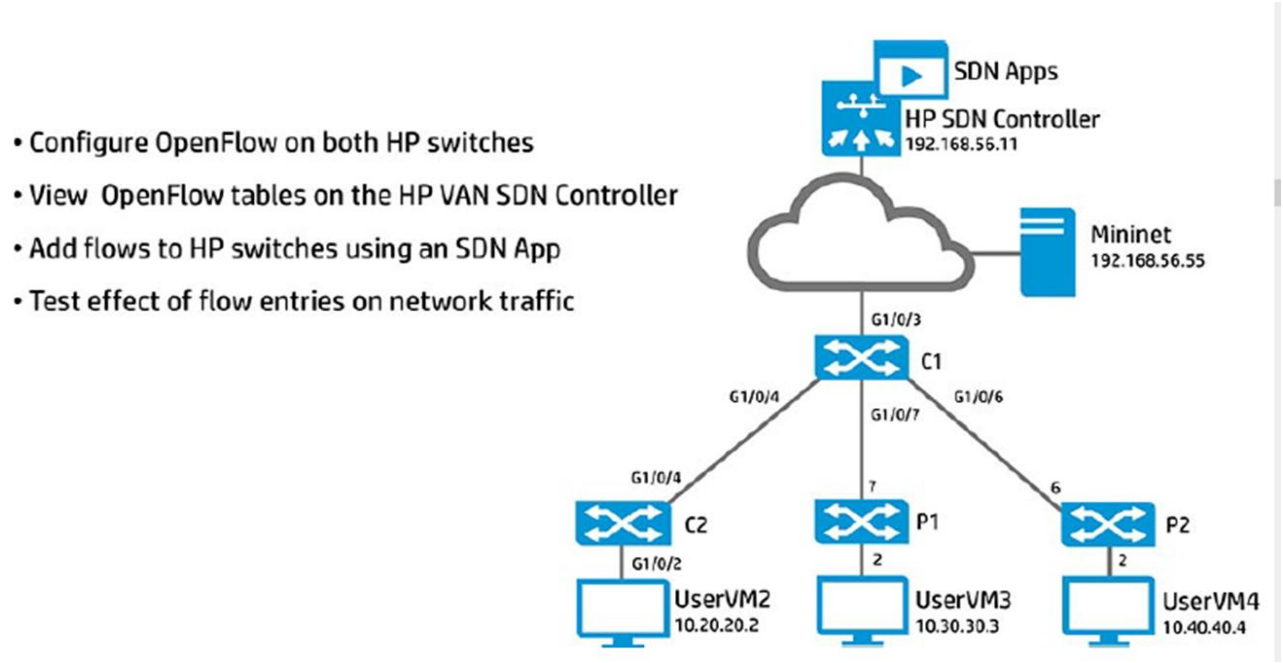
Плануйте свою мережу, включаючи продуктивність, OpenFlow VLANs, копії OpenFlow, порти контролера OpenFlow, найменування та стратегію нумерації.

Сплануйте кількість VLAN, налаштованих для OpenFlow у порівнянні з не-OpenFlow.

OpenFlow активується на копії лише тоді, коли виконуються наступні дії:

- OpenFlow увімкнено на копії OpenFlow.

- OpenFlow увімкнено глобально на комутаторі.



Для конфігурації OpenFlow в глобальному режимі **на комутаторі ProVision**, необхідно використати команду *openflow*. Це приведе до наступного контексту OpenFlow:

```
P1> enable
P1# configure
P1(config)# openflow
P1(openflow)#
```

Необхідно визначити ID контролера та IP-адрес. Можна налаштувати декілька контролерів для резервування та балансування навантаження. У такому випадку лише один контролер налаштовується на основі топології, яку ви бачите на малюнку. VLAN, який використовується для зв'язку з контролером – VLAN 1:

```
P1(openflow)# controller-id 1 ip 192.168.56.11 controller-interface vlan 1
```

Наступним кроком є конфігурація копії OpenFlow. На комутаторі ProVision, кожна копія OpenFlow точно співпадає з VLANs (коли використовується режим віртуалізації). Іншими словами, кожен VLAN вимагає окремої копії OpenFlow.

Але це не так для комутаторів Comware, для яких декілька VLANs можуть бути віднесені до однієї копії OpenFlow.

Коли на комутаторах ProVision використовується режим агрегації, усі VLANs (за виключенням VLAN, яка використовується для комунікації з контролером) будуть віднесені до однієї копії OpenFlow.

У цьому прикладі створюється копія OpenFlow з назвою “vlan30” :

```
P1(openflow)# instance vlan30
P1(of-inst-vlan30)#
```

Співставимо VLAN з копією OpenFlow використовуючи команду *member vlan*:

```
P1(of-inst-vlan30)# member vlan 30
```

Асоціюємо копію з контролером з OpenFlow:

```
P1(of-inst-vlan30)# controller-id 1
```

Версія OpenFlow, яка за замовчуванням використовується комутаторами HP ProVision - 1.0. У цьому прикладі було вказано версію 1.3. Існує декілька переваг використання OpenFlow 1.3, включаючи підтримку кількох таблиць (конвеєр).

```
P1(of-inst-vlan30)# version 1.3
```

Копія OpenFlow повинна бути включена. Ви можете мати декілька копій OpenFlow (VLANs) і можете деякі копії OpenFlow включити на деяких VLANs та виключити на інших VLANs. У цьому прикладі копія OpenFlow для VLAN 30 включається наступним чином:

```
P1(of-inst-vlan30)# enable
```

OpenFlow потім необхідно включити глобально на комутаторі:

```
P1(of-inst-vlan30)# exit
P1(openflow)# enable
```

У цьому міститься базова конфігурація OpenFlow на комутаторі HP ProVision.

Для конфігурації OpenFlow **на комутаторі HP Comware** необхідно перейти у *system-view*, використати команду *openflow instance* та визначити копію (*instance*). Це приведе до реалізації опції глобальної конфігурації OpenFlow:

```
<C2>system-view
System View: return to User View with Ctrl+Z.
[C2]openflow instance 1
```

У комутаторах ProVision існує повна відповідність між копіями та VLANs. Іншими словами, кожен VLAN потребує окрему копію OpenFlow.

Але це не обов'язково для комутаторів Comware (декілька VLANs можуть бути співвіднесені з однією копією OpenFlow).

Копія (*instance*) впливає також на Data Path ID (DPID) комутатора. Комутатор OpenFlow ідентифікується за допомогою DPIDs. Це 64-бітне число, яке складається із двох частин:

- Перші 16 біт визначають специфічного вендора. На комутаторі HP Comware, це дорівнює номеру налаштованої копії OpenFlow. Якщо номер дорівнює 10, то це еквівалентно "a" у шістнадцятирічній системі. Таким чином, комутатори мають DPID, який починається з 00:0a, якщо налаштована копія 10.
- Решта 48 біт: MAC-адреса комутатора.

Для асоціації одного VLAN або декількох VLANs з копією (*instance*) використовується команда *classification vlan*:

```
[C2-of-inst-1] classification vlan 20

This command isn't effective until the active instance command is issued.

[C2-of-inst-1]
```

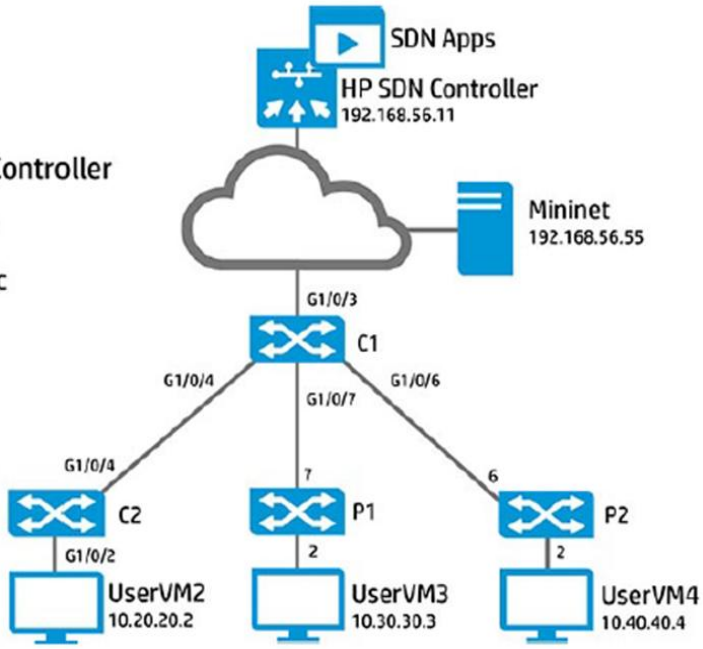
Необхідно вказати ID контролера та IP-адресу. Ви можете налаштувати декілька контролерів для резервування та балансування навантаження. У цьому випадку налаштовано лише один контролер:

```
[C2-of-inst-1]controller 1 address ip 192.168.56.11
```

Далі ми розглянемо, яким чином налаштовувати потоки на наступних комутаторах HP:

- Comware Switch 2 (C2)
- ProVision Switch 1 (P1)
- ProVision Switch 2 (P2)

- Configure OpenFlow on both HP switches
- View OpenFlow tables on the HP VAN SDN Controller
- Add flows to HP switches using an SDN App
- Test effect of flow entries on network traffic



Ми вивчили, яким чином налаштувати копію OpenFlow на комутаторі Comware. Щоб побачити цю копію, необхідно використати команду display openflow instance. Наступний приклад показує результат виконання цієї команди для копії 1, яку ми налаштували раніше:

```
[C2] display openflow instance 1
Instance 1 information:
Configuration information:
 Description : --
Active status : Active
Inactive configuration:
  None
Active configuration:
 Classification: VLAN, total VLANs(1)
   20
 In-band management VLAN, total VLANs(0)
   Empty VLAN
 Connect mode: Multiple
 MAC address learning: Enabled
 Flow table:
   Table ID(type): 0(Extensibility), count: 5
 Flow-entry max-limit: 65535
 Datapath ID: 0x0001784859392f96
Port information:
  Ten-GigabitEthernet1/0/2
  Ten-GigabitEthernet1/0/4
Active channel information:
  Controller 1 IP address: 192.168.56.11 port: 6633
[C2]
```

Як випливає з цього прикладу, ви повинні побачити активний канал до контролера, який прослуховує порт 6633, який є портом OpenFlow. Ви можете побачити інформацію контролера OpenFlow для копії 1, набравши команду *display openflow instance* <*instance number*> controller:

```
[C2] display openflow instance 1 controller
Instance 1 controller information:
 Reconnect interval: 60 (s)
 Echo interval : 5 (s)
 Controller ID : 1
 Controller IP address : 192.168.56.11
 Controller port : 6633
 Controller role : Equal
 Connect type : TCP
 Connect state : Established
 Packets sent : 4370
 Packets received : 1598
 SSL policy : --
 VRF name : --
[C2]
```

Як показує цей приклад, вихідний файл повинен відображати встановлене з'єднання з контролером за допомогою TCP-порту 6633.

Використайте команду *show openflow*, щоб побачити інформацію OpenFlow на комутаторі ProVision. Наступний приклад показує вихід використання OpenFlow комутатором P1.

```
OpenFlow : Enabled
IP Control Table Mode : Disabled
Egress Only Ports Mode : Disabled
Instance Information
                                    No. of    No. of     OpenFlow
Instance Name        Oper. Status H/W Flows  S/W Flows Version
-------------------- ------------ ---------- ---------- -------
vlan30                Up           6          4          1.3
P1#
P1#
```

Як видно з прикладу, команда *show openflow* відображає всі екземпляри OpenFlow, які налаштовані на комутаторі, з їх статусами та даними потоку.

У цьому прикладі узгоджена версія OpenFlow, для копії vlan30 — єдина копія, яка налаштована на комутаторі — є 1.3. Це залежить від версій, підтримуваних як комутатором так і контролером.

Робочий статус цього екземпляра - Up. Стан може бути Down, якщо існує проблема зв'язку між контролером і комутатором. Також показано кількість апаратних засобів (6) та програмних потоків (4).

Щоб побачити інформацію про певну копію, використайте команду *show openflow instance*. Далі показано результат цієї команди комутатора P1 та копії vlan30:

```
Configured OF Version : 1.3
 Negotiated OF Version : 1.3
 Instance Name : vlan30
 Admin. Status : Enabled
 Member List : VLAN 30
 Listen Port : None
 Oper. Status : Up
 Oper. Status Reason : NA
 Datapath ID : 001e1458d0f0db80
 Mode : Active
 Flow Location : Hardware and Software
 No. of Hw Flows : 6
 No. of Sw Flows : 4
 Hw. Rate Limit : 0 kbps
 Sw. Rate Limit : 100 pps
 Conn. Interrupt Mode : Fail-Secure
 Maximum Backoff Interval : 60 seconds
 Probe Interval : 10 seconds
 Hw. Table Miss Count : NA
 No. of Sw Flow Tables : 1
 Egress Only Ports : None
 Table Model : Policy Engine and Software
 Controller Id Connection Status Connection State Secure Role
 ------------- ----------------- ---------------- ------ ------
 1             Connected         Active           No     Equal
P1#
P1#
```

Використайте команду *show openflow controllers* щоб побачити інформацію контролера для комутатора ProVision. Показано приклад для комутатора P1.

```
P1# show openflow controllers

Controller Information
 Controller Id IP Address                    Port   Interface
 ------------- ----------------------------- ------ ----------
 1             192.168.56.11                 6633   VLAN 1
P1#
P1#
```

Якщо зараз здійснити налаштування копії vlan40 на комутаторі P2, використовуючи відповідні команди, запустивши потім інтерфейс контролера, можна побачити три комутатори у розділі Topology: C1, P1, and P2. По замовчуванню, інтерфейс відображає комутатори *як <IP address>: <OpenFlow instance number>*. Можна це змінити, натиснувши клавішу n.

Між комутаторами не відображаються жодні з'єднання, оскільки вони розділені пристроєм маршрутизації, що не підтримує OpenFlow (C1).

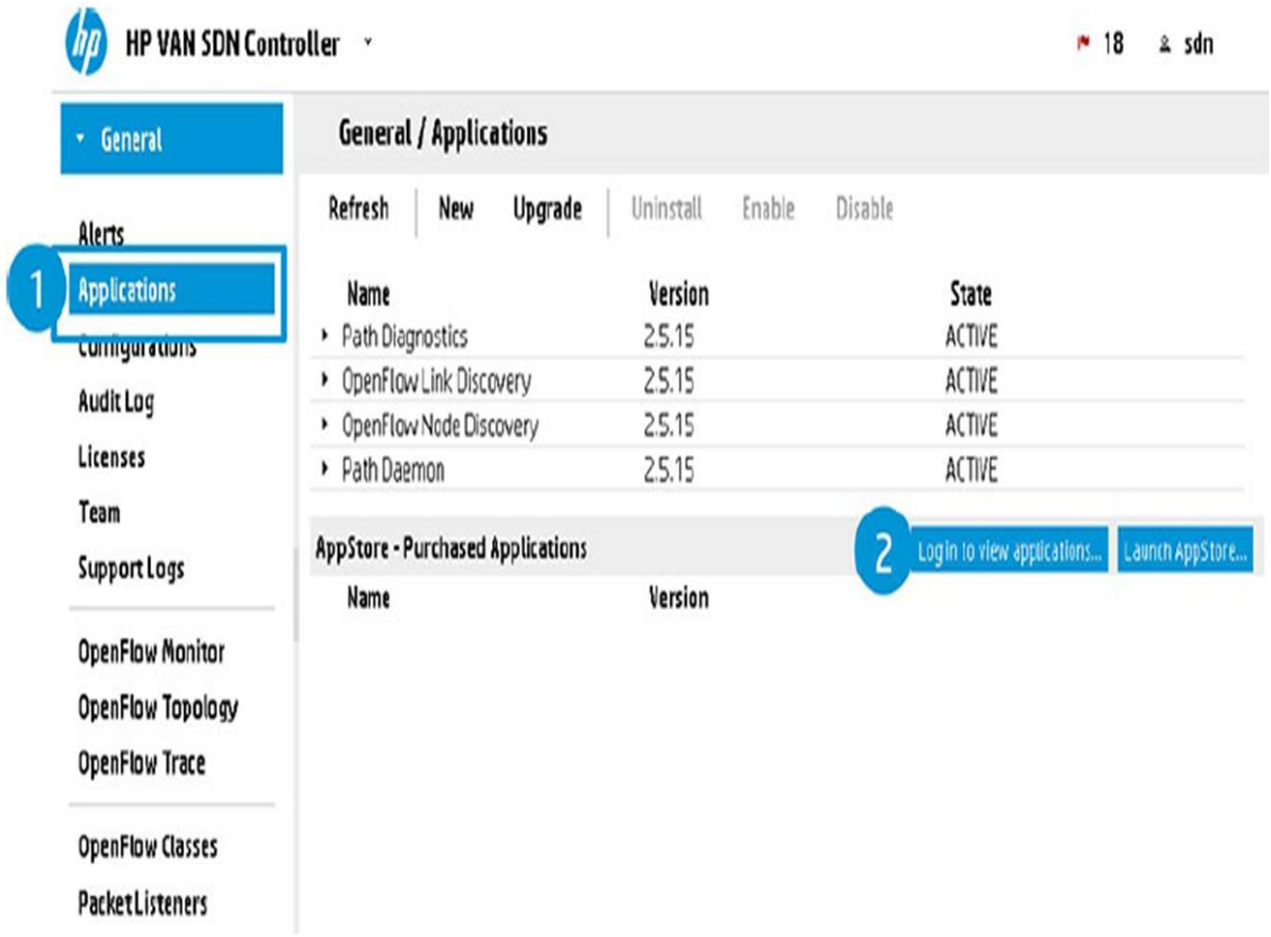
2.7 Встановлення нових програмних додатків через App Store

Application Manager підтримує стандартні та додаткові послуги мережі та дозволяє встановлювати, оновлювати, вмикати (запускати), відключати (зупиняти) та деінсталювати програми SDN. На малюнку нижче показано графічний інтерфейс HP VAN SDN Controller Application Manager.

Для того, щоб зайти на Application Manager, необхідно запустити графічний інтерфейс HP VAN SDN Controller та клікнути Applications. При

цьому буде відображено список програмних додатків, які вже встановлені на контролері.

The HP VAN SDN Controller має деякі вбудовані (embedded) програмні додатки, які допомагають контролерові виявляти вузли (nodes) та зв'язки (links) в топології мережі.



Ви можете придбати та завантажити програми для свого контролера із HP SDN App Store. Ви можете встановити програмні додатки на HP VAN SDN Controller безпосередньо із HP APP Store або вручну із локального комп'ютера.

Для встановлення програмного додатку необхідно на графічному інтерфейсі HP VAN SDN Controller клікнути *Applications*, а потім клікнути *Log in to view applications...*

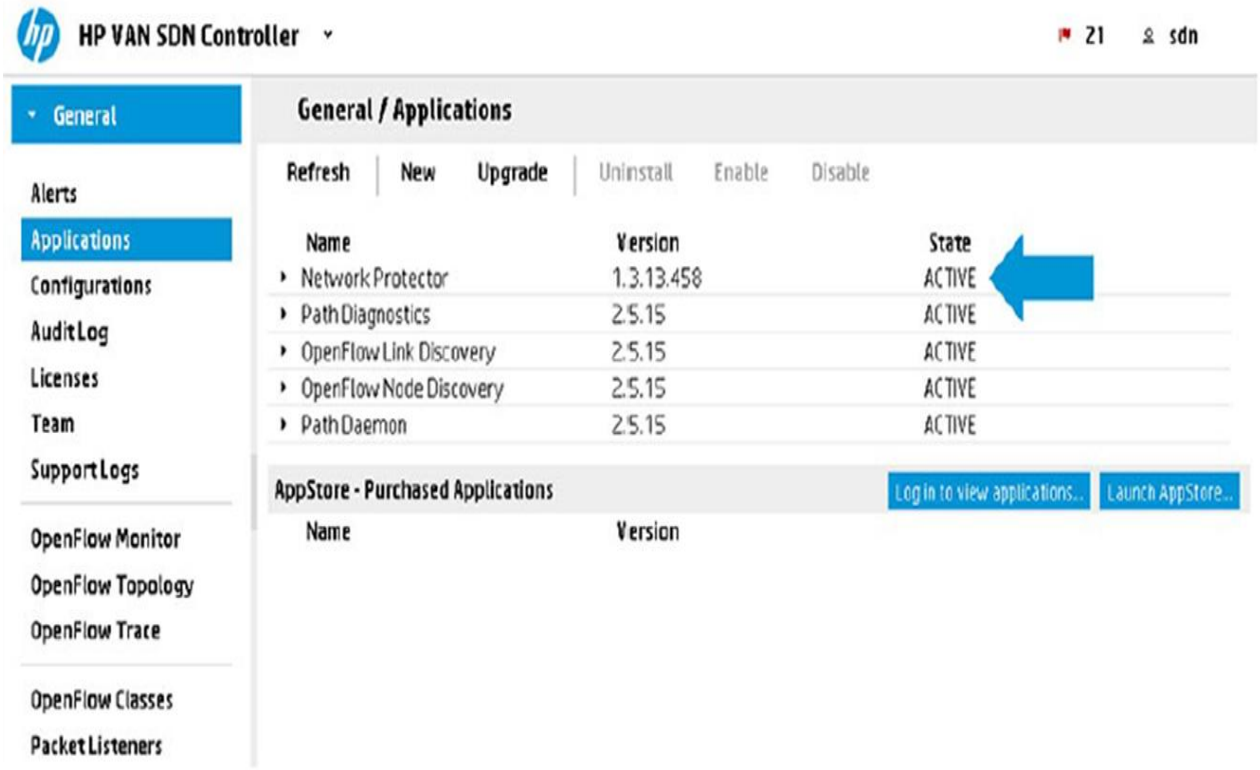
Відкриється нове вікно веб-браузера і вам потрібно буде ввести свої облікові дані (credentials) до HP SDN App Store.

Після перевірки автентичності контролер отримує токен, що дозволяє завантажувати додаток безпосередньо з App Store. Це вимагає від контролера доступу до Інтернету.

Після того, як додаток буде завантажено з App Store, ви можете клікнути *Deploy*, щоб встановити програму на контролері.

У стані за замовчуванням або коли програму було запущено, вона знаходиться в активному стані ACTIVE . На малюнку показано приклад того,

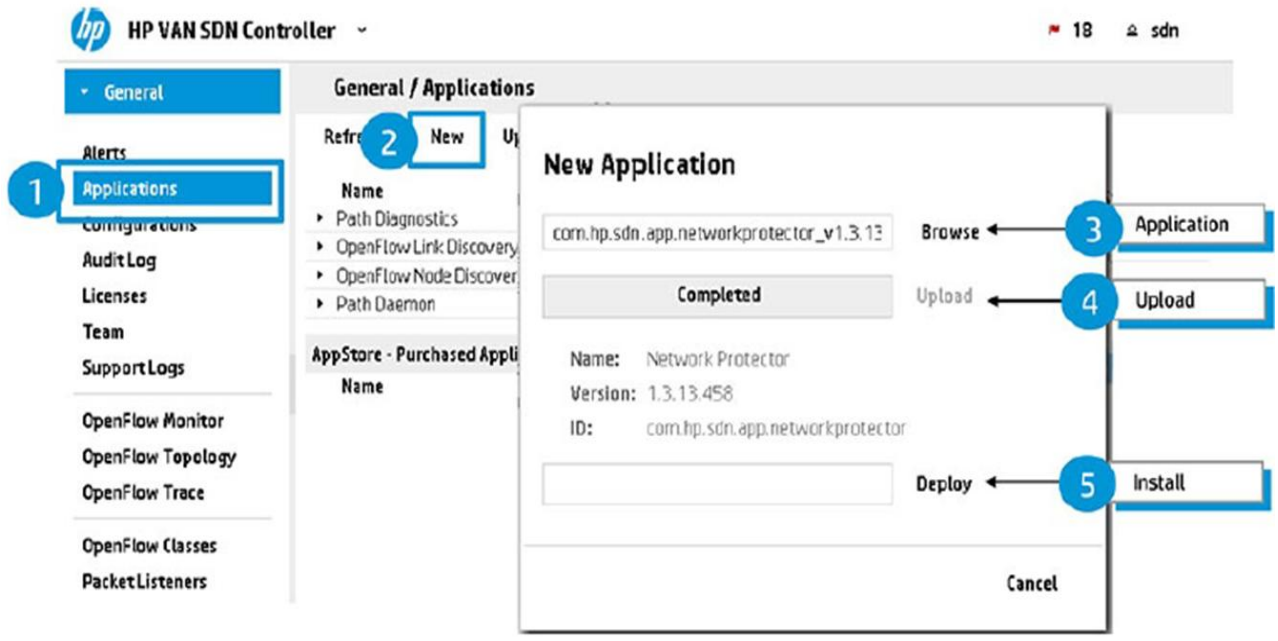
як інтерфейс HP VAN SDN Controller відображає програми, які знаходяться в активному стані.



Перелік станів, у якому можуть знаходитися програмні додатки, наступний:

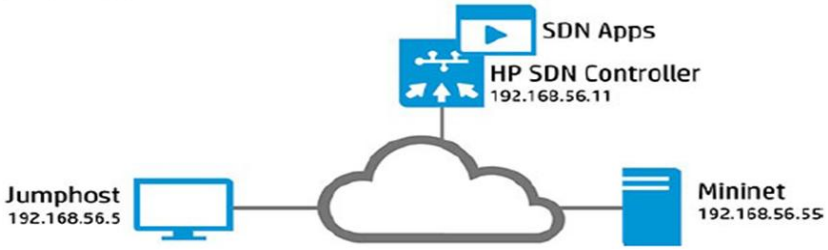
State	Description
ACTIVE	The application is running and servicing requests.
STAGED	A new application has been downloaded to the controller and is ready to be installed.
UPGRADE_STAGED	A new version of an existing running application has been downloaded to the controller and the new version is ready to be installed (upgrade/downgrade).
INSTALLING	A transitive state indicating a new application is in the process of being installed.
UPGRADING	A transitive state indicating the existing application is being stopped and a new version of the application is being installed.
CANCELING	A transitive state indicating a noninstalled version of an application is being deleted from the controller.
DISABLING	A transitive state indicating the application is in the process of being disabled (stopping).
DISABLED	The application is disabled (stopped). A disabled application is not automatically started when the controller is restarted.
ENABLING	A transitive state indicating the application is being started.
UNINSTALLING	A transitive state indication an application is being stopped and completely removed from the controller.
RESOLVED	The application is stopped and not servicing requests. An application can only be in this state when it is stopped externally to the HP VAN SDN Controller (e.g., the virgo console).

На малюнку HP Network Protector SDN Application було завантажено із HP SDN App Store на локальний PC. Програма потім завантажується до контролера з локального комп'ютера, а не з контролера HP VAN SDN, який завантажує її безпосередньо з магазину HP SDN App Store.

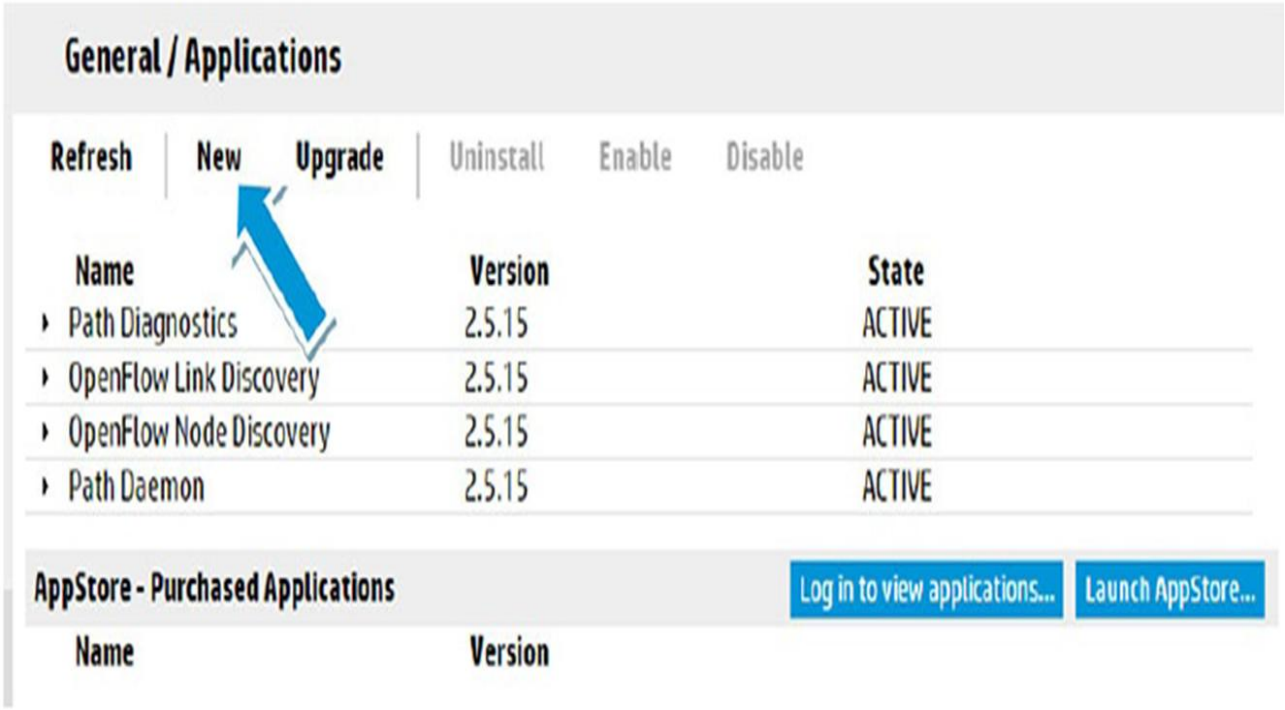


Припустимо, ви вже завантажили нову програму Flow Maker Deluxe з App Store і тепер ви хочете встановити її. Наведені нижче інструкції та приклади допоможуть вам встановити цю програму, додавати потоки до комутаторів за допомогою програми та протестувати вашу мережу, щоб визначити ефект додавання цих потоків. Усі приклади припускають, що ви використовуєте віртуальні пристрої через Mininet, як показано на малюнку.

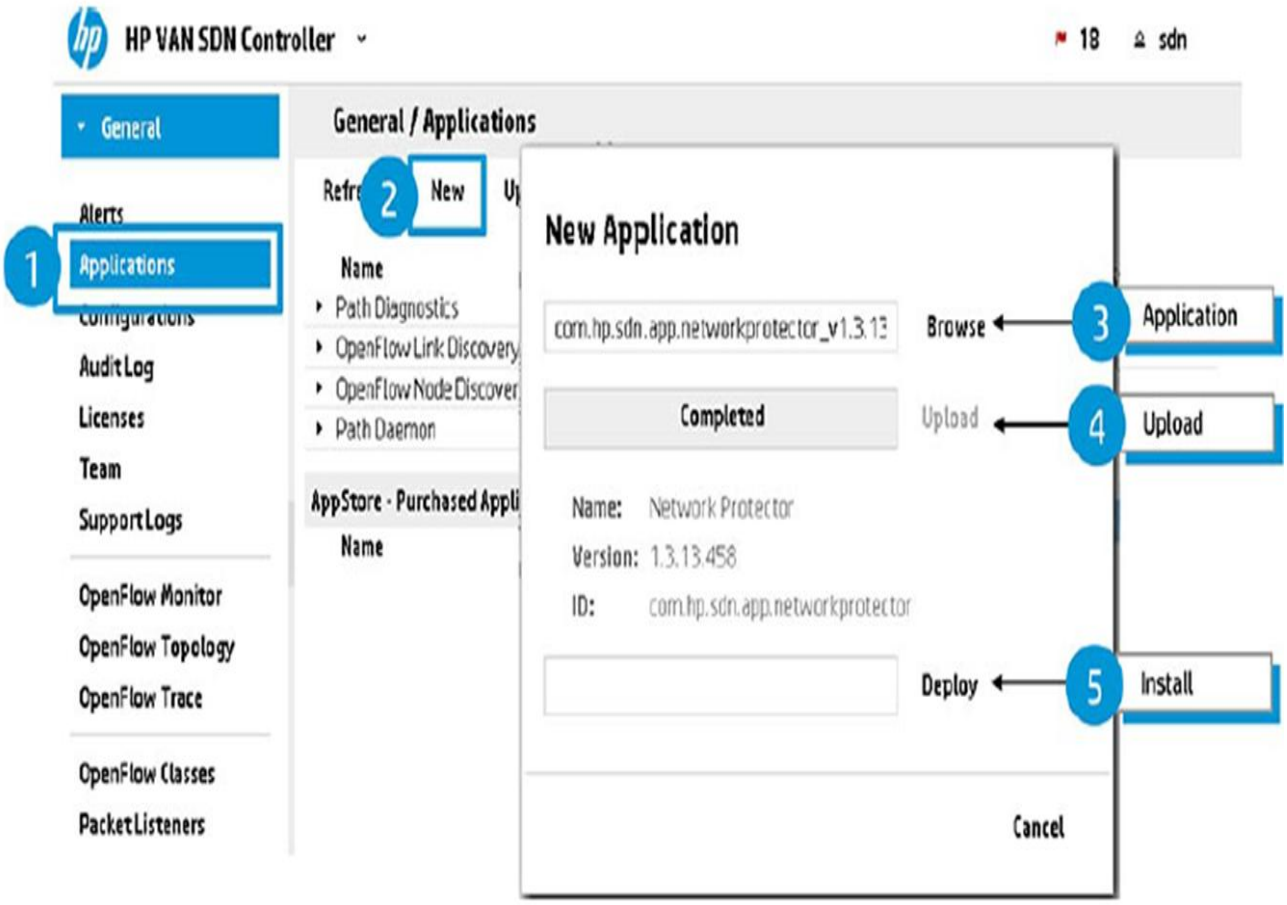
- Install an SDN application
- Add flows to Mininet switches
  - Use the SDN app
- Test network behavior of new flow entries



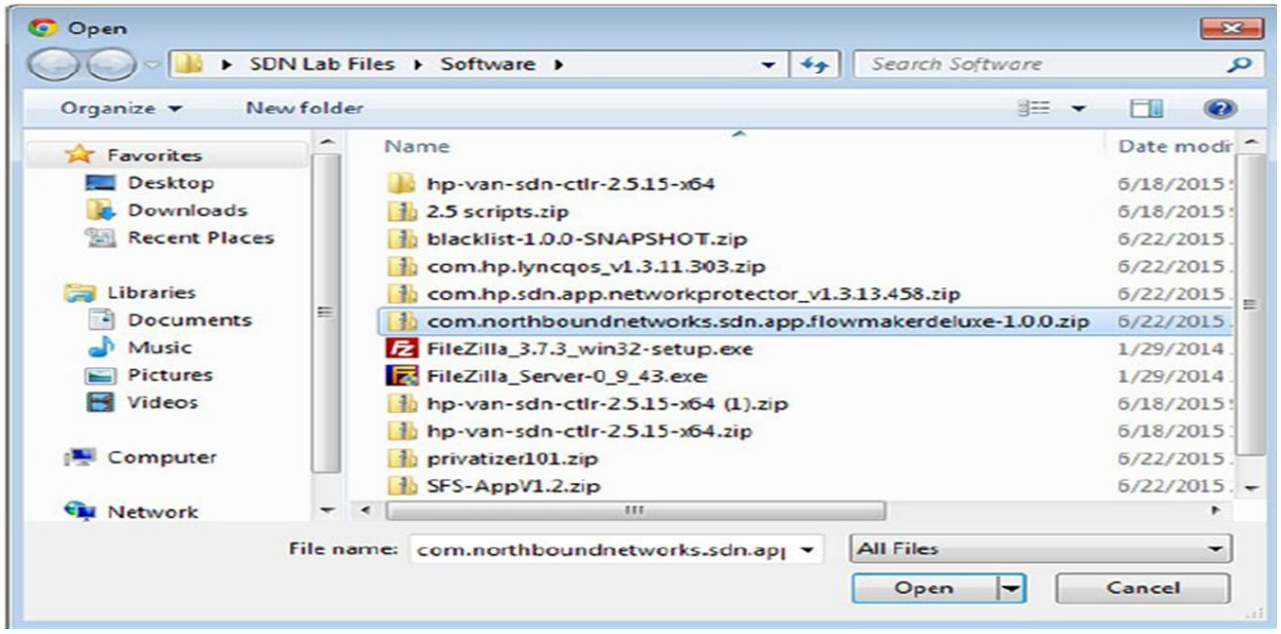
1. Клікніть *Applications* в меню HP VAN SDN Controller, а потім клікніть *New*.



2. Клікніть *Browse*. Перейдіть до розташування zip-файлу програми та виберіть файл.



На малюнку наведено приклад розташування для програми на комп'ютері під керуванням Windows.

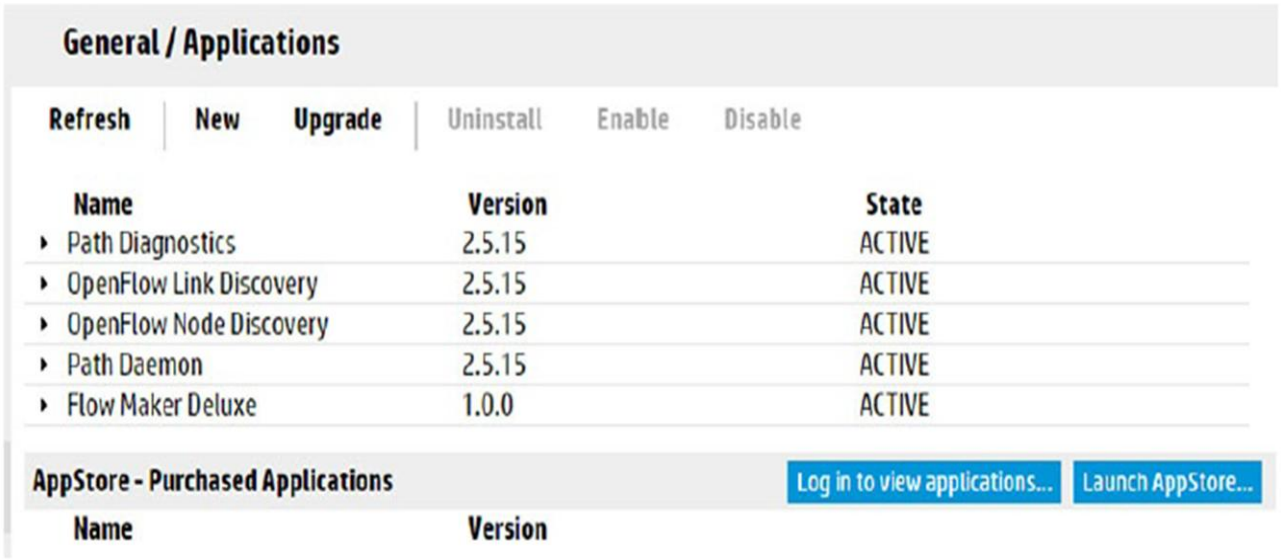


3. Клікніть *Upload* щоб завантажити файл. Дочекайтеся, коли появиться повідомлення у вікні “Completed” .

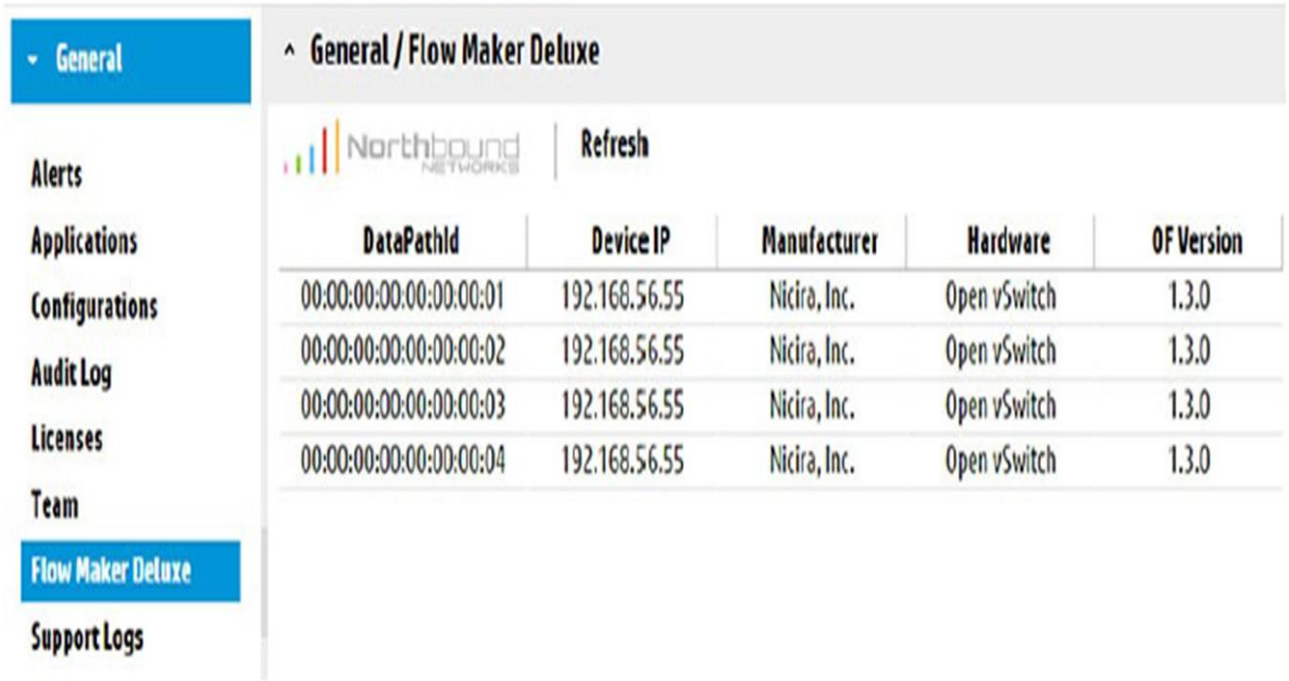
4. Клікніть *Deploy*, щоб розгорнути та активувати програму.

5. Програма повинна розгорнутися та відобразитись у списку програм як ACTIVE. На малюнку показано успішне розгортання додатків, як показано в інтерфейсі HP VAN SDN Controller.

6. Після оновлення браузера, Flow Maker Deluxe також з'явиться в меню інтерфейсу контролера HP VAN SDN, як показано на малюнку.



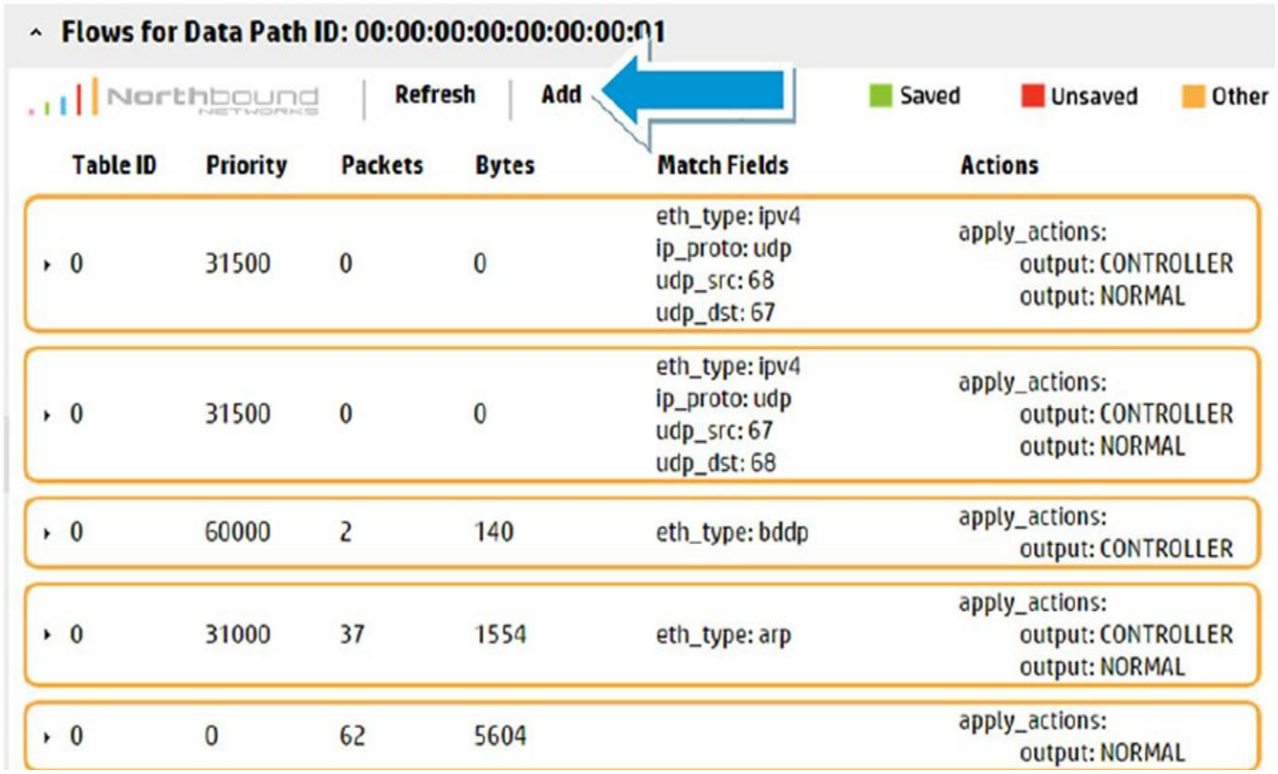
Програми SDN, такі як Flow Maker Deluxe, можуть створювати потоки на комутаторах OpenFlow. Щоб додати новий потік із інтерфейсу Deluxe Flow Maker, клікніть комутатор у вікні Flow Maker Deluxe General. Наприклад, клікніть комутатор з DPID 00:00:00:00:00:00:00:01. Відобразяться потоки на комутаторі.



Приклад 1. Наступні інструкції показують, як створювати потоки за допомогою інтерфейсу цієї програми. *Наступний приклад ілюструє*

результати створення потоку, який блокує хост.

1. Клікніть Add, як показано на малюнку, щоб додати новий потік.



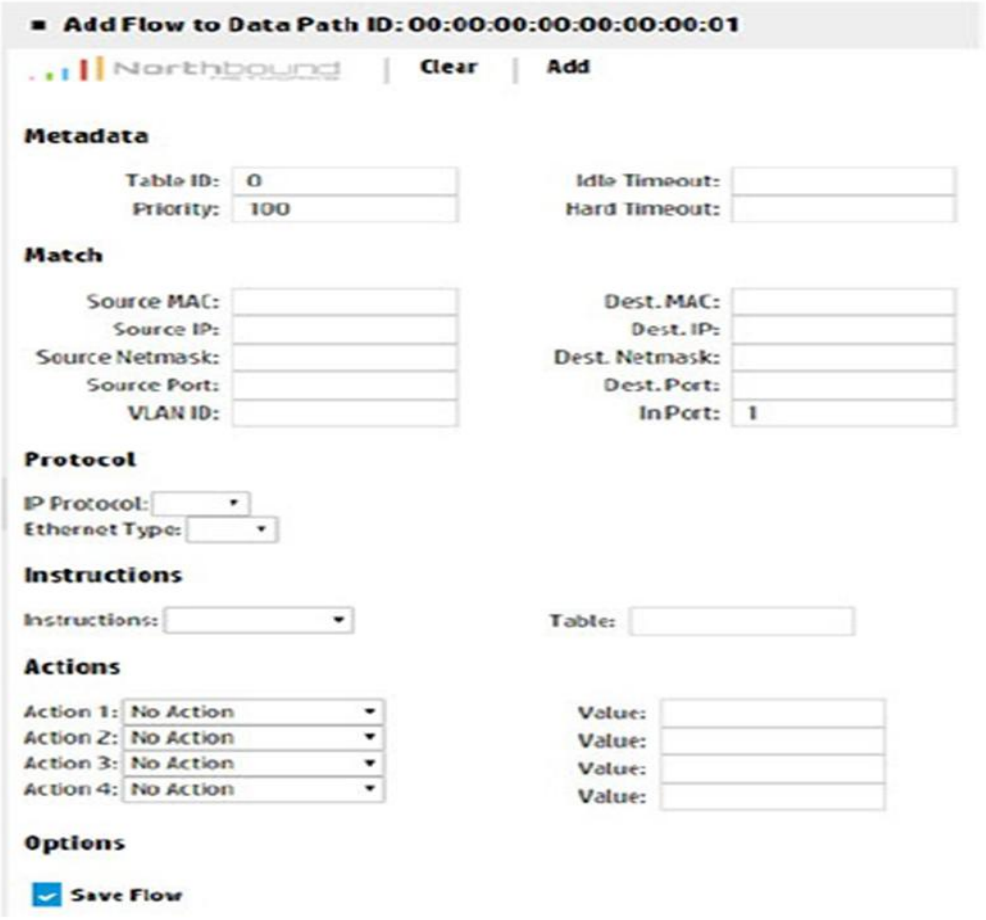
Перш ніж оновлювати таблицю потоків комутатора, ви можете перевірити підключення шляхом пінга з хосту 1 (10.0.0.1) до хосту 4 (10.0.0.4) в Mininet наступним чином:

```
mininet> h1 ping -c 5 h4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.157 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=0.160 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=0.137 ms
64 bytes from 10.0.0.4: icmp_seq=5 ttl=64 time=0.206 ms
--- 10.0.0.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.137/0.332/1.000/0.334 ms
mininet>
```

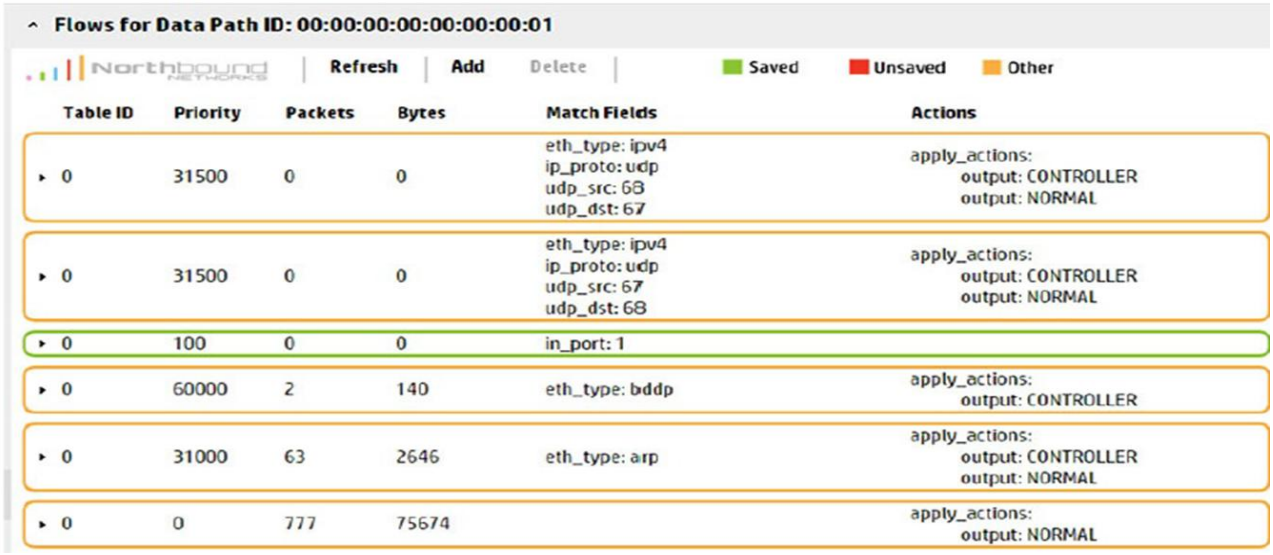
2. У Flow Maker, додайте потоковий запис (flow entry) з наступними атрибутами та натисніть кнопку Add:

- Table ID:0
- Priority: 100
- In Port: 1

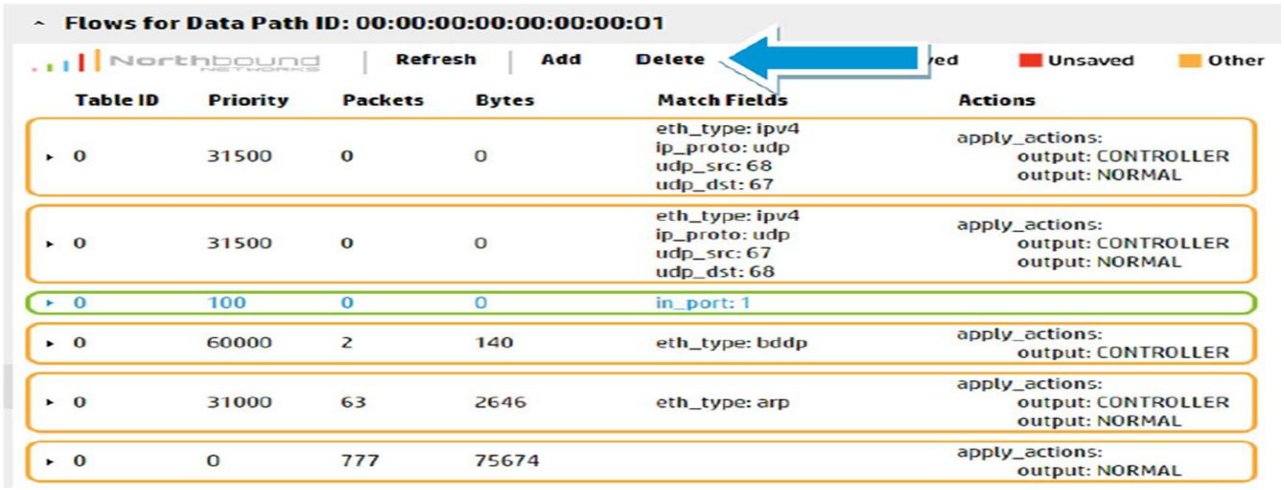
- Save Flow: True



Таблиця потоку оновлюється новим потоковим записом (потік із зеленою рамкою на малюнку).



3. У Flow Maker, клікніть потоковий запис, який ви створили, і клікніть Delete. Малюнок ілюструє вибраний потік і видалення. Перевірте видалення потоку:

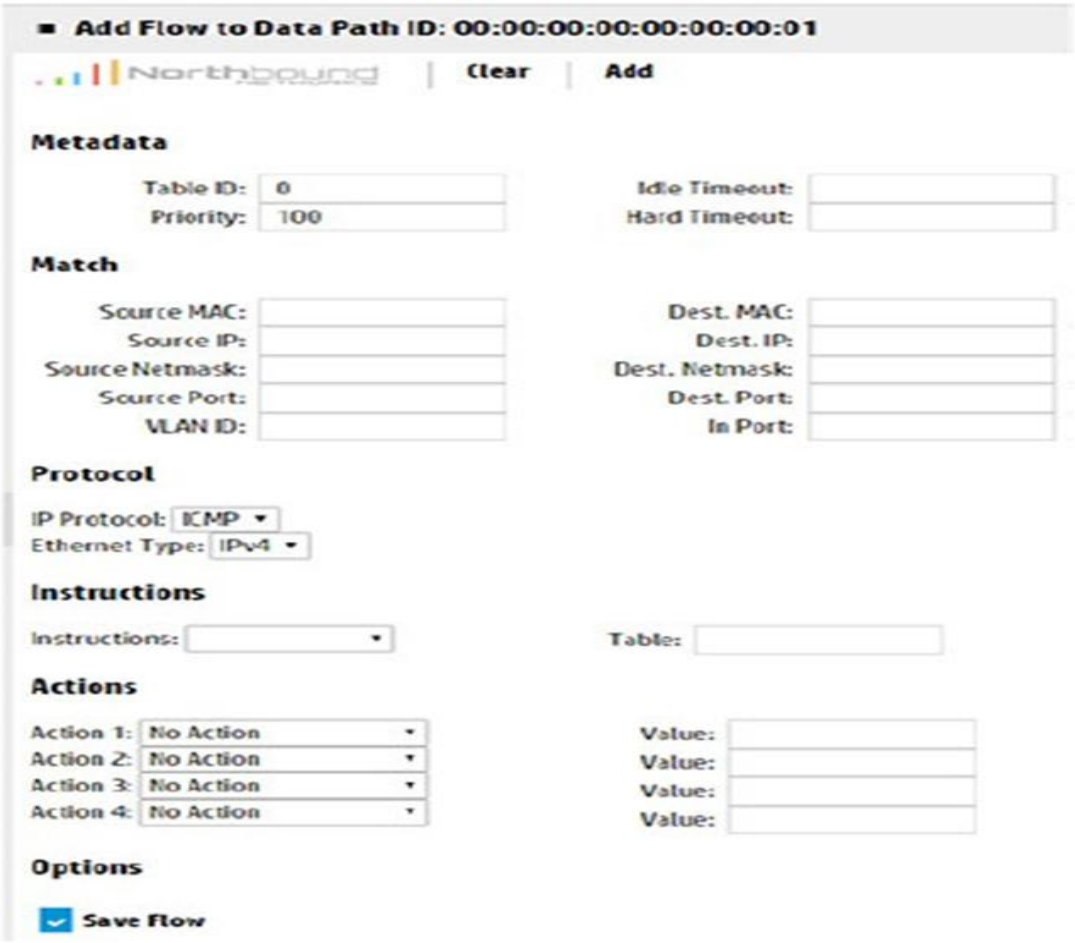


Приклад 2. У наступному прикладі ми створюємо *потік, який відповідає трафіку протоколу Internet Message Control Protocol (ICMP)* та перевіряє результати цього потоку.

1. У Flow Maker клікніть Add щоб додати новий потоковий запис на комутаторі 00:00:00:00:00:01.

2. Створіть потоковий запис з наступними параметрами і потім клікніть Add:

- Table ID:0
- Priority: 100
- IP Protocol: ICMP
- Ethernet Type: IPv4
- Save Flow: True



Як показано на малюнку, таким чином виглядає вікно таблиці потоку Flow Maker Deluxe з новим записом.

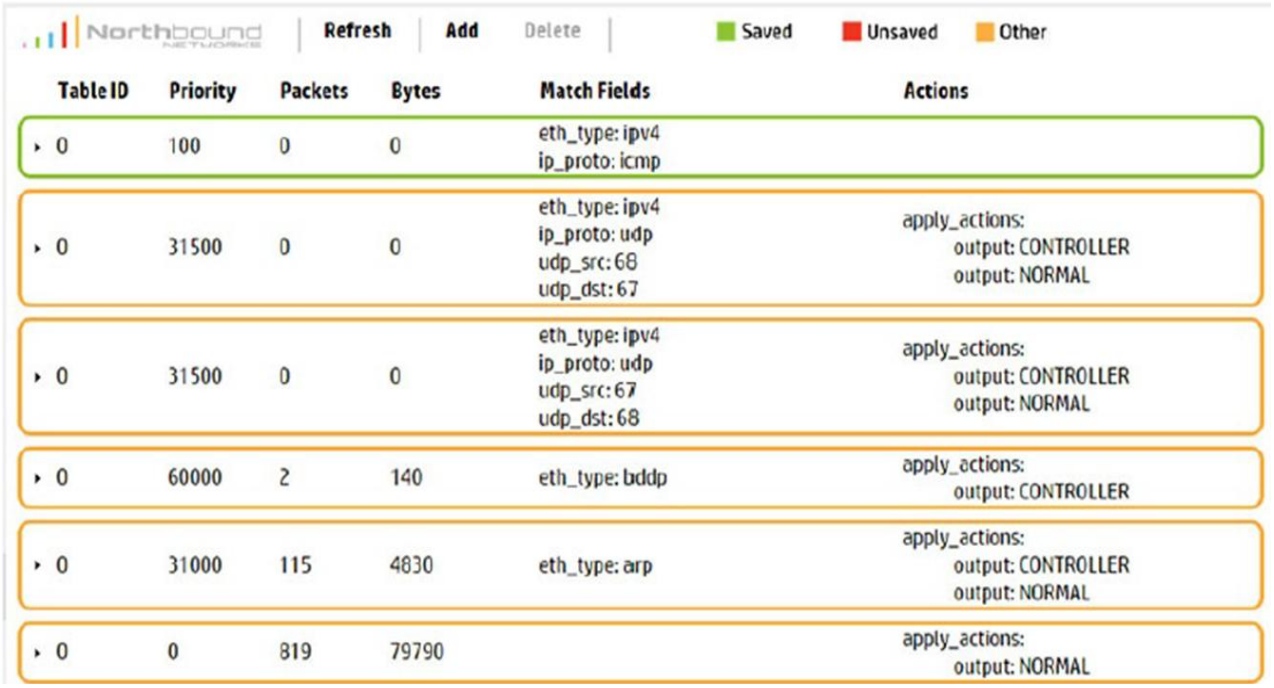
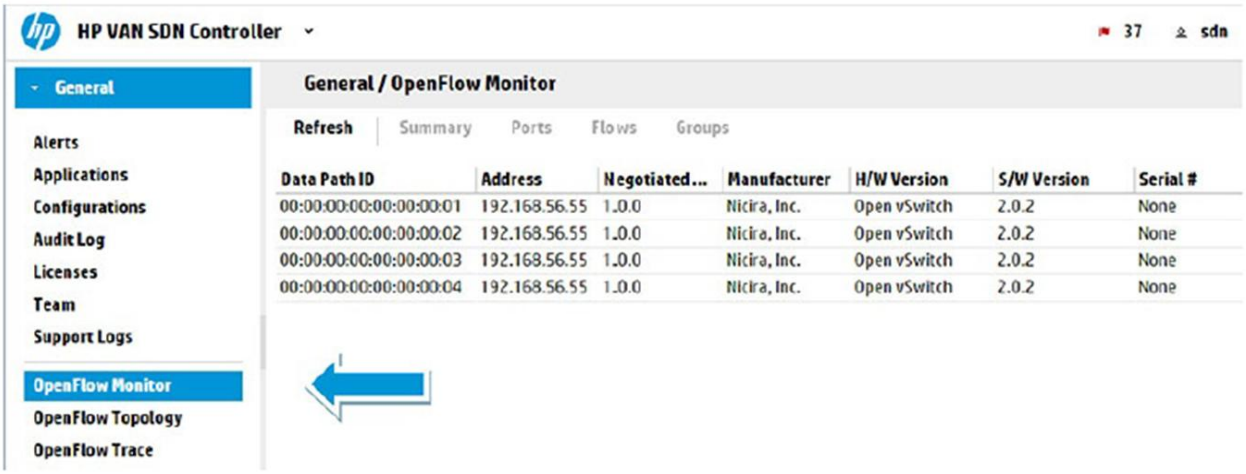
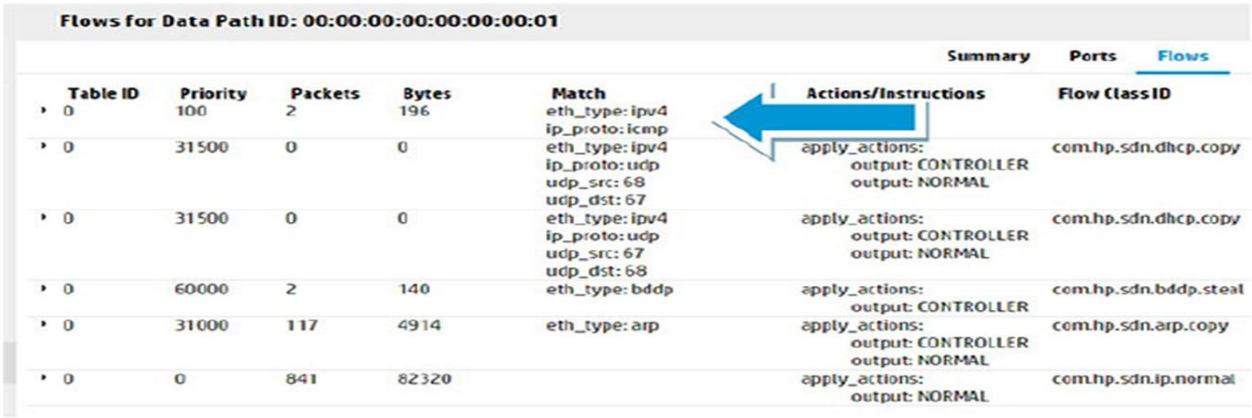


Table ID	Priority	Packets	Bytes	Match Fields	Actions
0	100	0	0	eth_type: ipv4 ip_proto: icmp	
0	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	apply_actions: output: CONTROLLER output: NORMAL
0	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	apply_actions: output: CONTROLLER output: NORMAL
0	60000	2	140	eth_type: bddp	apply_actions: output: CONTROLLER
0	31000	115	4830	eth_type: arp	apply_actions: output: CONTROLLER output: NORMAL
0	0	819	79790		apply_actions: output: NORMAL

2. На графічному інтерфейсі HP VAN SDN Controller клікніть OpenFlow Monitor.



3. Виберіть комутатор з DPID 00:00:00:00:00:00:00:01 та клікніть Flows. На малюнку показано потік, який створено за допомогою Flow Maker Deluxe.



Висновки.

Ви дізналися, як перевірити вимоги до програмного та апаратного забезпечення для контролера HP VAN SDN за допомогою матриці підтримки контролера HP VAN SDN.

Для контролера існують специфічні вимоги до мережі, OpenFlow, обладнання та програмного забезпечення. Вони повинні бути вирішенні перед встановленням програмного забезпечення контролера HP VAN SDN.

Ви також дізналися, де завантажити програмне забезпечення контролера та як встановити необхідне програмне забезпечення HP VAN SDN Controller. Після цього ви дізналися, як перевірити успішну установку контролера HP VAN SDN.

Крім того, ви дізналися про те, як інтегрувати контролер Mininet і HP VAN SDN та про параметри, доступні на діаграмі топології OpenFlow.

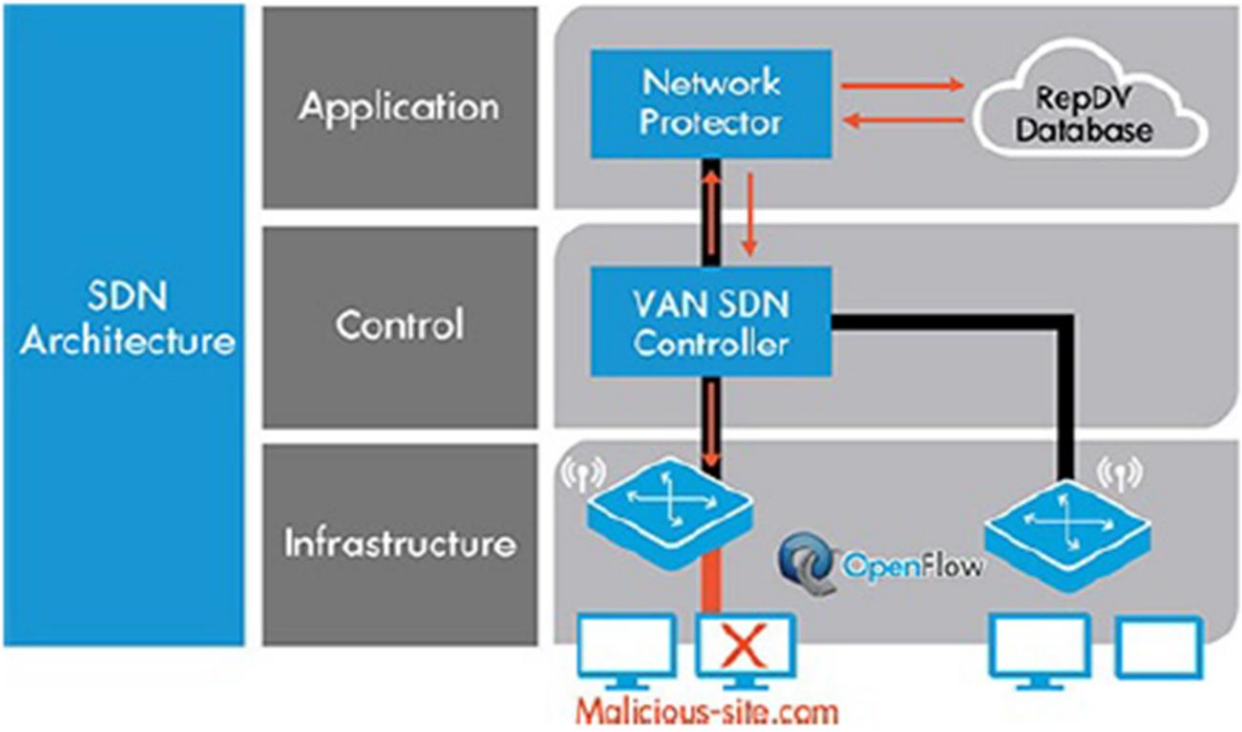
Ви дізналися про кроки, які вам потрібно буде вжити, щоб встановити додаток HP SDN App Store на контролері HP VAN SDN, а також про кроки, які потрібно виконати, щоб використовувати програму для керування поточними записами як на віртуальних комутаторах Mininet, так і на комутаторах HP.

Ви бачили практичну реалізацію архітектури SDN додатків (Flow Maker), контролера (HP VAN SDN Controller) та інфраструктури (комутатори Mininet та HP).

Розділ III. Протектор HP Network Protector SDN

У цьому розділі ви дізнаєтесь про програму HP Network Protector SDN (версія 1.3). HP Network Protector SDN Application використовує продукти HP Networking, TippingPoint та ArcSight, щоб забезпечити конвергентне рішення, яке реалізує підвищення безпеки зовсім іншим шляхом, використовуючи саму мережу.

Network Protector використовує OpenFlow на комутаторах рівня доступу. Коли комутатор завантажується та під'єднується до контролера HP VAN SDN з Network Protector, потік за замовчуванням проштовхується на пристрій. Це додатково до потоків, встановлених на пристрої базовим контролером, для підтримки гібридного середовища. Потокові записи пересилають весь трафік IP-UDP порт 53 (Domain Name Service - DNS) до Network Protector Application на контролері. На малюнку нижче показано архітектуру Network Protector.



Коли комутатор приймає трафік DNS, він передається контролеру. На контролері запит порівнюється з TippingPoint Reputation Database (RepDV). Якщо є спавпадання, тобто трафік має шкідливий характер, Network Protector створює DNS відповідь і надсилає його на комутатор, який передається клієнту. Це забезпечує негайне відмову клієнту, який здійснює запит, таким чином, що йому не доведеться чекати тайм-аут або спробувати подальше вирішення. Інший варіант - переадресовувати клієнта на сервер за вибором адміністратора. У цьому випадку клієнту може бути надано відгук про те, що

запит було заблоковано через політику безпеки компанії. З будь-яким із варіантів, шкідливий трафік буде заблоковано.

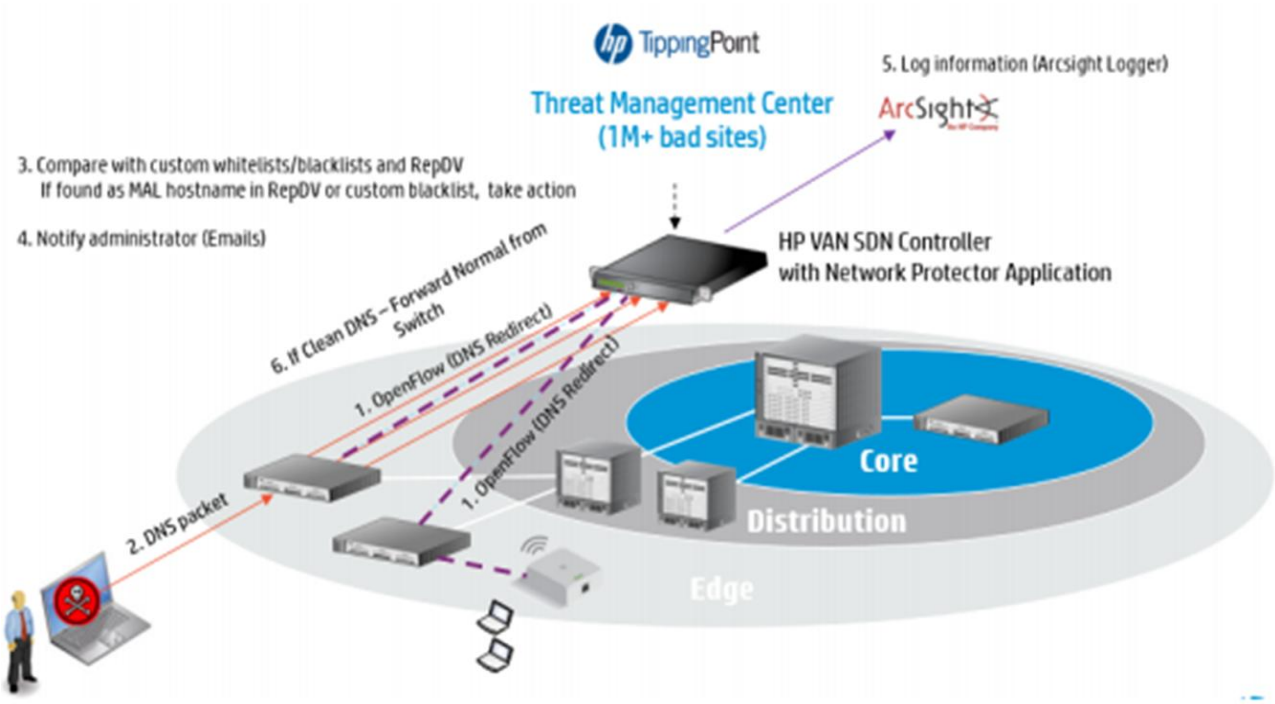
Якщо запит DNS не співпадає з базою даних RepDV або іншими користувальницькими "чорними списками" (blacklists) або "сірими списками" (graylists) , то це означає, що трафік має бути дозволено - Network Protecto доручає комутатору нормальну переадресацію трафіку.

3.1 Загальні відомості про HP Network Protector SDN

Цінність HP Network Protector SDN міститься в тому, що, блокуючи шкідливий трафік якнайближче до джерела, він таким чином зупиняє трафік від перетину мережі та, можливо, зараження інших клієнтів. Це також зменшує споживання пропускної здатності в мережі та ресурсів централізованою системою захисту від вторгнень (IPS).

HP Network Protector SDN доповнює правильно розгорнуте рішення IPS, але не виключає необхідності в IPS.

HP Network Protector SDN розгортається як додаток, що працює як ключовий елемент контролера HP VAN SDN. В якості автономного додатку, що входить у взаємодію з контролером, він використовує декілька функцій та підсистем контролера, таких як менеджер програм, менеджер конвеєра, інфраструктура ліцензування, база даних Cassandra, SKI UI framework, Representational State Transfer (REST) API UI framework, аудит, попередження, журнали підтримки та інші.



Одним з основних вимог до програми HP Network Protector Application є використання комутаторів з підтримкою протоколу OpenFlow. OpenFlow - це

механізм, за допомогою якого програма надає комутаторам інструкції про переадресацію всього трафіку DNS на себе. У програмі підтримуються декілька політик безпеки, які реалізуються за допомогою протоколу OpenFlow для просування потрібних потоків на комутатори. В даний час підтримуються протоколи OpenFlow 1.0 та OpenFlow 1.3.

Програмне забезпечення комутатора відіграє важливу роль у правильному функціонуванні програми. Комутатори ProVision з ОС версії 15.15 і вище підтримують додаткову функцію комутатора, яка називається “service insertion”, яка дозволяє передавати трафік даних DNS на комутатор за допомогою обладнання комутатора, обходячи центральний процесор комутатора і, отже, підвищуючи продуктивність. Обробка пакетів за допомогою CPU комутатора відбувається повільніше, ніж процес обробки пакетів за допомогою обладнання комутатора.

HP Switch model	Switch software version		
	K/KA/WB.15.10.yyyym K/KA/WB.15.10.yyyy K/KA/WB.15.11.yyyy K/KA/WB.15.12.yyyy K/KA/WB.15.13.yyyy	K/KA/WB.15.14.yyyy	K/KA/WB.15.15.yyyy
2920	OpenFlow 1.0	OpenFlow 1.3[1]	OpenFlow 1.3[2]
3500	OpenFlow 1.0	OpenFlow 1.3	OpenFlow 1.3
3800	OpenFlow 1.0	OpenFlow 1.3[1]	OpenFlow 1.3[2]
5400zl v1 modules 5400zl v1/v2 module mix[3]	OpenFlow 1.0	OpenFlow 1.3	OpenFlow 1.3
5400zl v2 modules only	OpenFlow 1.0	OpenFlow 1.3[1]	OpenFlow 1.3[2]
6200	OpenFlow 1.0	OpenFlow 1.3	OpenFlow 1.3
6600	OpenFlow 1.0	OpenFlow 1.3	OpenFlow 1.3
8200zl v1 modules 8200zl v1/v2 module mix[3]	OpenFlow 1.0	OpenFlow 1.3	OpenFlow 1.3
8200zl v2 modules only	OpenFlow 1.0	OpenFlow 1.3[1]	OpenFlow 1.3[2]
Legend: y = software build version, m = software maintenance version			

ArcSight - це універсальне рішення для керування журналами подій, яке об'єднує журнали подій у всій мережі для збору, зберігання та пошуку. HP ArcSight Logger може покращити відповідність, управління ризиками, розвідку безпеки, IT-операції та зусилля, які перешкоджають інсайдерським та просунутим постійним загрозам. Це універсальне рішення для керування журналами подій збирає машинні дані з будь-якого джерела, що генерує журнал подій і об'єднує дані для пошуку, індексації, звітування, аналізу та збереження. І в епоху власних пристроїв, які приносяться із собою (BYOD), і мобільності, це дозволяє комплексне управління зростаючим обсягом даних журналу подій зі зростаючої кількості джерел.

HP Network Protector SDN підримує ArcSight Common Event Format (CEF) передавання системних подій, тому події можна надсилати

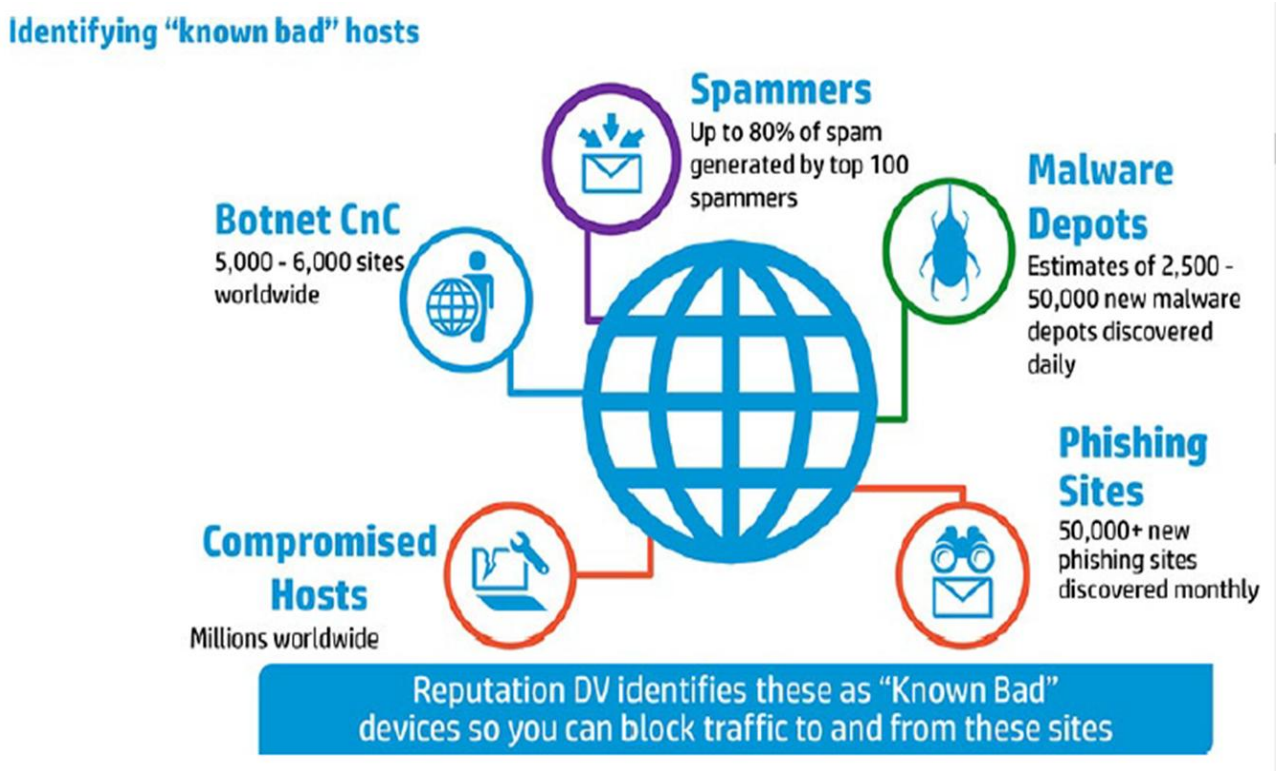
безпосередньо на ArcSight Logger для забезпечення прозорості підприємства. ArcSight CEF сумісний з багатьма загальними серверами Syslog і підтримує всі стандартні сервери Syslog.

HP Network Protector SDN розкриває інтерфейс REST, який Intelligent Management Center (IMC) може використовувати для отримання інформації про політику та статистику.

Програма також може використовувати REST API модуля IMC User Access Management (UAM) для отримання і кореляції кінцевих користувачів за допомогою IP-адрес та MAC-адрес кінцевих точок, що збираються з пакетів DNS, отриманих у програмі.

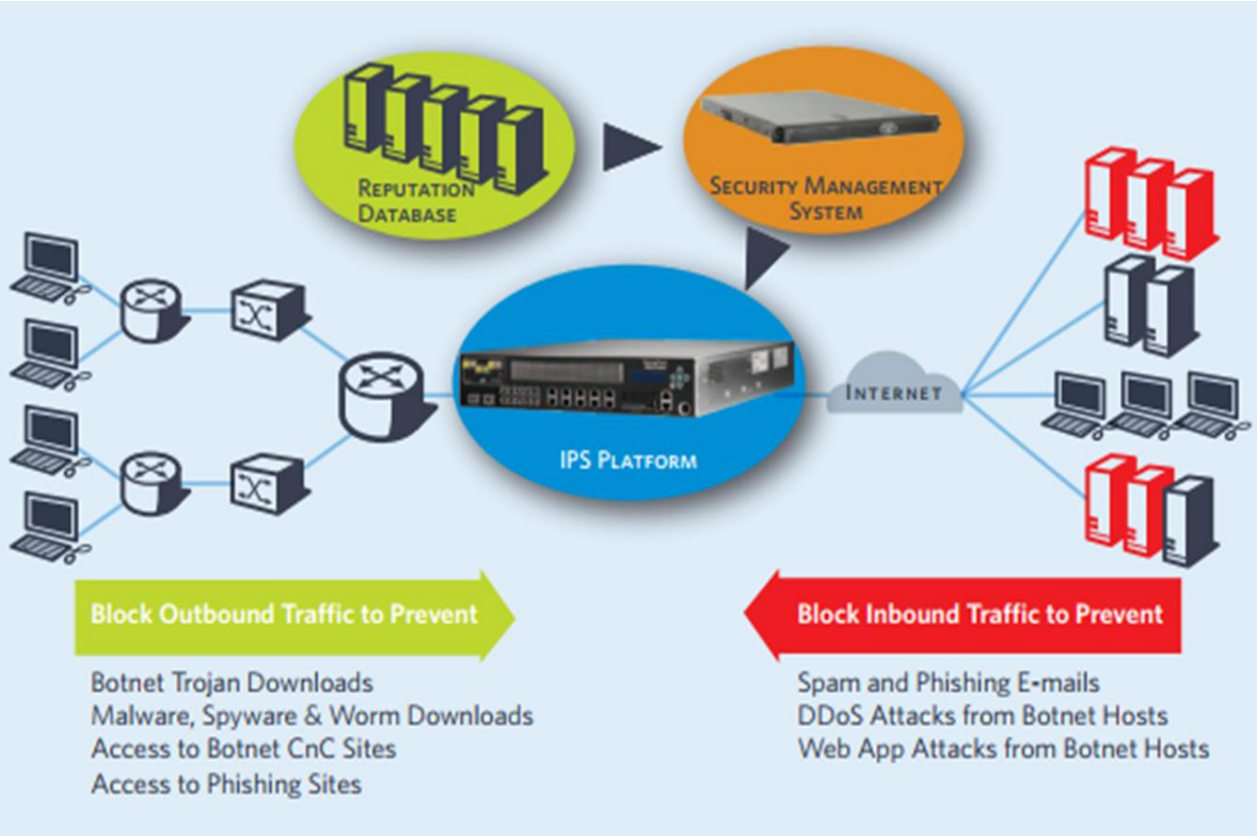
TippingPoint Reputation Digital Vaccine (RepDV), це служба підписки, яка дозволяє організаціям контролювати та блокувати вхідні та вихідні повідомлення з відомими шкідливими та небажаними хостами. RepDV - надійний інформаційний сигнал безпеки, який використовує розширені аналітики та глобальну базу даних репутації IPv4, IPv6 та DNS-імен.

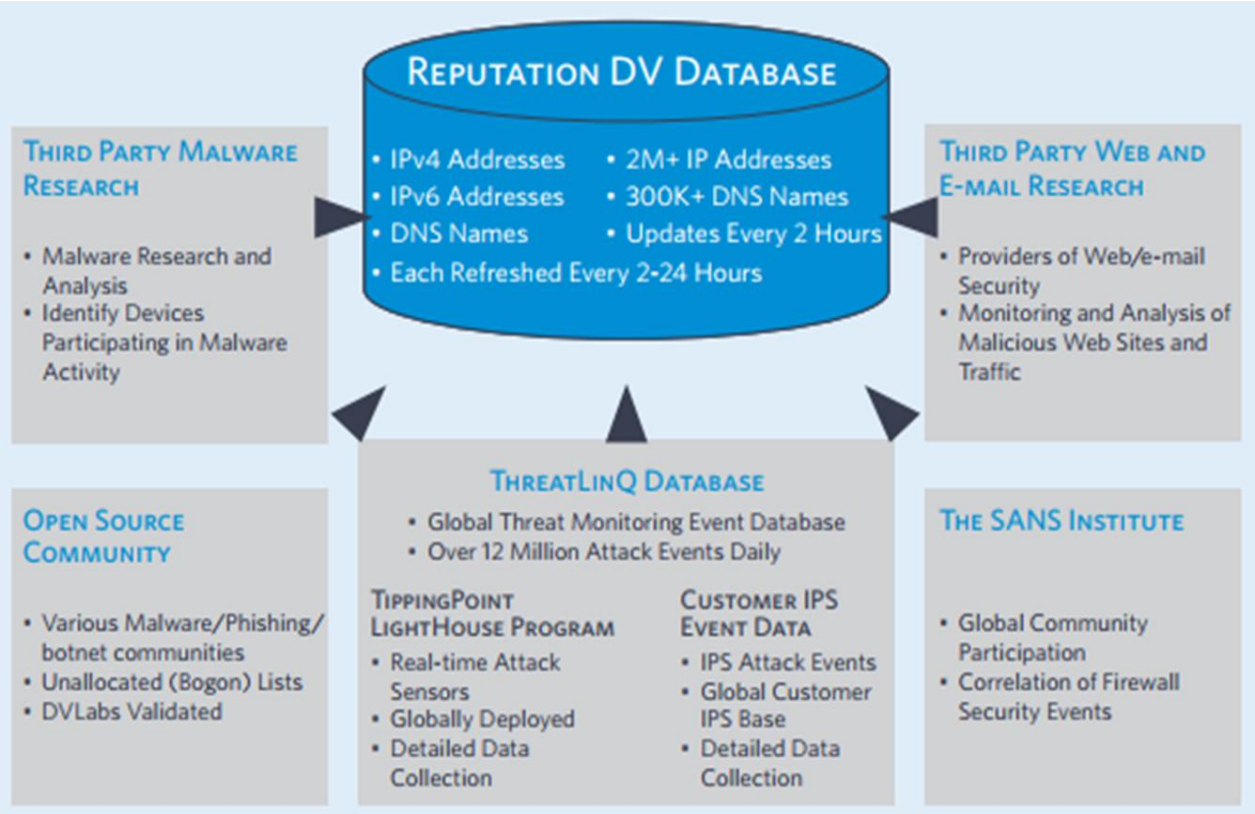
База даних RepDV містить більше мільйона відомих шкідливих або небажаних хостів, зібраних з глобальної інтелектуальної мережі HP TippingPoint ThreatLinQ, репозитарія зловмисного програмного забезпечення DVLabs, комерційних джерел сторонніх виробників та чорних списків з відкритим кодом (дивись малюнок нижче).



Базова оцінка загрози 1-100 призначається для кожного запису на основі аналізу активності, джерела, категорії та загрози DVLabs. Клієнти можуть настроювати політику RepDV на основі репутаційного рейтингу, категорії або геолокації, щоб задовольнити власні вимоги до безпеки. RepDV оновлюється кілька разів на день, щоб попередити нові загрози та зменшити ризики для клієнтів.

Програма взаємодіє з хмарною службою RepDV, щоб завантажити базу даних RepDV та оновити її локальну копію. Після фільтрації на основі політики, визначеної в програмі, ця база даних є основою для порівняння назв імен DNS. Програма опитує служби оновлень кожні 2 години (регулюється з графічного інтерфейсу), щоб зберегти себе оновленою за останніми загрозами.





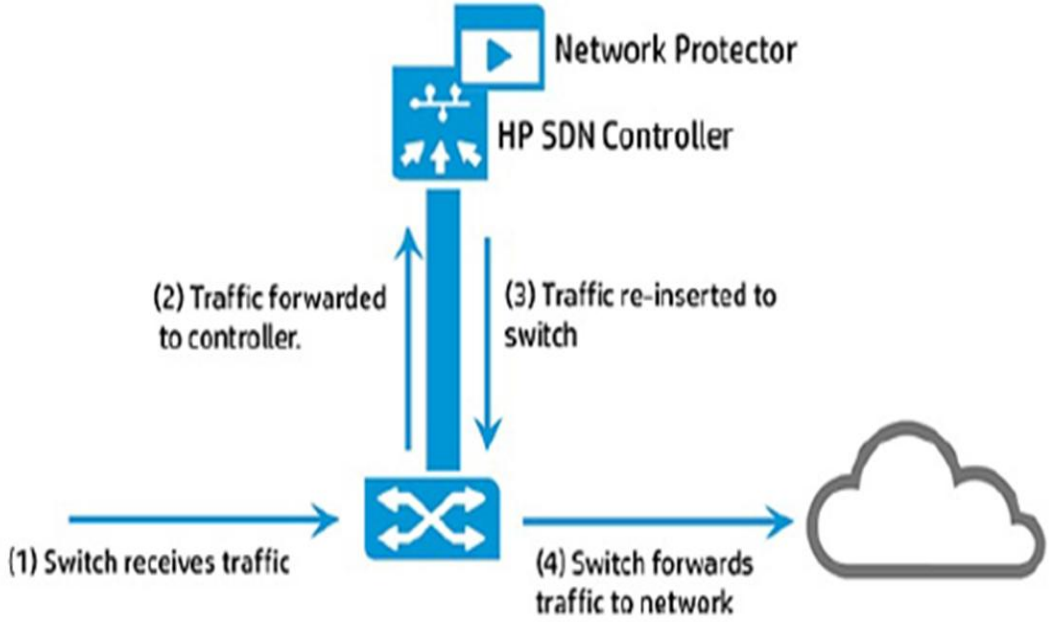
HP Network Protector SDN є програмою безпеки для HPE Virtual Application Networks SDN Controller. HP Network Protector реалізує 2 головні функції: охорона DNS та охорона IP. Обидві функції надають можливість TippingPoint's Cloud Reputation Services забезпечити захист від ботнетів та шкідливих програм розподіленим способом через інфраструктуру комутації.

Service Insertion є функцією, що дозволяє вставляти службу інспектування пакетів у звичайний трафік. Використовуючи правила потоку OpenFlow, трафік може бути перенаправлений на Protector контролера для перевірки та прийняття рішень. Існує два режими, в яких трафік перевіряється Protector:

1. Внутрішня перевірка, яка називається перехопленням (intercept), де трафік перенаправляється на Protector. Protector знову вставляє легітимний трафік у конвеєр комутатора для обробки та переадресації, як звичайно.

2. Зовнішня перевірка, яка називається краном (tap), де трафік відзеркалюється на Protector, який повторно активує потокові записи списків blacklist та whitelist, які потрібно кешувати та застосувати за допомогою комутатора. Після цього комутатор керує видаленням шкідливих потоків або пересиланням легітимних потоків і продовжує надсилати копії нових потоків до контролера для прийняття рішень. Тунелі крана відзеркалюють потік з комутатора на віддалений кінцевий пристрій і є однонаправленими за визначенням. Комутатор не отримує пакети назад із тунеля.

HP Network Protector SDN використовує протокол OpenFlow для перенаправлення трафіку від комутатора до програмного додатку і там порівнюється з TippingPoint RepDV для прийняття рішення щодо переадресації або блокування (дивись малюнок).



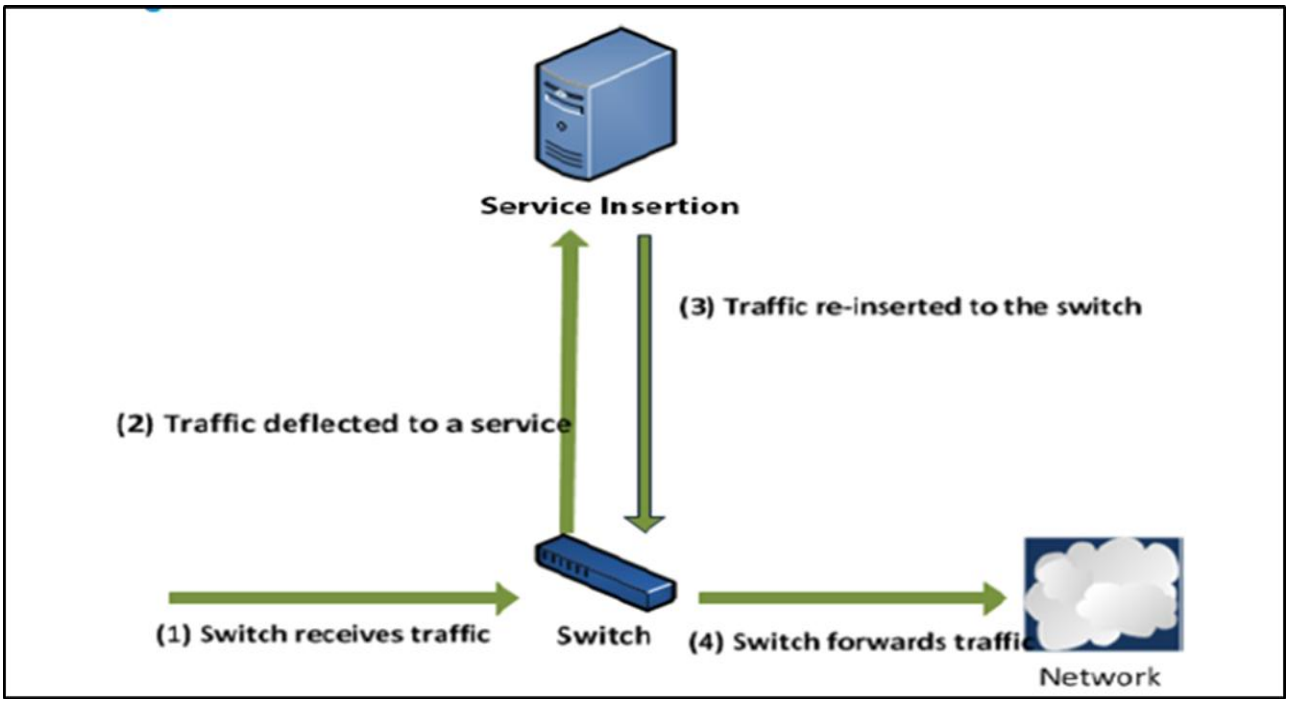
Проте пакети нових потоків потрібно скопіювати на процесор комутатора для обробки, а потім перенаправлення до програми Network Protector, що обмежує продуктивність в діапазоні десятків мегабіт на секунду.

Щоб максимально збільшити продуктивність і підтримати комутатор, що робить те, що найкраще, тобто комутацію пакетів, обладнання комутатора використовується для передачі трафіку безпосередньо на програму Network Protector, що дає потенційне покращення продуктивності в діапазоні гігабіт на секунду.

Іншими словами, пакети перенаправляються за допомогою обладнання комутатора через service insertion tunnel, а не за допомогою CPU комутатора через порт OpenFlow.

Бажана найкраща продуктивність для програми досягається за допомогою комутаторів, що підтримують технологію OpenFlow і тунельну технологію service insertion.

- Service insertion tunnels are GRE tunnels between Network Protector Controller and the switch
- Service Insertion tunnels are created one per switch per controller
  Service Insertion is handled by the ASIC (no CPU processing overhead)
- DNS not be sent to controller OpenFlow port, but rather the service insertion tunnel



Апаратні IP тунелі використовуються для ввімкнення service insertion. Вони представлені у вигляді віртуальних портів для агента OpenFlow, що працює на комутаторі. Коли створюється тунель (наприклад, програмою HP Network Protector SDN Application), агент OpenFlow повідомляє про наявність нового інтерфейсу. Агент OpenFlow здійснює комунікацію через цей інтерфейс, як через новий логічний порт для контролера SDN. Цей логічний порт рекламується у всіх випадках протоколом OpenFlow версії 1.3, налаштованим на комутаторі.

Якщо дія вихідного порту OpenFlow для правила потоку вказує на логічний порт тунелю, пакети, що відповідають цьому правилу потоку, перенаправляються на налаштований тунель кінцевого пристрою через тунельний інтерфейс.

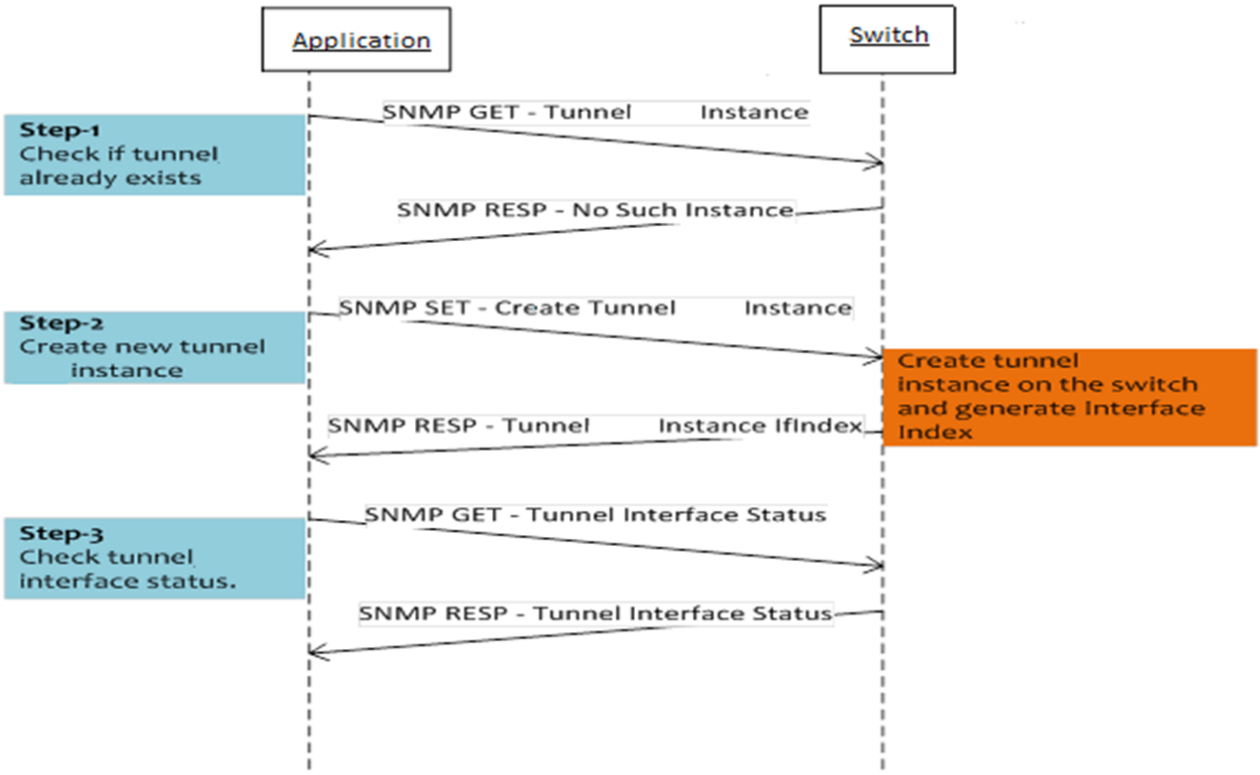
Коли фрейм інкапсулюється і надсилається контролеру, фрейм містить заголовки MAC та тег VLAN. Навіть якщо оригінальний фрейм не має тега VLAN, комутатор здійснює тегування цього фрейму за допомогою ідентифікатора VLAN-ID, встановленого для стандартного VLAN вхідного порту перед його інкапсуляцією. Оскільки кадри є інкапсульованими, шлях, який перетинає інкапсулізований пакет, повинен бути налаштований з більшим максимальним блоком передачі (MTU).

Можна створити до 16 унікальних тунельних інтерфейсів для активного пересилання трафіку. Тунелі є лише IPv4. Тунелі IPv6 не підтримуються у поточній версії.

Тунелі можуть бути створені за допомогою протоколу Simple Network Management Protocol (SNMP). Комутатор керує тунелями, при цьому кожен тунель представляє унікальний індекс інтерфейсу.

Перший крок програмного додатку (наприклад такого як HP Network Protector SDN) міститься у запиті комутатора, щоб визначити, чи підтримує він конфігурування тунелів. Це здійснюється через SNMP, який визначає кількість тунельних інтерфейсів, що підтримуються на комутаторі.

Після визначення того, що тунелі можуть бути налаштовані, контролер може перейти до наступного кроку - створити відповідний інтерфейс.

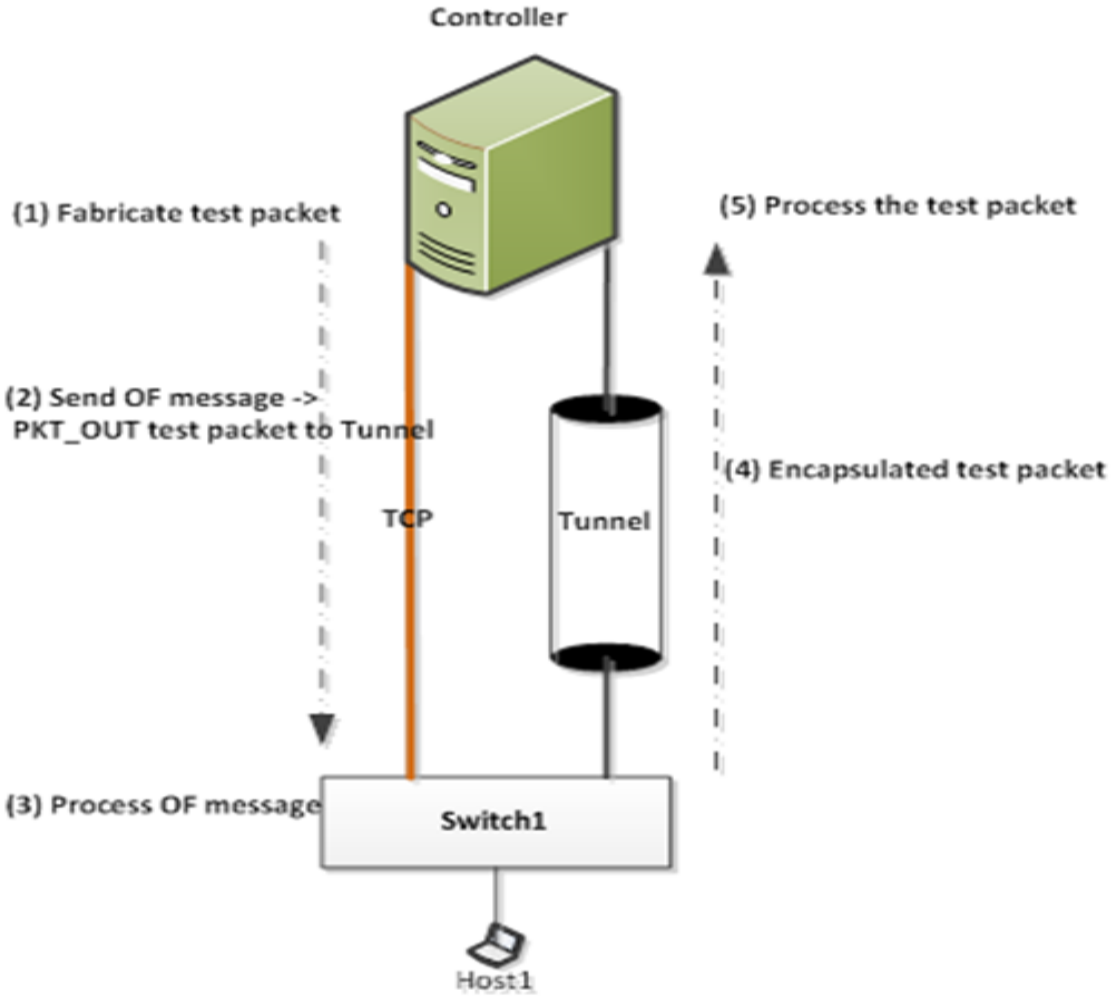


Виявлення статусу підключення тунелю за допомогою повідомлення OpenFlow:

Якщо програмний додаток не отримує будь який пакет через інтерфейс тунеля протягом певного періоду часу, він може перевірити, чи активний тунельний канал передачі шляхом створення "heartbeat" пакета та відправки OpenFlow пакета повідомлення OUT на комутатор з вихідним портом для "heartbeat" пакета як тунельного інтерфейса.

Коли комутатор приймає повідомлення OpenFlow, він надсилає "heartbeat" інкапсульований фрейм через тунельний інтерфейс до програми.

Програма може використовувати це повідомлення, щоб підтвердити, що канал передачі тунелю працює нормально.



3.2 Встановлення та налаштування HP Network Protector SDN та ліцензії SDN

The HP Network Protector SDN інсталюється через графічний інтерфейс HP VAN SDN Controller, точно также як Flow Maker Deluxe, як показано у Lecture 2.

1. Щоб увійти до HP VAN SDN Controller, необхідно відкрити вікно браузера та ввести таку веб-адресу: https://<IP_Address_of_controller>:8443/sdn/ui

2. Введіть логін та пароля натисніть Login.

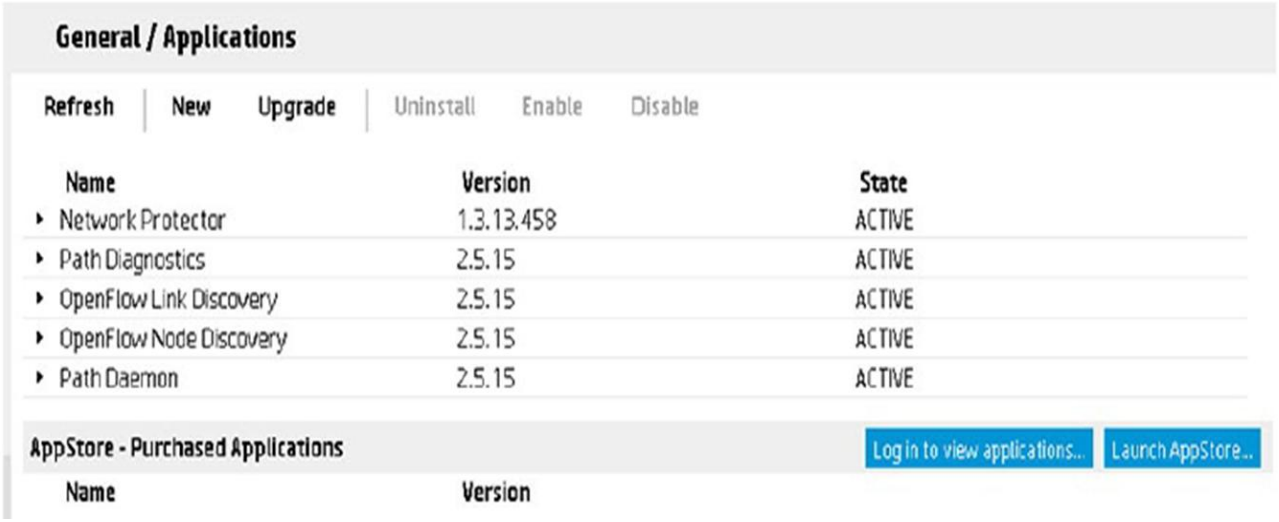
3. З'явиться головна сторінка HP VAN SDN Controller.

4. Перейдіть до General→Applications.

5. Виберіть New→Browse. Перейдіть на локацію, де розміщено zip file програмного додатку (com.hp.sdn.app.networkprotector_v1.3.X.YYY.zip) та клікніть Open.

6. Виберіть Upload щоб завантажити додаток.

7. Виберіть Deploy для розгортання додатку. Програма встановлена, як показано на малюнку.



Наступні ліцензії доступні для HP VAN SDN Controller, як показано на малюнку.

Product Numbers

J9863AAE - HP VAN SDN Ctrl Base SW w/ 50-node E-LTU

- Base controller license (1 controller node)
- Enables the HP VAN SDN Controller to communicate with up to 50 OpenFlow DPIDs
- Prerequisite for other licenses

J9864AAE - HP VAN SDN Ctrl 50-node E-LTU

- Base controller plus 50 "Add Nodes" license
- Extends by 50 the number of DPIDs the base controller can communicate with using OpenFlow
- Requires J9863AAE

J9865AAE - HP VAN SDN Ctrl HA E-LTU

- High Availability "Add Controller" license
- Enables the HP VAN SDN Controller to form a team for increased availability
- Requires J9863AAE

Базова ліцензія контролера. HP VAN SDN Ctrl Base SW w/50–node E-LTU. Включає HP VAN SDN Controller для зв'язку з 50 OpenFlow Datapath IDs (DPID). Ця ліцензія є обов'язковою умовою для інших ліцензій та повинна бути встановлена для отримання технічної підтримки протягом перших 90 днів використання.

Базова ліцензія контролера плюс 50 "Add Nodes". HP VAN SDN Ctrl 50–node E-LTU. Розширює базову ліцензію на 50 DPIDs для зв'язку з використанням OpenFlow. Ви можете встановити декілька ліцензій Add Nodes. Наприклад:

1. Якщо встановили одну ліцензію Add Nodes на HP VAN SDN Controller разом із базовою ліцензію, то буде підтримуватись 100 OpenFlow комутаторів.
2. Якщо встановили три ліцензії Add Nodes на HP VAN SDN Controller разом із базовою ліцензію, то буде підтримуватись 200 OpenFlow комутаторів.

Ліцензія високої доступності “Add Controller”. HP VAN SDN Ctrl HA E-LTU. Дозволяє HP VAN SDN Controller сформувати команду для підвищення доступності. Застосовуються наступні правила:

1. Мінімальна кількість членів команди для HP VAN SDN Controller має бути три.

2. Під час формування команди потрібна лише одна базова ліцензія HP VAN SDNController разом із, як мінімум, двома ліцензіями високої доступності. Після створення команди, може бути додана ліцензія Add Nodes до лідера команди для збільшення підтримки. Крім того, необхідно:

Використовувати неліцензовані контролери для створення команди.

Використовувати нову апаратну платформу (або віртуальну машину) з новою інсталяцією контролера HP VAN SDN.

Запускати однакову версію програмного забезпечення на всіх контролерах.

HP Network Protector SDN використовує електронні ліцензії. Ви повинні мати встановлені ліцензії HP VAN SDN Controller і після цього можна встановити ліцензії HP Network Protector. Малюнок і таблиця (показана на наступному слайді) надають більше інформації про ліцензії HP Network Protector SDN.

Required Licenses	License Product #	Description	Quantity (no of clients)	Validity	Pre-requisite license product #
1. Network Protector Base License	JL004AAE	HP Net Protector SDN App 250 User E-LTU	250	Never Expires	J9863AAE (SDN Controller Base License)
2. Network Protector RepDV Subscription License	JL005AAE	HP Net Protector RepDV 250 User 1yr E-LTU	250	1 year	JL004AAE (Network Protector Base License)
	JL006AAE	HP Net Protector RepDV 1k User 1yr E-LTU	1000	1 year	
	JL007AAE	HP Net Protector RepDV 2k User 1yr E-LTU	2000	1 year	
	JL008AAE	HP Net Protector RepDV 4k User 1yr E-LTU	4000	1 year	
	JL092AAE	HP Net. Protector RepDV Sub 8000 1yr E-LTU	8000	1 year	
	JL093AAE	HP Net. Protector RepDV Sub 20,000 1yr E-LTU	20,000	1 year	
	JL094AAE	HP Net. Protector RepDV Sub 40,000 1yr E-LTU	40,000	1 year	

Product number	Product description	Validity
JL004AAE	HP Network Protector SDN Application 250 Concurrent Users E-LTU	Perpetual
JL005AAE	HP Network Protector RepDV Subscription 250 Concurrent Users 1 Year E-LTU	1 year
JL006AAE	HP Network Protector RepDV Subscription 1000 Concurrent Users 1 Year E-LTU	1 year
JL007AAE	HP Network Protector RepDV Subscription 2000 Concurrent Users 1 Year E-LTU	1 year
JL008AAE	HP Network Protector RepDV Subscription 4000 Concurrent Users 1 Year E-LTU	1 year
JL092AAE	HP Network Protector RepDV Subscription 8000 Concurrent Users 1 Year E-LTU	1 year
JL093AAE	HP Network Protector RepDV Subscription 20,000 Concurrent Users 1 Year E-LTU	1 year
JL094AAE	HP Network Protector RepDV Subscription 40,000 Concurrent Users 1 Year E-LTU	1 year

JL004AAE HP Net Protector SDN App 250 User E-LTU є базовою ліцензією HP Network Protector. Придбана ліцензія ніколи не закінчується. Необхідно придбати принаймні одну базову ліцензію. Кількість необхідних базових ліцензій визначається максимальною кількістю одночасних користувачів, які використовують програму в активному сеансі. Тривалість кожного активного сеансу - 15 хвилин.

Наприклад, якщо ви купуєте чотири базові ліцензії HP Network Protector SDN Application на 250 користувачів кожна, то максимальна кількість користувачів із додатком у активному сеансі становить 1000 (4 × 250).

Ліцензія HP Net Protector RepDV використовується для підписки на базу даних RepDV. Термін дії підписки на ліцензії HP Network Protector RepDV - 1 рік. Існує чотири види підписки на ліцензії HP Network Protector RepDV, які розраховані на 250, 1000, 2000, 4000, 20,000 та 40,000 користувачів. Необхідність в підписці на ліцензії HP Network Protector RepDV визначається кількістю користувачів, які користуються базовою ліцензією. Користувачі HP Network Protector SDN Application мають унікальну пару MAC і IP адреси.

Наприклад, якщо ви придбали чотири базові ліцензії HP Network Protector на 250 користувачів кожна (1000 users), потім ви повинні придбати ліцензію HP Network Protector RepDV на 1000 або більше ніж 1000 користувачів.

Якщо ви не придбали підписку на ліцензію HP Network Protector RepDV, ви можете використовувати програму зі своїми власними списками, такими як blacklist або whitelist. Однак ви не зможете отримати доступ до бази даних TippingPoint RepDV. Якщо ви не оновили підписку на ліцензію HP Network Protector RepDV після закінчення терміну дії, ви можете зайти на базу даних RepDV, але не будете отримувати оновлення RepDV із сервера TippingPoint.

Під час підписки на RepDV користувачі можуть отримати доступ до підписки на ліцензію RepDV більше ніж базова ліцензія HP Network Protector. Після закінчення терміну дії підписки на ліцензію RepDV, необхідно більш

високий рівень підписки на ліцензію RepDV для співпадання з базовою ліцензію.

Ви можете додати ліцензії на контролер HP VAN SDN наступним чином. Також дивись Малюнок:

HP SDN Controller Base license key:

https://<sdn_controller_ip_address>:8443/sdn/ui

HP Network Protector Application Base license key:

https://<sdn_controller_ip_address>:8443/networkprotector/ui

Order of License addition	License keys	URL to use
1	HP SDN Controller Base license key	HP VAN SDN Controller GUI (under Licenses) (https://<sdn_controller_ip_address>:8443/sdn/ui)
2	HP Network Protector App Base license key	
3	HP Network Protector RepDV Activation key	HP Network Protector Application GUI (Setup Wizard) (https://<sdn_controller_ip_address>:8443/networkprotector/ui)

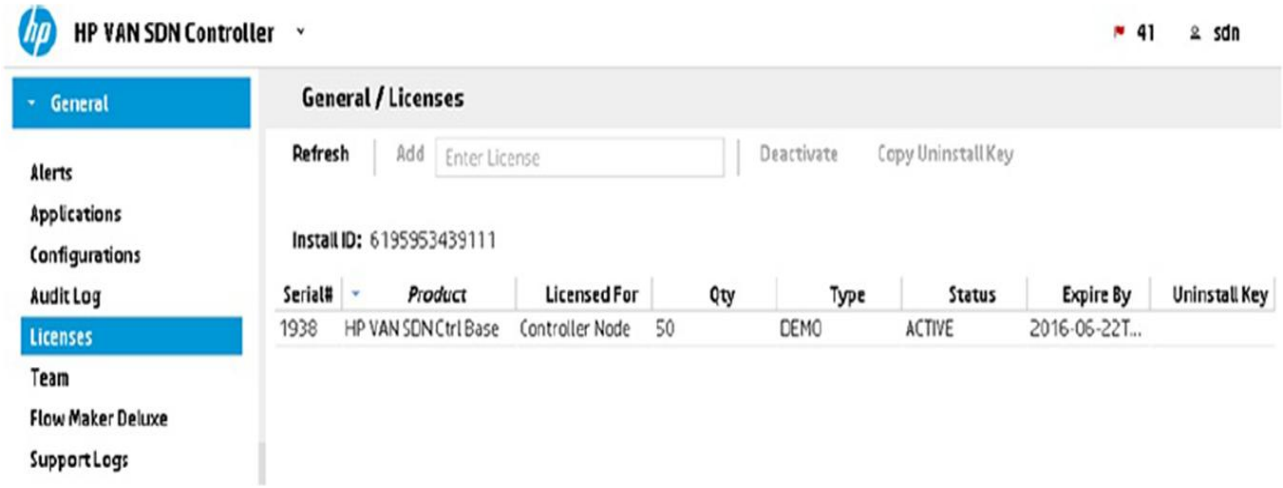
Ви можете отримати ліцензійні ключі від порталу HP My Networking. Після придбання електронних ліцензій HP Network Protector, ви можете зареєструвати їх на My Networking Portal, використовуючи ідентифікатор встановлення контролера HP VAN SDN та отримання ліцензійних ключів програми (дивись Малюнок для URL-адреси). Ви також можете використовувати My Networking Portal для передачі ліцензій на додаток від одного комп'ютера до іншого.

Important. Щоб отримати додаткові відомості про те, як зареєструвати ліцензії на My Networking Portal, дивись Розділ 3 HP Network Protector SDN Application—1.3 Administrator Guide, доступний тут.:

http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c04647299

Нижче наведені **інструкції щодо перевірки ліцензій** HP VAN SDN Controller.

Клікніть Licenses (дивись малюнок). На малюнку приведено приклад демо ліцензії на 50 вузлів.



Якщо ви завантажили оціночні копії HP VAN SDN Controller та Mininet, то можете слідувати інструкціям щоб також **встановити оціночні ліцензії** HP Network Protector.

Використайте App Store для встановлення додатка Trial Mode SDN .

1. Встановіть додаток.
2. Зайдіть на My Networking Portal за адресою http://hp.com/networking/mynetworking та виберіть SDN Evaluation Licenses.
3. Введіть інсталяціонний ID. Networking Portal згенерує ліцензію для цього інсталяціонного ID.
4. Застосуйте ліцензію.

Наведено приклад повідомлення, яке ви отримуєте, коли створюєте базову ліцензію Network Protector. У сповіщення входить Controller Install ID та ліцензійний ключ (дивись нижче малюнок інтерфейса контролера):

This is a confirmation of your registration with the license details:

License key:

AEETMFRDFRCBO-NJTFY7S2ARTOQ-NVM4QKEQZQKGB-RCUESCAAJEEAA

Registration ID: PCR3GVH-J8R7TTW-QDRJBDK-K6RXY89

Product number: JL004AAE

Product name: HP Net Protector SDN App 250 User E-LTU

License quantity: 1

Install ID: 6195953439111

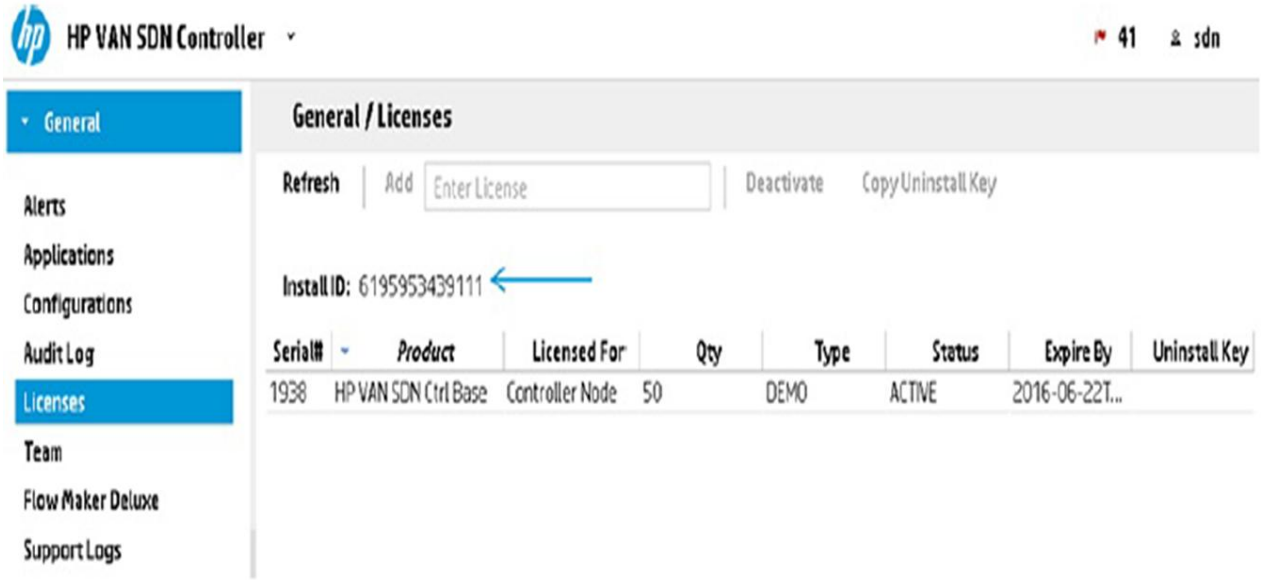
Status: Active

Activation date: 22-Jun-2015

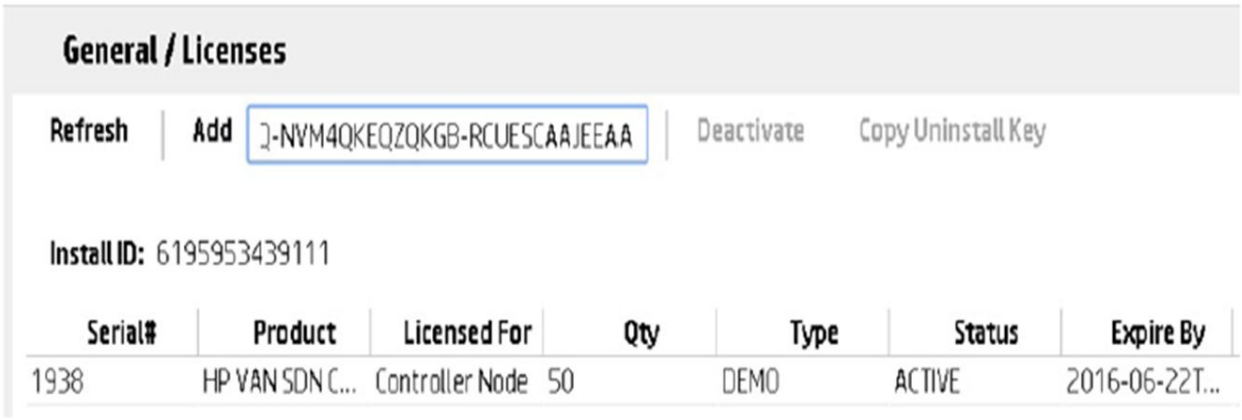
Expiration date: 21-Jun-2016

Friendly name: Net Protector

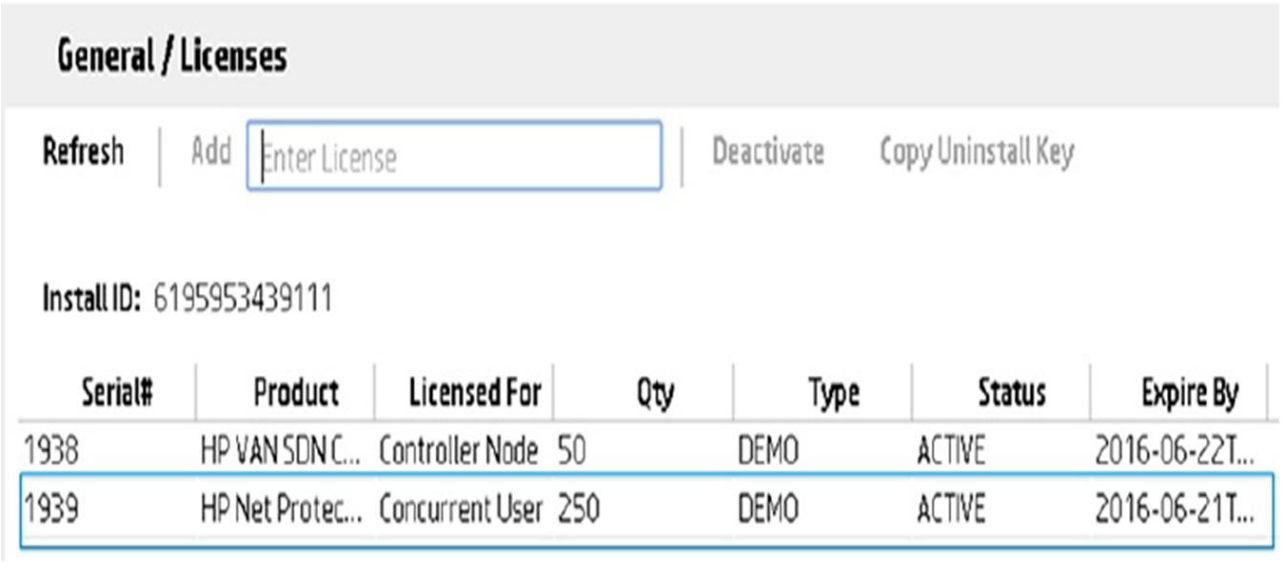
Customer notes:



5. Скопіюйте ліцензійний ключ в Enter License box контролера (дивись малюнок) і клікніть Add:



Ліцензія буде додана на контролер, як показано на малюнку:



3.3 Інтеграція HP Network Protector SDN з комутаторами HP

OpenFlow-сумісні комутатори мають два типи: OpenFlow-only та OpenFlow-hybrid.

OpenFlow-only switches підтримує лише функцію OpenFlow, в цих комутаторах всі пакети обробляються конвеєром OpenFlow і не можуть бути оброблені інакше.

OpenFlow-hybrid switches підтримує як функцію OpenFlow, так і звичайну Ethernet комутацію, тобто традиційну комутацію L2 Ethernet, ізоляцію VLAN, маршрутизацію L3 (маршрутизацію IPv4 та маршрутизацію IPv6), обробку ACL та QoS. Ці комутатори повинні забезпечувати механізм класифікації за межами OpenFlow, який спрямовує трафік на конвеєр OpenFlow або звичайний конвеєр. Наприклад, комутатор може використовувати тег VLAN або вхідний порт пакета, щоб вирішити, чи

обробляти пакет, використовуючи один конвеєр або інший, або він може спрямовувати всі пакети на конвеєр OpenFlow.

Установки гібридного режиму визначають, які рішення щодо переадресації пакетів виконуються контрольованими комутаторами OpenFlow і які з цих рішень приймає лише контролер.

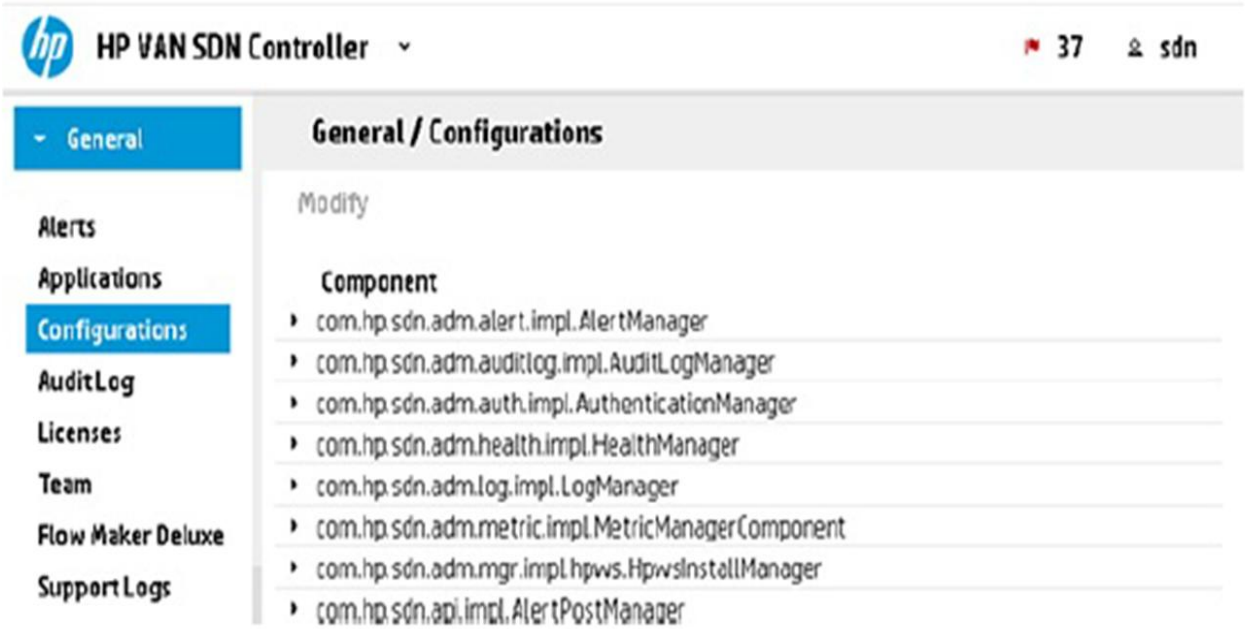
If hybrid mode is enabled (установки за замовчуванням), контролер делегує нормальну переадресацію пакетів до контрольованих комутаторів, але ігнорує ці комутатори та замінює їх на нестандартні рішення для пересилання пакетів, які необхідні встановленим програмам для певних типів пакетів. У цьому режимі контролер покладається на контрольовані комутатори, щоб забезпечити усунення мережних петель та визначення шляхів переадресації за допомогою традиційних мережевих механізмів (таких як протокол Spanning Tree Protocol [STP] і Open Shortest Path First [OSPF].

If hybrid mode is disabled, контролер приймає рішення про перенаправлення для всіх пакетів у мережі, контрольованої OpenFlow. У цьому стані контролер сам усуває мережеві петлі та визначає шляхи переадресації.

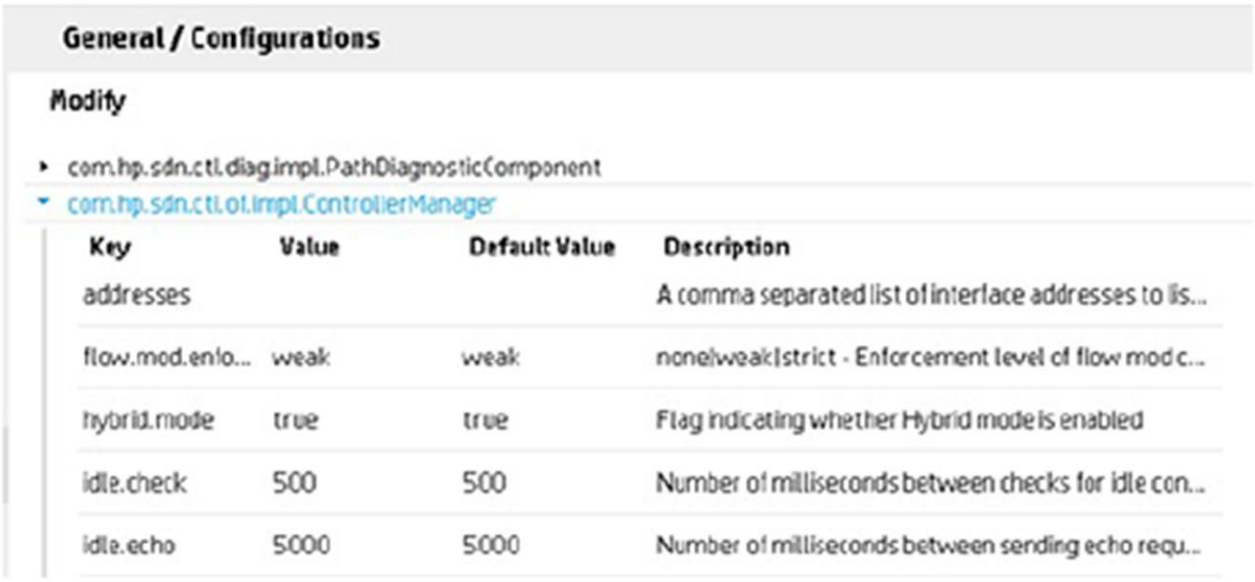
Наступні інструкції покажуть, яким чином перевірити, що гібридний режим увімкнено на контролерах HP VAN SDN.

- Запустити Google Chrome on a Windows desktop.
- Здійснити навігацію за адресою https://<controller IP address>:8443/sdn/ui
- The HP VAN SDN Controller за замовчуванням використовує самопідписаний сертифікат. Прийміть сертифікат і продовжуйте входити.
- 4. Якщо буде запропоновано, увійдіть, використовуючи такі облікові дані: Username: sdn Password: skyline

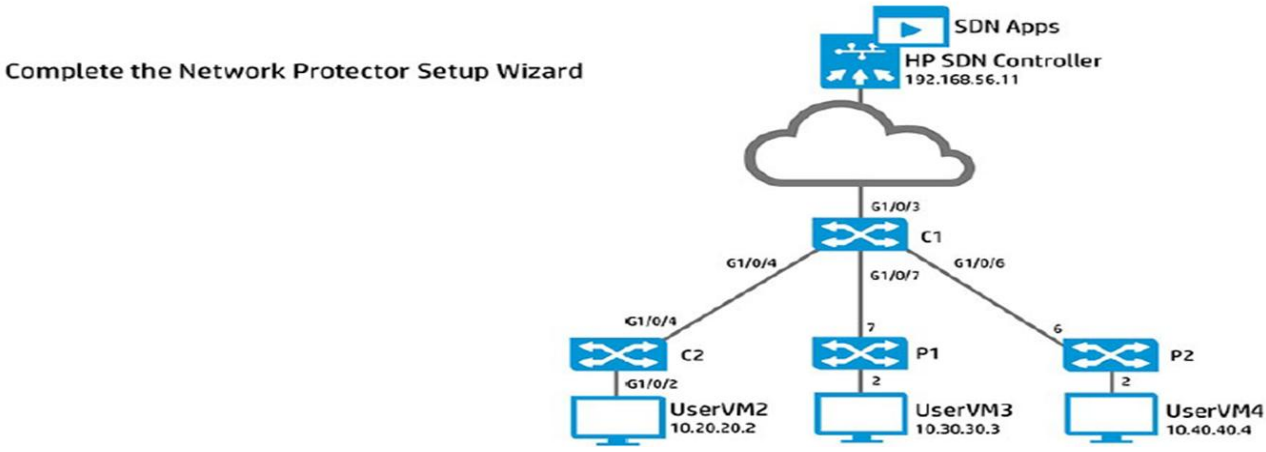
5. Клікніть Configurations, як показано на малюнку:



6. Вибери *com.hp.sdn.ctl.of.impl.ControllerManager*. Якщо гібридний режим включено, значення ключа hybrid.mode має бути true, як показано на малюнку.



Для налаштування програми знадобиться ліцензійний ключ RepDV та облікові дані SNMPv3 принаймні одного комутатора вашої мережі. (На малюнку ілюструється приклад топології мережі.) Ви можете ввести облікові дані SNMPv3 не більше ніж трьох комутаторів вашої мережі. Програма використовує облікові дані для спілкування з комутатором та аналізу деталей комутатора. Вона використовує ці дані для налаштування *service insertion tunnels.*



Якщо ви не надасте облікові дані SNMPv3, тоді програма зв'язується з комутатором через канал OpenFlow.

Використовуйте браузер для доступу до інтерфейсу програми за такою IP-адресою: *https://<system ip_addr:8443>/networkprotector/ui*, де ip_addr є IP-адресою системи, на якій встановлено додаток. Наприклад: *https://192.168.56.7:8443/ networkprotector/ui*.

Як показано на малюнку, майстер налаштування з'являється при першому вході в програму.

Введіть ліцензійний ключ RepDV до поля TippingPoint RepDV Activation Key (дивись малюнок). Появиться сторінка активаційного ключа TippingPoint RepDV. Перед регістрацією підписки на ліцензію HP Network Protector RepDV, необхідно впевнитися, що зареєстрована та активована базова ліцензія HP Network Protector. Controller вимагає доступу до Internet, щоб забезпечити доступ до сервера TippingPoint RepDV Server для перевірки валідності ліцензії та завантаження RepDV database.

1. Введіть proxy server та proxy port, якщо це необхідно (дивись малюнок).

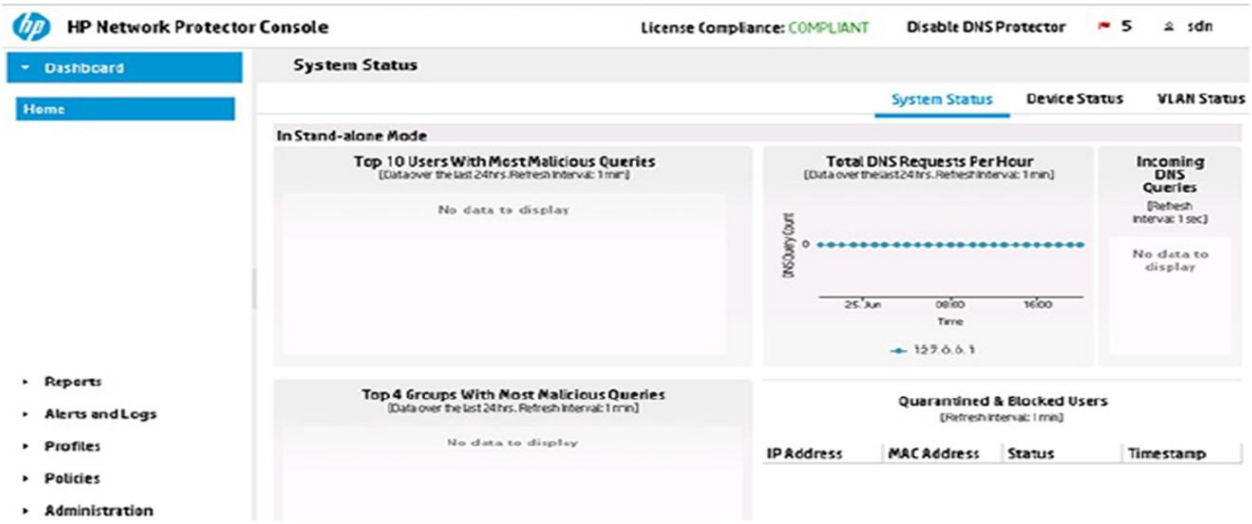
2. Клікніть Next.

3. Введіть облікові дані SNMPv3 принаймні на один комутатор. Облікові дані SNMPv3 використовуються Network Protector для комунікації з мережними пристроями. На малюнку показано Add SNMP credentials інтерфейс. Для HP Network Protector для забезпечення захисту мережі, ці конфігурації є необхідними. Максимум три SNMPv3 облікових даних можуть бути введені і принаймні одні повинні бути введені тут.

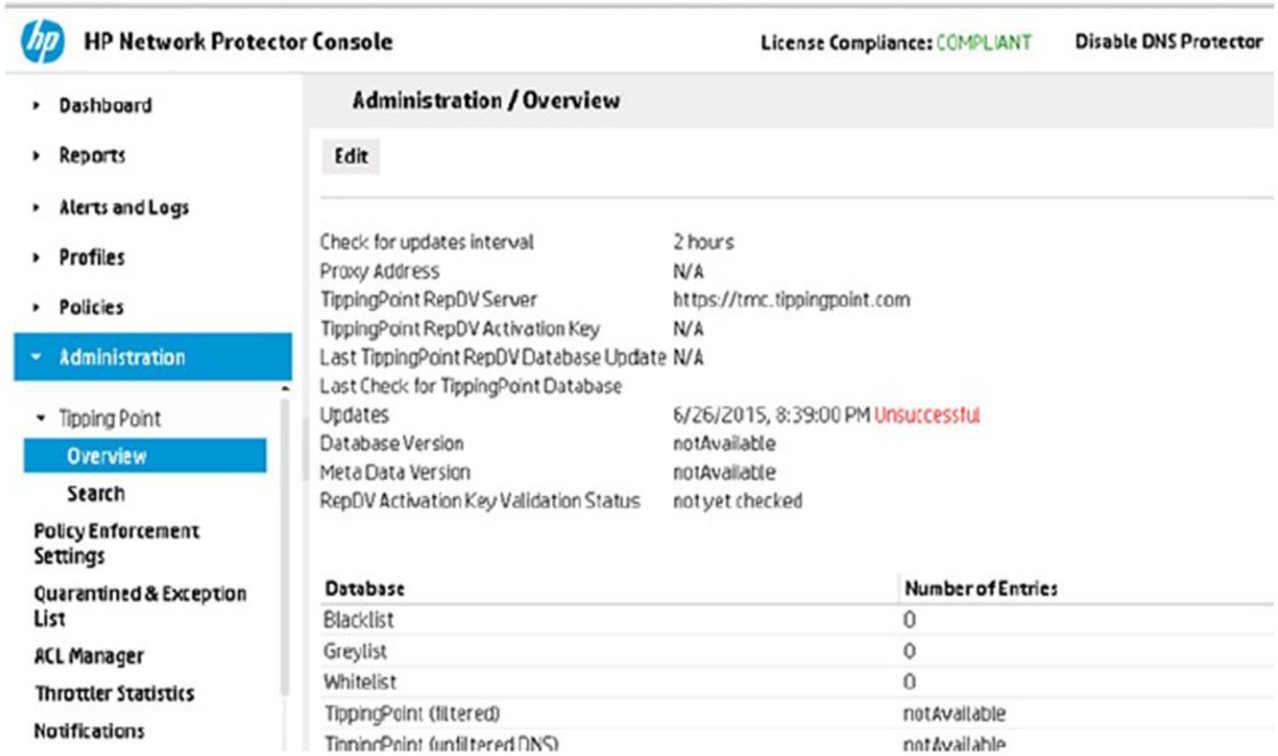
Приклад введення облікових даних SNMPv3:

- Username: sdn
- Authentication type: MD5
- Authentication Password: skyline
- Privacy Type: DES
- Privacy Password: skyline
- Timeout (ms): 10000
- Retries: 2

Консоль HP Network Protector Console появляється тоді, коли буде успішно встановлений та налаштований Network Protector Setup Wizard (дивись малюнок).

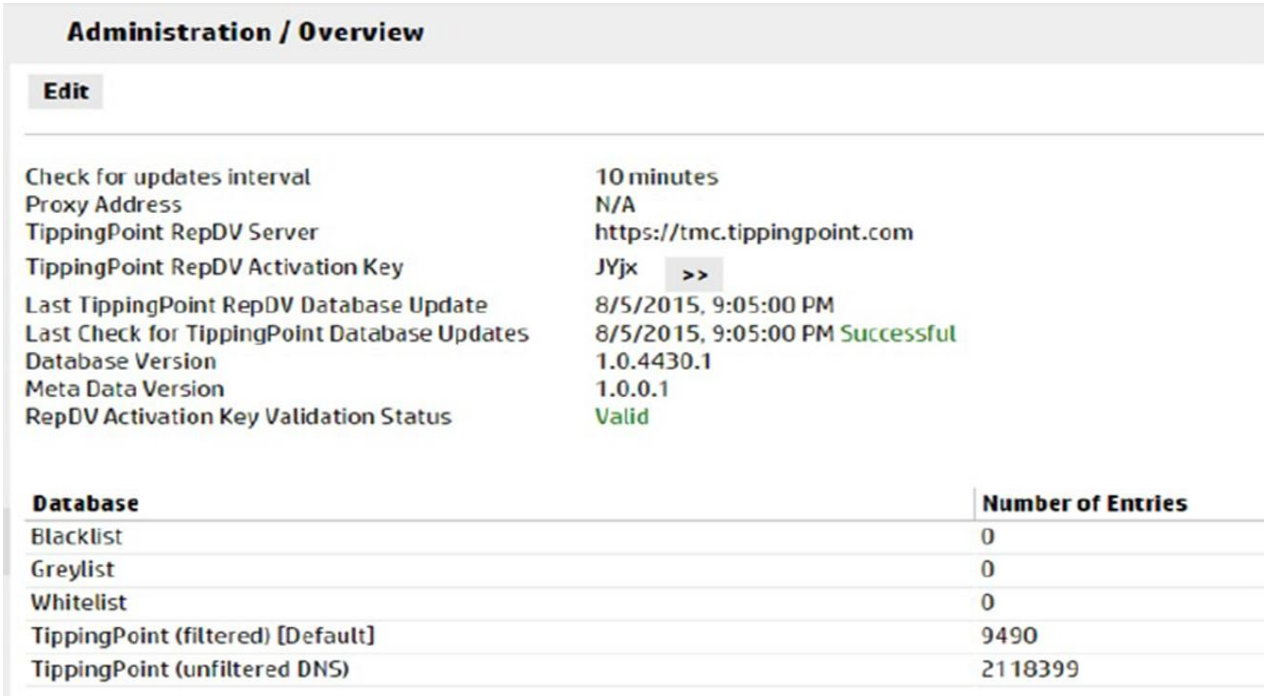


Необхідно зайти на HP Network Protector Console, розділ Administration, сторінка Overview. Серед багатьох інших аспектів цей розділ відображає статус оновлень бази даних RepDV Tipping. У наступному прикладі захоплення екрану (дивись малюнок) ви побачите, що база даних не була успішно оновлена.



Діюча база даних TippingPoint буде виглядати так, як знімок екрана на малюнку. Зверніть увагу на наступне:

- Ліцензія TippingPoint дійсна.
- База даних TippingPoint містить понад 2 мільйони записів.



Switch configuration.

OpenFlow version. OpenFlow потрібен для комутаторів в мережі для програми HP Network Protector SDN для перехоплення запитів DNS.

На малюнку, версія 1.3 OpenFlow використовується для OpenFlow копії vlan20.

```
openflow
  controller-id 1 ip 192.168.56.12 controller-interface vlan 1
  instance “vlan20"
      member vlan 20
      controller-id 1
       version 1.3 only
      enable
      exit
  enable
```

SNMP v3 configuration. Конфігурація SNMPv3 на комутаторах ProVision необхідна для Network Protector, щоб працювати корректно. (На малюнку показано приклад конфігурації SNMPv3.)

SNMP v3 configuration:

```
snmpv3 enable
snmpv3 restricted-access
snmpv3 user sdn auth md5 skyline priv des skyline
snmpv3 group ManagerPriv user sdn sec-model ver3
```

Нижче наведено приклад налаштування SNMPv3 на комутаторі серії 3800:

```
P1(config)# snmpv3 enable

SNMPv3 Initialization process.
```

```
Creating user 'initial'

Authentication Protocol: MD5

Enter authentication password: *******

Privacy protocol is DES

Enter privacy password: *******


User 'initial' has been created

Would you like to create a user that uses SHA? [y/n] n


User creation is done. SNMPv3 is now functional.

Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can
set this later by the command 'snmpv3 restricted-access')? [y/n] y

P1(config)# snmpv3 user sdn auth md5 skyline priv des skyline

P1(config)# snmpv3 group ManagerPriv user sdn sec-model ver3
```

Configure the switch to use the licensed HP Network Protector controller. Наступний приклад конфігурації показує, яким чином здійснити конфігурацію на комутаторі з налаштованим SNMPv3, щоб використати Network Protector controller:

```
P1(config)# openflow

P1(openflow)# controller-id 2 ip 192.168.56.12 controller-interface vlan 1

P1(openflow)# instance vlan30

P1(of-inst-vlan30)# disable

P1(of-inst-vlan30)# no controller-id 1

P1(of-inst-vlan30)# controller-id 2

P1(of-inst-vlan30)# enable

P1(of-inst-vlan30)# end

P1#
```

У наступному прикладі комутатор налаштовується з OpenFlow копія vlan30. Ви можете скористатися командою *show openflow instance <instance>* для перевірки статусу контролера. Нижче наведено приклад цієї команди.

```
P1# show openflow instance vlan30

Configured OF Version : 1.3

Negotiated OF Version : 1.3

Instance Name : vlan30

Admin. Status : Enabled

Member List : VLAN 30

...<omitted>...

Controller Id Connection Status Connection State Secure Role

------------ ---------------- --------------- ------ -----

2 Connected Active No Equal

P1#
```

Ви можете переглядати потоки на комутаторі та знаходити відповідний DNS, використовуючи команду *show openflow instance <instance> flows*. Наступним прикладом цієї команди є команда для копії vlan30.

```
...<omitted>...
Flow 6
 Match
   Incoming Port : Any Ethernet Type : IP
   Source MAC : Any Destination MAC : Any
   Destination MAC Mask : 000000-000000
   VLAN ID : Any VLAN priority : Any
   Source IP Address : Any
   Destination IP Address : Any
   IP Protocol : UDP
   IP ECN : Any IP DSCP : Any
   Source Port : Any Destination Port : 53
 Attributes
   Priority : 50301 Duration : 0 seconds
   Hard Timeout : 8 seconds Idle Timeout : 0 seconds
   Byte Count : NA Packet Count : 21
   Flow Table ID : 100 Controller ID : 2
   Cookie : 0xbadbabe
```

```
   Hardware Index: 1
 Instructions
   Apply Actions
   Output : ServiceTunnel01
```

У цьому прикладі, DNS трафік відправляється на service insertion tunnel. Якщо використовується комутатор 3500, то можна побачити, що порт контролера є вихідним портом.

Якщо комутатор використовує service insertion tunnel, можна скористатися командою *show interfaces tunnel type intercept*, щоб побачити деталі про тунель:

```
P1# show interfaces tunnel type intercept
Status - Service Tunnel Information Brief
  Max. Supported Tunnels : 16
  Total Tunnels : 1
  Interface Index : 100664146
  Name : ServiceTunnel01
  Key : 51966
  Local Address : 10.1.1.253
  Remote Address : 192.168.56.12
  Interface State : Up
P1#
```

Номер *interface index* відображається для *service insertion tunnel*. Це той самий номер, який показано на інтерфейсі HP VAN SDN Controller.

Як показано на прикладі CLI комутатора, команда *show interfaces tunnel* відображає деталі про інтерфейс тунеля.

```
P1# show interfaces tunnel
Tunnel Configuration :
  Tunnel : 100664146
  Tunnel Name : ServiceTunnel01
  Tunnel Status : Enabled
  Source Address : 10.1.1.253
  Destination Address : 192.168.56.12
  Mode : Service Tunnel
  TOS : 0
  TTL : 64
  IPv6 : n/a
  MTU : 1468
Current Tunnel Status :
  Interface State : Up
  Destination Address Route : 0.0.0.0/0
  Next Hop IP : 10.1.1.251
  Next Hop Interface : vlan-1
  Next Hop IP Link Status : Up
  Source Address : 10.1.1.253
P1#
```

Як показує приклад для команди show *interfaces tunnel type intercept statistics*, вона відображає IP-адресу комутатора та контролера серед багатьох інших деталей:

```
P1# show interfaces tunnel type intercept statistics
Service Tunnel Information
Aggregate Statistics
  Fragmented Packets Dropped (Rx) : 0
  Packets to Non-Existent Tunnel : 0
  Unknown Source MAC Packets Dropped (Rx) : 0
  MTU Violation Drop : 0
Service Tunnel Statistics
  Interface Index : 100664146
  Name : ServiceTunnel01
  Rx Packets : 8468
  Tx Packets : 10078
  Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0
  Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
  Rx Heartbeat : 8038
  Tx Heartbeat : 8038
  Last Received Heartbeat Timestamp : 10/05/00 06:18:02
P1#
```

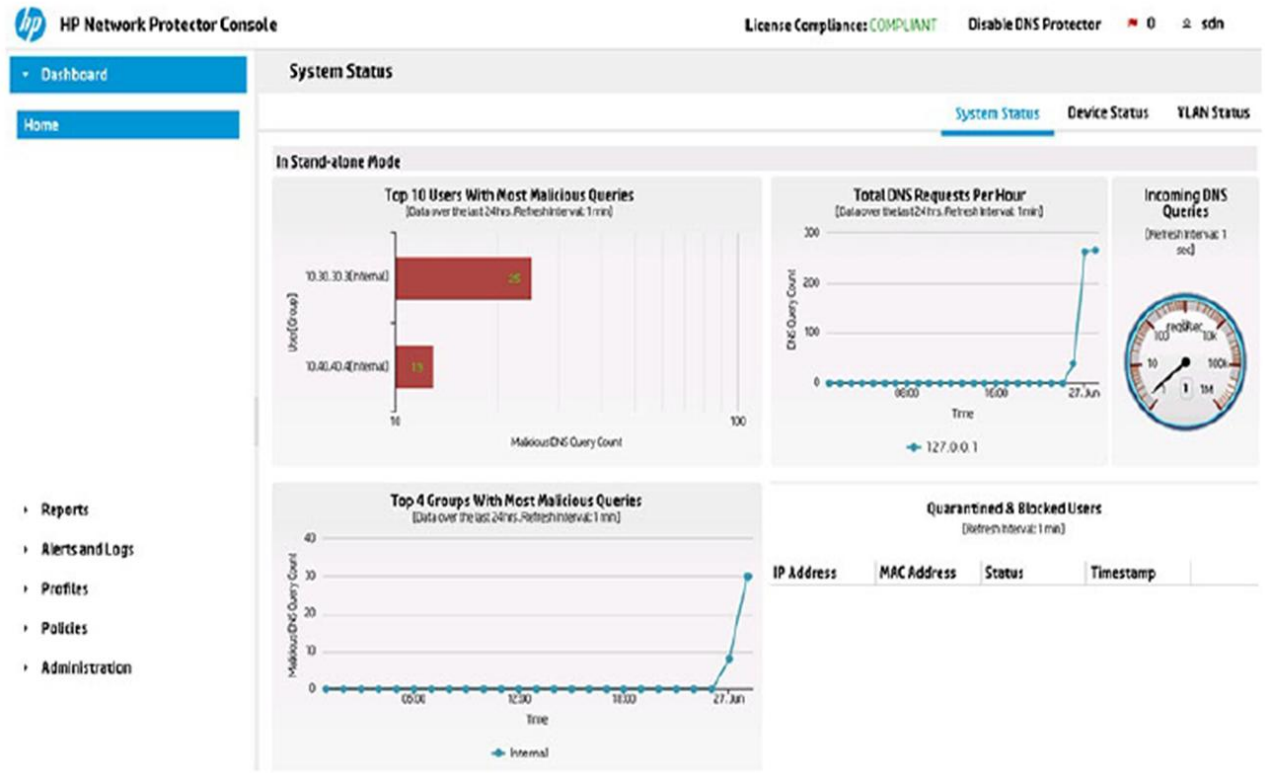
3.4 Network Protector Console

Консоль HP Network Protector забезпечує наочну прозорість стану безпеки своєї мережі з діаграмами та графіками, які постійно оновлюються, щоб відобразити стан та події, пов'язані з мережевим трафіком. Консоль також надає статус усіх комутаторів та VLAN, що взаємодіють із програмним додатком. Цей огляд, що складається з налаштовуваних кольорових графіків і таблиць, є відправною точкою для:

- Моніторингу стану та статусу мережних пристроїв та VLANs.
- Моніторинг попереджень про безпеку або проблеми.
- Усунення несправностей подій та проблем у мережі.

Консоль Network Protector містить настроювані панелі, які дозволяють переглядати, відслідковувати та аналізувати стан здоров'я, а також події на рівні системи та комутатора. Ці панелі забезпечують систему попередження про високий рівень потенційних проблем зі станом та продуктивністю у системі та пристроях. Інструменти стану системи стежать

за характеристиками системи та звітують про основний стан та статус мережі.



Як зазначено в попередньому розділі, використовуйте підтримуваний браузер для доступу до інтерфейсу програми за такою IP-адресою: https://<ip_addr>:8443/networkprotector/ui

Де ip_addr - це IP-адреса системи, на якій ви встановлено програму Network Protector.

Наприклад: https://192.168.56.7:8443/ networkprotector/ui

Введіть облікові дані користувача та пароль, а потім натисніть «Login».

Відображається головна сторінка програми.

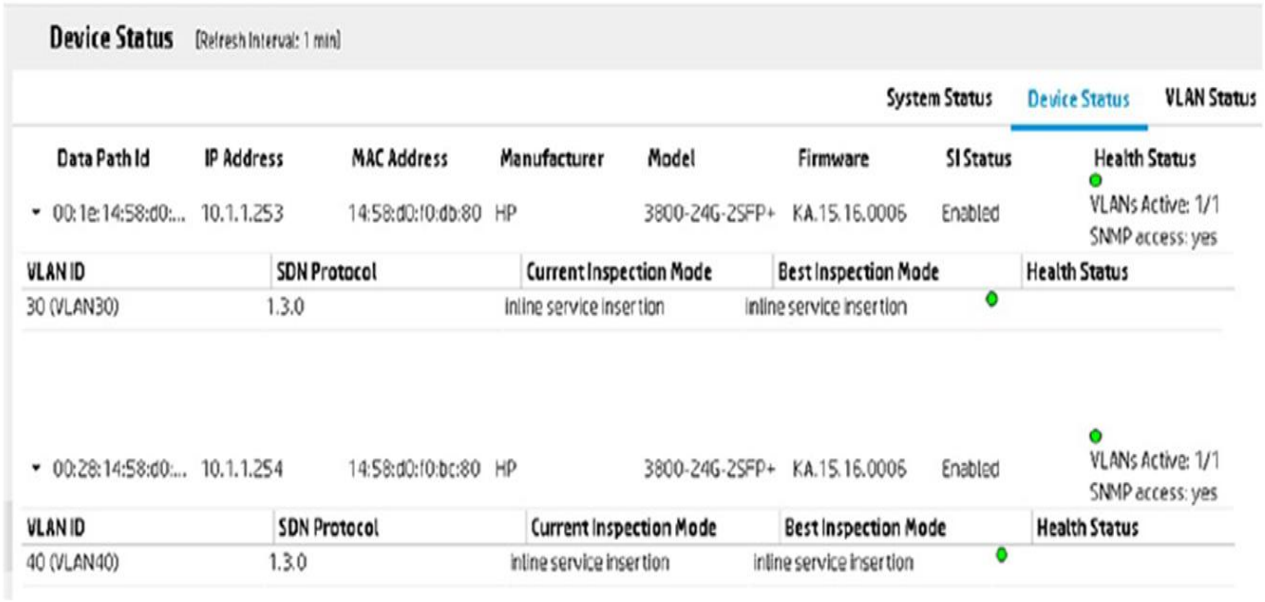
Панель *System Status* забезпечує графічне представлення наступних системних параметрів. Ця інформація оновлюється кожну хвилину.

- Топ десять користувачів із найбільшою кількістю зловмисних запитів протягом останніх 24 годин.
- Загальна кількість запитів DNS за годину протягом останніх 24 годин.
- Вхідні запити DNS за секунду.
- Топ чотири групи VLAN із найбільшою кількістю зловмисних запитів протягом останніх 24 годин.
- Останні десять заблокованих або ізольованих хостів, а також їх IP-адреси, MAC-адреси, статуси та часові штампи.

Виберіть *Device Status* щоб відобразити деталі комутатора та стан статусу VLAN, налаштованого на комутаторі, як показує на малюнку екрану. Докладна інформація включає (але не обмежується):

- IP і MAC адреси комутатора.
- Виробник та деталі моделі комутатора.
- Вбудоване програмне забезпечення, яке встановлено на комутатор та системна інтеграція (SI) статусу комутатора.
- Статус зв'язку комутатора та VLAN.

Device Status Panel:



Програма використовує інформацію про прошивку комутатора, щоб вирішити, чи підтримується зв'язок з цим комутатором через OpenFlow channel або через service insertion tunnel.

Для вбудованого програмного забезпечення версії K.15.14 та нижче, Network Protector взаємодіє з комутатором через OpenFlow channel.

Для вбудованого програмного забезпечення версії KA.15.15.0015 та вище, Network Protector взаємодіє з комутатором або через OpenFlow channel або через service insertion tunnel.

Малюнок вище показує, шо комутатор використовує service insertion tunnel. Тільки комутатор версії 2 ASICs та пізніше підтримують service insertion. У більшості прикладів цього курсу використовуються комутатори або 3800 або 3500. Один із цих комутаторів підтримує service insertion, а інший ні:

- 3800 = v2 ASIC комутатор, service insertion підтримується
- 3500 = v1 ASIC комутатор, service insertion не підтримується

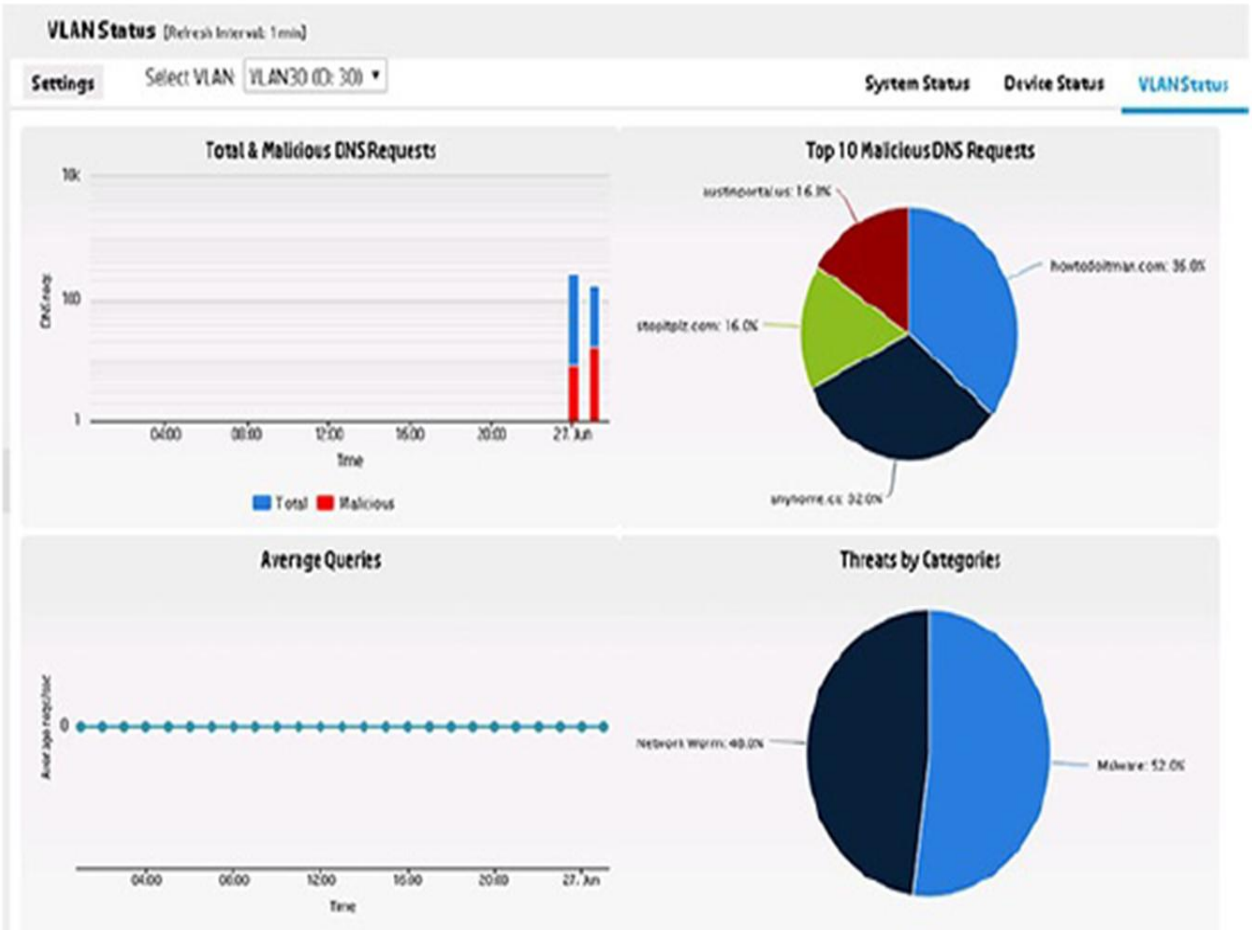
Для перевірки стану *cmamycy VLANs*, налаштованих на комутаторі, виберіть Device Status. Чотири кольори — green, red, yellow, and gray — відображають стан статусу VLANs.

Health status of VLANs	Description
Green	All the conditions are true: • The VLAN is active • The VLAN instance is connected • The SNMPv3 credentials to the switch are correct • The VLAN link is stable • The current mode is reported as the maximum mode
Red	Any one of the conditions is true: • The VLAN instance is not active • The VLAN instance is active but not connected • The SNMPv3 credentials to the switch are incorrect or not working

Health status of VLANs	Description
Yellow	Generally indicates service insertion tunnel issues and any one of the conditions is true: • The VLAN instance is not active • The link is unstable • The current inspection mode
Gray	The VLAN has been disabled from DNS inspection

Клікніть VLAN Status, щоб переглянути деталі запитів DNS від кожного VLAN (див. малюнок нижче). Дані DNS представлені графічно та надають детальну інформацію про запити DNS, що походять від кожної VLAN, налаштованої в мережі. Ви можете налаштувати політику для кожної VLAN на основі наступних звітів і типів загроз:

- Загальні та шкідливі запити DNS
- Середня кількість запитів DNS
- Найпопулярніші запити DNS



Ви можете включити або виключати програмний додаток на VLAN. Якщо ви вимикаєте програму на VLAN, трафік DNS на VLAN не відстежується програмою та трафік передається у звичайному режимі. Відключення програми на VLAN не впливає на конфігурацію та роботу VLAN на підключених комутаторів.

1. Клікніть кнопку VLAN на сторінці консолі. Відображається сторінка статусу VLAN.

2. Виберіть VLAN, який ви хочете вимкнути, у списку «Увімкнути або Вимкнути DNS VLAN».

3. Натисніть «Увімкнути або Вимкнути DNS VLAN», щоб вимкнути додаток на VLAN. Коли програма вимикається на VLAN, вона не контролює трафік на VLAN.

3.5 Користувальницькі blacklists, graylists та whitelists

Ви можете керувати категоріями користувачів, трафіком DNS або VLAN по-різному. Ви також можете керувати трафіком по-різному протягом різних періодів дня чи тижня.

Наприклад, ви можете створити політику, яка дозволить певним користувачам отримати доступ до Інтернет-сайтів, необхідних для виконання своїх обов'язків, або заблокувати їх від сайтів, які можуть використовувати

надто багато пропускної здатності мережі або іншим чином зменшити продуктивність праці.

Ви можете додати *інспекційну політику* перевірки трафіку DNS у вашій мережі та вжити відповідних заходів. Наприклад, інспекційна політика може дозволити певний трафік, але заблокувати або знищити трафік до шкідливих доменів. Політика перевірки може застосовуватися до груп VLAN у вашій мережі. Ви можете застосувати графіки для реалізації політики перевірки.

Щоб створити інспекційну політику та застосувати її до VLAN, необхідно застосувати blacklist та graylist і визначити профіль RepDV. Коли трафік DNS генерується з VLAN, що входить до групи VLAN, пов'язаної з політикою інспектування, а також, коли згенерований DNS міститься у blacklist або graylist, або якщо він співпадає з фільтром RepDv, яка пов'язаний з політикою, то програма виконує вказану дія, наприклад, знищує трафік DNS чи повідомляє адміністратору або одночасно те і інше.

Політика за замовчуванням схожа на інспекційну політику, за винятком того, що вона активна постійно. Ви можете застосовувати політику за замовчуванням лише до внутрішньої (за замовчуванням) групи VLAN. Жодна інша група VLAN не може бути долучена до цієї політики. Ця політика перевіряє вхідні пакети DNS лише на фільтр RepDV за замовчуванням. Ви не можете приєднатися до іншого фільтру RepDV.

Ви можете призначити blacklist та graylist за замовчуванням. Весь трафік DNS у мережі постійно порівнюється з профілями, доданими до політики за замовчуванням. Якщо трафік у мережі відповідає політиці за замовчуванням, ця політика застосовується до мережевого трафіку DNS.

На відміну від інших політик, де ви можете призначити графік, щоб дозволити чи блокувати доступ на основі часу, правило політики за замовчуванням завжди активне.

Як було зазначено раніше у цьому розділі, ви можете сгрупувати VLAN у логічні групи для призначення політик. Ви можете створювати правила для кожної групи VLAN відповідно до вимог.

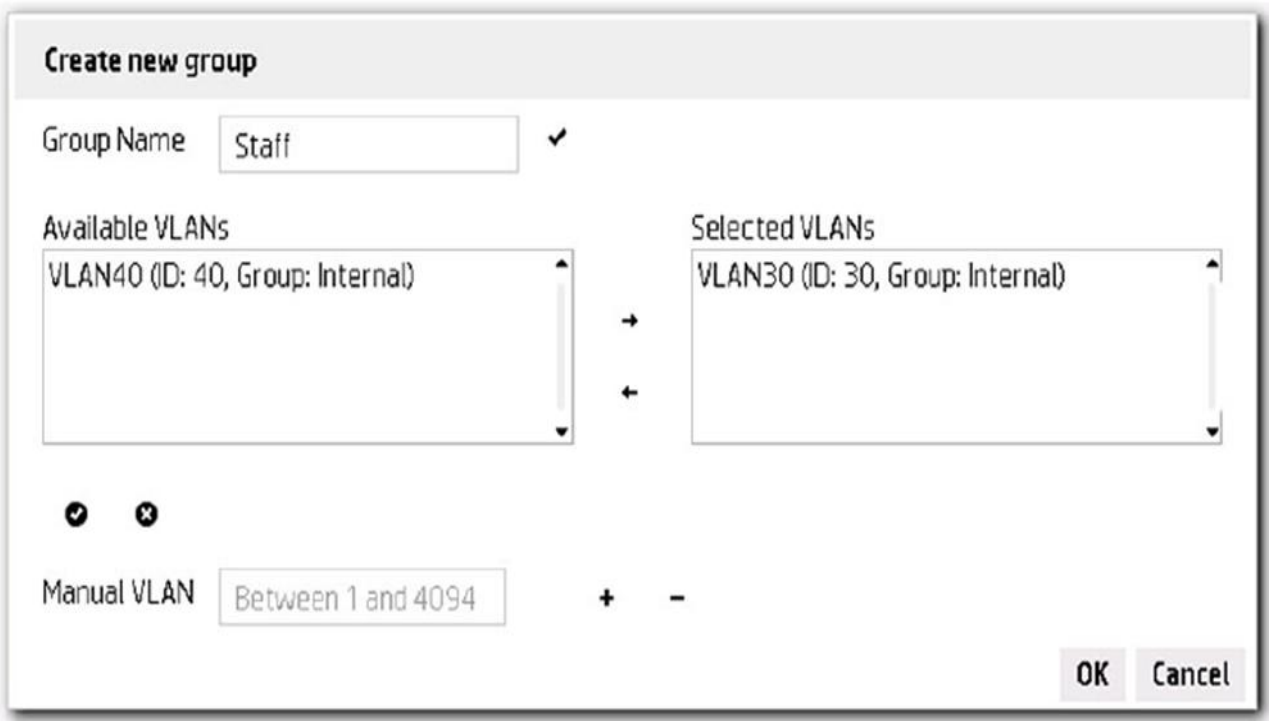
Наприклад, в університетському містечку можна створити дві групи VLAN. Ви можете об'єднати всі VLAN у головному університетському містечку в одну групу та всі VLAN у гуртожитку в іншу групу.

Ви можете застосувати індивідуальні політики для управління обома групами.

1. Для створення нової групи VLAN, необхідно зробити наступне:

2. Виберіть *Profiles*, а потім виберіть *VLAN Groups*.

3. Клікніть клавішу *New,* як показано на малюнку. Буде відображена сторінка *Create new group*.



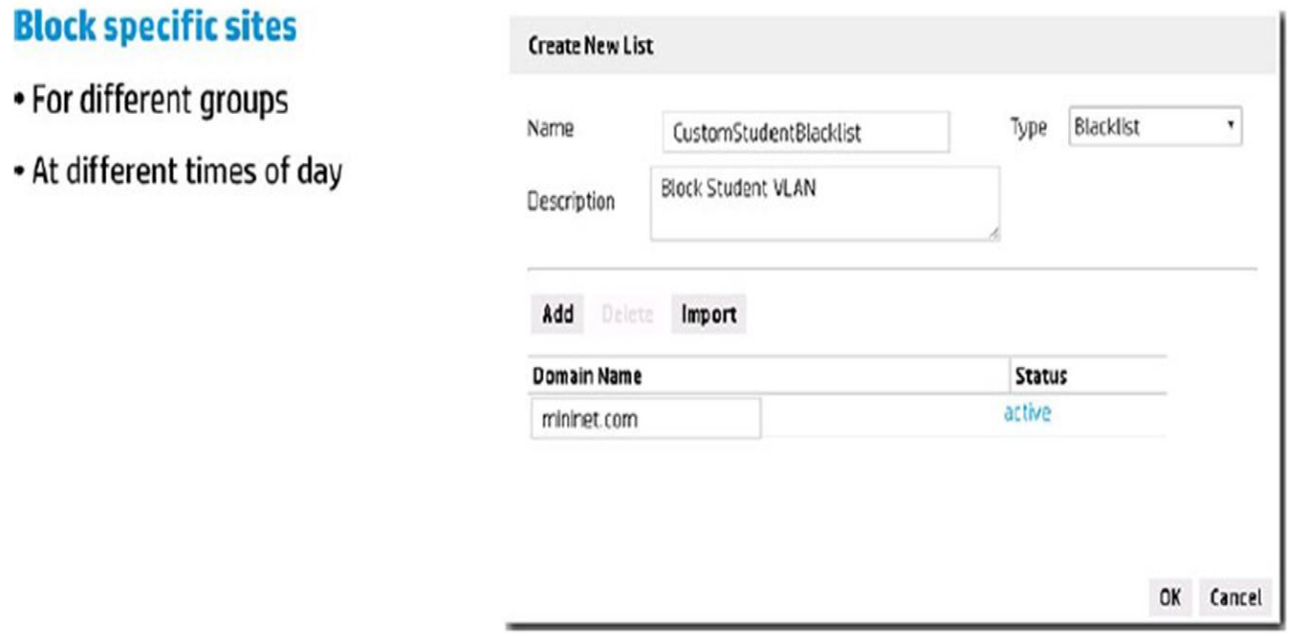
4. Введіть логічне ім'я для групи у текстовому полі *Group Name*, наприклад, *Staff*.

5. Виберіть VLANs, які потрібно згрупувати із списку доступних VLANs. VLAN30 вибрано на малюнку.

6. Натисніть стрілку, щоб перемістити вибрані VLANs у групу.

7. Щоб додати VLAN, не вказаний у списку, введіть номер VLAN у текстовому полі *Manual VLA*N та натисніть *Add.*

Окрім обмеження доступу через базу даних RepDV, ви можете додавати, наприклад, *blacklist* для обмеження доступу (див. Малюнок). Коли користувач отримує доступ до домену, переліченого в blacklist, програма відкидає трафік та оновлює свій журнал зі статистикою, яку він генерує, коли кінцеві користувачі намагаються отримати доступ до заблокованих сайтів.



Ви можете працювати з чотирма типами спеціальних списків для керування трафіком у вашій мережі:

- Whitelist
- Priority whitelist
- Blacklist
- Graylist

HP Network Protector SDN Application виконує послідовний пошук дозволених і заблокованих доменів, перш ніж він дозволяє хосту отримати доступ до зовнішніх імен хостів. Це послідовність, в якій вона використовує: whitelist, blacklist, and finally the RepDV database.

Коли додаток знаходить доменне ім'я у whitelist, він перестає шукати запис у чорному списку або в базі даних RepDV і дозволяє користувачеві отримати доступ до доменного імені. Якщо ім'я домену вказано у whitelist та в blacklist, або в базі даних RepDV, програма дозволяє користувачеві отримати доступ до доменного імені.

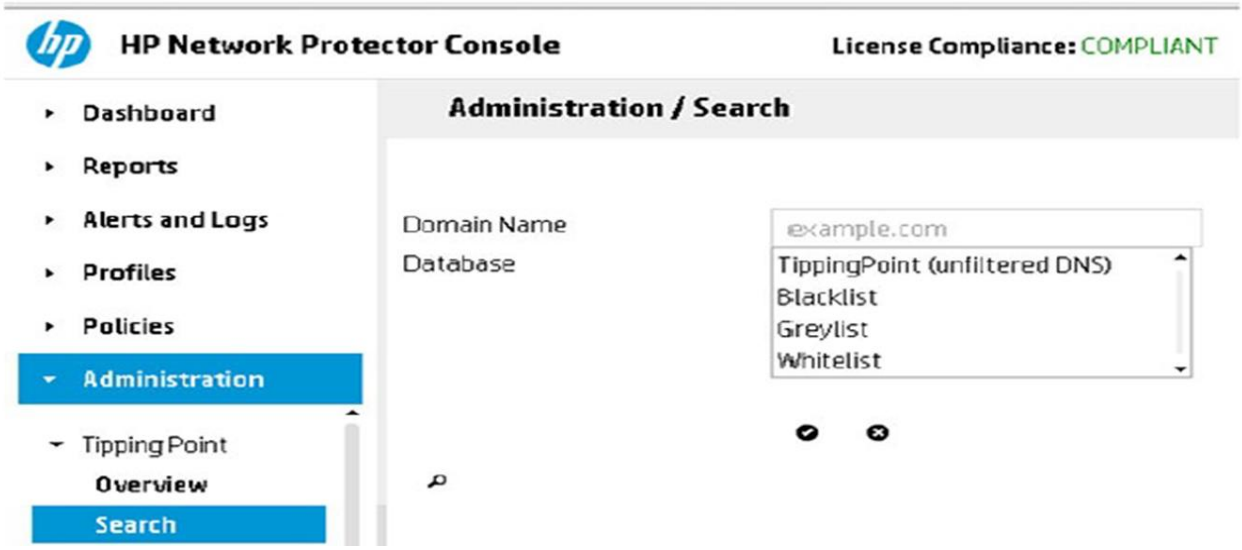
Наприклад, якщо ви додасте example.com у білий список, а example.com зареєстровано як зловмисний сайт у базі даних RepDV, ви все одно зможете отримати доступ до цього сайту. Whitelist домени дозволяють нехтувати blacklist доменами та доменами в базі даних RepDV.

Перш ніж налаштувати blacklist, цікаво дізнатись, чи знаходяться сайти, які ви збираєтеся включити, вже в базі даних RepDV TippingPoint. Проте, виконуючи пошук в базі даних, вам стає відомо значно більше, ніж чи є там домен, який вас цікавить. Він також розповідає вам, чому він саме там. Наприклад, він повідомляє вам репутаційний рейтинг домену (рейтинг більше 79 балів за замовчуванням блокується) і тип загрози - наприклад, вірус.

У наведеному нижче прикладі інструкцій для виконання пошуку в базі даних, розшукуваний домен anyhome.ca вже знаходиться в базі даних RepDV TippingPoint.

Пошук домену *anyhome.ca* здійснюється наступним чином:

1. На HP Network Protector Console, клікніть *Administration* і потім клікніть *Search*.

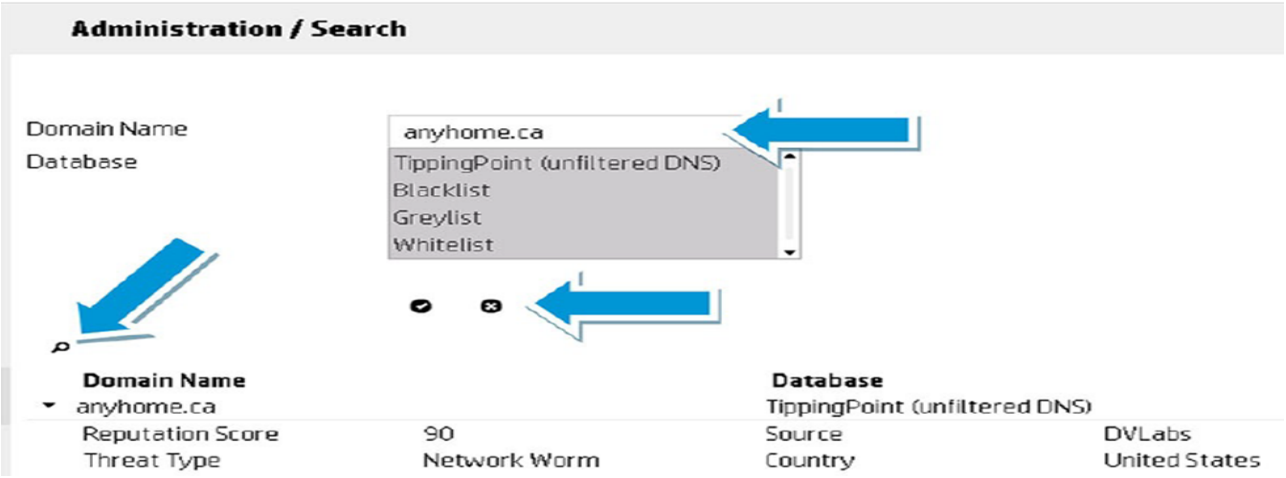


2. Наберіть доменне ім'я anyhome.ca у полі *Domain Name* (дивись малюнок).

3. Клікніть позначку ( ), щоб вибрати усі бази даних.

4. Клікніть позначку ( ), щоб виконати пошук.

5. Клікніть стрілку ( ) щоб побачити більше деталей.

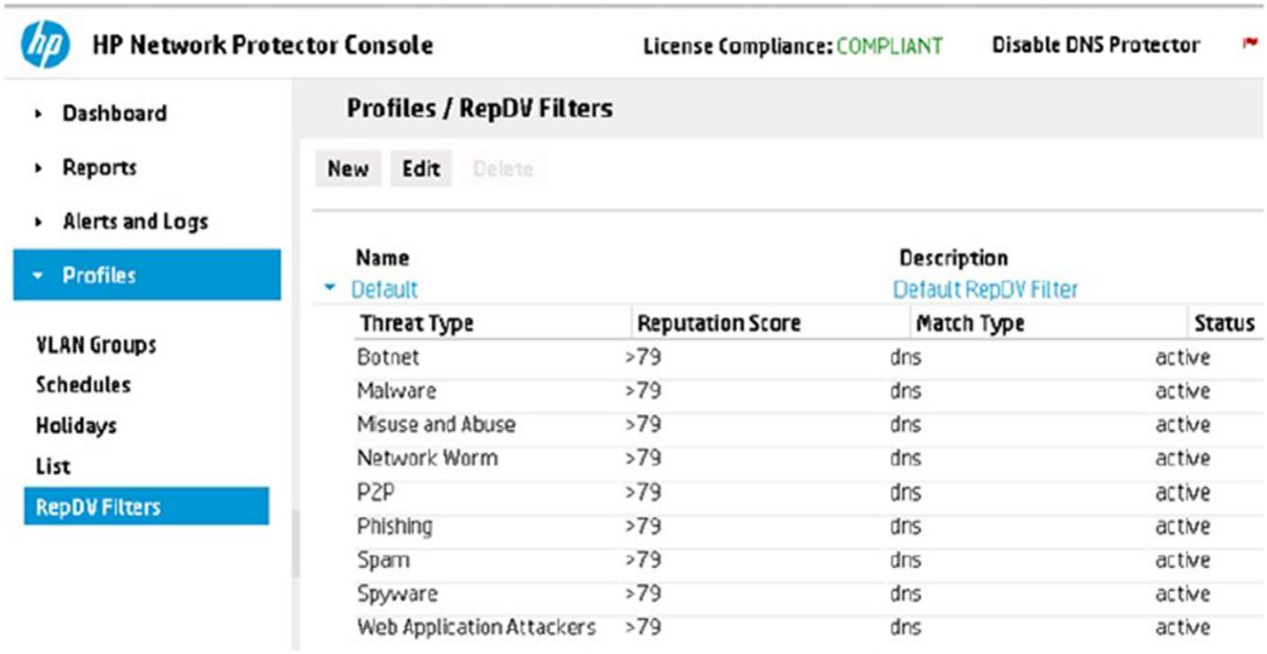


Як приклад для цих інструкцій, *anyhome.ca* знаходиться в базі даних TippingPoint. Оцінка репутації - 90, а тип загрози Network Worm.

Як згадувалося раніше, база даних RepDV - це служба підписки, яка дозволяє додатку контролювати та блокувати вихідні повідомлення з відомими зловмисними та небажаними іменами хостів. База даних RepDV містить сотні тисяч відомих шкідливих або небажаних хостів. Базова оцінка загрози 0-100 присвоюється кожному імені хоста на основі аналізу діяльності, джерела, категорії та загрози.

Якщо б ви шукали базу даних RepDV для Facebook і Mininet, ви не знайдете ці домени в списку. У цих випадках пошук не дасть результатів.

Щоб переглянути *поточні налаштування профілю*, клікніть Profiles, а потім *RepDV Filters* на HP Network Protector Console. Розгорніть деталі для фільтру RepDV за замовчуванням, натиснувши стрілку ( ). Як показує малюнок, всі перераховані типи загроз мають репутаційний бал більший ніж 79, а тому їм відмовлено.



Ви можете налаштувати результати репутації та застосовувати індивідуальну інспекційну політику для перевірки, щоб захистити вашу мережу від конкретних видів загроз.

Дальше представлені різні типи загроз:

Botnet: Шкідливе програмне забезпечення встановлюється на ваш комп'ютер через Інтернет без вашого відома і ваш комп'ютер використовується для виконання повторюваних завдань. Завдання можуть включати відправку спаму, розповсюдження шкідливого програмного забезпечення та виконання інших незаконних дій. Під час виконання цих завдань продуктивність вашого комп'ютера може сповільнитися.

Malware: Скорочена назва шкідливого (зловмисного) програмного забезпечення. Malware встановлюється на ваш комп'ютер без вашого відома, щоб порушити роботу комп'ютера або зібрати конфіденційну інформацію. Зібрана інформація може використовуватися для відображення небажаної реклами або перенаправлення афілійованих маркетингових надходжень до розробника зловмисного програмного забезпечення.

Misuse and Abuse: Зловживання мережевими ресурсами. Це схоже на однорангові, децентралізоóвані (пірінгові) протоколи, де мережевий ресурс і пропускна здатність використовуються, перш за все, для обміну музичними та відеофайлами.

Network Worm: Мережевий черв'як (worm) - це автономна комп'ютерна програма зловмисного програмного забезпечення, яка повторює себе для

поширення на інші комп'ютери. Він часто використовує комп'ютерну мережу для розповсюдження себе, спираючись на невдачі безпеки на цільовому комп'ютері, щоб отримати доступ до нього. На відміну від комп'ютерного вірусу, не потрібно приєднуватися до існуючої програми.

Peer-to-Peer (P2P): Протоколи однорангового доступу використовуються, перш за все, для обміну музичними та відеофайлами і, по суті, перетворюють персональний комп'ютер на файловий сервер, який робить свої ресурси та ресурси своєї мережі доступним для однорангової спільноти.

Spam: Електронний спам - це використання електронних систем обміну повідомленнями для безоплатного надсилання небажаних масових повідомлень (спаму), особливо реклами.

Spyware: Шпигунське програмне забезпечення - це тип програмного забезпечення, яке передає інформацію без знання чи дозволу користувача. Шпигунське програмне забезпечення може бути результатом вірусної інфекції або може бути встановлено разом з іншими програмами. Шпигунські програми часто використовують великі ресурси і можуть сповільнити роботу системи, а в деяких випадках завдають стати нестабільними або непридатними для використання.

Web Application Attackers: Нападники на веб-додатки зазвичай шукають уразливості в мережі. Написавши шкідливий код, вони намагаються знайти слабкі місця в системі безпеки мережі, щоб обійти фільтри та дістатися до даних та послуг. Ці зловмисники намагаються використовувати методи вторгнення в такі області, як брандмауер програмного забезпечення та погано захищені хости та порти.

Worm: Worm також є шкідливим програмним забезпеченням, яке поширюється з одного комп'ютера на інший, залишаючи інфекції під час подорожей. Worms використовують мережеву вразливість або соціальну інженерію, щоб змусити користувача розповсюджувати їх. Мережеві черв'яки здатні пошкодити дані чи програмне забезпечення та викликати умови відмови в обслуговуванні (DoS).

Створеня та налаштування *graylist*.

Ви можете включити імена хостів у *graylist*, які не є шкідливими для вашої мережі, але можуть бути заблоковані для дотримання бізнес-політики (див. Малюнок нижче). Ви також можете додати імена хостів до graylists, щоб обмежити доступ до певних сайтів у певні години дня. Коли ви додасте імена хоста до graylist, користувач не зможе отримати доступ до хосту. На відміну від blacklists, програма не зберігає статистику користувачів, які намагалися отримати доступ до graylist записів як зловмисних запитів DNS.

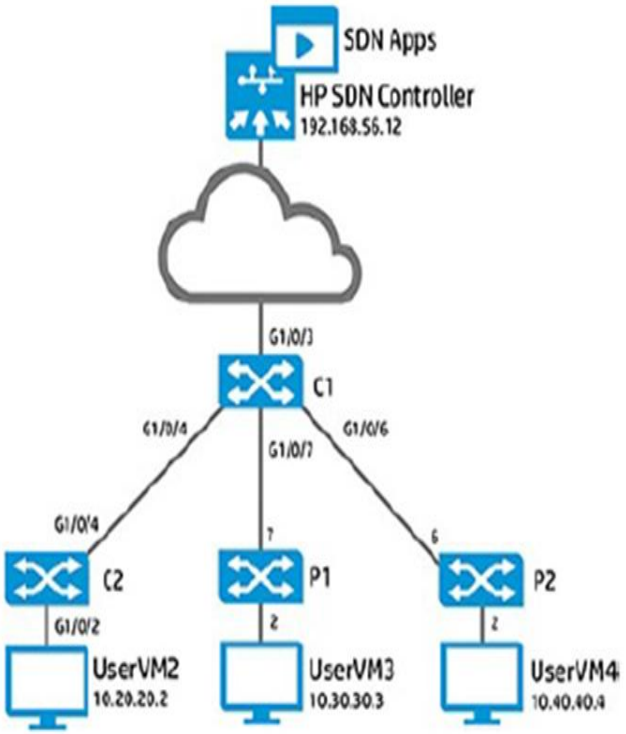
Наприклад, в університетському містечку ви можете встановити graylist, щоб обмежити доступ до сайтів соціальних мереж, які відволікаються під час годин навчання. Обмеження доступу до сайтів соціальних мереж заохочує співробітників та студентів до більш активного спілкування під час заняття.

Overview

- Non-harmful domains
- Block to adhere to business policies
- No statistics

Припустимо, що UserVM4 у прикладі топології (малюнок) знаходиться у студентській VLAN (VLAN 40) і що студент може зараз отримати доступ до facebook.com. Також припустимо, що UserVM3 в топології знаходиться у штатному VLAN (VLAN 30) і цей користувач може також зараз отримати доступ до facebook.com.

- Create a custom Greylist
- Test access to sites
  - With a Greylist applied
  - Without a Greylist applied
- Apply the Greylist to different groups

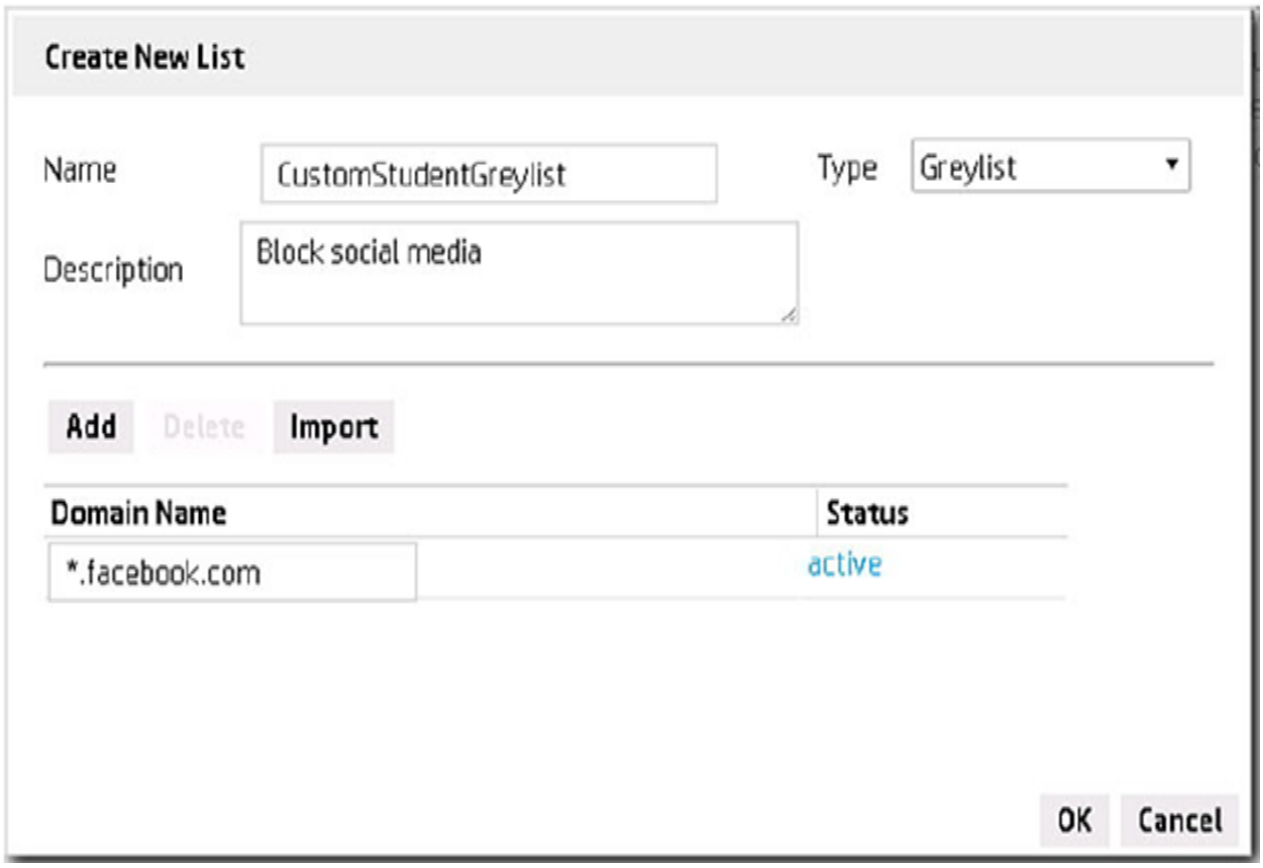


Першим кроком є створення graylist, який включає в себе домен facebook.com:

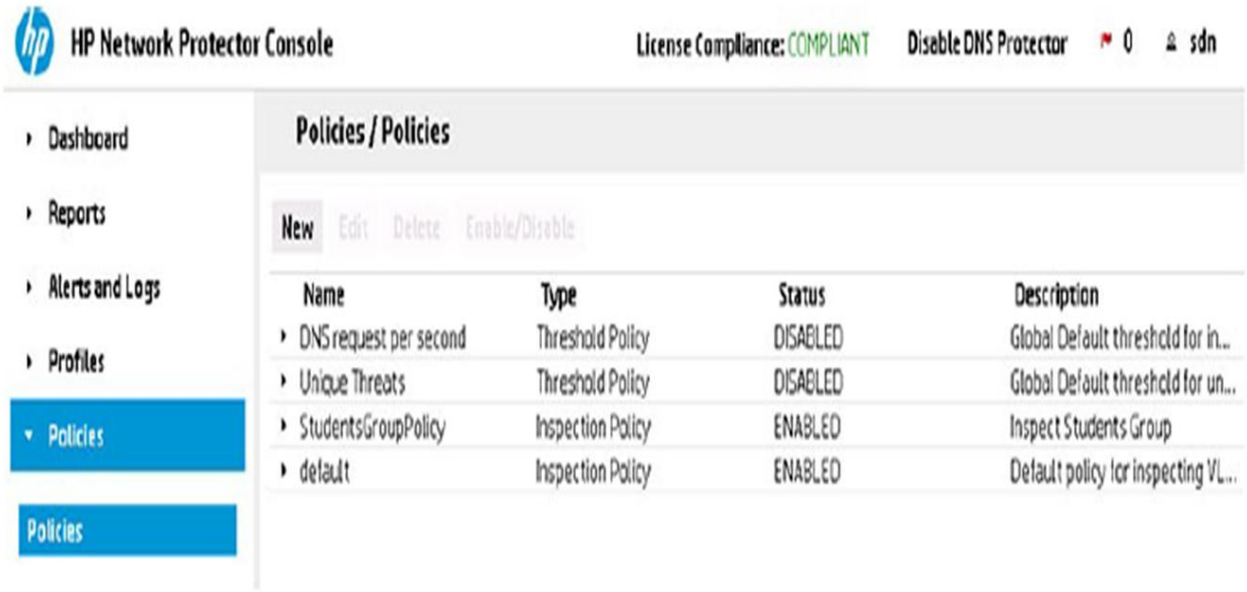
1. На Network Protector Console, клікніть Profiles і потім клікніть List. Після цього клікніть New.

2. Наступний приклад показує додавання домена facebook.com до graylist. Малюнок ілюструє, де необхідно додати інформацію в діалоговому вікні Create New List.

- Name: CustomStudentGraylist
- Type: Graylist
- Description: Block social media
- Click Add, and add a name of *.facebook.com

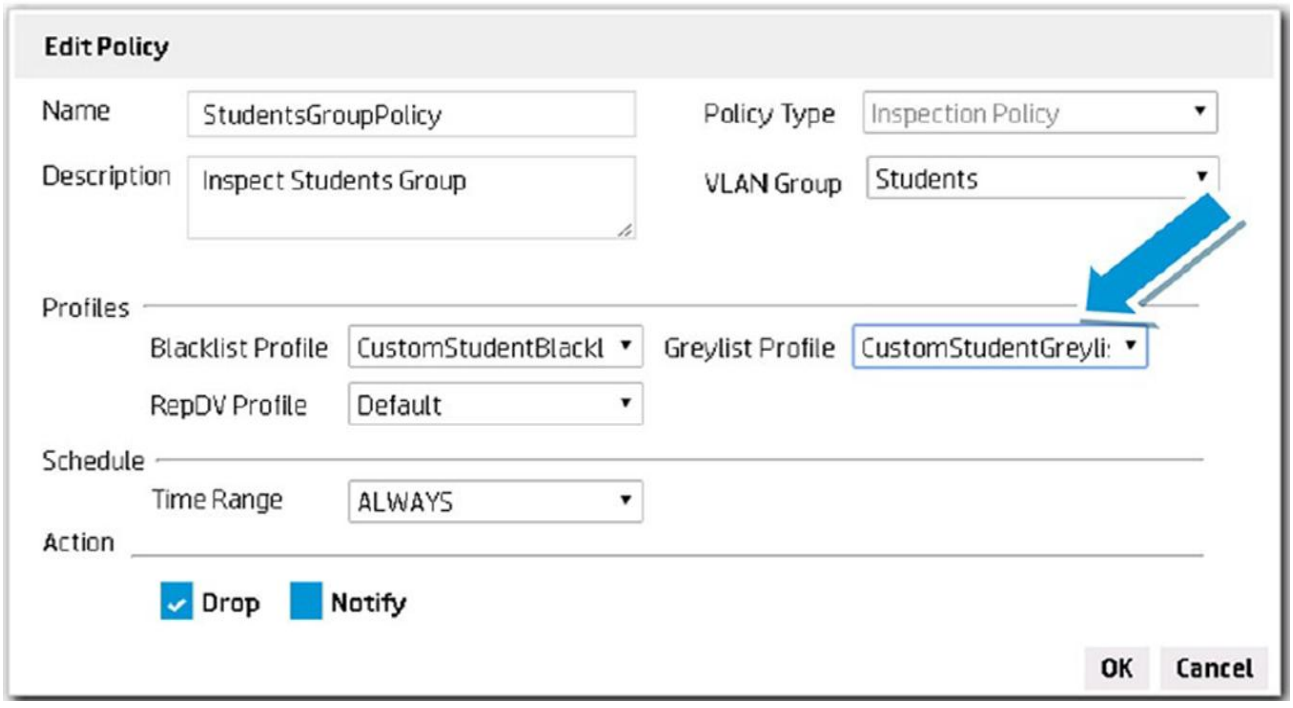


4. Клікніть меню *Policie*s і потім клікніть підменю *Polices*. У цьому прикладі нам необхідно додати *graylist* до існуючої політики під назвою “StudentGroupPolicy” (дивись малюнок).



5. Клікніть StudentsGroupPolicy і потім клікніть Edit.

6. У діалоговому вікні *Edit Policy*, встановіть у *Graylist Profile* назву *CustomStudentGraylist* і клікніть OK.



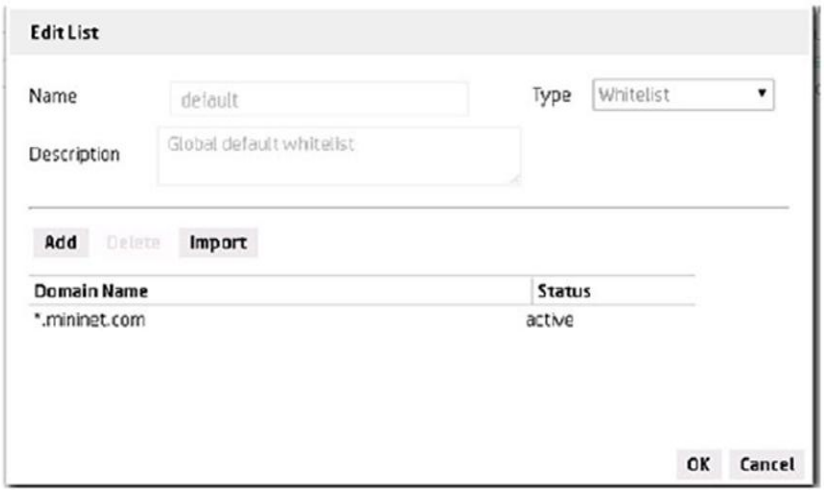
Створеня та налаштування whitelist.

Ви можете додати імена хостів до whitelist (див. Малюнок). Програма порівнює імена хостів у цьому списку та дозволяє отримати доступ до імен хостів, не вивчаючи blacklist або базу даних RepDV. Ви можете додавати назви вузлів у whitelist, коли програмі потрібно пропустити пошук імен хостів у blacklist та базі даних RepDV. Ви також можете нехтувати записами у базі даних RepDV проти записів імен хостів whitelist. На відміну від blacklist або

graylist, де ви можете встановити діапазони часу, білий список завжди активний.

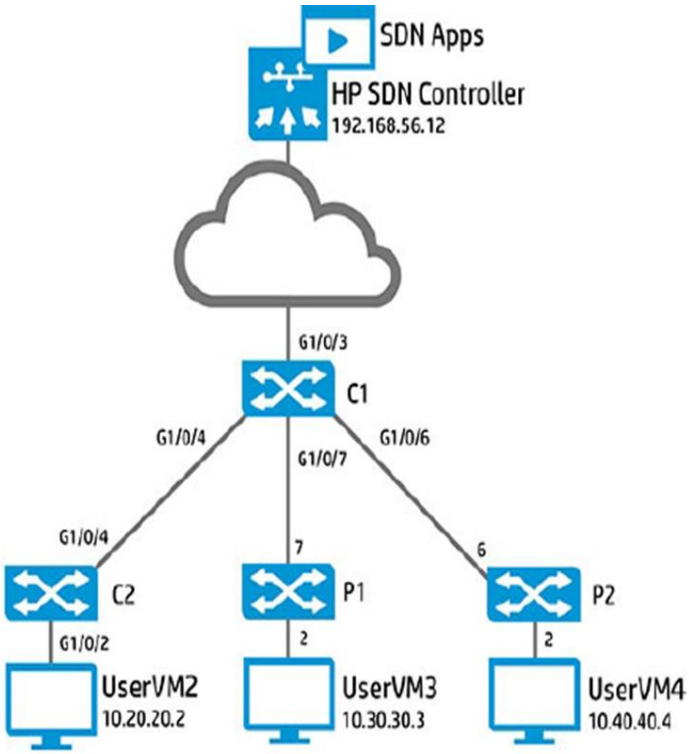
Overview

- Overrides all blacklists
  - Custom blacklist
  - RepDV database
- Always active



У цьому розділі ви дізнаєтеся, як створити та застосувати *whitelis*t. Крім того можна перевірити, що *whitelists* нехтують усіма blacklists.

- Create a whitelist
- Test that whitelists override all blacklist entries



Для наступних інструкцій, припустимо, що UserVM4 знаходиться на VLAN 40 (тобто VLAN для студентів), а UserVM3 знаходиться на VLAN 30 (VLAN персоналу).

Також припустимо, що ви налаштували домен mininet.com у чорному списку, а також, що домени anyhome.ca і howtodoitman.com знаходяться в базі даних RepDV як шкідливі сайти.

Якщо ви повинні перевірити істинність цих припущень за допомогою nslookup, вихід буде виглядати так, як ви бачите в наступному прикладі:

For mininet.com

```
C:\Windows\system32> nslookup mininet.com
DNS request timed out.
   timeout was 2 seconds.
Server: UnKnown
Address: 192.168.56.50
Non-authoritative answer:
Name: mininet.com
Addresses: 192.168.56.12
   192.168.56.12
```

UserVM4 cannot access mininet.com.

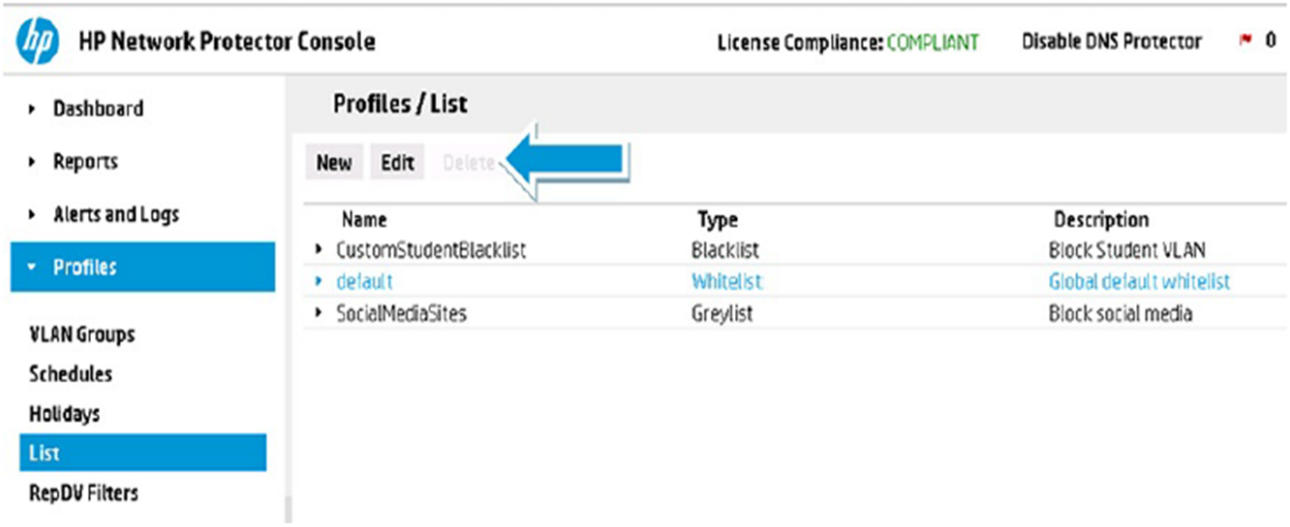
For anyhome.ca

```
C:\Windows\system32> nslookup anyhome.ca
DNS request timed out.
   timeout was 2 seconds.
Server: UnKnown
Address: 192.168.56.50
Non-authoritative answer:
Name: anyhome.ca
Addresses: 192.168.56.12
   192.168.56.12
C:\Windows\system32>
```

UserVM4 cannot access anyhome.ca.

1. На HP Network Protector Console, виберіть Profiles і потім виберіть List.

2. Виберіть default Whitelist та клікніть Edit (дивись малюнок):



3. Додайте Add наступні домени до whitelist і клікніть OK:

- Override the custom blacklist: *.mininet.com
- Override the RepDV blacklist: *.anyhome.ca

1. Ви можете скористатись браузером на UserVM4, щоб переконатися, що студенти тепер можуть отримати доступ до домену mininet.com. Ви також можете використовувати nslookup. Якщо ви це зробили, ви побачите наступний результат:

```
C:\Windows\system32> nslookup mininet.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.56.50
Name:  mininet.com
Address:  192.168.56.54
C:\Windows\system32>
```

Як ви бачите, студент має доступ до mininet.com. Whitelist не приймає до уваги blacklist.

2. Ви можете використовувати браузер на UserVM4, щоб переконатися, що студенти не можуть отримати доступ до anyhome.ca. Ви також можете використовувати nslookup, у цьому випадку вихід з UserVM4 буде виглядати приблизно так:

```
C:\Windows\system32> nslookup anyhome.ca
DNS request timed out.
   timeout was 2 seconds.
Server: UnKnown
Address: 192.168.56.50
Name: anyhome.ca
Address: 192.168.56.52
C:\Windows\system32>
```

Студенти мають доступ до anyhome.ca. Whitelist не приймає до уваги RepDV blacklist.

3. Ви можете скористатись браузером на UserVM3, щоб перевірити, чи працівники можуть отримати доступ до anyhome.ca (RepDV blacklist). Ви також можете використовувати nslookup. Якщо ви хотіли б протестувати доступ за допомогою nslookup в цьому прикладі, ви побачите щось подібне до такого виходу:

```
C:\Windows\system32> nslookup anyhome.ca
DNS request timed out.
   timeout was 2 seconds.
Server: UnKnown
Address: 192.168.56.50
Name: anyhome.ca
Address: 192.168.56.52
C:\Windows\system32>
```

Staff має доступ до anyhome.ca. Whitelist не приймає до уваги RepDV blacklist.

4. Якщо ви хотіли б перевірити доступ персоналу на howtodoitman.com за допомогою nslookup, ви побачите щось подібне до такого випуску:

```
C:\Users\Student> nslookup howtodoitman.com
DNS request timed out.
   timeout was 2 seconds.

Server: UnKnown

Address: 192.168.56.50

Non-authoritative answer:

Name: howtodoitman.com

Addresses: 192.168.56.12

   192.168.56.12

C:\Users\Student>
```

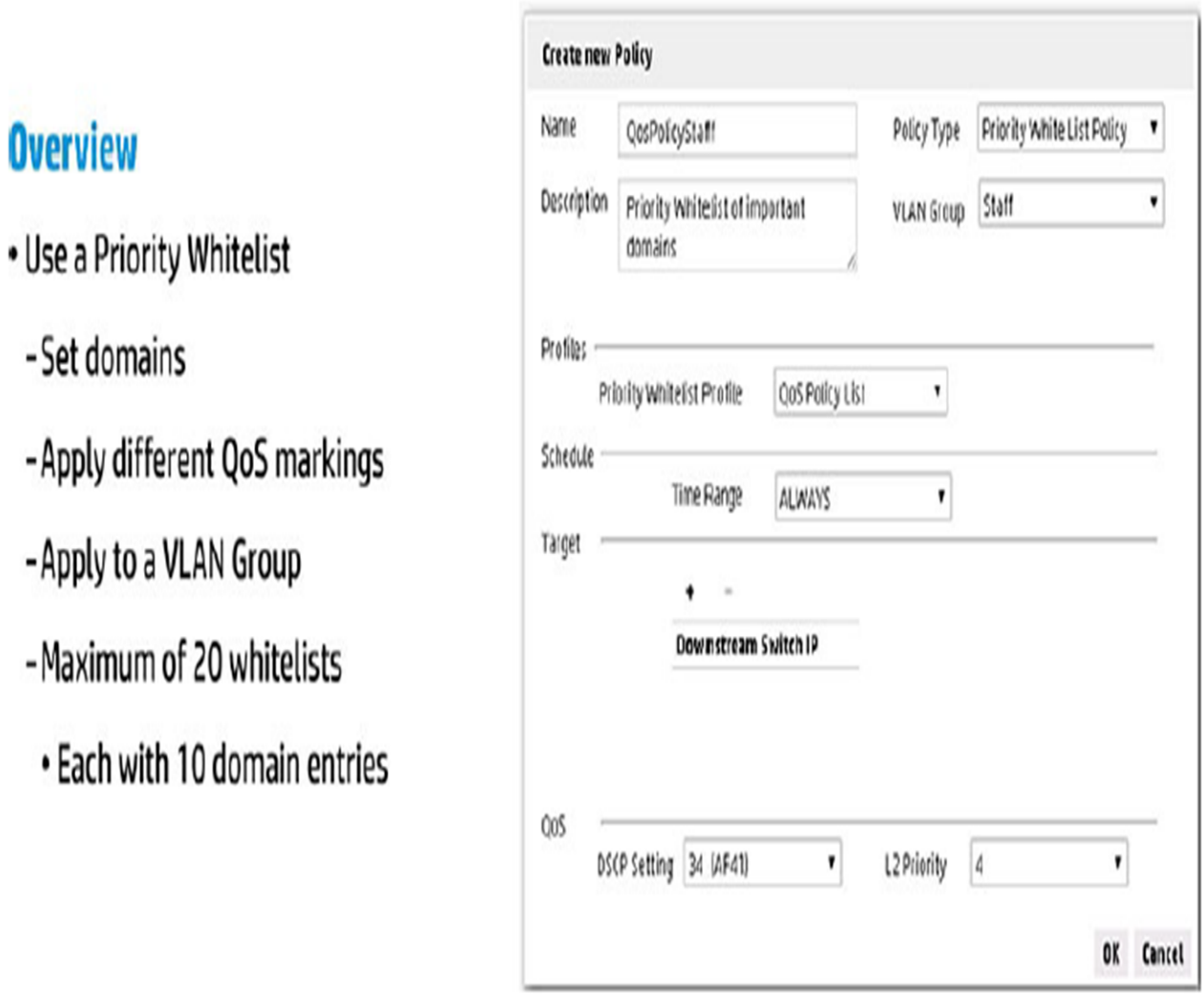
Як ви бачите, співробітники не можуть отримати доступ до howtodoitmain.com. RepDV blacklist все ще використовується для блокування доменів, які не відмінені білим списком.

3.6. Quality of service (QoS).

Трафік у мережах не має однакового значення або пріоритету. Іншими словами, деякі типи трафіку є критично важливими, а інші не є. Без QoS весь трафік конкурує за певний обсяг та, можливо, за обмежену кількість пропускної спроможності. QoS забезпечує преференцію звернення до певних типів трафіку, таких як Voice over IP (VoIP).

Щоб керувати критичним трафіком та надавати йому преференцію, ви можете створити записи білого списку (whitelist) та прив'язати пріоритети QoS до трафіку (диись малюнок нижче). Залежно від значення QoS та пріоритету, програма обробляє різноманітні типи потоків даних, що передаються по вашому мережевому трафіку, по-різному.

Ви можете створити максимум 20 білих списків (whitelist) і кожен білий список може містити до десяти записів доменів.



Значення Various Differentiated Service Code Point (DSCP) або Priority Code Point (PCP) можуть бути налаштовані для відповідного трафіку. DSCP передбачає маркування класифікації трафіку на Layer 3 і PCP на Layer 2.

Пристрої, налаштовані на відповідність значенням DSCP або PCP, можуть визначати пріоритетність трафіку відповідно до бізнес політики.

Наприклад, ви можете позначити весь трафік сайту соціальної мережі з сьнижчою ціною DSCP/PCP, щоб трафік на facebook.com та інші сайти соціальних мереж не оброблялися на шкоду критичному трафіку бізнесу.

Після того, як ви застосовуєте пріоритетне правило білого списку (whitelist), HP Network Protector створює потоки на комутаторах, які позначають відповідність трафіку з налаштованими значеннями DSCP та PCP. (дивись малюнок).

Network Protector не виконує маршрутизацію чи визначення пріоритетів трафіку на основі значення DSCP або PCP. Традиційні механізми QoS використовуються для маршрутизації або визначення пріоритетів трафіку на основі значень, встановлених у таблиці OpenFlow

Switch applies

- DSCP or PCP to traffic

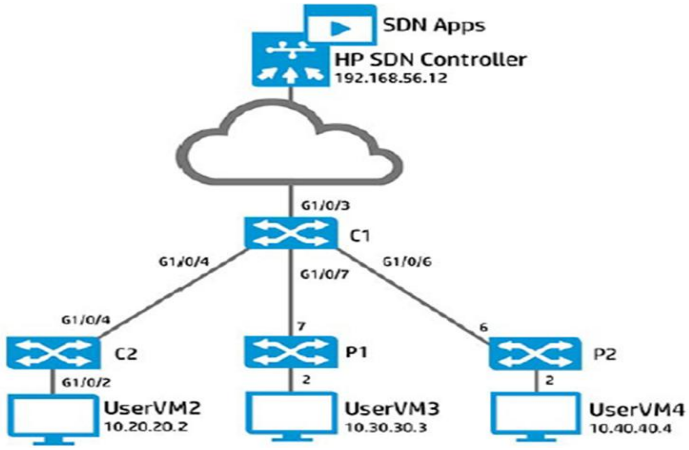
Flows for Data Path ID: 00:1e:14:58:d0:f0:db:80

Summary | Ports | Flows

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	30020	0	0	eth_type: ipv4 ipv4_dst: 192.168.56.51	apply_actions: set_field: [ip_dscp: 34] set_field: [vlan_pcp: 4] output: NORMAL	
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	goto_table: 200	com.hp.sdn.dhcp.copy
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	goto_table: 200	com.hp.sdn.dhcp.copy

У цьому розділі ви навчитеся налаштувати QoS на HP Network Protector whitelist. Інструкції будуть використовуватись на прикладі топології, яка показана на малюнку.

- Create a QoS Priority Whitelist
- Verify DSCP and PCP markings



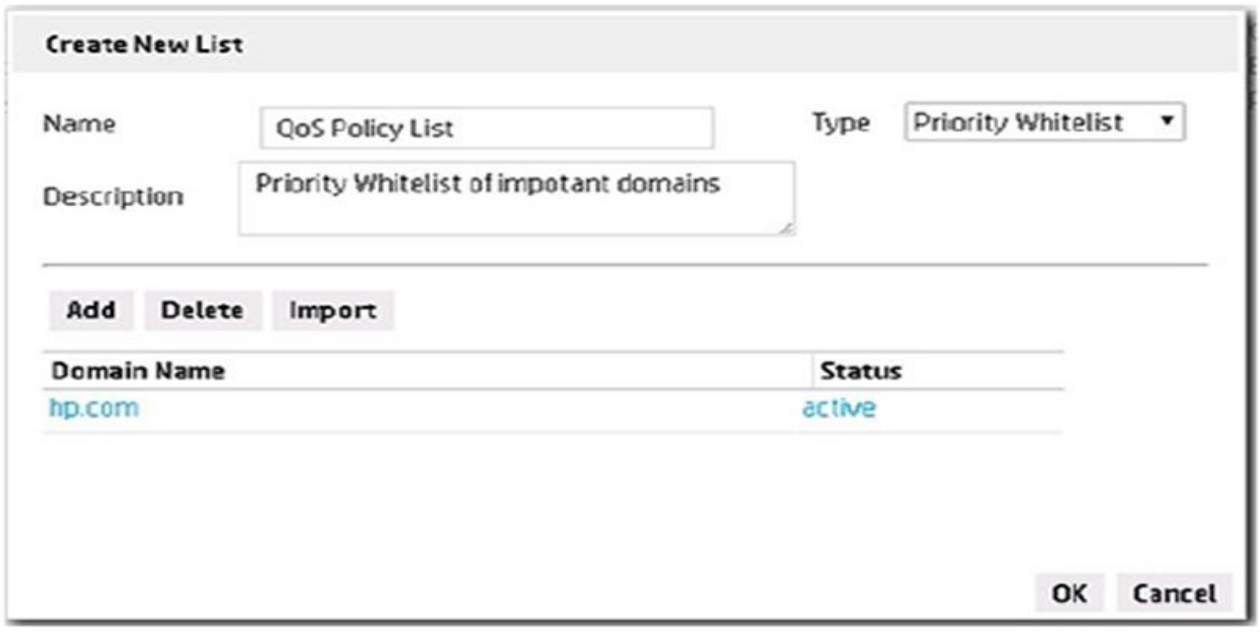
1. На HP Network Protector Console, клікніть *Profiles* і потім *List*. Клікніть *New* для створення нової політики, як показано на малюнку.

2. Введіть інформацію про нову політику та натисніть "ОК". Наступний список містить детальні відомості, як приклад:

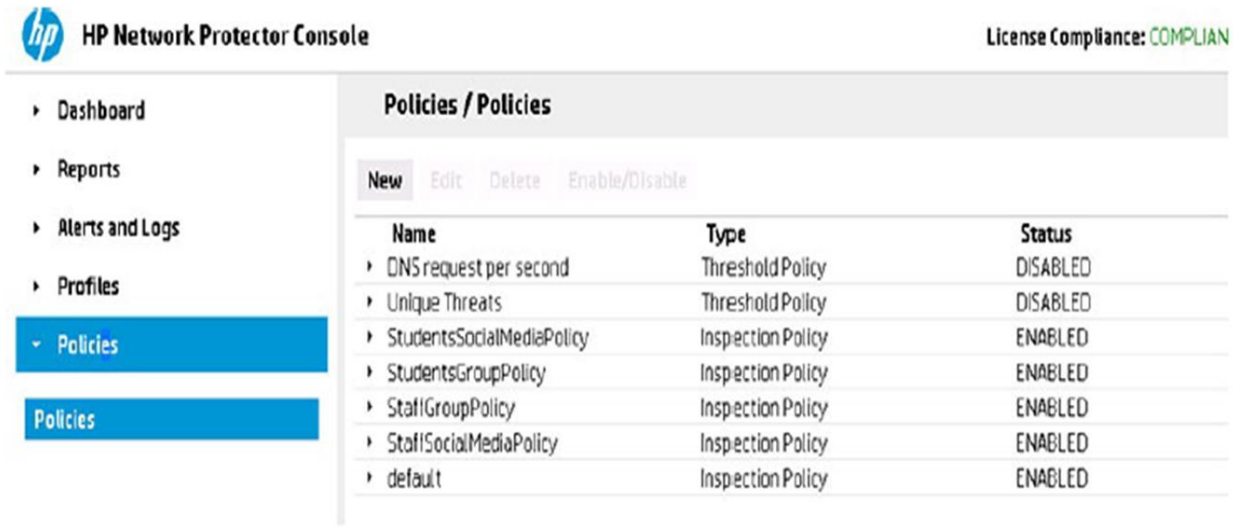
- Name: QoS Policy List
- Type: Priority Whitelist

- Description: Priority Whitelist of important domains

Додайте домен до списку. У прикладі, показаному на малюнку, доменом є hp.com. Натисніть клавішу Enter, якщо потрібно, перш ніж натиснути OK.



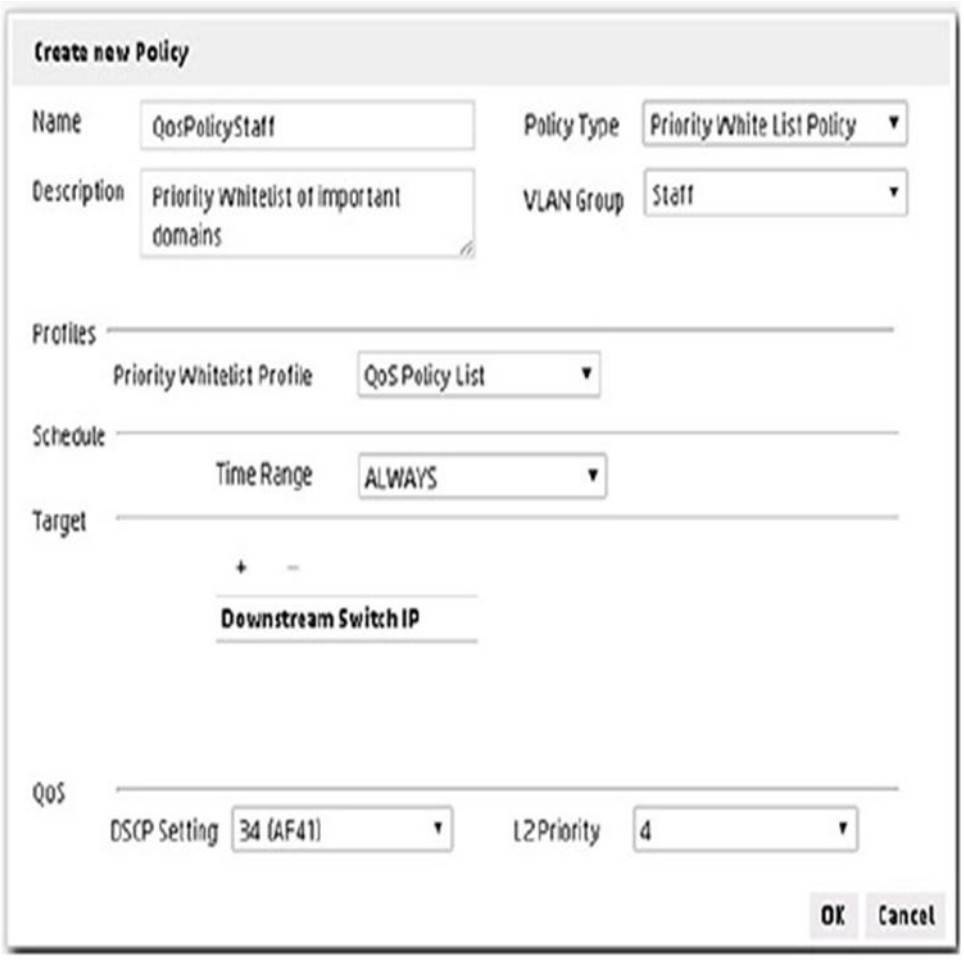
3. Клікніть меню *Policies* і потім підменю Policies. Клікніть *New* для створення нової політики (дивись малюнок).



4. Введіть інформацію про нову політику та натисніть OK. Нижче наведено приклад списка деталей.

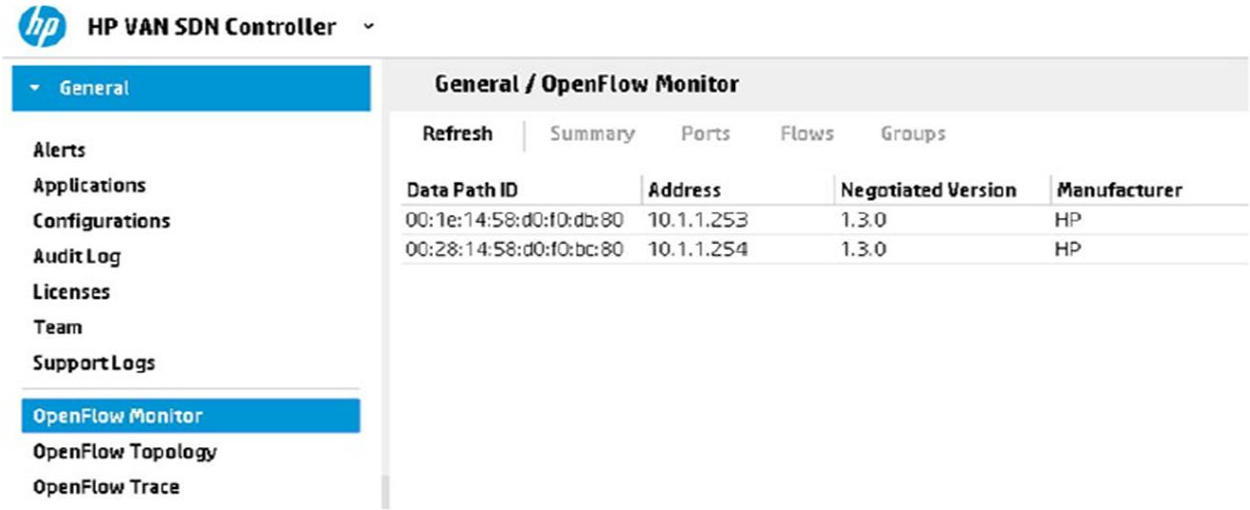
- Name: QoSPolicyStaff
- Type: Priority White List Policy
- Description: Priority Whitelist of important domains
- VLAN Group: Staff
- Priority Whitelist Profile: QoS Policy List
- Time Range: ALWAYS

- DSCP Setting: 34 (AF41)
- L2 Priority: 4

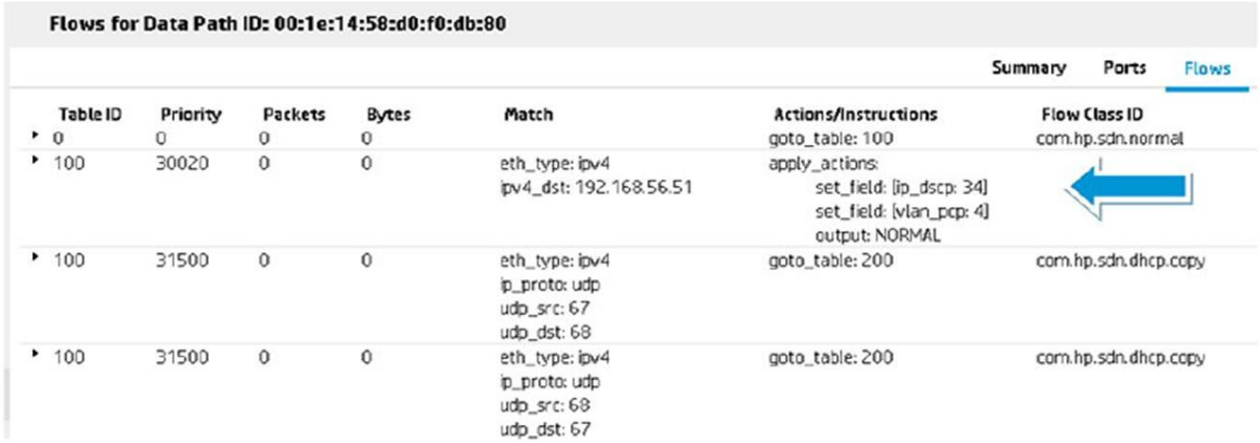


Network Protector додає нові потоки на основі ваших конфігурацій QoS. Щоб переглянути ці потоки

1. На HP VAN SDN Controller Console клікніть OpenFlow Monitor і виберіть комутатор, і потім клікніть Flows. У цьому прикладі був вибраний ProVision Switch 1 (10.1.1.253).



Як показує малюнок, до комутатора додано новий потік:



Flows for Data Path ID: 00:1e:14:58:d0:f0:db:80

Summary | Ports | Flows

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	30020	0	0	eth_type: ipv4 ipv4_dst: 192.168.56.51	apply_actions: set_field: [ip_dscp: 34] set_field: [vlan_pcp: 4] output: NORMAL	
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	goto_table: 200	com.hp.sdn.dhcp.copy
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	goto_table: 200	com.hp.sdn.dhcp.copy

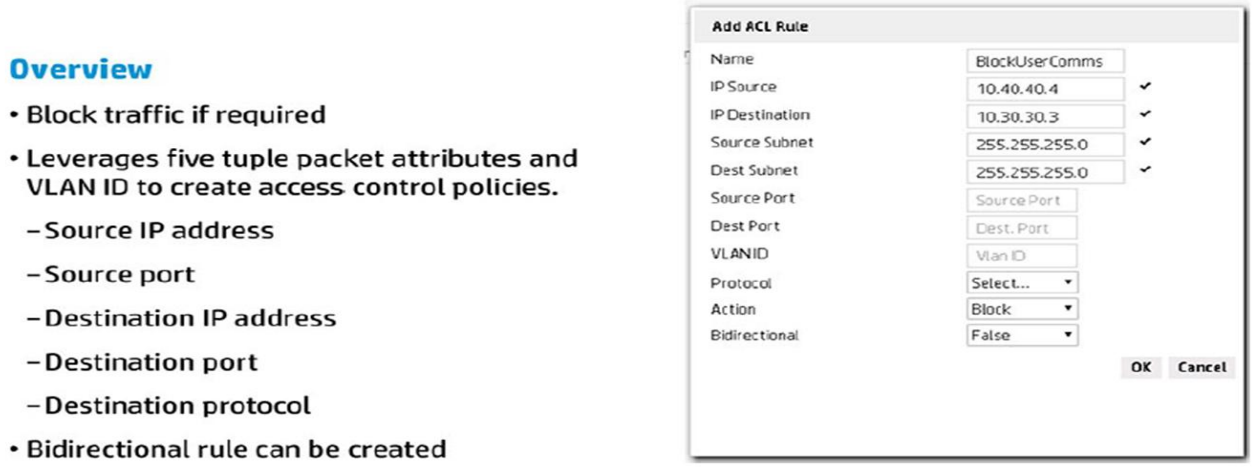
Новий потік відповідає трафіку IPv4 з IP адресою призначення 192.168.56.51. Відповідний трафік має значення DSCP, встановлене на 34, а значення COS/PCP встановлено на 4. Трафік надсилається на традиційний конвеєр маршрутизації та комутації для подальшої обробки. Цей потік був доданий тільки до ProVision Switch 1 (P1), а не до ProVision Switch 2 (P2), оскільки P2 не має на ній налаштовану VLAN 30.

Використовуйте команду *show openflow instance <instance> flows* щоб переглянути новий потік на консолі комутатора. Нижче наведено приклад з комутатора P1:

```
P1# show openflow instance vlan30 flows
OpenFlow Flow Table
Flow 2
Match
   Incoming Port : Any Ethernet Type : IP
   Source MAC : Any Destination MAC : Any
   Destination MAC Mask : 000000-000000
   VLAN ID : Any VLAN priority : Any
   Source IP Address : Any
   Destination IP Address : 192.168.56.51/32
   IP Protocol : Any
   IP ECN : Any IP DSCP : Any
   Source Port : Any Destination Port : Any
Attributes
   Priority : 30020 Duration : 1118 seconds
   Hard Timeout : 43349 seconds Idle Timeout : 0 seconds
   Byte Count : NA Packet Count : 0
   Flow Table ID : 100 Controller ID : 2
   Cookie : 0xebabe
   Hardware Index: 17
Instructions
   Apply Actions
   Modify IP DSCP : 34
   Modify VLAN PCP : 4
   Normal
```

ACL Manager

Менеджер ACL використовує атрибути пакетів п'яти версій та ідентифікатор VLAN для створення політики контролю доступу.



Політика керування доступом базується на атрибутах пакета, наведених на малюнку вище. Якщо вхідний пакет відповідає політиці контролю доступу, програма відкидає пакет або пересилає його на основі встановленої вами політики. Ви також можете використовувати ACL Manager для застосування мережевих масок на IP-адресах джерела чи призначення.

Ви можете ввести атрибути, такі як IP-адреса, адреса підмережі та номер порту джерела чи адресата для створення правила ACL. Якщо ви встановлюєте IP-адресу підканалу джерела чи призначення, тоді програма відповідає всій підмережі для введеної IP-адреси як для джерела, так і для призначення, а також для блоків або для будь-якого трафіку для підмережі. Якщо ви встановлюєте лише назву поля та дію, то правило застосовується до будь-якого трафіку IPv4, блокуючи або дозволяючи в залежності від обраної дії.

На малюнку був створений потоковий запис, який співпадає з наступними деталями:

- Ethernet type = IPv4
- IPv4 source address: 10.40.40.0/24
- IPv4 destination address: 10.30.30.0/24

HP VAN SDN Controller

Flows for Data Path ID: 00:28:14:58:d0:f0:bc:80

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions
0	0	0	0		goto_table: 100
100	34050	4	0	eth_type: ipv4 ipv4_src: 10.40.40.0, mask: 255.255.255.0 ipv4_dst: 10.30.30.0, mask: 255.255.255.0	apply_actions:
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	goto_table: 200

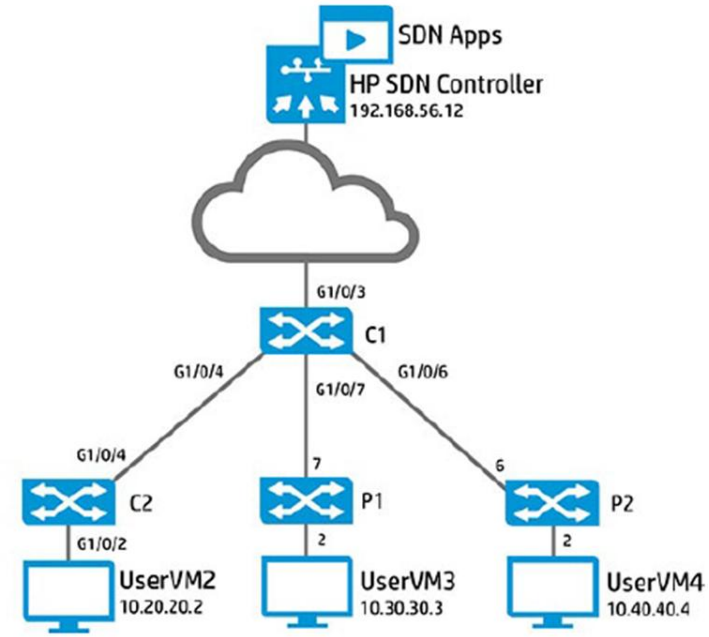
На малюнку, інструкція apply_action є порожньою, що означає, що відповідний трафік відкидається за допомогою комутатора.

Політика контролю доступу вимагає від Network Protector виконувати Deep Packet Inspection (DPI).

У цьому розділі ви навчитесь налаштувати ACL, щоб заборонити студентам відвідувати комп'ютери персоналу.

Це буде зроблено шляхом блокування трафіку, відправленого в підмережу персоналу із підмережі студентів.

- Create an ACL to block students from accessing staff computers
- View flows created
- Verify that traffic is blocked

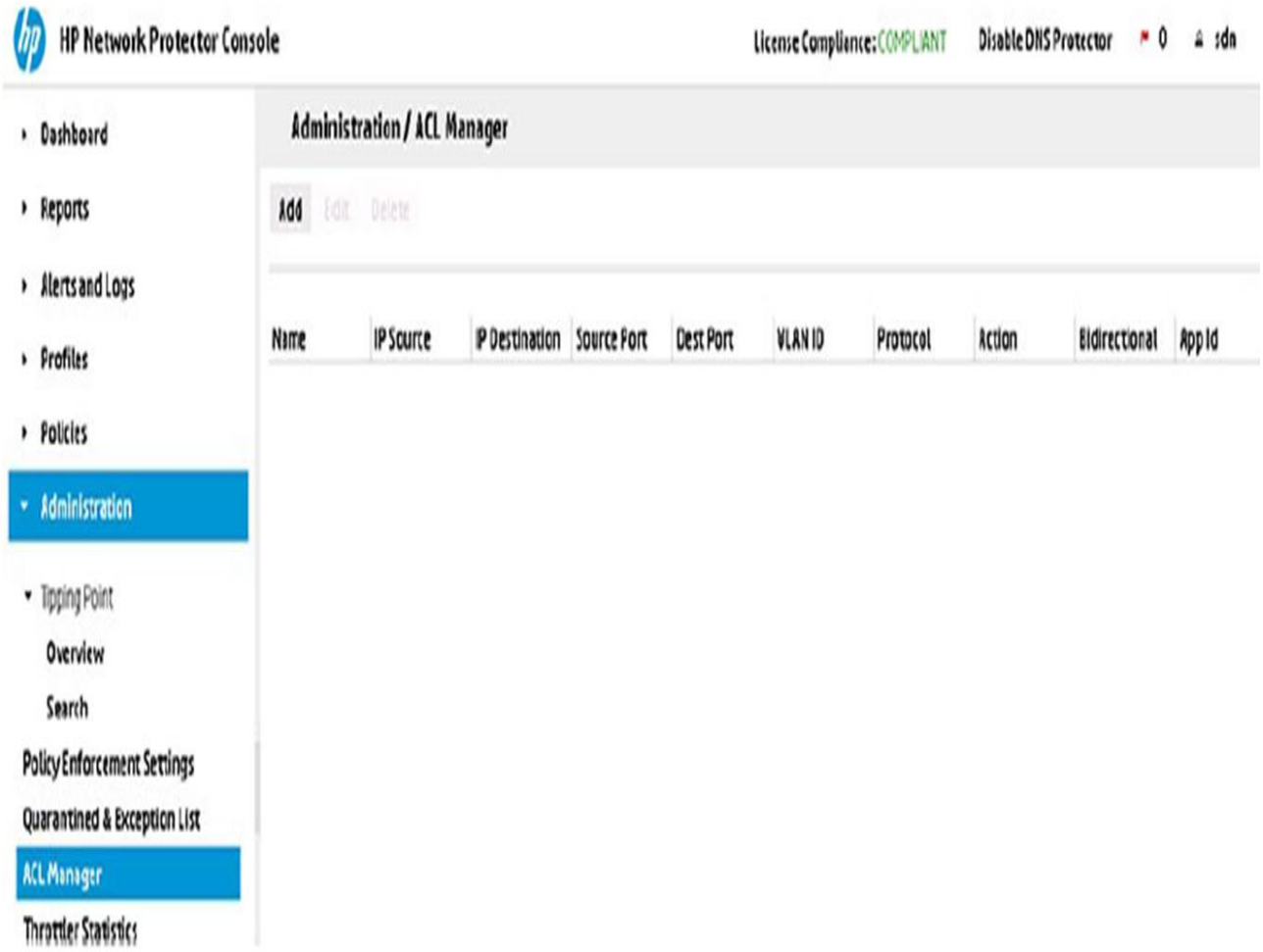


Наведені нижче інструкції, які основані на прикладі сценарію, який використовує топологію на малюнку вище. Припустимо, що UserVM4 (10.40.40.4) у Student VLAN може успішно пінгувати UserVM3 (10.30.30.3) у Staff VLAN. Щоб перевірити це припущення з UserVM4, можна побачити наступний вихід з команди *ping*.

```
C:\Windows\system32> ping 10.30.30.3
Pinging 10.30.30.3 with 32 bytes of data:
Reply from 10.30.30.3: bytes=32 time=4ms TTL=127
Reply from 10.30.30.3: bytes=32 time<1ms TTL=127
Reply from 10.30.30.3: bytes=32 time<1ms TTL=127
Reply from 10.30.30.3: bytes=32 time<1ms TTL=127
Ping statistics for 10.30.30.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:\Windows\system32>
```

1. На Network Protector Console, клікніть *Administration* і потім *ACL* Manager.

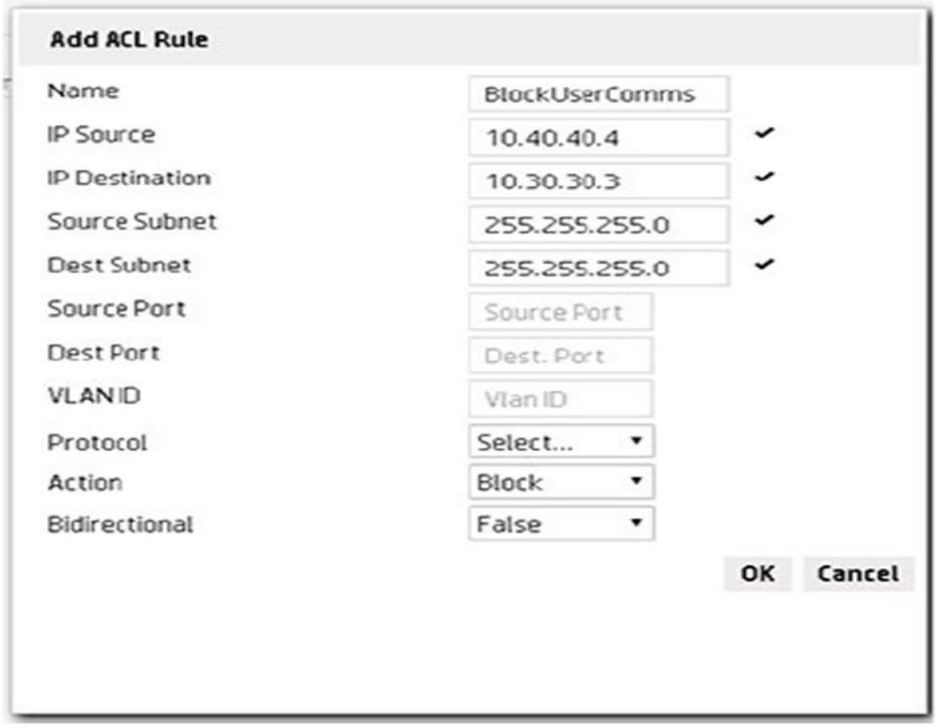
Як видно на малюнку, ACLs по замовчуванню не налаштована.



2. Клікніть Add щоб додати нову ACL, заповнити деталі і клікнути OK. Приклад деталей наведено на малюнку:

- Name: BlockUserComms

- IP Source: 10.40.40.4 (The Subnet mask setting will result in the OpenFlow flow entry being converted to 10.40.40.0 when you click OK)
- IP Destination: 10.30.30.3 (The Subnet mask setting will result in the OpenFlow flow entry being converted to 10.30.30.0 when you click OK)
- Source Subnet: 255.255.255.0
- Destination Subnet: 255.255.255.0
- Action: Block

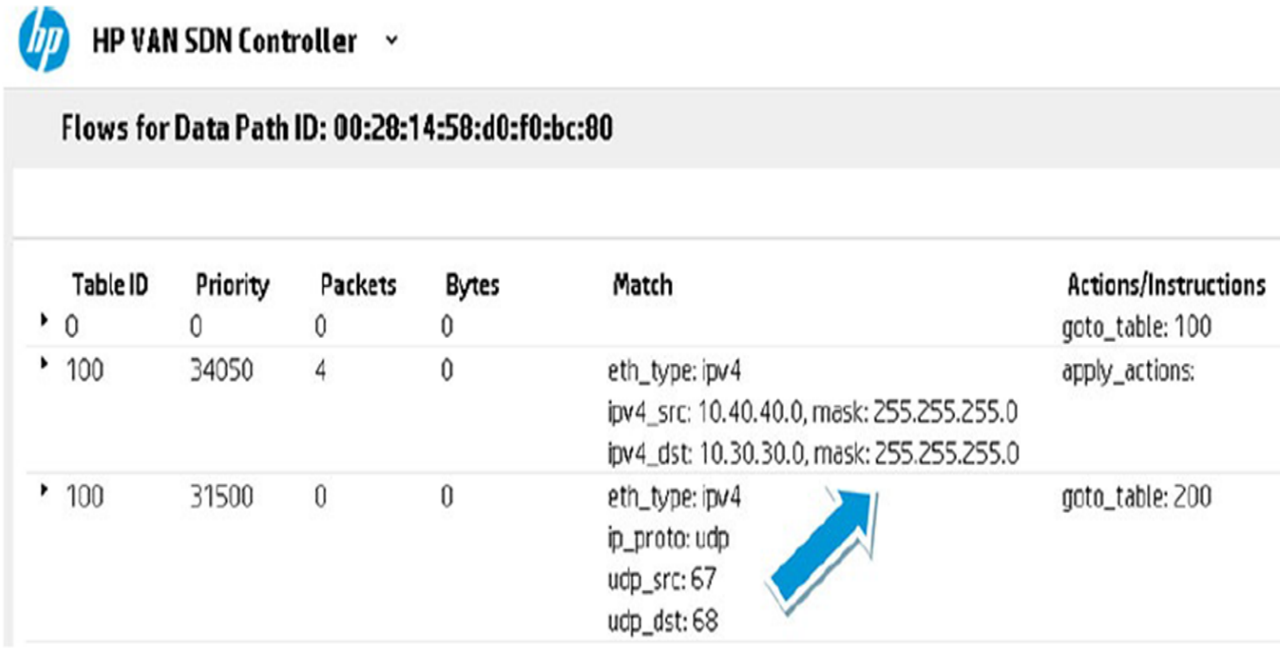


3. Перевіримо, що ACL налаштування працює. У прикладі, UserVM4 (10.40.40.4) у Student VLAN не може пінгувати UserVM3 (10.30.30.3) у Staff VLAN. У цьому випадку команда ping буде мати наступний результат:

```
C:\Windows\system32> ping 10.30.30.3

Pinging 10.30.30.3 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 10.30.30.3:

  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Конфігурація успішна і на комунікаторі записано потік, як показано на малюнку нижче.

Приклад потоку відповідає трафіку IPv4 з вихідної мережі 10.40.40.0/24 та цільової мережі 10.30.30.0/24. Співпадаючий трафік відкидається (apply_action = blank).



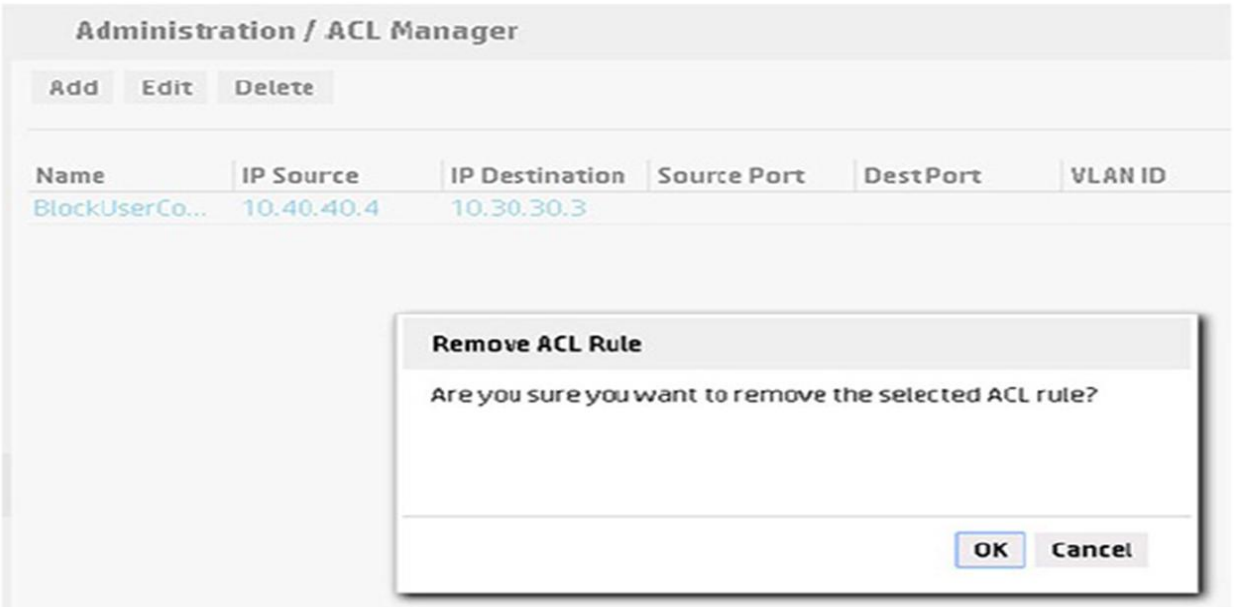
1. Щод подивитися потік, необхідно використати команду *show openflow instance <vlan> flows*.

Нижче наведено приклад виходу на консолі комутатора P2:

```
P2# show openflow instance vlan40 flows
Flow 2
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : 10.40.40.0/24
 Destination IP Address : 10.30.30.0/24
 IP Protocol : Any
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
 Attributes
 Priority : 34050 Duration : 622 seconds
 Hard Timeout : 3600 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 4
 Flow Table ID : 100 Controller ID : 2
 Cookie : 0xcebcbeef
 Hardware Index: 0
 Instructions
 Apply Actions
```

Оскільки *Apply Actions* є порожньою, співпадаючий потік відкидається.

Можна видалити приклад ACL на Network Protector Console, як показано на малюнку.



Висновки.

У цій лекції було вивчено матеріал про HP Network Protector SDN, який є комерційною корпоративною програмою SDN. Програма використовує мережу з підтримкою OpenFlow для покращення характеристик та функціональності мережі.

Network Protector не вимагає OpenFlow на всіх мережевих пристроях, а лише на краю мережі. Network Protector додає додатковий рівень безпеки за рахунок використання гібридного режиму роботи комутаторів з підтримкою OpenFlow. Таблиці потоку оновлюються контролером HP VAN SDN для використання звичайного пересилання для більшості трафіку. Network Protector додає додатковий потоковий запис з вищим пріоритетом для пересилання DNS-трафіку до контролера, а потім у свою чергу, до Network Protector для перевірки. Використовується база даних RepDV TippingPoint, оскільки вона містить сотні тисяч записів зловмисних веб-сайтів.

Інтегруючи Network Protector з мережею з підтримкою OpenFlow, додається додатковий рівень безпеки для блокування трафіку на шкідливі веб-сайти.

У цій лекції було розглянуто про те, як встановити, налаштувати та впровадити деякі функції, доступні в Network Protector, включаючи:

- DNS interception
- Redirection servers
- Custom blacklists, graylists, and whitelists
- QoS
- ACL Manager

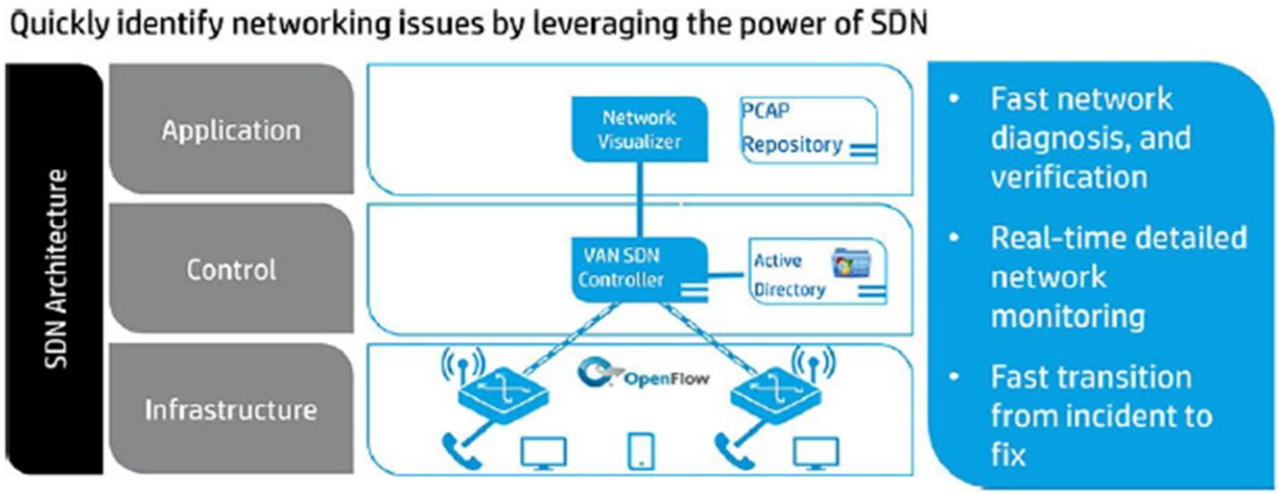
Розділ IV. HP Network Visualizer SDN

HP Network Visualizer SDN встановлюється на HP Controller та може здійснювати динамічну переадресацію трафіку на моніторинговий пристрій, який розташований в мережі з підтримкою OpenFlow або без підтримки OpenFlow.

Пристрій моніторингу мережі навіть може бути відокремлений від контрольованих пристроїв мережею WAN (wide area network). Це вимагатиме достатньої пропускної здатності для захопленого трафіку, IP-з'єднання комутатора з підтримкою OpenFlow з пристроєм захоплення та тунелей Generic Routing Encapsulation (GRE), дозволених брандмауером.

Автоматичні захоплення можуть бути заплановані на певний час у майбутньому.

HP Network Visualizer SDN забезпечує видимість мережного трафіку та пропонує гнучке рішення для отримання копій мережевих пакетів для перевірки, підтвердження та з метою динамічного пошуку несправностей (дивись малюнок).



Ви можете отримати копії мережевих пакетів з декількох пристроїв та здійснити переадресацію захоплених пакетів на пристрій збору, розташований в будь-якій точці мережі, за допомогою тунелю GRE.

HP Network Visualizer SDN динамічно встановлює правила OpenFlow для моніторингу мережевого трафіку за критеріями фільтра, визначеними адміністратором мережі через графічний інтерфейс користувача GUI (graphical user interface). Критерії фільтра визначаються атрибутами політики SDN, побудованими на атрибутах відповідності мережевих списків контролю доступу ACL (access control list) та застарілих діях.

Атрибутами політики SDN є наступні:

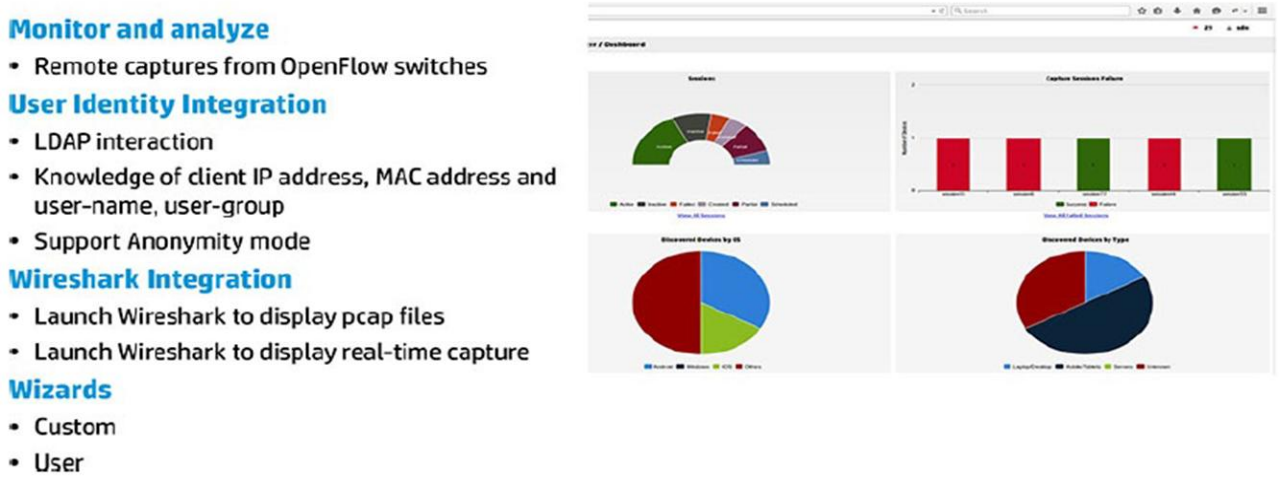
- Users
- User devices

- Location
- Application
- Status of network
- Time

HP Network Visualizer SDN отримує інформацію про інтеграцію на користувацьких пристроях з HP VAN SDN Controller.

4.1 Переваги HP Network Visualizer SDN

Основні характеристики HP Network Visualizer SDN є наступними:



Monitor and analyze the network: Ви можете значно звузити джерело мережевих проблем, знаючи піки трафіку з будь-якого мережевого пристрою, та перевірити підключення до мережі.

Visibility: HP Network Visualizer SDN використовує утиліту Tshark (консольна утиліта із складу Wireshark) для забезпечення прозорості мережі, захоплюючи активність сеансу, статус та узагальнену інформацію.

Комбінація наступних характеристик забезпечує прозорість мережі:

- Ідентифікація адреси клієнта
- Контроль у реальному часі захоплених пакетів на базі графічного інтерфейсу користувача GUI
- Діаграми інформаційної панелі
- Детальний перегляд захопленого сеансу.

Прозорість мережі гарантує, що даний сеанс захоплення функціонує на основі кожного мережевого пристрою. Якщо функціонал відсутній, відзначається причина невдалого захоплення сесії.

Можна переглядати більше 100 останніх пакетів у файлі захоплення пакетів (packet capture - pcap) сеансу. Щоб переглянути усі пакети та проаналізувати пакети, необхідно відкрити файл pcap в утиліті TShark.

Event Logs: Інструмент забезпечення прозорості і моніторингу мережі повинен бути надійним і забезпечити належну доступність до налагодження. Журнали подій є основним джерелом налагоджувальної інформації.

Наприклад, якщо сеанс захоплення активний, і жоден пакет не перехоплений, адміністратор мережі повинен бути поінформований про те, що відповідний трафік не надсилається з джерела моніторингу.

Журнал подій фіксує джерело та причину невдалого захоплення. Журнал подій зберігає записи події на протязі 180 днів. Network Visualizer генерує попередження, коли журнал подій очищується адміністратором мережі або системою.

Create Capture Session wizard: Це покроковий майстер конфігурації для створення нового сеансу захоплення.

Підтримуються наступні режими конфігурації:

- Custom — Налаштування IP-адреси джерела/призначення, MAC адреси джерела/призначення, порт і протокол для сеансу захоплення.
- User — Налаштування користувача, групи користувачів, пристроїв та програми для сеансу захоплення.

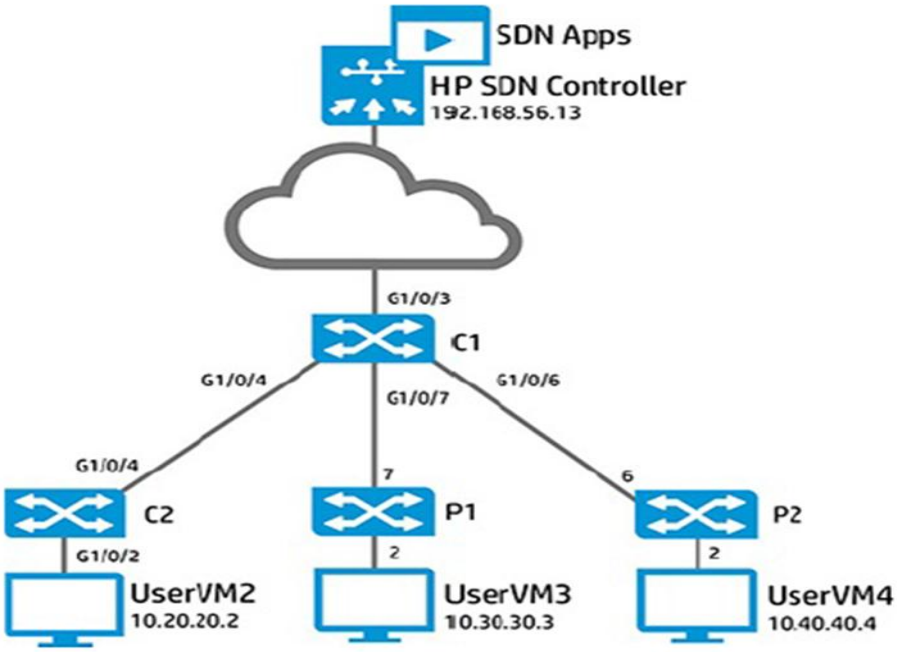
HP Network Visualizer SDN підтримує анонімність, щоб приховати ідентифікатор користувача.

HP Network Visualizer SDN підтримує фізичні мережеві пристрої з підтримкою OpenFlow разом із пристроями Open vSwitch (OVS).

4.2 Встановлення і конфігурація HP Network Visualizer SDN

У цьому розділі наведено інструкції щодо встановлення та ліцензування HP Network Visualizer SDN на контролері HP VAN SDN.

У інструкціях використовуються IP-адреси та конфігурація, які показані на малюнку.



У цьому розділі наведено кроки, які можна зробити, щоб встановити додаток HP Network Visualizer SDN на контролері HP VAN SDN, у цьому прикладі 192.168.56.13. А також наведені кроки для його ліцензування.

Пам'ятайте, що в топології, наведеній на малюнку нижче, OpenFlow вмикається лише на кінцевих комутаторах і лише на портах untagged/access (для користувальницьких VLANS). На висхідних лініях (tagged/trunk ports) OpenFlow не вмикається.

1. Використайте Google Chrome на Windows Jumphost для навігації за адресою: http://192.168.56.13:8443/sdn/ui.

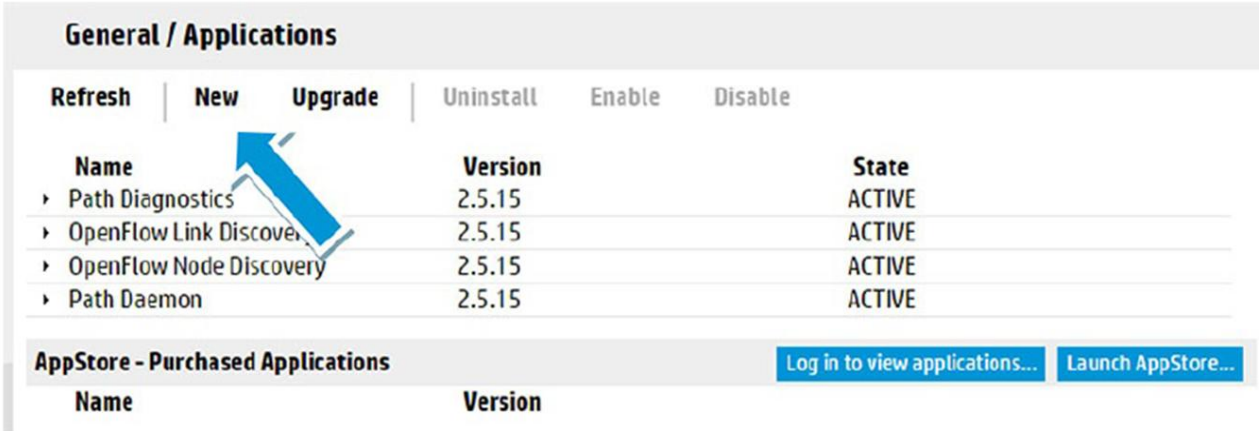
2. Якщо буде запрошення, прийміть самопідписаний сертифікат і продовжуйте вхід на сервер.

3. Увійдіть, використовуючи такі облікові дані:

- Username: sdn
- Password: skyline

5. Вам потрібно встановити HP Network Visualizer SDN вручну, якщо у вас немає доступу до Інтернету. Якщо у вас є доступ до Інтернету, ви можете встановити програму безпосередньо з магазину HP App Store.

6. Клікніть New, як показано на малюнку:



7. Клікніть Browse, як показано на малюнку.

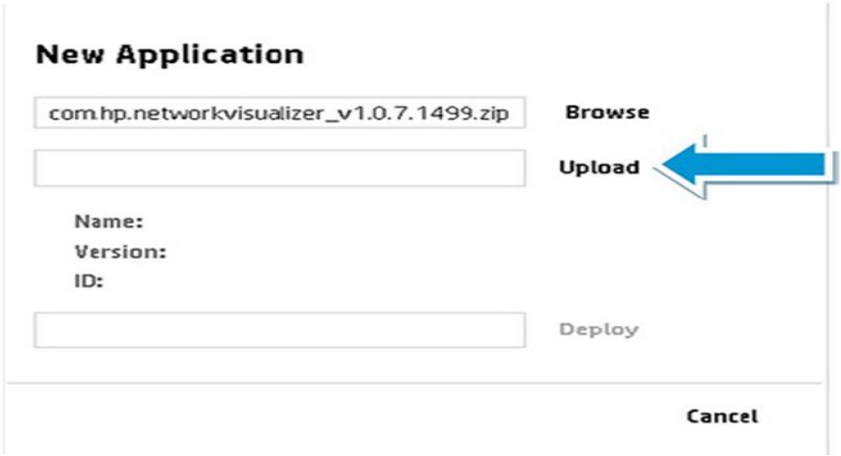
8. Перейдіть на Desktop і відкрийте необхідну папку, у цьому прикладі папка SDN Lab Files. Потім відкрийте папку Software.

WARNING! Програма HP Network Visualizer SDN завантажується як частина zip файлу, що також містить документацію. Переконайтеся, що ви вибрали правильний файл zip, який перелічено нижче, який був розпакований з оригінального завантаженого zip файлу.

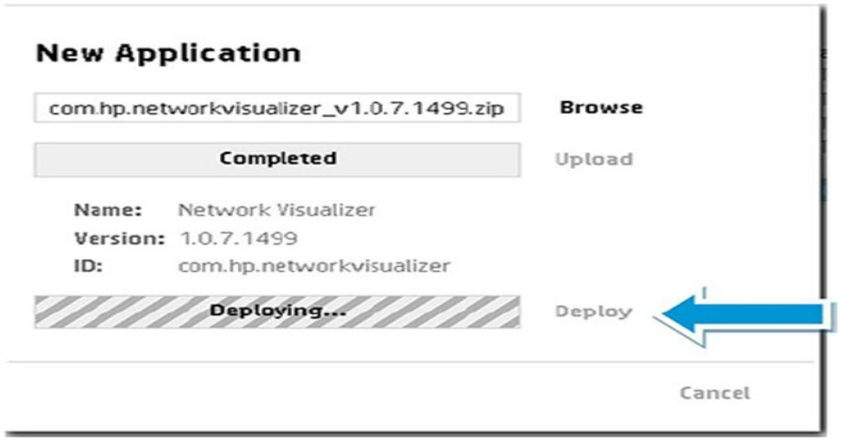
9. Увійдіть на директорію Visualizer: hp-net-visualizer-v1.0.7-x64

10. Виберіть файл com.hp.networkvisualizer_v1.0.7.1499.zip та клікніть Open, як показано на малюнку.

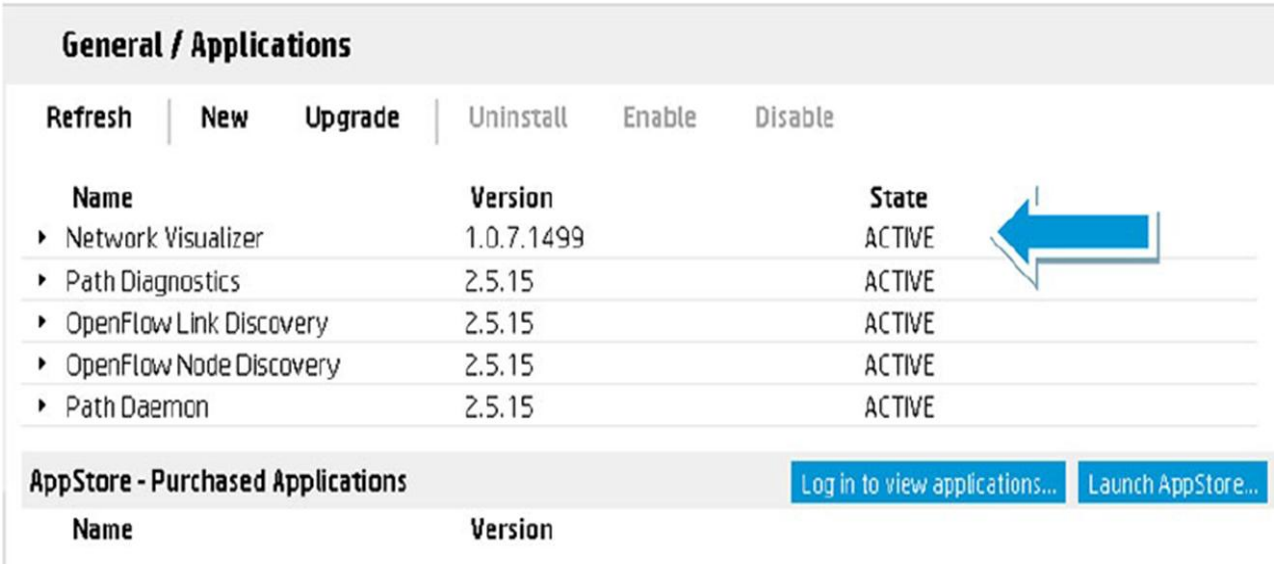
11. Клікніть Upload, як показано на малюнку:



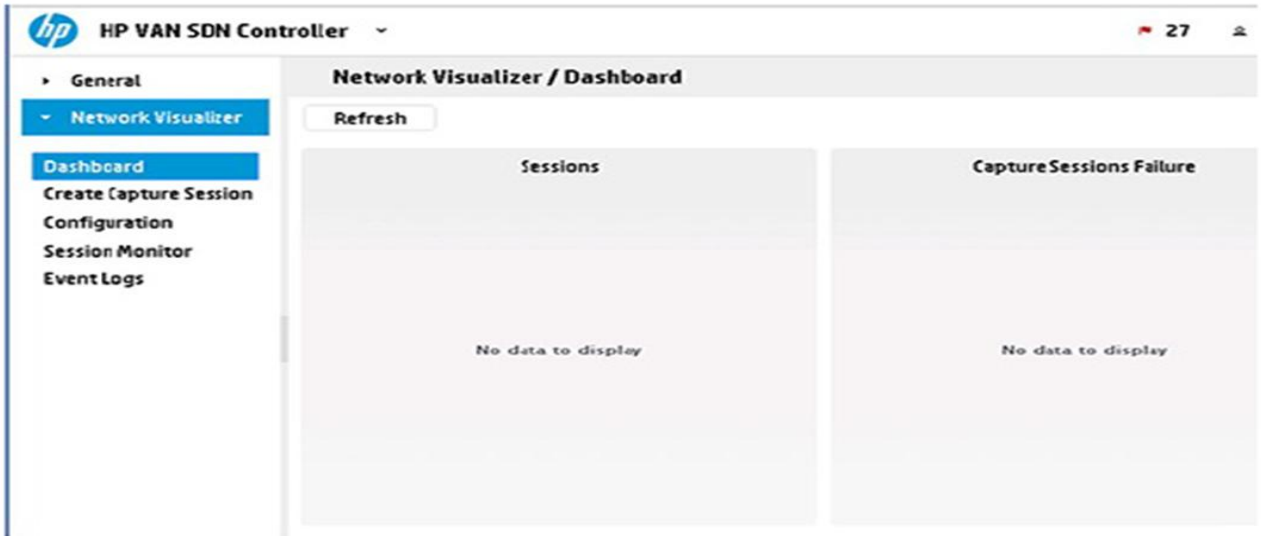
12. Коли додаток буде завантажений, клікніть Deploy, як показано на малюнку:



13. Коли програма буде розгорнута, сторінка контролера оновлюється, щоб показати, що Network Visualizer успішно розгорнута і його стан є ACTIVE, як наведено на малюнку:

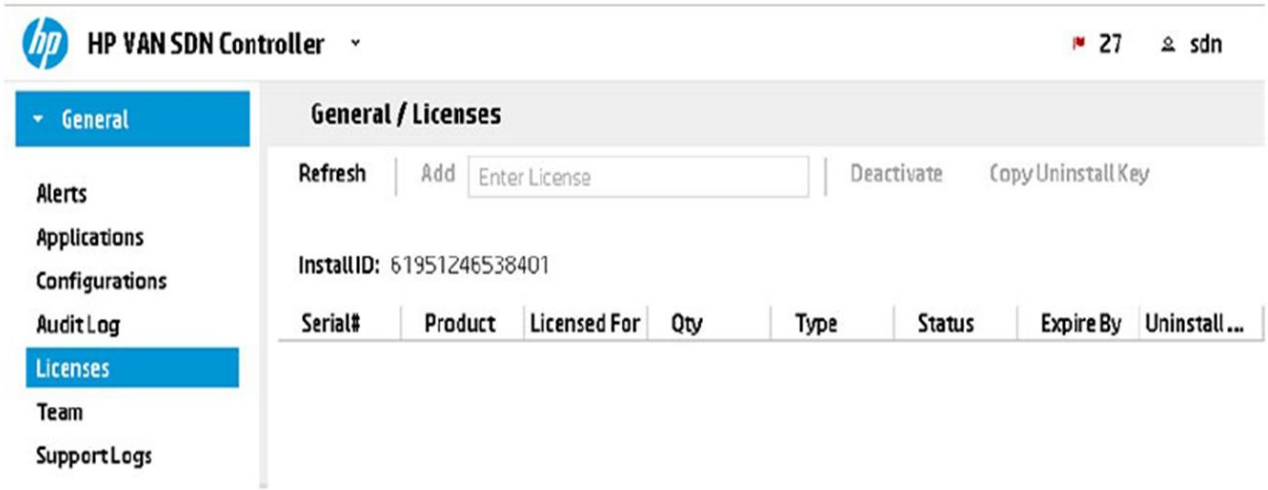


14. Клікніть Network Visualizer (якщо меню не відображається, оновіть свій веб-браузер) і потім клікніть Dashboard, як показано на малюнку:



На даний момент дані сеансу не відображаються.

15. Клікніть General і потім Licenses, як показано на малюнку:



Жодної ліцензії на даний момент не встановлено.

16. HP Network Visualizer SDN вимагає наявності електронної ліцензії для його функціонування. Потрібні такі ліцензії:

- A VAN SDN Controller Base license
- A Network Visualizer license

Наступні ліцензії доступні для покупки:

- JL091AAE HP Network Visualizer SDN App E-LTU
- J9863AAE HP VAN SDN Controller Base Software with 50-node License E-LTU

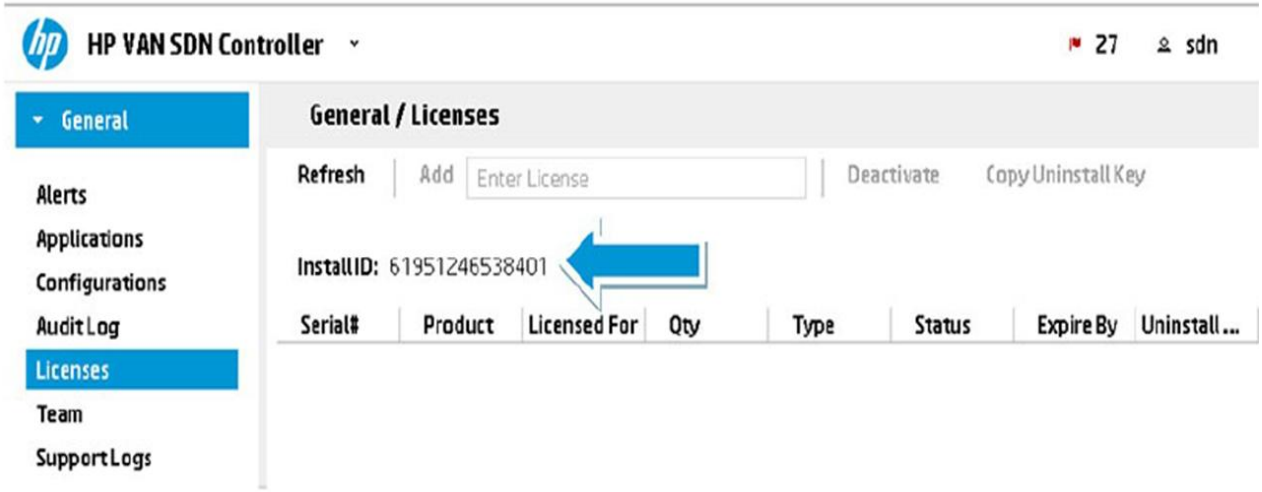
17. Вам це не потрібно, але якщо ви хочете встановити локальну копію HP Network Visualizer SDN, ви можете отримати ліцензію на оцінку. Доступні безкоштовні 60-денні ліцензії на оцінку. Ці ліцензії призначені для оцінки продукту до покупки. Щоб отримати ліцензію на оцінку, виконайте цей процес:

- Встановіть HP VAN SDN Controller.
- Встановіть SDN Applications, які бажаєте оцінити. Якщо ви використовуєте AppStore, встановіть Trial Mode SDN.
- Перейдіть до My Networking Portal http://www.hp.com/networking/mynetworking виберіть SDN Evaluation Licenses.
- Введіть ваш install id. MNP генерує будь-яку ліцензію на оцінку, яка можливо для цього install id.
- Застосуйте відповідні ліцензії для контролера та додатків.

Наступна Network Visualizer Base License була згенерована для Controller Install ID, який використовується у топології:

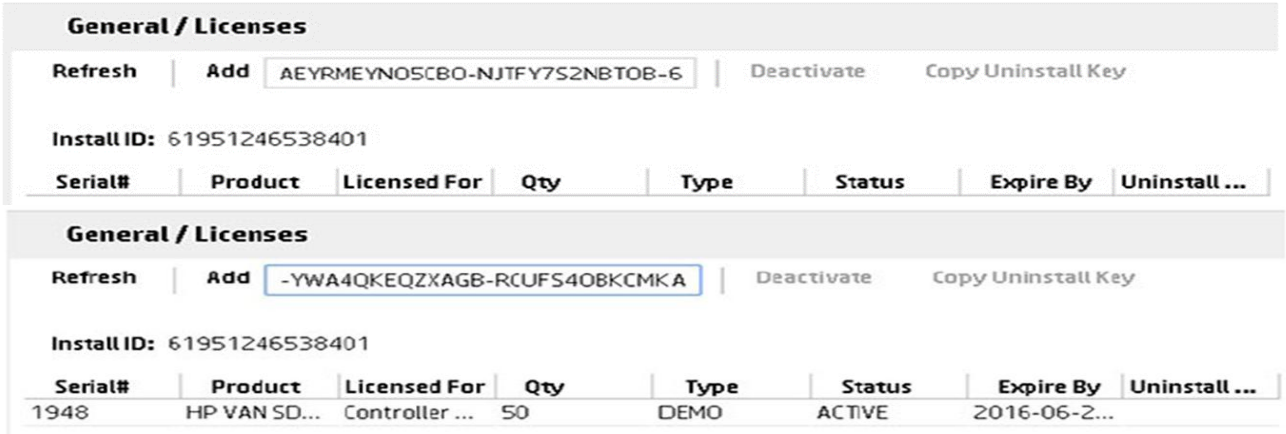
```
This is a confirmation of your registration with the license details:
License key: BUYRMEYNO5CBO-NJTFY7S4NBTPN-YWA4QKEQZXAGB-RCUFS4OBKCMKA
Registration ID: CF7MHX2-X6QP79T-FJ4VFVY-4MCWXC8
Product number: JL091AAE
Product name: HP Network Visualizer SDN App E-LTU
License quantity: 1
Install ID: 61951246538401
Status: Active
Activation date: 22-Jun-2015
Expiration date: 21-Jun-2016
Friendly name: Visualizer App
Customer notes:
```

Чи є цей ліцензійний ключ правильним для Install ID?

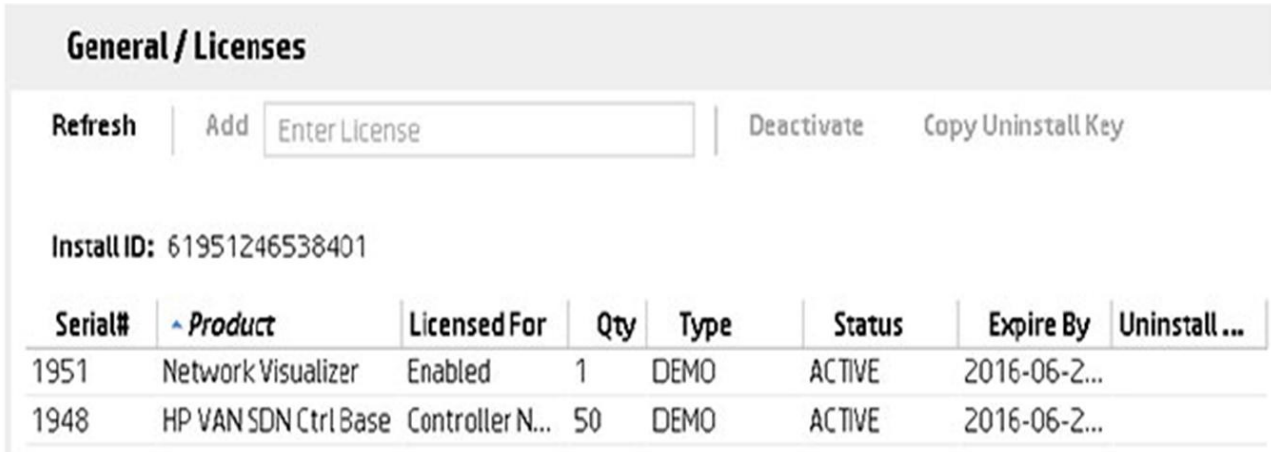


18. Скопіюйте ліцензійний ключ на Windows Jumphost з потрібного файлу, в цьому прикладі: \Desktop\SDN Lab Files\Software\Network Visualizer license Key.txt

19. Вставити обидва ліцензійні ключі (один за раз і в порядку) у поле Enter License box на контролер (див. малюнок нижче), а потім натисніть кнопку Add, як показано на наступному малюнку:



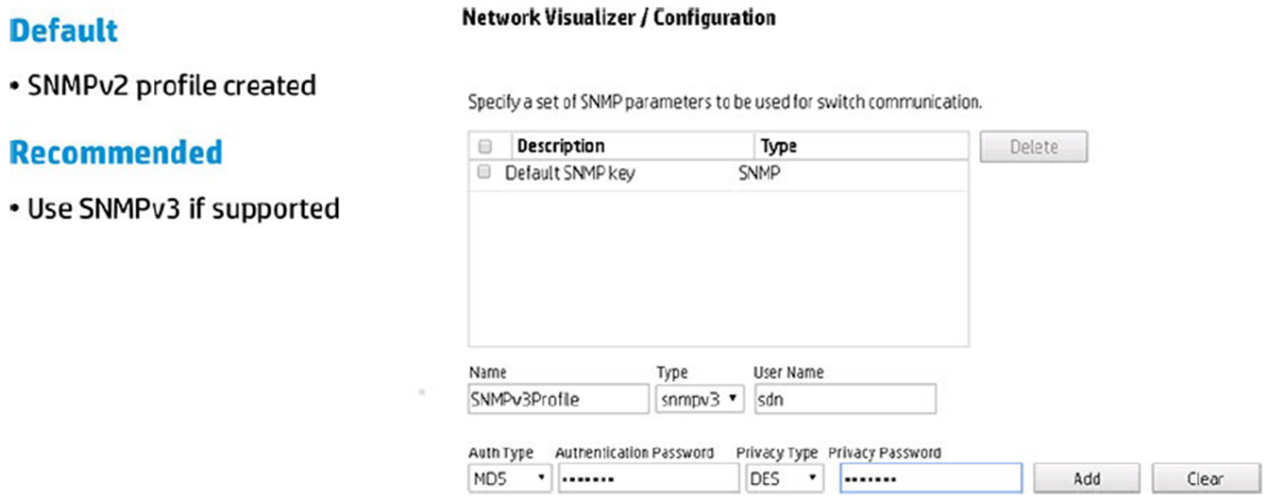
Result: Ліцензії додаються до контролера, як показано на малюнку:



4.3 Взаємодія HP Network Visualizer SDN з мережевими пристроями

HP Network Visualizer SDN підтримує конфігурацію облікових даних SNMPv2 та SNMPv3 для взаємодії з мережевими пристроями. Ви можете створити більше одного набору профілів SNMP, але лише один профіль SNMP для кожного мережевого пристрою.

Створення профіля SNMP показано на малюнку:



1. На сторінці Configurations, натисніть стрілку ліворуч від SNMP Profiles.

2. Виберіть тип SNMP (snmpv2 or snmpv3) із випадаючого списку

3. Введіть такі облікові дані:

- Name — Name of the SNMP profile
- Type — Type of SNMP profile
- Read Community — Community name for read access
- Write Community — Community name for write access
- User Name — Name of the user
- Auth Type — Authentication protocol
- Authentication Password — Authentication password
- Privacy Type — Privacy protocol
- Privacy Password — Privacy password

4. Клікніть Add.

HP Network Visualizer SDN вимагає налаштування OpenFlow на комутаторах, з яких програма захопить трафік. На малюнку, версія 1.3 OpenFlow використовується як OpenFlow копія для vlan20 (комутатор HP ProVision).

```
openflow
  controller-id 1 ip 192.168.56.13 controller-interface vlan 1
  instance “vlan20"
      member vlan 20
      controller-id 1
       version 1.3 only
      enable
      exit
  enable
```

Рекомендується налаштування SNMPv3 для комутатора ProVision, як показано на малюнку.

```
snmpv3 enable
snmpv3 restricted-access
snmpv3 user sdn auth md5 skyline priv des skyline
snmpv3 group ManagerPriv user sdn sec-model ver3
```

WARNING! Не використовуйте майстер SNMP для конфігурації користувача. Увімкніть SNMP, а потім вручну створіть необхідну обліковий запис користувача (sdn у цьому прикладі). Рекомендується видалити створеного первинного користувача, якщо це явно не потрібно.

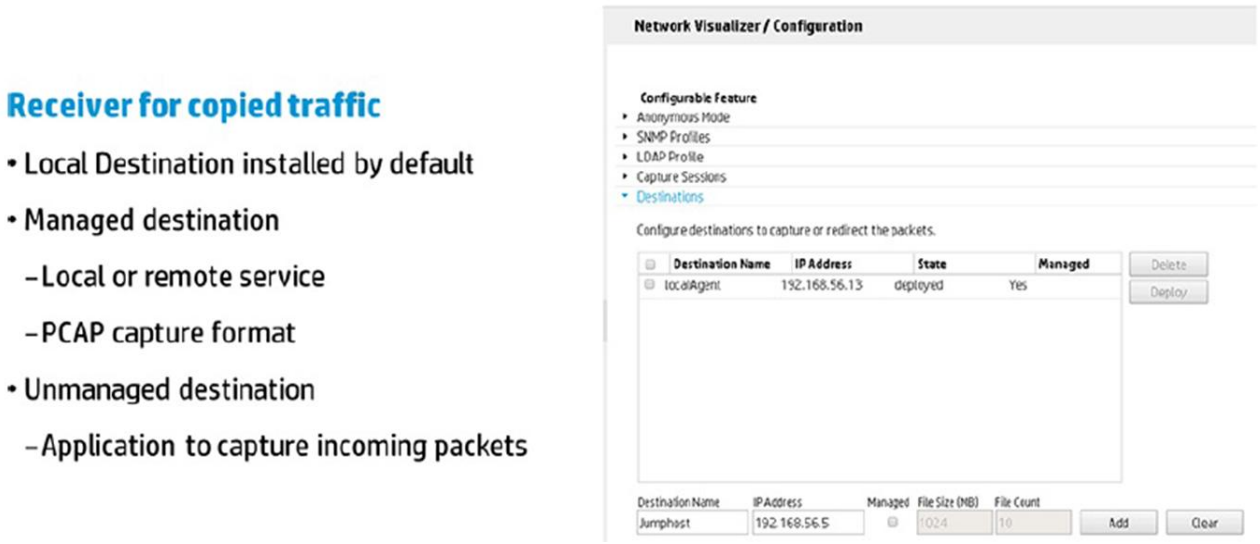
```
This is an example of SNMPv3 configuration on a 3800 series switch:

P1(config)# snmpv3 enable

SNMPv3 Initialization process.

Creating user 'initial'

Authentication Protocol: MD5

Enter authentication password: *******

Privacy protocol is DES

Enter privacy password: *******


User 'initial' has been created

Would you like to create a user that uses SHA? [y/n] n


User creation is done. SNMPv3 is now functional.

Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can
set this later by the command 'snmpv3 restricted-access')? [y/n] y

P1(config)# snmpv3 user sdn auth md5 skyline priv des skyline

P1(config)# snmpv3 group ManagerPriv user sdn sec-model ver3
```

Адресат призначення або сховище pcap є приймачем для копіюваного трафіку. Це може бути на локальній або віддаленій системі. Ви можете налаштувати адресата призначення наступним чином:

Керований адресат призначення: Працює як daemon service, яка отримує захоплені пакети і зберігає їх у форматі pcap. Місцевий керований адресат призначення встановлюється, коли ви встановлюєте Network Visualizer. Ви повинні налаштувати та розгорнути віддалені адресати призначення за допомогою Network Visualizer.

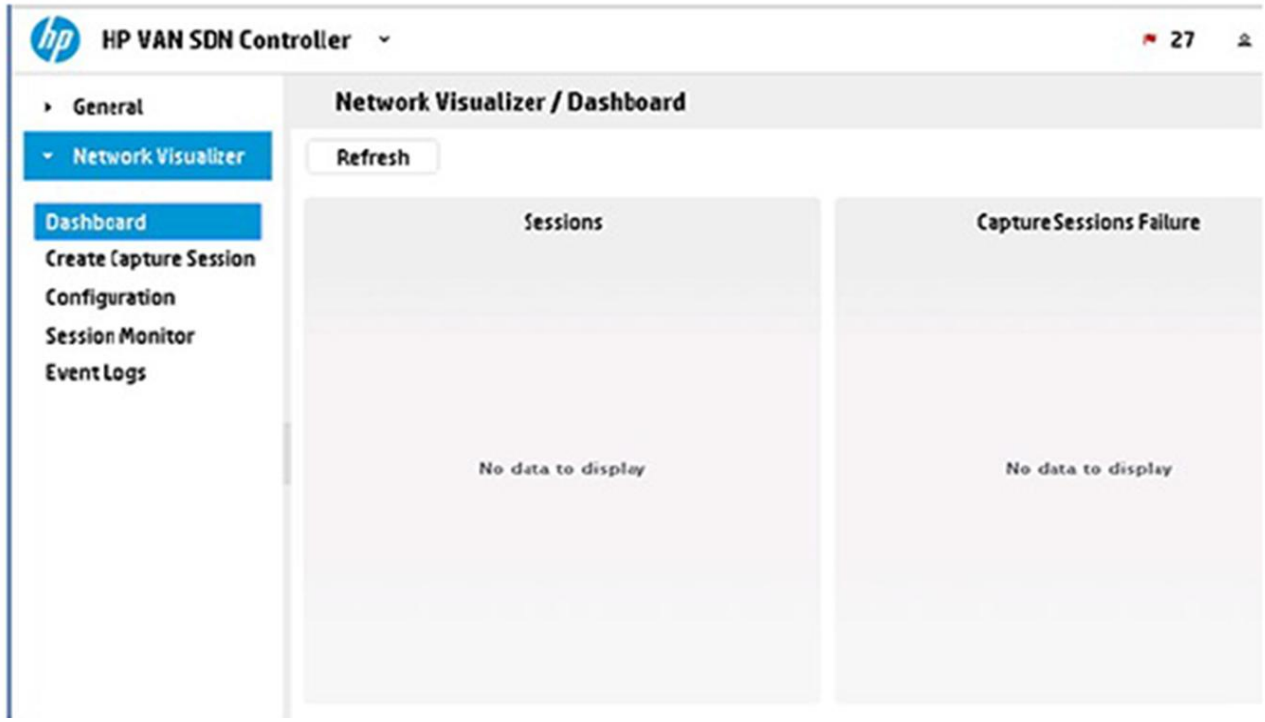
Некерований адресат призначення: Ви можете запустити програму або рішення для обробки вхідного трафіку копіювання з мережевого пристрою.

Для успішного встановлення, State показує з’єднання на панелі Destinations, як показано на малюнку.



Ви можете створювати сеанс захоплення за допомогою майстра **Create Capture Session** а потім вибрати політику фільтра, адресата призначення та графік, щоб відстежувати сеанс. Щоб увійти до майстра, клікніть Create Capture Session з навігаційного дерева Network Visualizer.

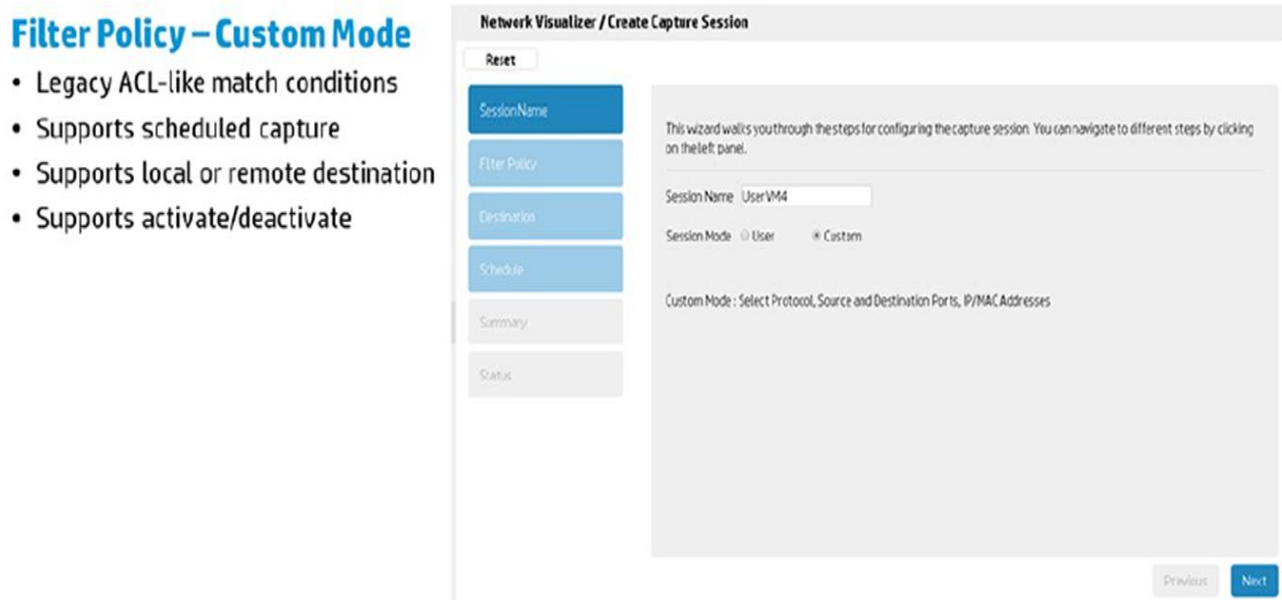
Network Visualizer/Create Capture Session - це покроковий майстер конфігурації для створення нового сеансу захоплення (дивись малюнок).



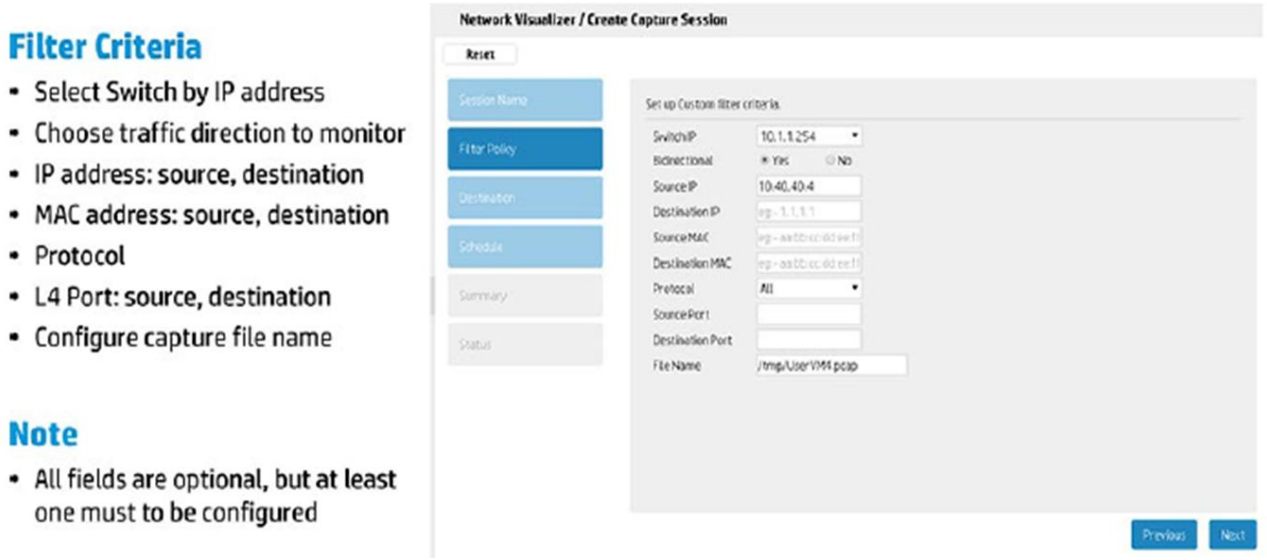
На першому кроці додайте назву сесії та оберіть режим сеансу на панелі Session Name. Введіть ім'я сеансу захоплення в текстовому полі Session Name. За замовчуванням режим сеансу є User.

Custom: Налаштування IP-адреси джерела/призначення, MAC адреси джерела/призначення, порт і протокол для сеансу захоплення.

User: Налаштування користувача, групи користувачів, пристроїв та програми для сеансу захоплення.



На другому кроці встановіть критерії фільтра, як показано на малюнку:



Switch IP: IP address of the network device

Bidirectional: Select the traffic capture direction by clicking:

Yes: Captures packets sent and received by the user.

No: Captures packets sent by the user

Source IP: IP address of the source (for example, 10.40.40.4)

Destination IP: IP address of the destination (for example, 192.168.56.51)

Source MAC: MAC address of the source (for example, aa:bb:cc:dd:ee:ff)

Destination MAC: MAC address of the destination (for example, aa:bb:cc:dd:ee:ff)

Protocol: Network protocol. By default, protocol is All

Source Port: Layer 4 port for the source

Destination Port: Layer 4 port for the destination

File Name: Name of the pcap file in which to save the packets

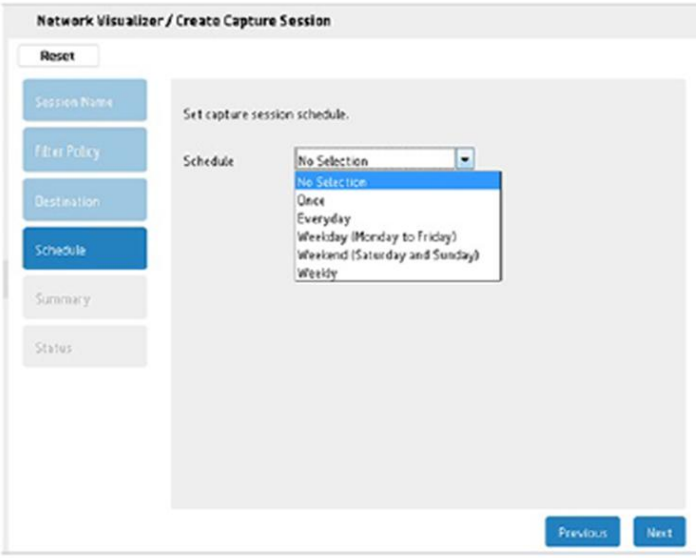
Налаштуйте графік для моніторингу сеансу захоплення на панелі Schedule, як показано на малюнку.

Schedule

- Select one schedule type

Note

- No selection results in activated session running immediately, and only stops when session is deactivated.



No Selection: Monitoring of a capture session is not scheduled.

Once: Monitor the capture session once. Specify the Start Time and Stop Time.

Everyday: Monitor the capture session everyday. Specify the repeat interval in Repeat every (days), Start Time, Stop Time, and End Date.

Weekday (Monday to Friday): Monitor the capture session on weekdays. Specify the Start Time, Stop Time, and End Date.

Weekend (Saturday and Sunday): Monitor the capture session on weekends. Specify the Start Time, Stop Time, and End Date.

Weekly: Monitor the capture session on a weekly basis. Select the days of the week to capture the sessions with Repeat on check boxes. Specify the Start Time, Stop Time, and End Date.

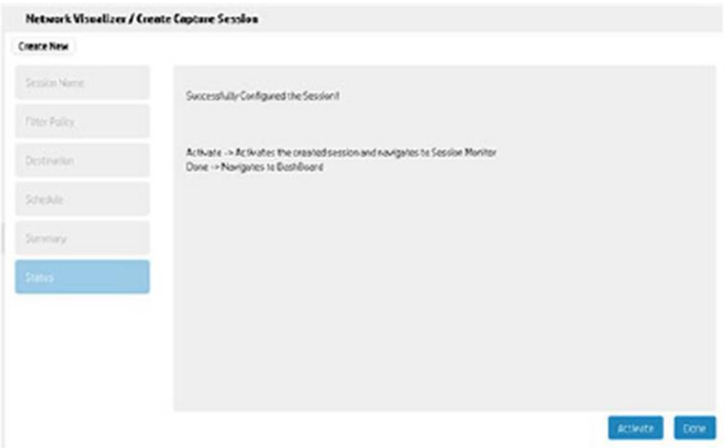
Останній крок у майстрі полягає в тому, щоб активувати сеанс, як показано на малюнку. Захоплення може розпочатися негайно або згідно графіку.

Behavior after Activation

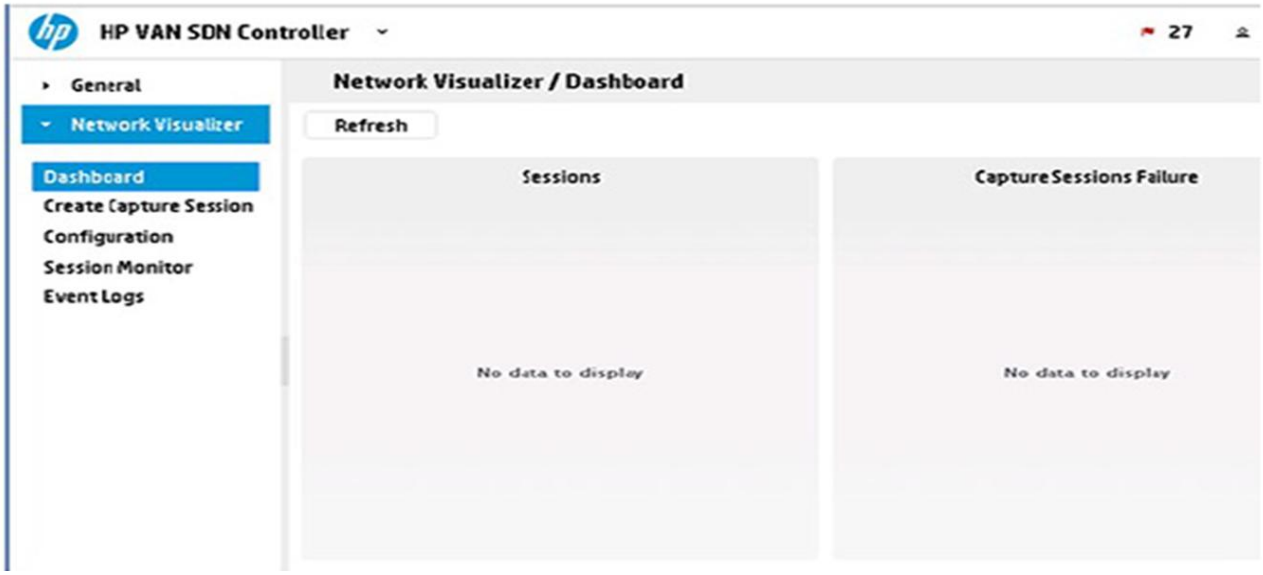
- Non-scheduled session: capture rule is installed immediately if devices are discovered
- Scheduled session: scheduled session is saved, and once time range is reached, capture rule is installed if devices are discovered
- In both case, system updates number of runs

How to Activate

- At the end of wizard, click "Activate" button to activate session.
- Configuration → Capture Session, click "Activate" to activate selected session
- Session Monitor → Select session and click "Activate"

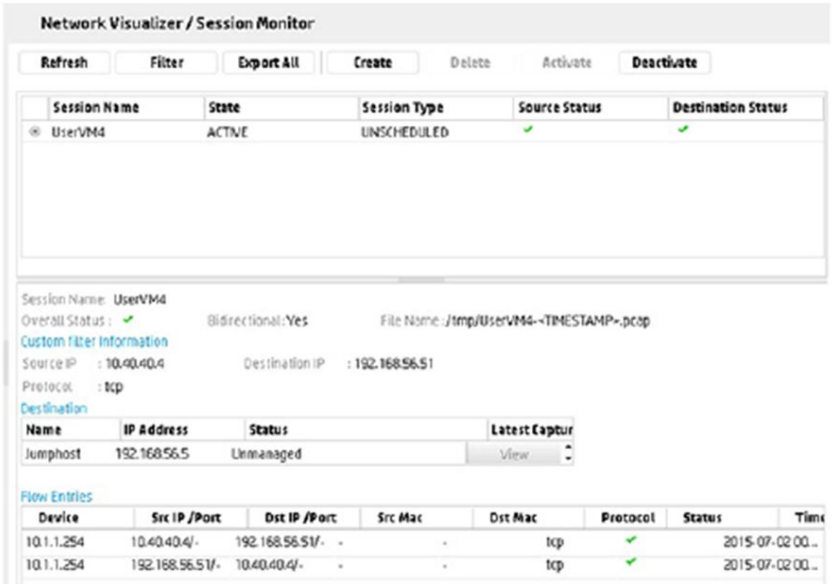


Session Monitor надає докладну інформацію про сеанс захоплення та дозволяє керувати сеансами, як показано на малюнку.



Session Operational Status

- Session failure reason
- Flows installed for activated session
- Number of runs



• Натисніть кнопку біля сеансу, щоб переглянути записи про Destination та Flow Entries.

• Клікніть View щоб переглянути останні 100 пакетів, захоплених Destination.

• Клікніть Refresh для оновлення таблиці.

• Клікніть Filter для фільтрації сеансу за назвою в таблиці.

• Клікніть Export All щоб експортувати всі дані сеансу монітора до файла a.csv.

• Клікніть Create щоб запустити Create Capture Session wizard.

• Клікніть Delete щоб видалити сеанс.

• Клікніть Activate або Deactivate для активації або дезактивації сеансу.

• Клікніть Enable або Disable щоб включити або виключити запланований сеанс.

На Session Monitor можна переглядати захоплення в режимі реального часу (дивись малюнок).

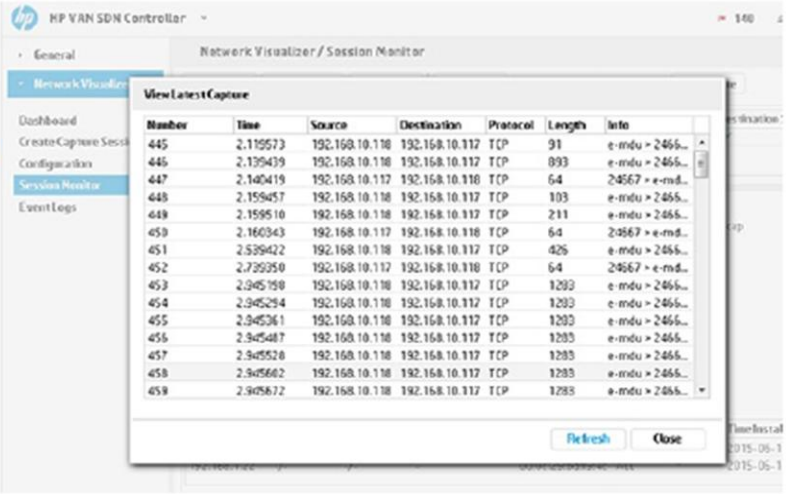
Клікніть View для відображення останніх 100 пакетів, захоплених обраним активованим сеансом. Клікніть Refresh щоб побачити наступних 100 пакетів.

Session Monitor

- Activated session
- Click "View" Button

Configuration → Capture Session

- Activated session
- Click "View" Button



Інформаційна панель **(Network Visualizer Dashboard)** забезпечує графічне представлення поточної конфігурації сеансу захоплення, збоїв сеансу захоплення та виявлених пристроїв за типом та операційною системою (ОС). Щоб зайти на інформаційну панель, клікніть Dashboard із навігаційного дерева HP Network Visualizer SDN.

На інформаційній панелі відображаються наступні діаграми для Sessions і Capture Sessions, як показано на малюнку.

Sessions

- Sessions chart displays the current state of all the capture sessions

Capture Sessions Failure

- The information about the deployment of monitoring policies across configured network devices for the most recent five unique sessions

Discovered Devices by OS

- Discovered devices by operating systems

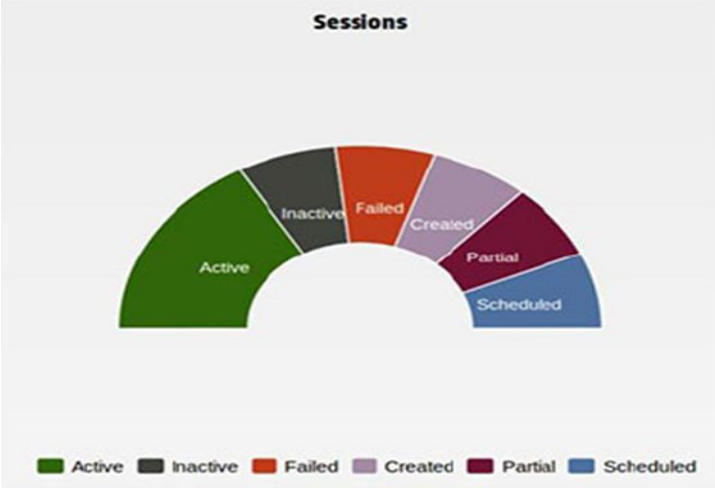
Discovered Devices by Type

- Discovered devices by device types

Діаграми несправностей надають додаткову інформацію:

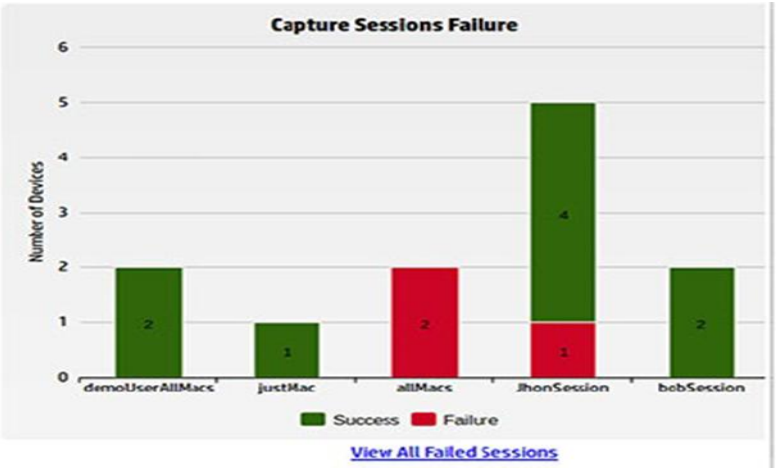
- Sessions
- Capture sessions failure
- Discovered devices by OS
- Discovered devices by type

Половинна діаграма Sessions, як показано на малюнку, відображає поточний стан всіх сеансів захоплення. Сеанси можуть бути в будь-якому з наступних станів у будь-який момент часу:



- Created — Number of created capture sessions.
- Active — Number of active capture sessions.
- Inactive — Number of inactive capture sessions.
- Partial — Number of sessions for which the network traffic capture failed on a few devices.
- Failed — Number of sessions for which the network traffic capture failed.
- Scheduled — Number of sessions for which network traffic capture is scheduled.

Діаграма Capture Sessions Failure, яка показана на малюнку, відображає інформацію про розгортання політик моніторингу на налаштованих мережевих пристроях для останніх п'яти унікальних сеансів.



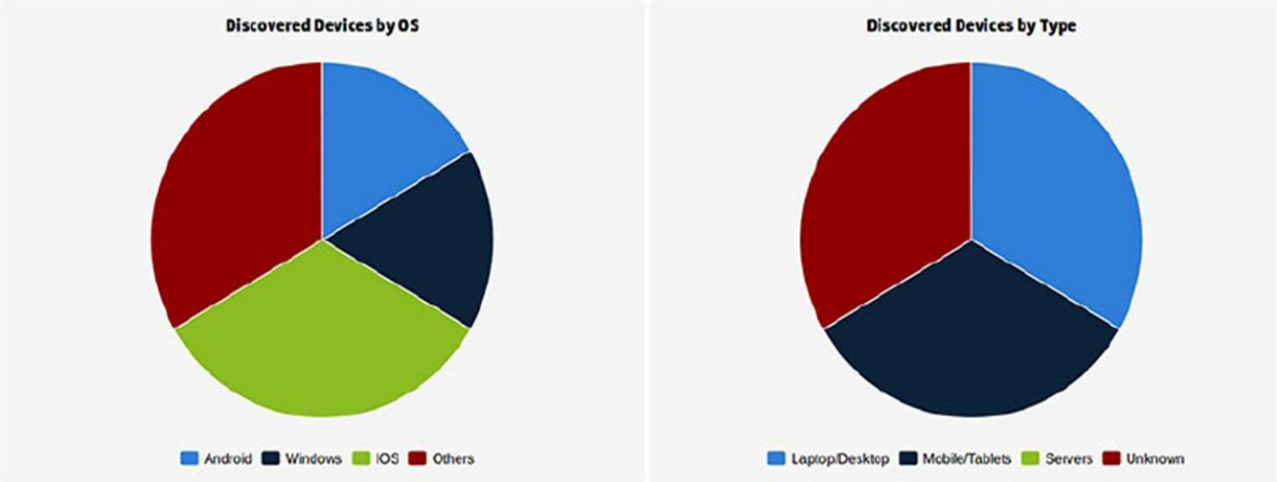
Ось **y** вказує кількість налаштовуваних мережевих пристроїв для сеансу, а ось **x** вказує назву сеансів. Стовпчик вказує кількість мережевих

пристроїв, на яких конфігурація монітора розгорнута успішно та не вдалося для кожного сеансу.

На графіку відображається така інформація:

- Success: Відображає загальну кількість мережевих пристроїв, на яких конфігурація монітора розгорнута успішно для сеансу.
- Failure: Відображає загальну кількість мережевих пристроїв, на яких конфігурація монітора розгорнута невдало для сеансу.

Діаграма Discovered Devices by OS відображає частку відкритих пристроїв операційними системами у вигляді кругової діаграми (дивись малюнок).



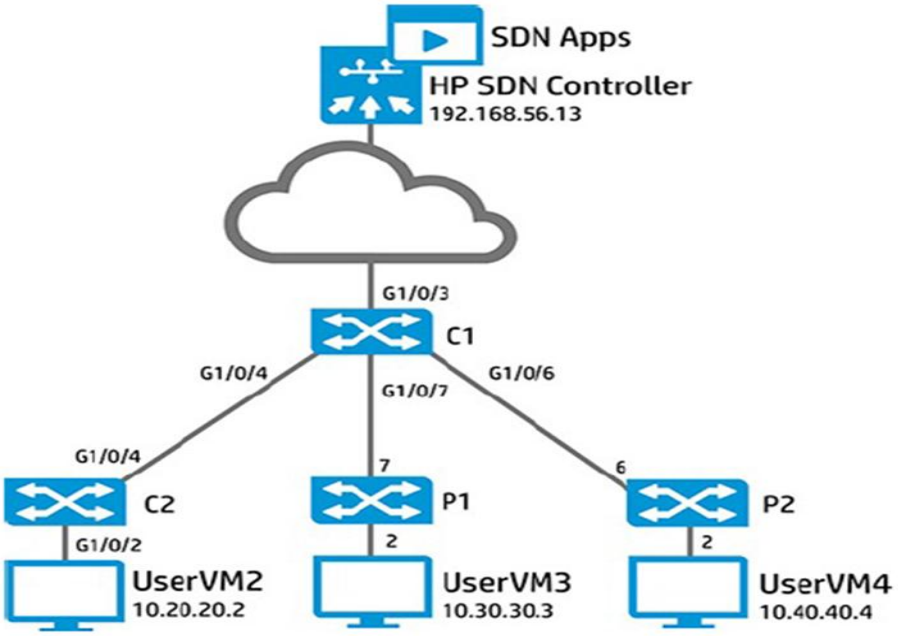
У діаграмі ви можете переглянути таку інформацію:

- Android: Indicates the number of devices with Android operating system.
- Windows: Indicates the number of devices with Windows operating system.
- IOS: Indicates the number of devices with iOS operating system.
- Others: Indicates the number of devices with any other operating system.
- Діаграма Discovered Devices by Type відображає частку типів пристроїв, відкритих HP Network Visualizer SDN:
- У діаграмі ви можете переглянути таку інформацію:
- Laptop/Desktop: Indicates the number of discovered laptops and desktops.
- Mobiles/Tablets: Indicates the number of discovered mobile devices and tablets.
- Servers: Indicates the number of discovered servers.
- Unknown: Indicates the number of discovered unknown devices.

4.4 Інтеграція HP Network Visualizer SDN з HP комутаторами

У цьому розділі описано, як інтегрувати HP Network Visualizer SDN з існуючою мережею HP. Для цього потрібна конфігурація SNMP як на комутаторах HP (налаштовується раніше), так і на HP Network Visualizer SDN. На малюнку ілюструється топологія, що використовується для інструкцій.

Також розглядається, як налаштувати сеанс захоплення та переадресацію захопленого трафіку на Jumphost, використовуючи Wireshark, а також переглядаються потокові записи OpenFlow, які створені за допомогою HP Network Visualizer SDN.



1. Як вже було сказано, комутатори ProVision P1 і P2 вимагають версії 15.17 програмного забезпечення комутатора.

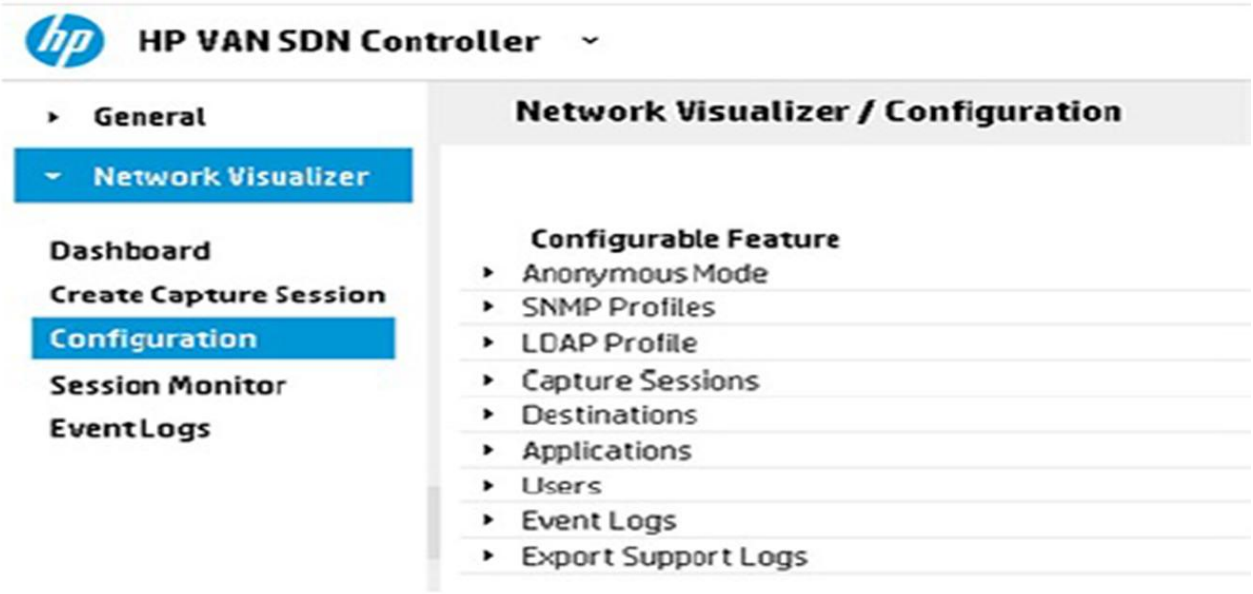
2. Перевірте версії програмного забезпечення у флеш памяті - підтвердьте, що доступно саме 15.17.

3. Завантажте комутатор ProVision (P1 та P2) використовуючи 15.17.

4. Перевірте, що комутатори використовують 15.17 (*show version*).

```
P2# show version

Image stamp:

/ws/swbuildm/rel_portland_qaoff/code/build/tam(swbuildm_rel_portland_qaoff_rel_portland)

Jun 17 2015 16:04:30

KA.15.17.0007

238

Boot Image: Secondary

Boot ROM Version: KA.15.09

Active Boot ROM: Primary
```

5. На графічному інтерфейсі HP Controller GUI, клікніть Network Visualizer і потім клікніть Configuration, як показано на малюнку.

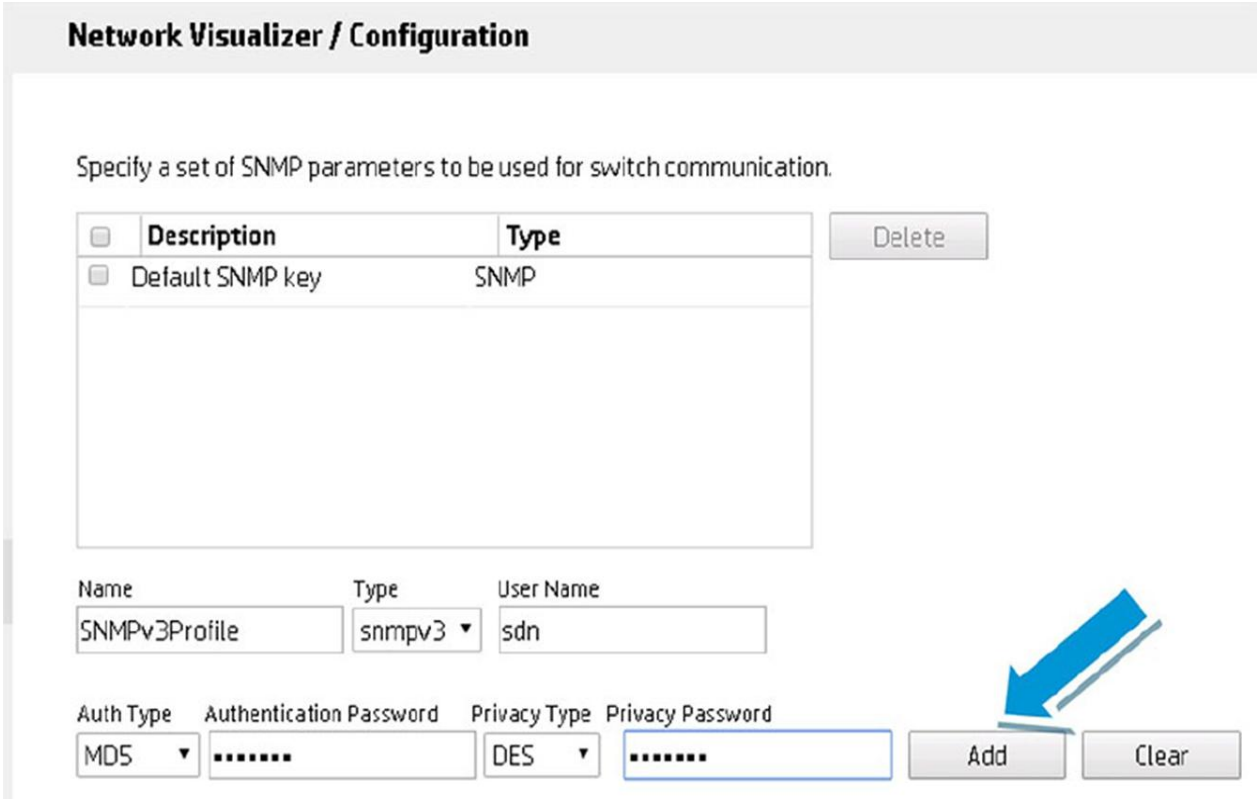


6. HP Network Visualizer SDN підтримує конфігурацію облікових даних SNMPv2 та SNMPv3 для взаємодії з мережевими пристроями. Оскільки SNMPv3 був попередньо налаштований на комутаторах, у цьому прикладі буде використовуватись SNMPv3.

Клікніть **SNMP Profiles** і створіть профіль із наведеними нижче деталями та натисніть кнопку **Add**, як показано на малюнку нижче.

- Name: SNMPv3Profile
- Type: snmpv3
- Username: sdn
- Auth Type: MD5
- Authentication Password: skyline
- Privacy Type: DES

- Privacy Password: skyline



7. Використайте PuTTY на Jumphost для з'єднання з HP VAN SDN Controller використовуючи SSH:

- IP address: 192.168.56.13
- Port number: 22
- Protocol: SSH

Перевірте, чи контролер HP VAN SDN може пінгувати всі комутатори HP у вашому середовищі:

Result:
All pings should succeed.

```
sdn@sdnctl3:~$ ping 192.168.56.251
sdn@sdnctl3:~$ ping 10.1.1.252
sdn@sdnctl3:~$ ping 10.1.1.253
sdn@sdnctl3:~$ ping 10.1.1.254
```

8. Налаштуйте комутатор ProVision (P1) для використання HP Network Visualizer SDN Controller (192.168.56.13):

```
P1# conf

P1(config)# openflow

P1(openflow)# controller-id 3 ip 192.168.56.13 controller-interface vlan 1

P1(openflow)# instance vlan30

P1(of-inst-vlan30)# disable

P1(of-inst-vlan30)# no controller-id 2

P1(of-inst-vlan30)# controller-id 3

P1(of-inst-vlan30)# enable

P1(of-inst-vlan30)# end

P1#
```

9. Перегляньте конфігурацію комутатора та перевірте, чи є конфігурація OpenFlow та SNMP такою, як вказано на прикладі:

```
P1# show running-config
...<omitted>
snmp-server community "public" unrestricted
snmpv3 enable
snmpv3 restricted-access
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "initial"
snmpv3 user "sdn"
openflow
 controller-id 1 ip 192.168.56.11 controller-interface vlan 1
 controller-id 2 ip 192.168.56.12 controller-interface vlan 1
 controller-id 3 ip 192.168.56.13 controller-interface vlan 1
 instance "vlan30"
 member vlan 30
 controller-id 3
 version 1.3
 enable
 exit
 enable
 exit
```

10. Check controller status:

```
P1# show openflow instance vlan30

Configured OF Version : 1.3

Negotiated OF Version : 1.3

Instance Name : vlan30

Admin. Status : Enabled

Member List : VLAN 30

... <omitted>...

Controller Id Connection Status Connection State Secure Role

------------ ----------------- --------------- ------ ------

3 Connected Active No Equal

P1#
```

Result:
Switch has an active connection to controller 192.168.56.13 .

11. Configure ProVision switch 2 (P2) to use the Network Visualizer Controller:

```
P2# conf

P2(config)# openflow

P2(openflow)# controller-id 3 ip 192.168.56.13 controller-interface vlan 1

P2(openflow)# instance vlan40

P2(of-inst-vlan40)# disable

P2(of-inst-vlan40)# no controller-id 2

P2(of-inst-vlan40)# controller-id 3

P2(of-inst-vlan40)# enable

P2(of-inst-vlan40)# end

P2#
```

12. Перегляньте конфігурацію комутатора та перевірте, чи є конфігурація OpenFlow та SNMP такою, як вказано на прикладі:

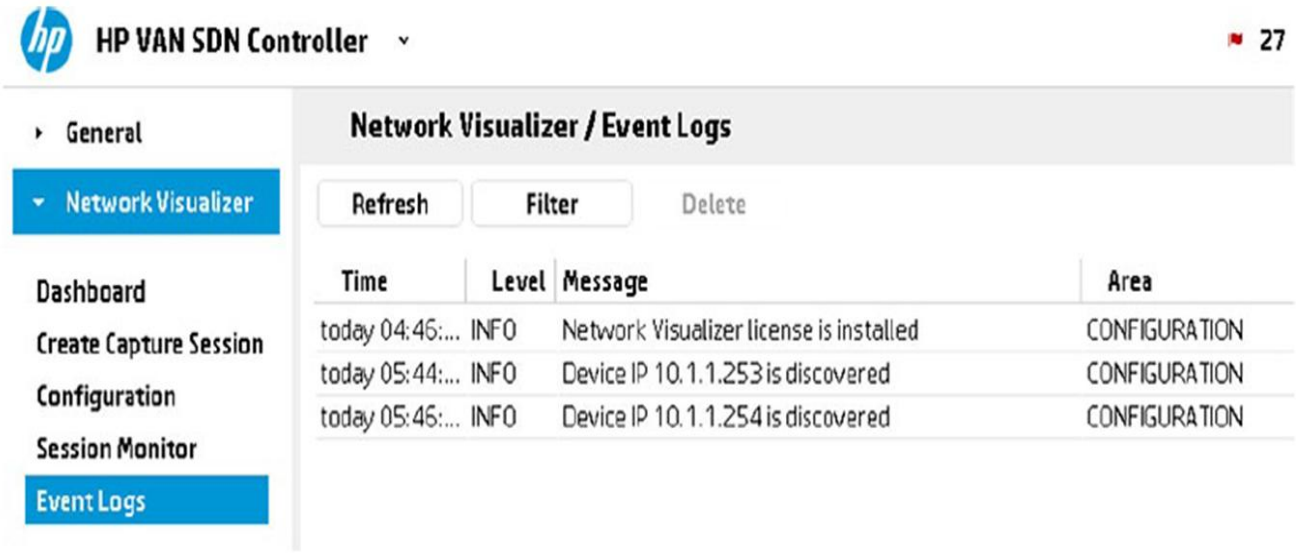
```
P2# show running-config
...<omitted>
snmp-server community "public" unrestricted
snmpv3 enable
snmpv3 restricted-access
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "initial"
snmpv3 user "sdn"
openflow
 controller-id 1 ip 192.168.56.11 controller-interface vlan 1
 controller-id 2 ip 192.168.56.12 controller-interface vlan 1
 controller-id 3 ip 192.168.56.13 controller-interface vlan 1
 instance "vlan40"
 member vlan 40
 controller-id 3
 version 1.3
 enable
 exit
 enable
```

13. Перевірте статус контролера:

```
P2# show openflow instance vlan40
Configured OF Version : 1.3
Negotiated OF Version : 1.3
Instance Name : vlan40
Admin. Status : Enabled
Member List : VLAN 40
...<omitted>...
Controller Id Connection Status Connection State Secure Role
------------ ----------------- ---------------- ------ ------
3 Connected Active No Equal
P2#
```

Result: Switch has an active connection to controller 192.168.56.13.

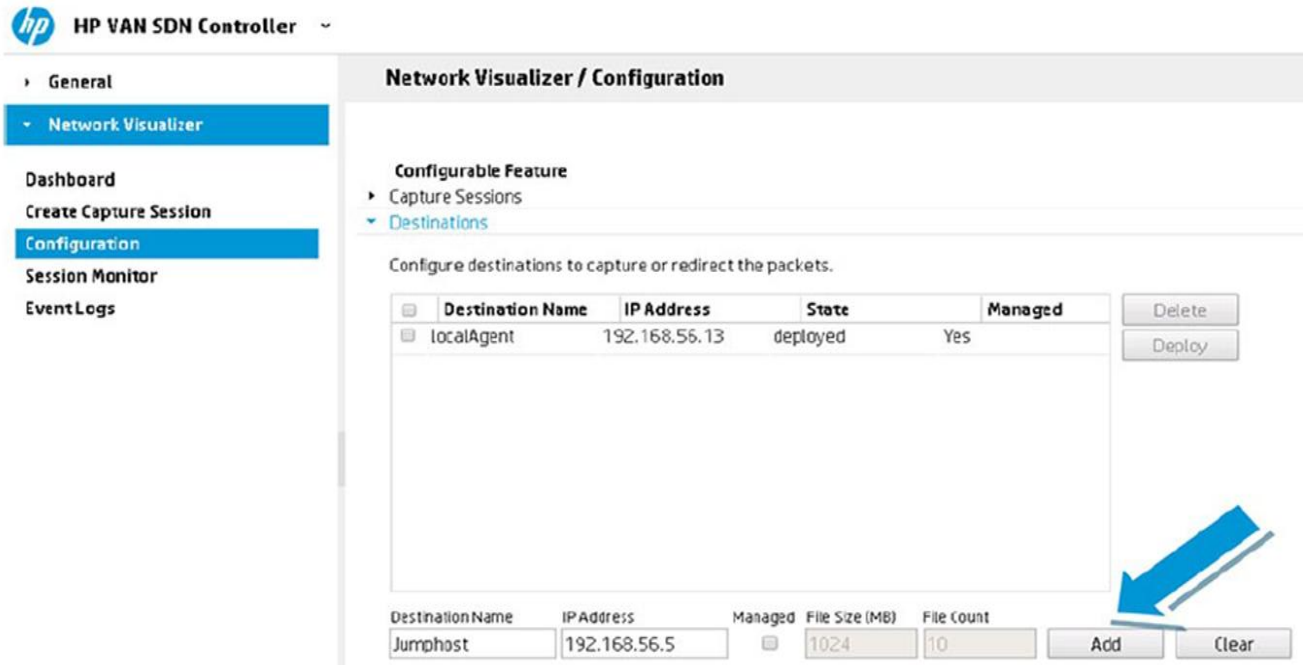
14. На графічному інтерфейсі HP Network Visualizer SDN GUI, клікніть **Event Logs**, як показано на малюнку:



Result: Switches 10.1.1.253 and 10.1.1.254 are discovered.

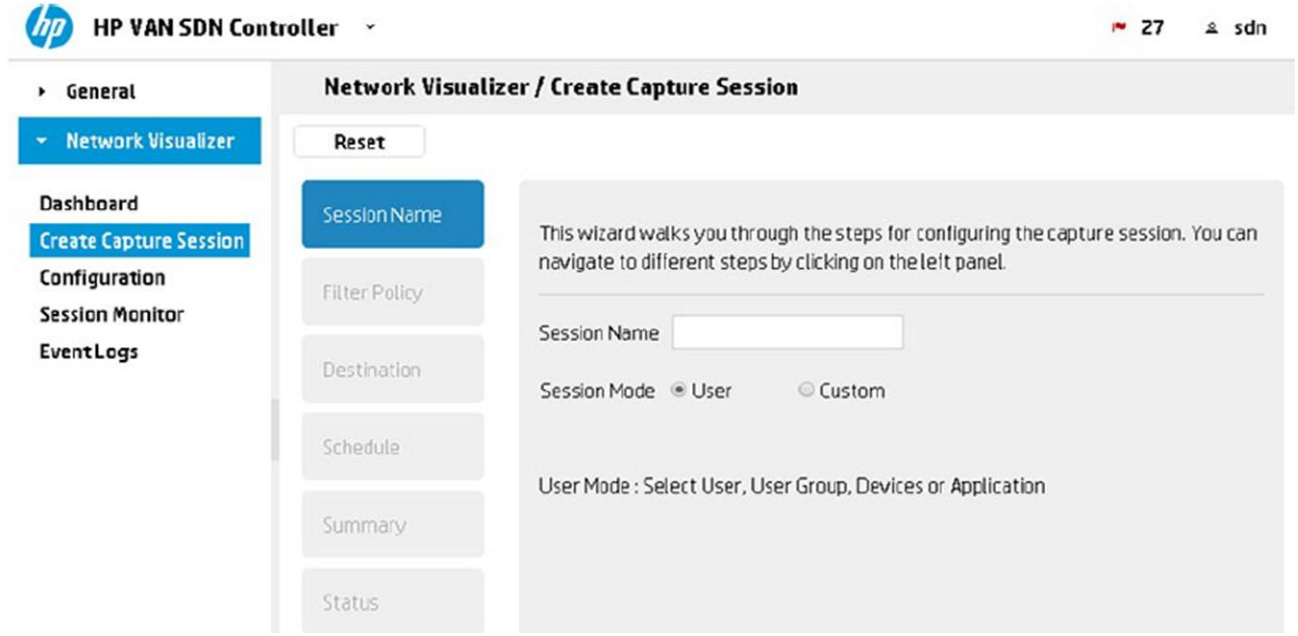
15. Клікніть Configuration а потім Destinations.
16. Налаштуйте наступні значення та клікніть **Add**:

- Destination Name: Jumphost
- IP address: 192.168.56.5 (this is the IP address of the Jumphost PC)
- Managed = Unchecked (off)
- Click Add (see Figure):



17. Ви можете створити сеанси захоплення, використовуючи майстра Create Capture Session. Ви можете вибрати політику фільтра, адресата

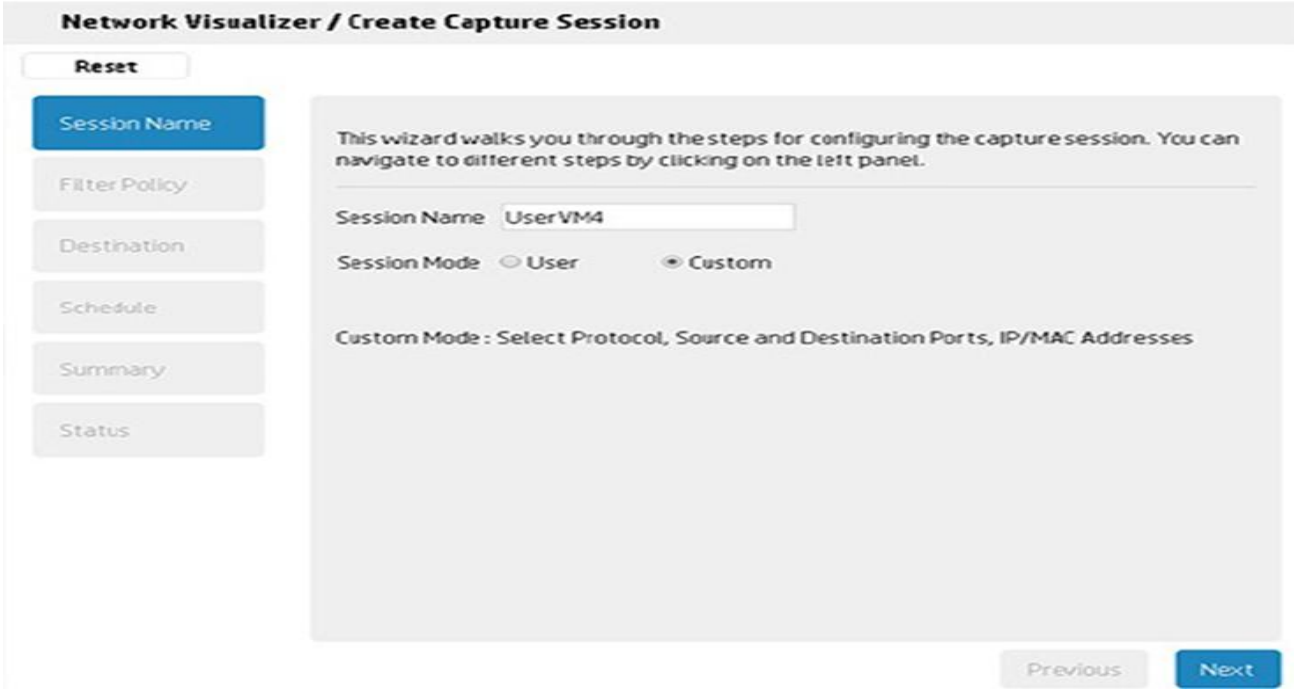
призначення та графік, щоб відстежувати сеанс. Щоб увійти до майстра, клікніть Create Capture Session (дивись малюнок):



18. На **першому кроці** використання майстра налаштовується ім'я сеансу та режим роботи.

Сеанси можуть бути налаштовані як для User або Custom:

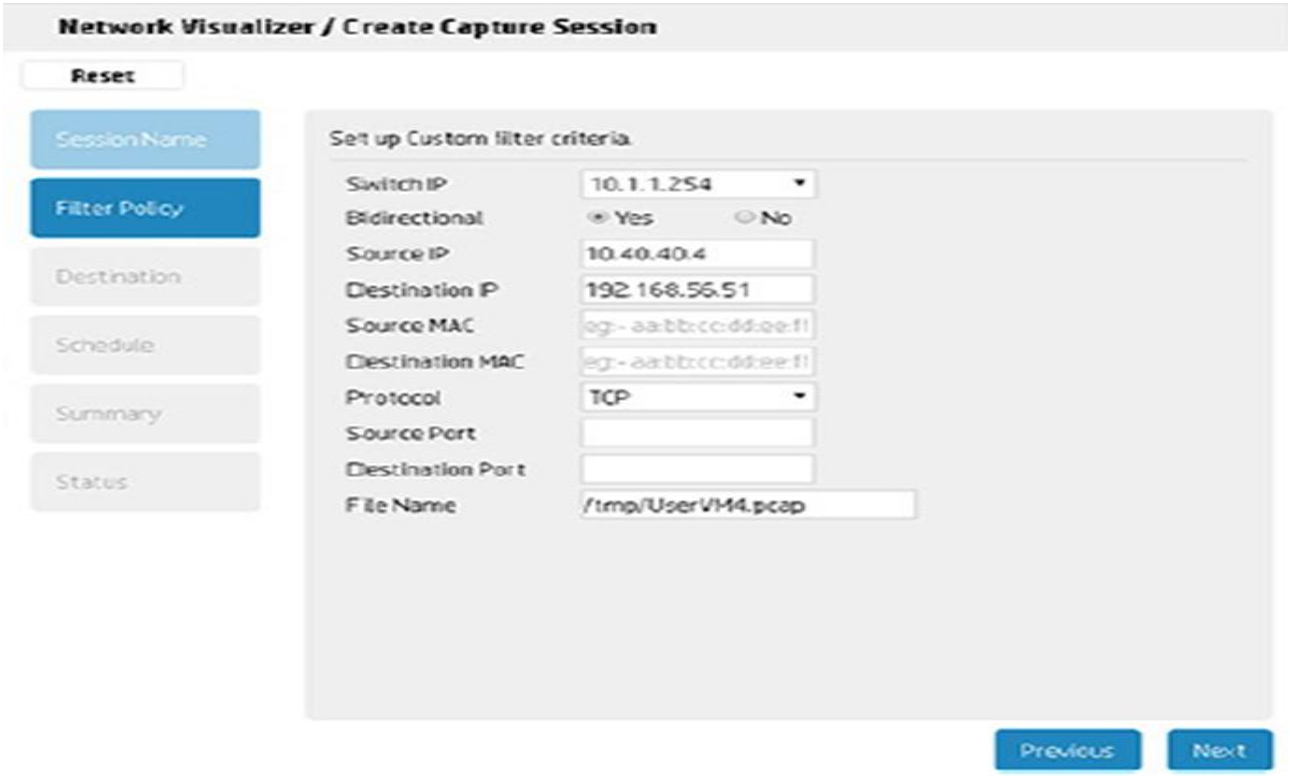
- User: Ви можете налаштувати користувача, групу користувачів, пристрій та програму для моніторингу сеансу захоплення.
- Custom: Ви можете налаштувати IP-адресу джерела/призначення, MAC-адресу джерела/призначення, порт і протокол для моніторингу сеансу захоплення.



19. На **другому кроці** здійснюється налаштування Filter Policy. Встановіть наступні значення, як показано на малюнку:

- Switch IP: 10.1.1.254
- Bidirectional: Yes
- Source IP: 10.40.40.4
- Destination IP: 192.168.56.51
- Protocol: TCP

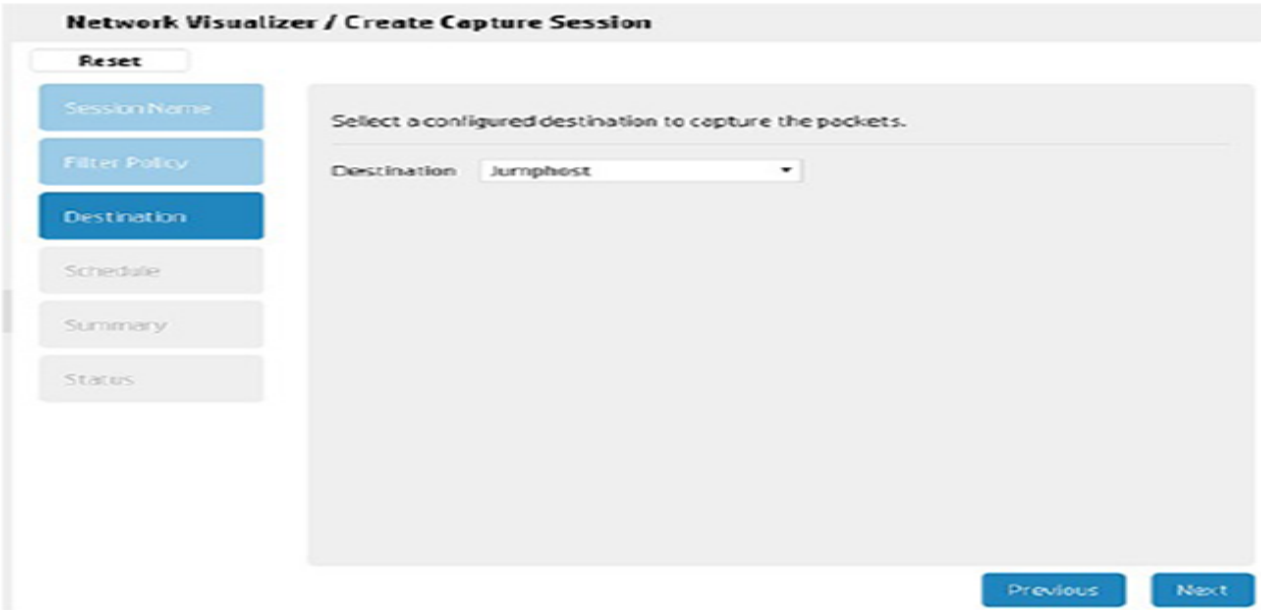
Залиште інші параметри та значення за замовчуванням без змін та клікніть Next:



Інформація Filter Policy:

- Switch IP: IP-адреса мережного пристрою
- Bidirectional: Виберіть напрямок захоплення трафіку, натиснувши одне з наступного:
- Yes – Захоплює пакети, надіслані та отримані користувачем
- No – Захоплює пакети, надіслані користувачем
- Source IP: IP-адреса джерела передачі (for example, 10.40.40.4)
- Destination IP: IP-адреса адресата призначення (for example, 192.168.56.51)
- Source MAC: MAC-адреса джерела передачі (for example, aa:bb:cc:dd:ee:ff)
- Destination MAC: MAC-адреса адресата призначення (for example, aa:bb:cc:dd:ee:ff)
- Protocol: Мережевий протокол; по замовчуванню, визначено All
- Source Port: Layer 4 port for the source
- Destination Port: Layer 4 port for the destination
- File Name: Ім’я файлу pcap для збереження пакетів

20. **Третім кроком** майстра є Destination. Визначте Jumphost і клікніть Next (see Figure):



21. **Четвертим кроком** є Schedule. Не встановлюйте графік захоплення (No Selection) і клікніть Next (see Figure):

Schedule options:

- No Selection: Моніторинг сеансу захоплення не запланований.
- Once: Моніторинг сеансу захоплення один раз. Визначено Start Time та Stop Time.
- Everyday: Моніторинг сеанс захоплення без обмежень дня. Вкажіть інтервал повтору - Repeat every (days), Start Time, Stop Time та End Date.

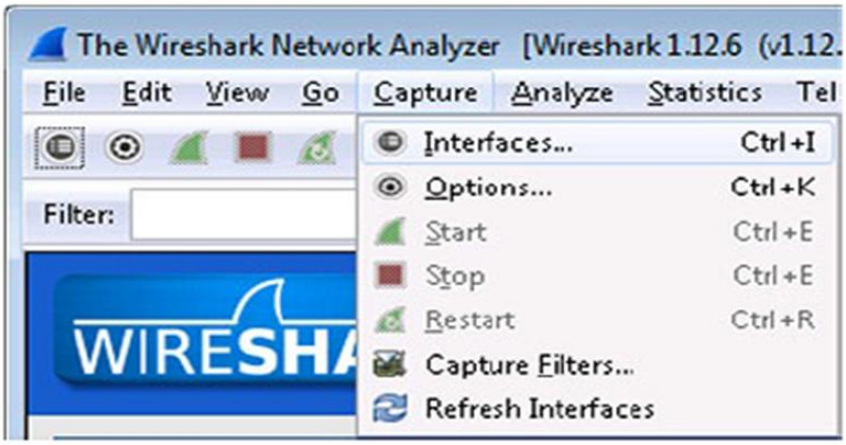
- Weekday (Monday to Friday): Моніторинг сеансу захоплення в будні дні. Вкажіть Start Time, Stop Time та End Date.
- Weekend (Saturday and Sunday): Моніторинг сеансу захоплення у вихідні. Specify the Start Time, Stop Time та End Date.
- Weekly: Моніторинг сеансу захоплення щотижня. Виберіть дні тижня для сеансів захоплення за допомогою Repeat on check boxes. Вкажіть Start Time, Stop Time та End Date.

22. **Зведений підсумок** вибраних параметрів. Перегляньте зведену інформацію та натисніть кнопку Finish (дивись малюнок):

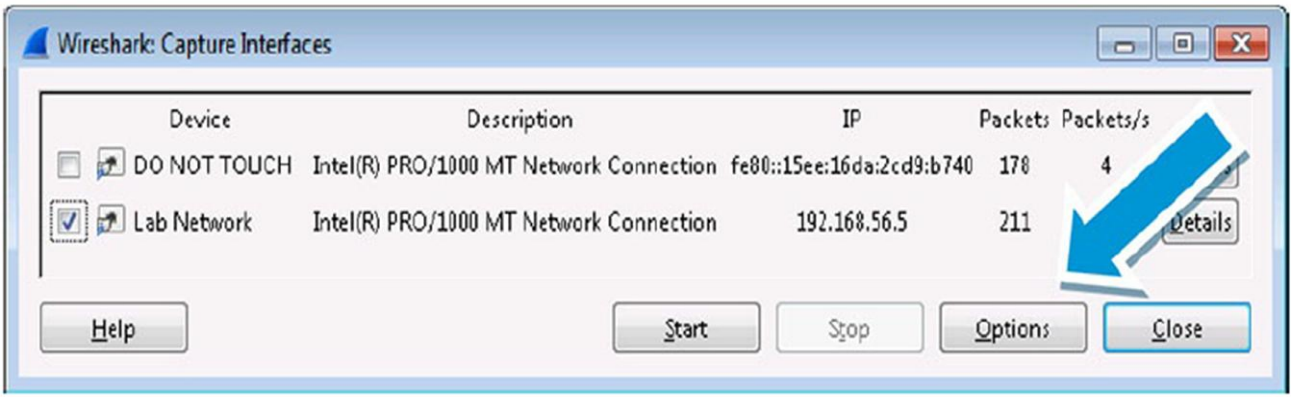
4.4.1 Активація сеансу

1. Перед активацією сеансу, запустіть Wireshark.

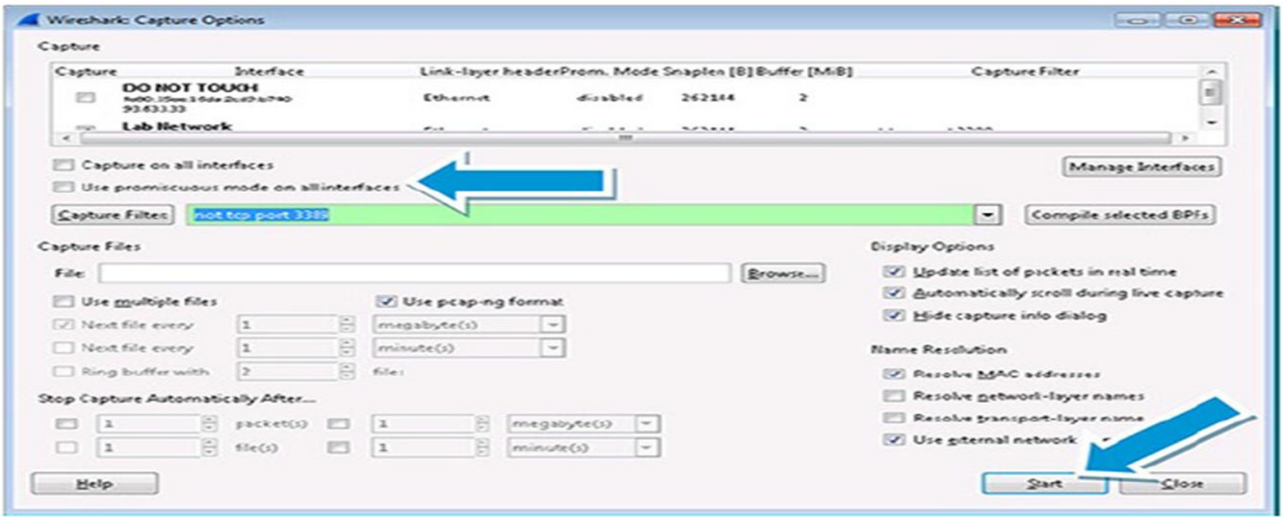
2. Клікніть *Capture* і потім *Interfaces*



3. Виберіть необхідну мережу, у цьому прикладі, *Lab Network*, та клікніть *Options.*

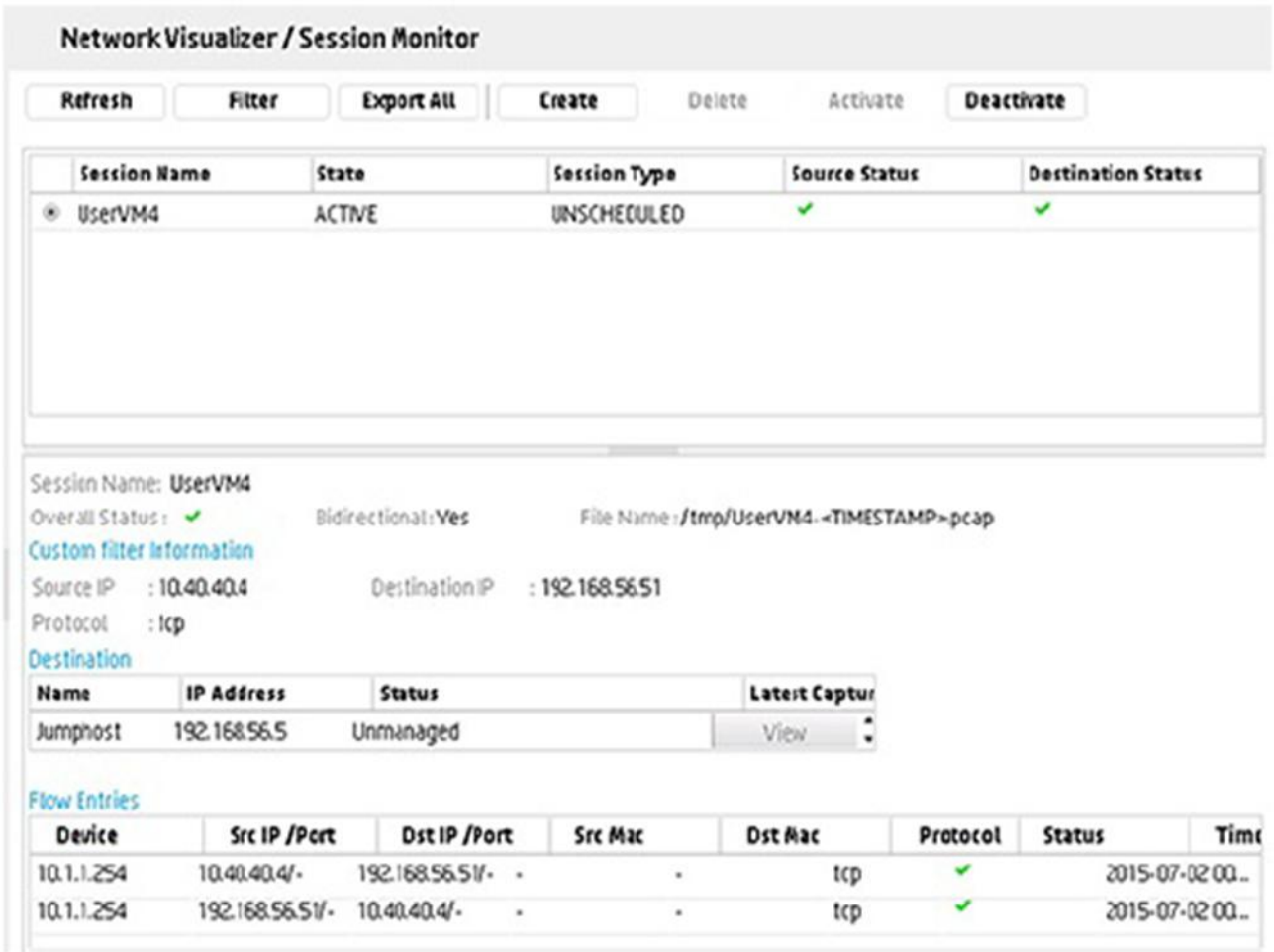


4. Скасуйте вибір *Use promiscuous mode on all interfaces* та клікніть *Start*. Змішаний режим не потрібен, оскільки трафік буде переадресовано безпосередньо на ПК за допомогою тунелю GRE:

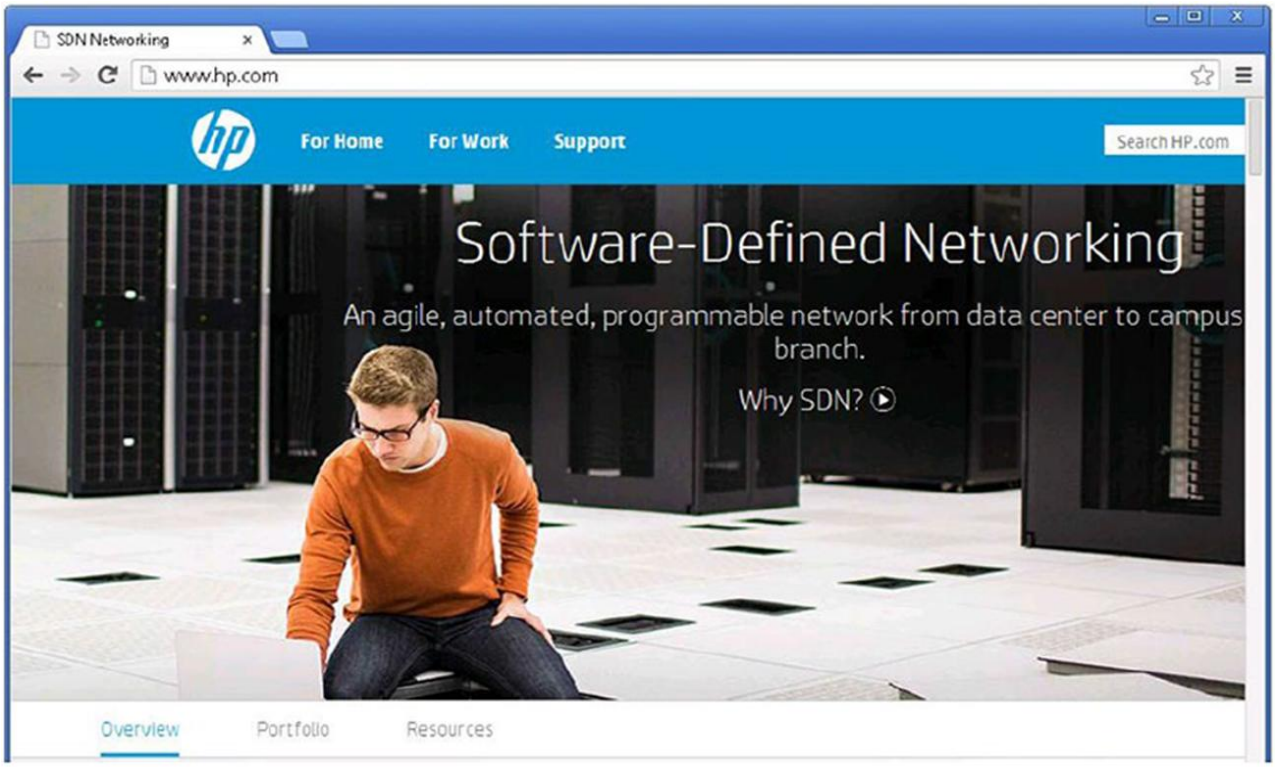


5. На Network Visualizer клікніть *Activate* для запуску сеансу

6. Session Monitor відображає інформацію про захоплення



7. На UserVM4 (10.40.40.4), перейдіть до hp.com



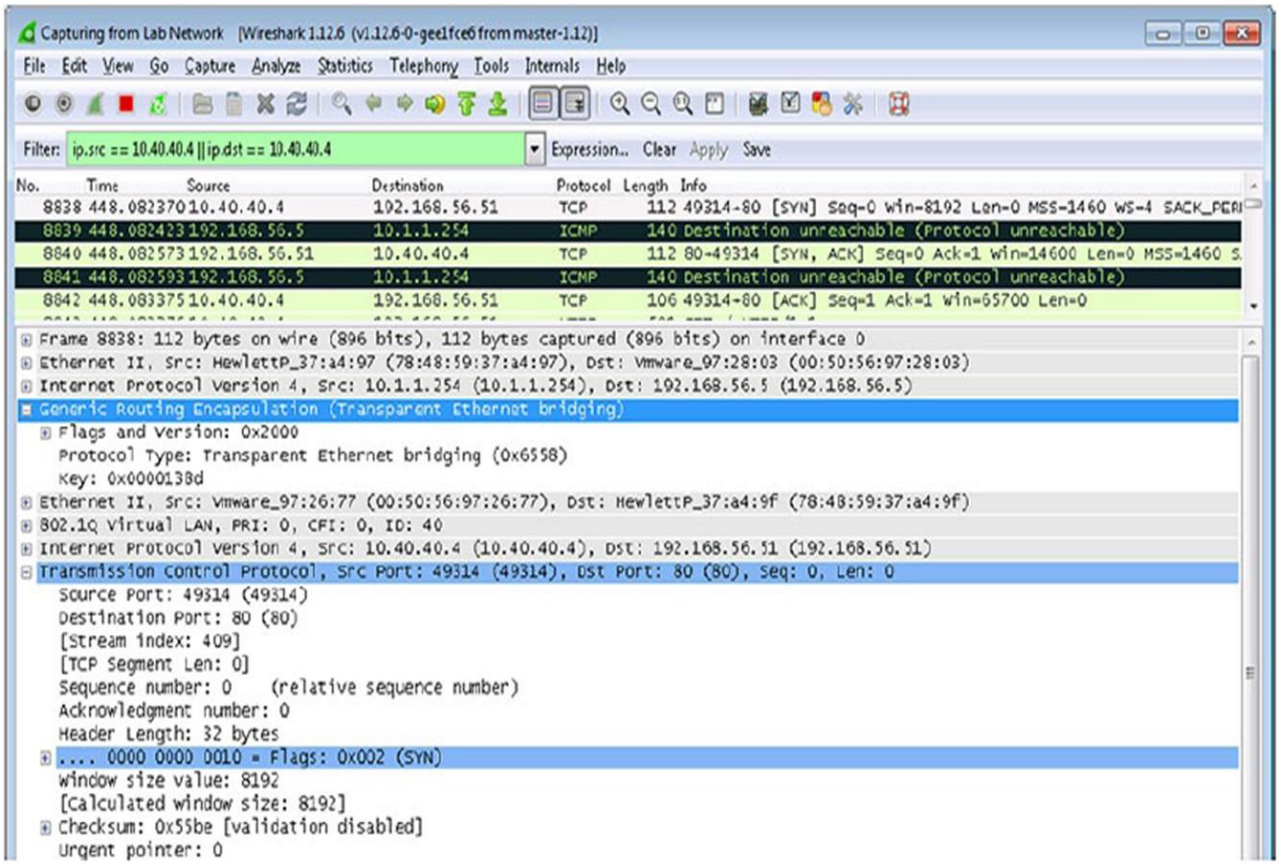
8. Wireshark збирає велику кількість даних, тому застосуйте наступний фільтр:

```
ip.src == 10.40.40.4 || ip.dst == 10.40.40.4 and click Apply:
```

Ви можете скористатись наступним більш коротким фільтром Wireshark:

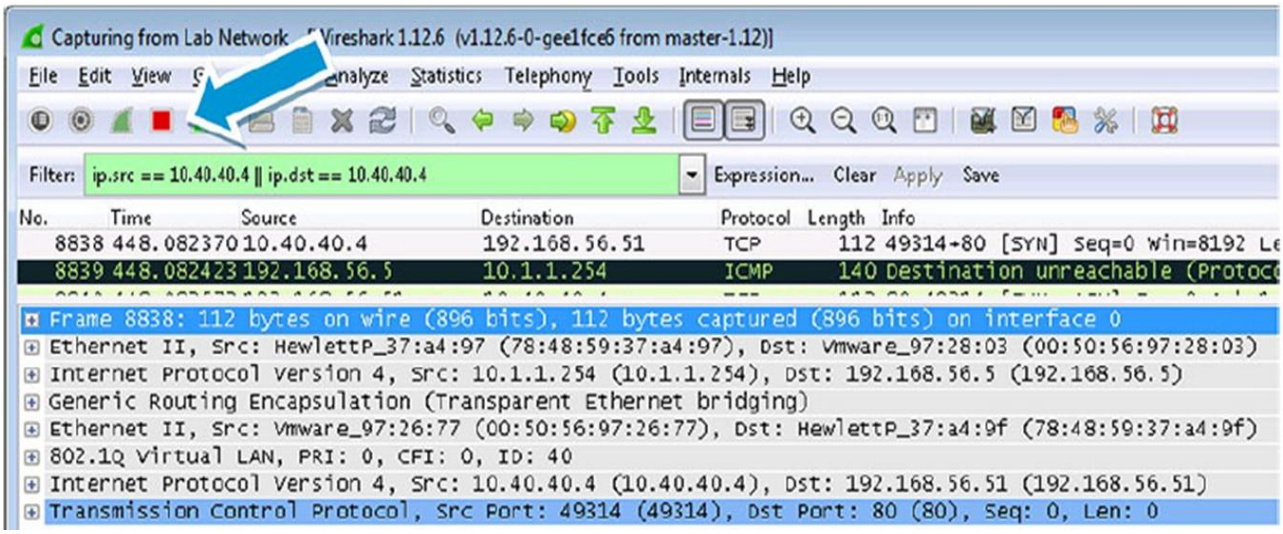
```
ip.addr == 10.40.40.4
```

Обидва варіанти призведуть до показу трафіку до або від 10.40.40.4.



9. Якщо трафік не отримано, переконайтеся, що шлюз за замовчуванням 192.168.56.251 налаштований на Jumphost. Ви також можете змінити фільтр Wireshark на GRE, щоб перевірити, чи приймаються тунельні пакети GRE.

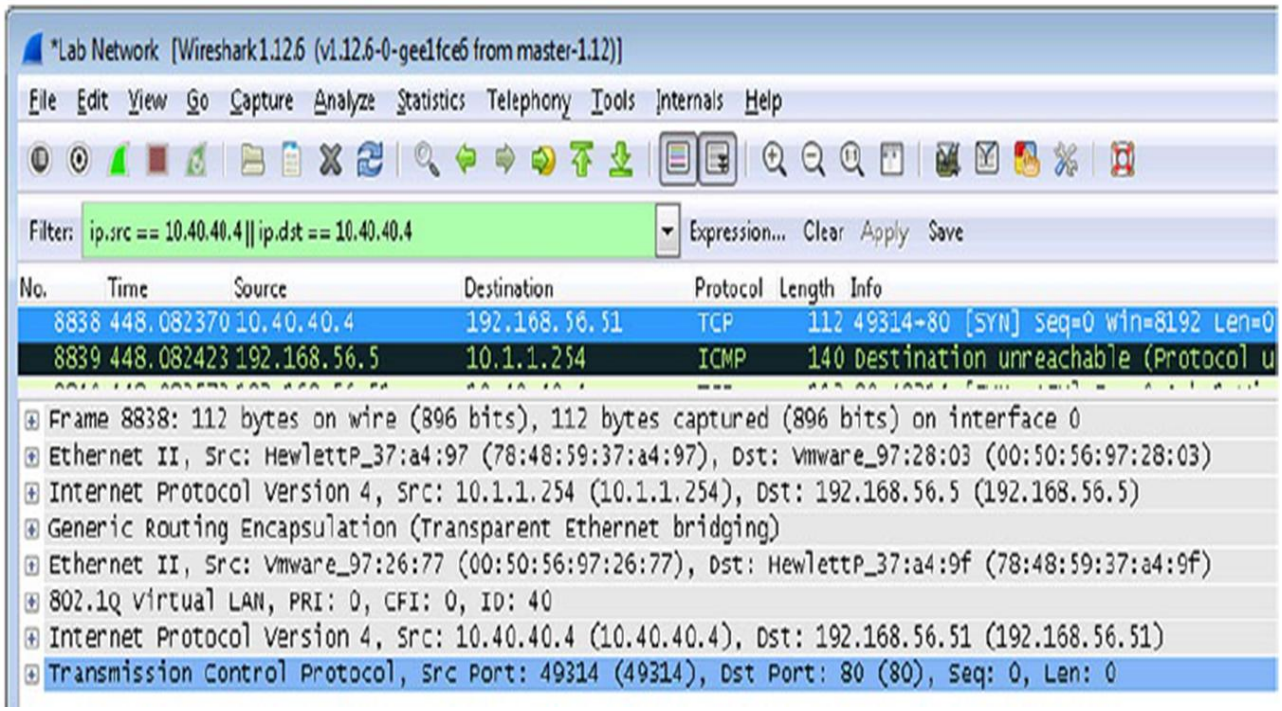
10. Зупиніть захоплення Wireshark



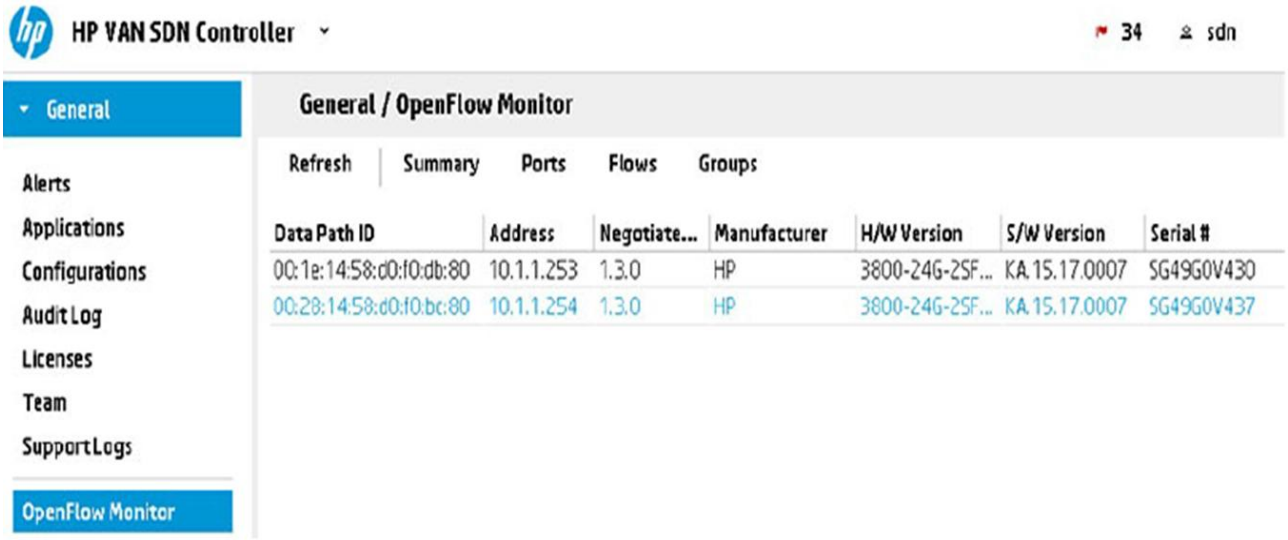
11. Перегляд деталей захопленого пакета:

- Layer 2: Ethernet фрейм із вихідною MAC-адресою комутатора HP та адресатом призначення віртуальної машини VMware (Jumphost)
- Layer 3: IP адреса джерела передачі 10.1.1.254 (ProVision P2) та IP адреса призначення 192.168.56.5 (Jumphost)
- Layer 4: GRE tunnel

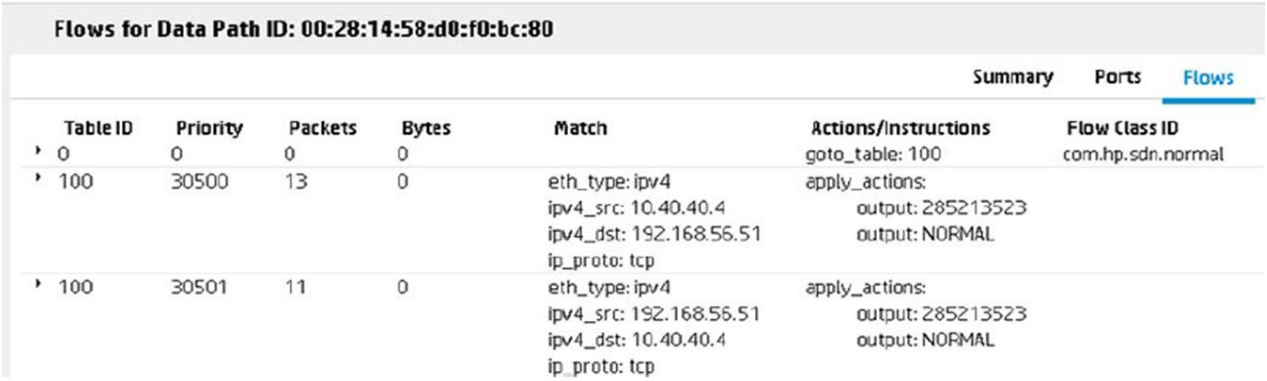
- Encapsulated Layer 2: Source MAC address of VMware host (UserVM4) and destination MAC address of an HP switch (Comware switch C1)
- Encapsulated 802.1Q VLAN information
- Encapsulated Layer 3: Source IP address of 10.40.40.4 (UserVM4) and destination IP address of 192.168.56.51 (hp.com test website)
- Encapsulated Layer 4: TCP destination port 80



12. На графічному інтерфейсі HP Controller GUI, клікніть General, а потім OpenFlow Monitor. Виберіть ProVision Switch 2 (10.1.1.254).



13. Клікніть Flows для перегляду таблиці потоку комутатора.



Flows for Data Path ID: 00:28:14:58:d0:f0:bc:80

Summary | Ports | Flows

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	30500	13	0	eth_type: ipv4 ipv4_src: 10.40.40.4 ipv4_dst: 192.168.56.51 ip_proto: tcp	apply_actions: output: 285213523 output: NORMAL	
100	30501	11	0	eth_type: ipv4 ipv4_src: 192.168.56.51 ipv4_dst: 10.40.40.4 ip_proto: tcp	apply_actions: output: 285213523 output: NORMAL	

Result: Потокові записи додані програмою Network Visualizer. Потоки спрямовують трафік до service insertion tunnel. Було додано два потокові записи, оскільки обрана двонаправленість.

This can also be seen on the console of the switch:

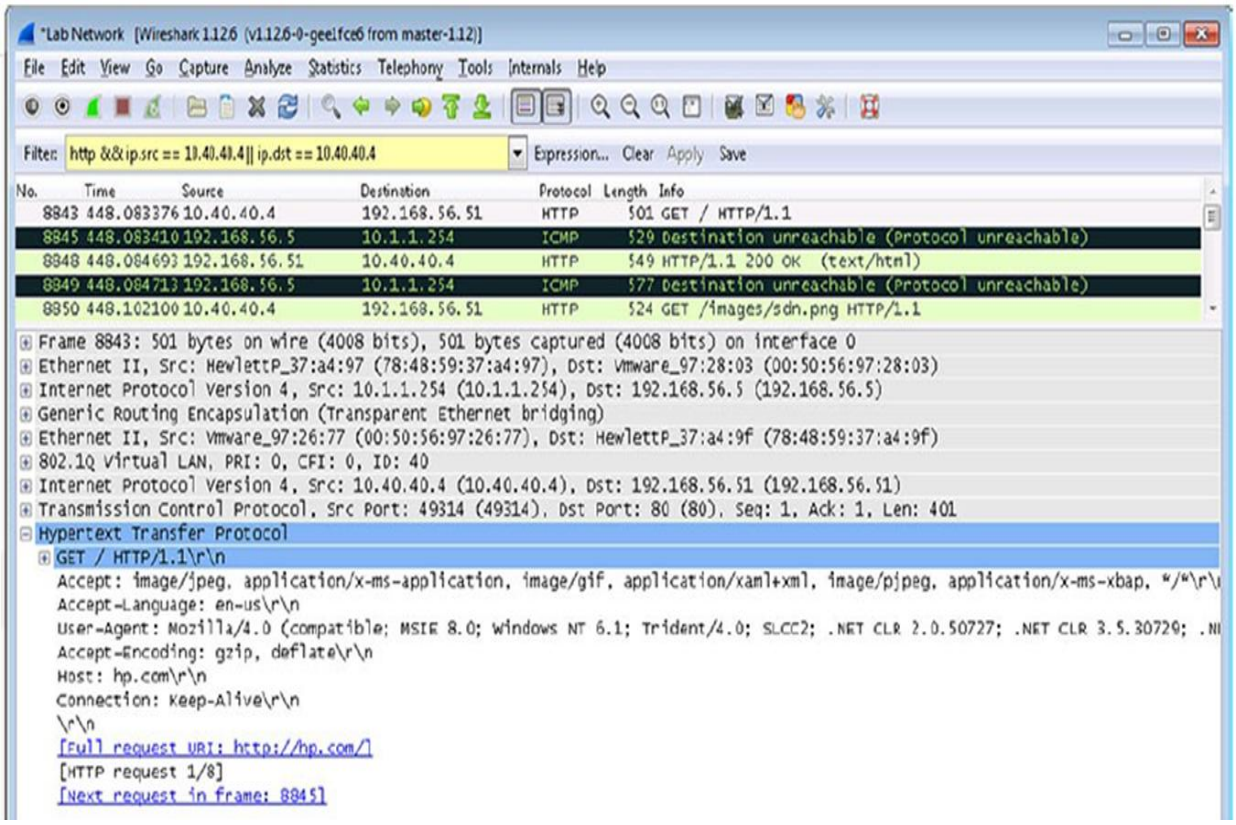
```
P2# show openflow instance vlan40 flows
Flow 2
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : 10.40.40.4/32
 Destination IP Address : 192.168.56.51/32
 IP Protocol : TCP
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30500 Duration : 1420 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 13
 Flow Table ID : 100 Controller ID : 3
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
 Output : ServiceTunnel18
 Normal
```

```
Flow 3
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : 192.168.56.51/32
 Destination IP Address : 10.40.40.4/32
 IP Protocol : TCP
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30501 Duration : 1420 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 11
 Flow Table ID : 100 Controller ID : 3
```

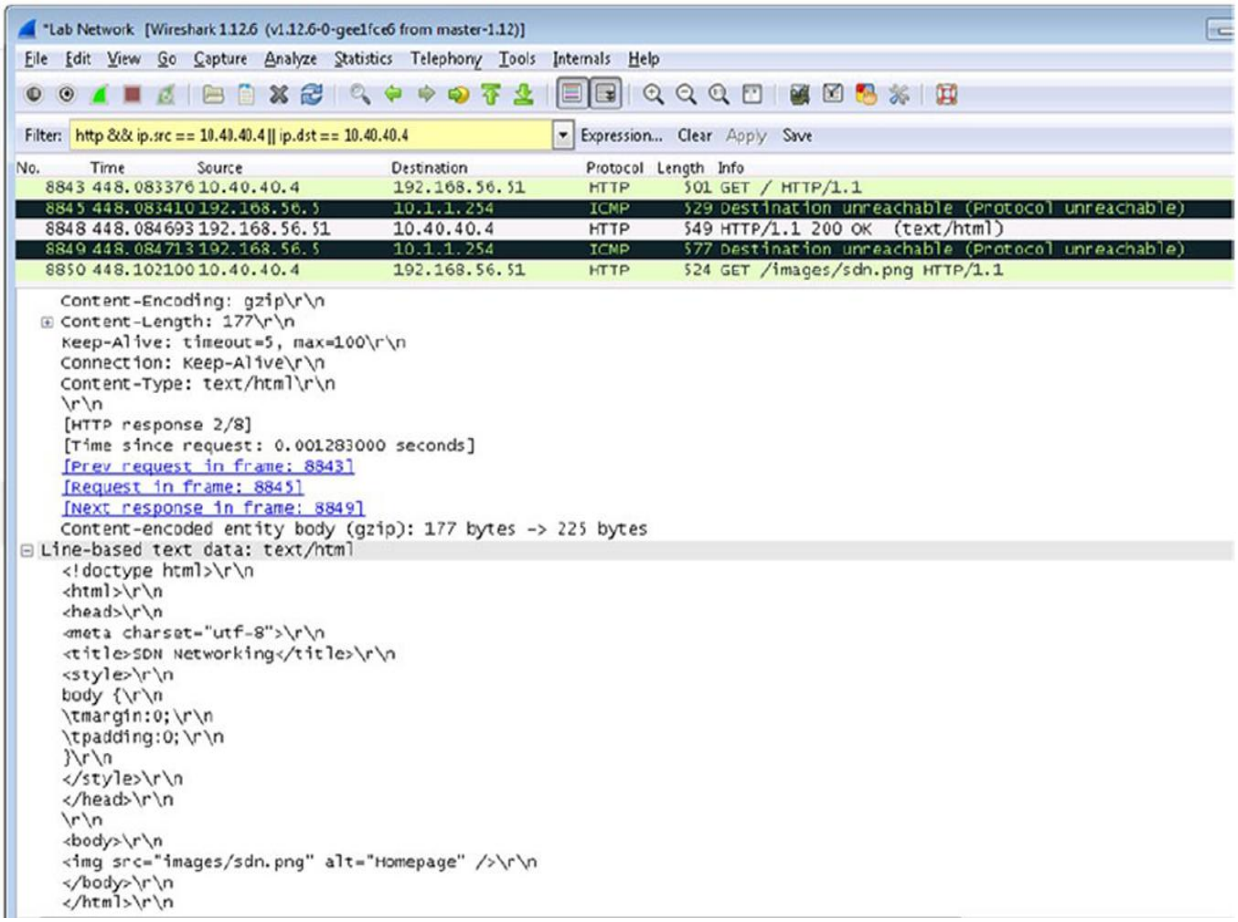
```
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
 Output : ServiceTunnel18
 Normal
```

14. У Wireshark додайте http && до фільтра, щоб переглянути лише HTTP-пакети. На малюнку нижче показано пакет HTTP GET.

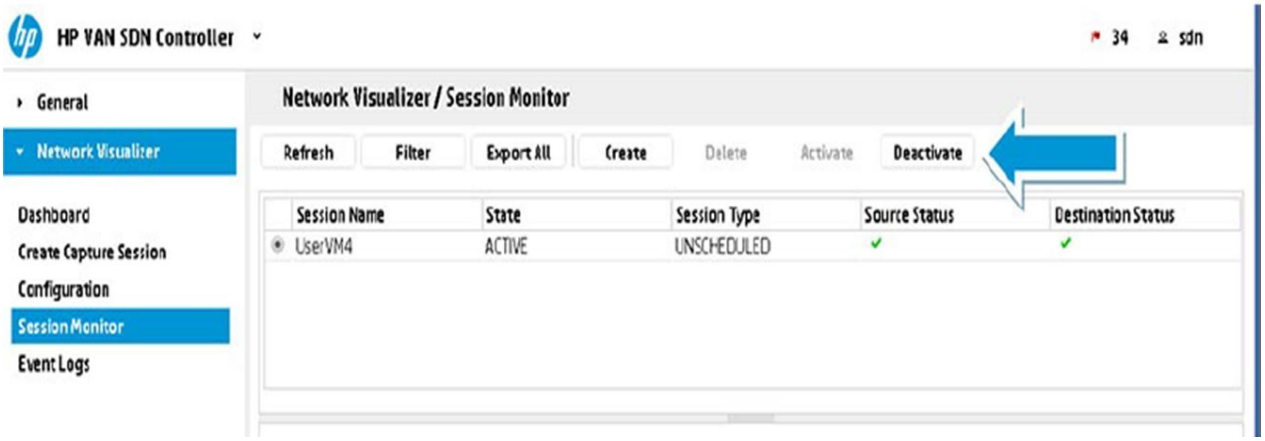
Filter: http && ip.src == 10.40.40.4 || ip.dst == 10.40.40.4



На малюнку нижче показано HTML з сервера.

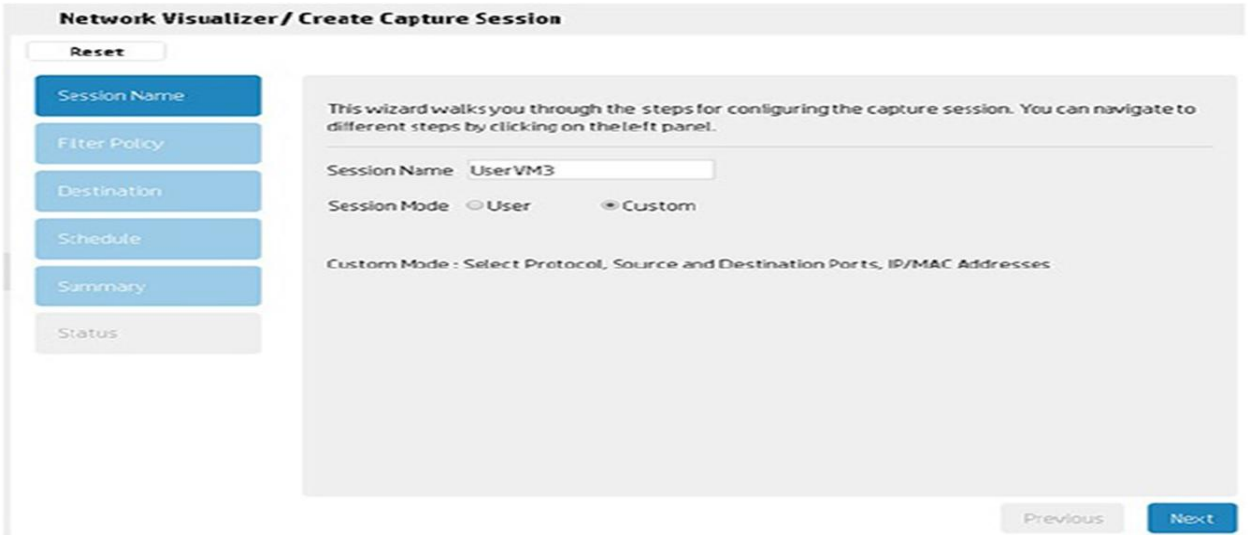


15. У Network Visualizer дезактивуйте сеанс UserVM4, натиснувши Deactivate.



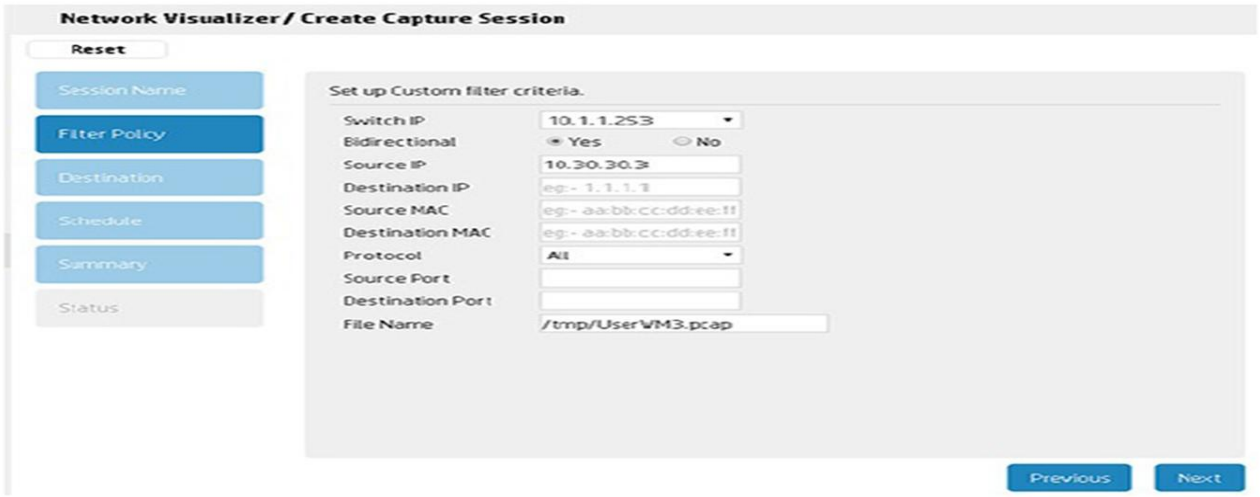
16. Встановіть новий сеанс захоплення клікнувши Create Capture Session. Додайте Session Name для UserVM3.

17. Виберіть на Session Mode режим Custom та клікніть Next.

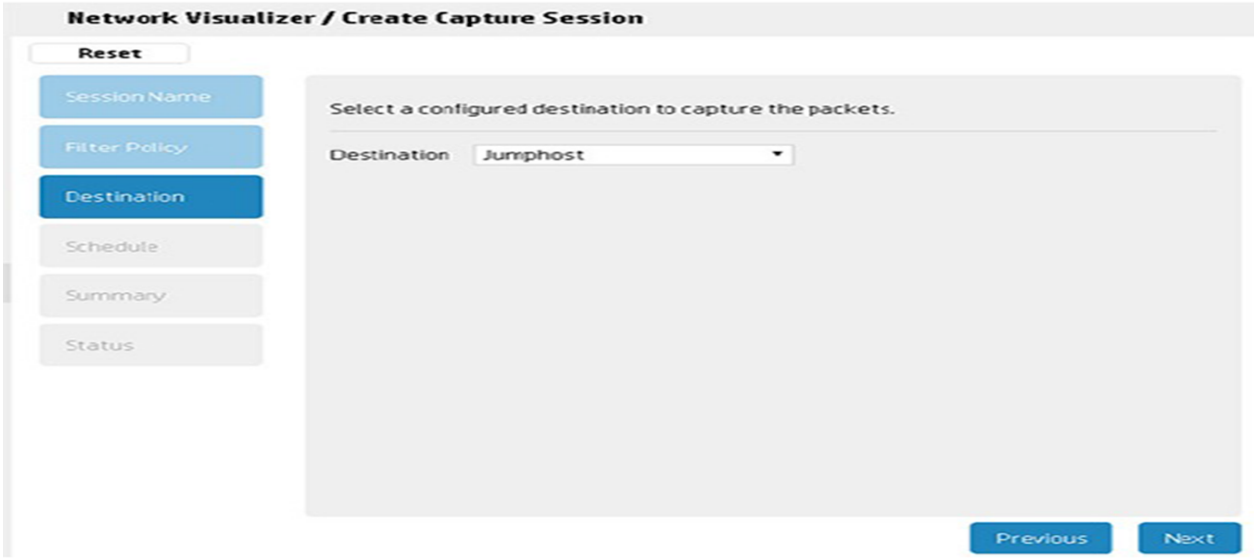


18. Створіть Filter Policy з наступними значеннями:

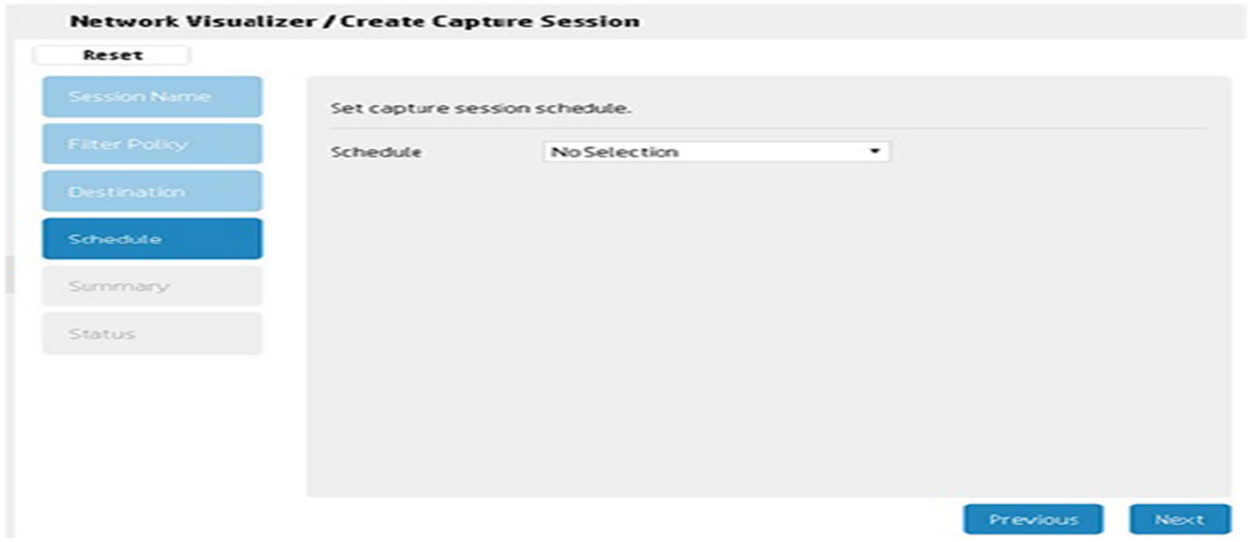
- Switch IP: 10.1.1.253
- Bidirectional: Yes
- Source IP: 10.30.30.3
- Leave other options and default values and click Next:



19. Для Destination, виберіть Jumphost та клікніть Next.



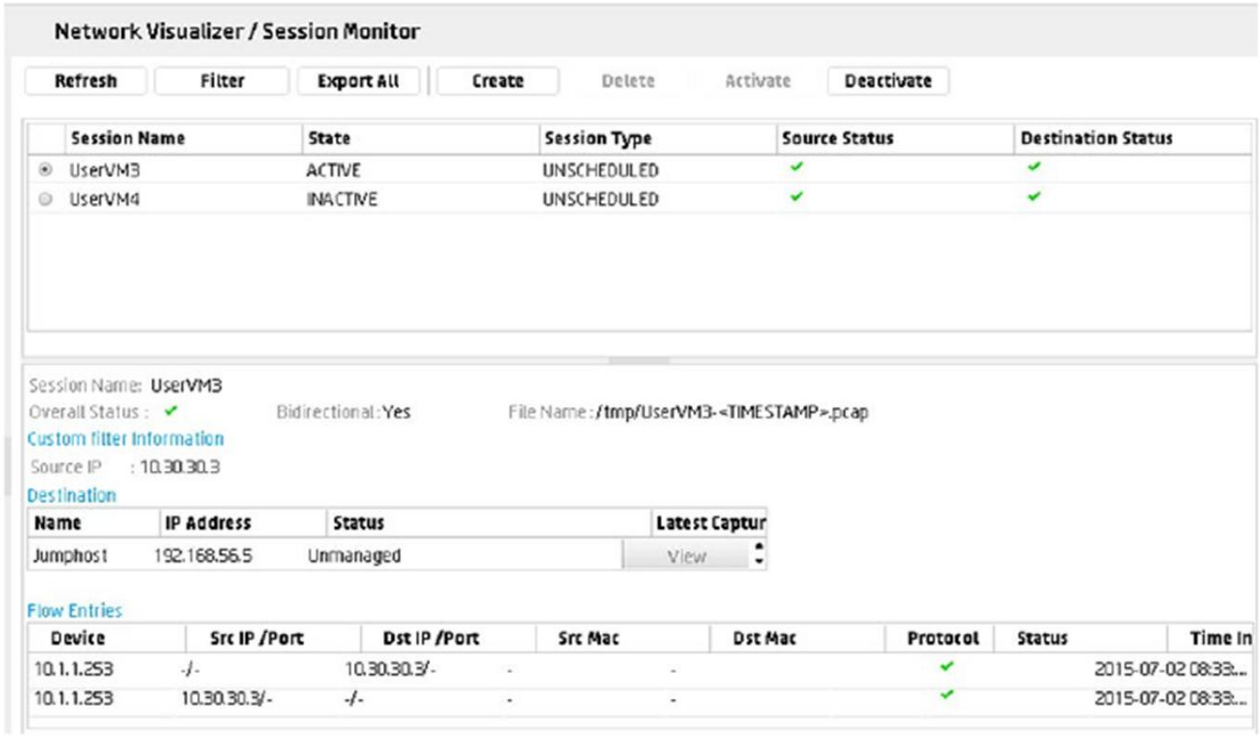
20. Не встановлюйте графік захоплення (No Selection) і натисніть кнопку Next.



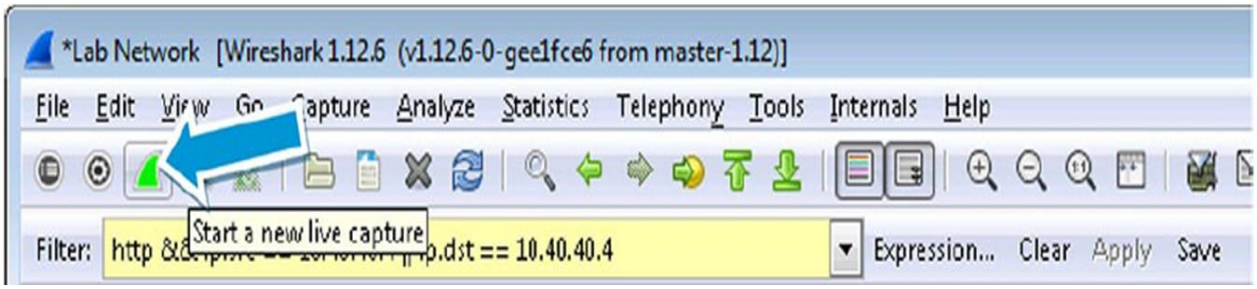
21. Перегляньте зведену інформацію та натисніть кнопку Finish.

22. Клікніть Activate щоб розпочати сеанс.

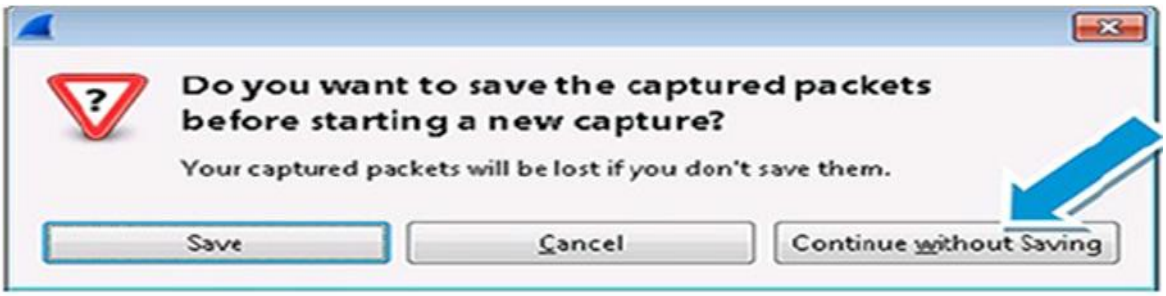
23. Session Monitor відображає інформацію про захоплення, як показано на малюнку:



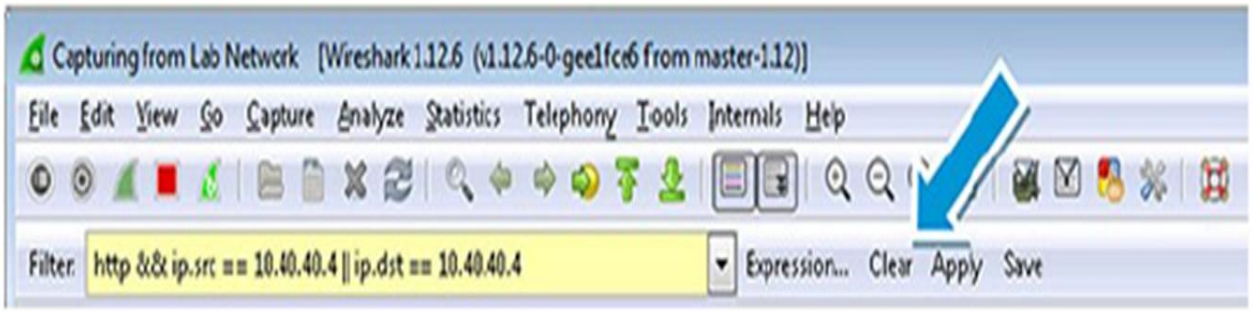
24. Запустіть нове захоплення Wireshark



25. Клікніть Continue without Saving



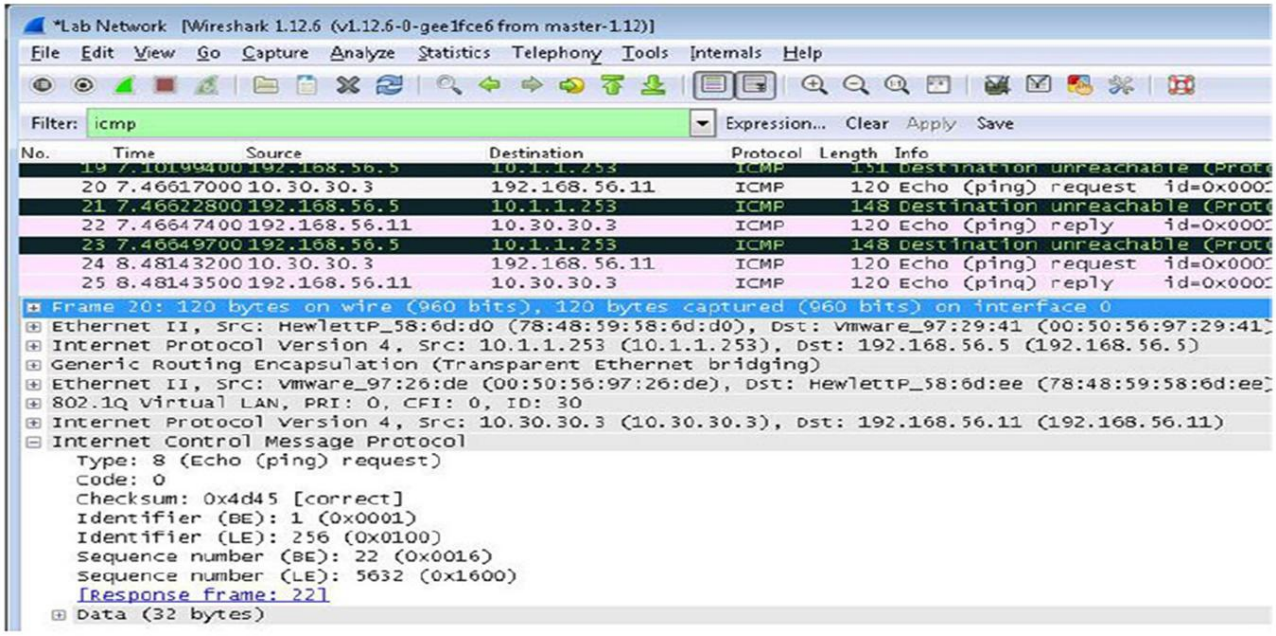
26. Очистіть фільтр Wireshark



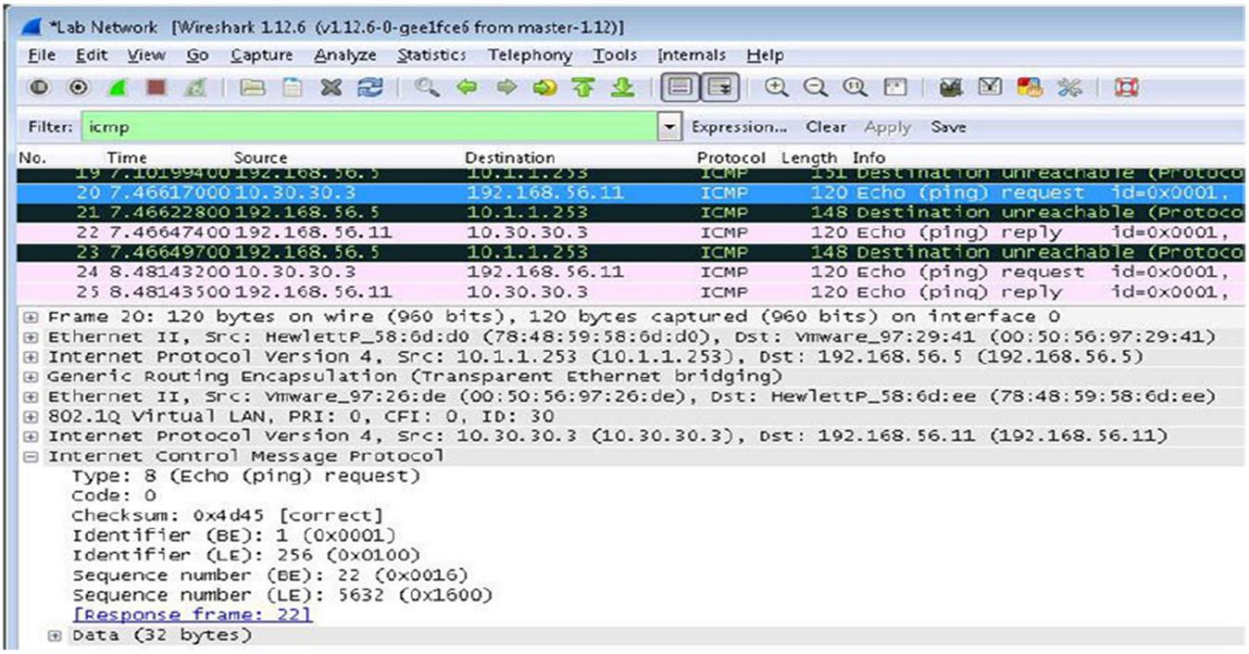
27. На UserVM3 (10.30.30.3), пінгуйте 192.168.56.11:

```
C:\Users\Student>ping 192.168.56.11

Pinging 192.168.56.11 with 32 bytes of data:

Reply from 192.168.56.11: bytes=32 time<1ms TTL=63

Reply from 192.168.56.11: bytes=32 time<1ms TTL=63

Reply from 192.168.56.11: bytes=32 time<1ms TTL=63

Reply from 192.168.56.11: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.56.11:

 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Student>
```

28. Stop заплення Wireshark:
29. Застосувати наступний фільтр: icmp



30. Знайдіть ICMP message з 10.30.30.3 на 192.168.56.11

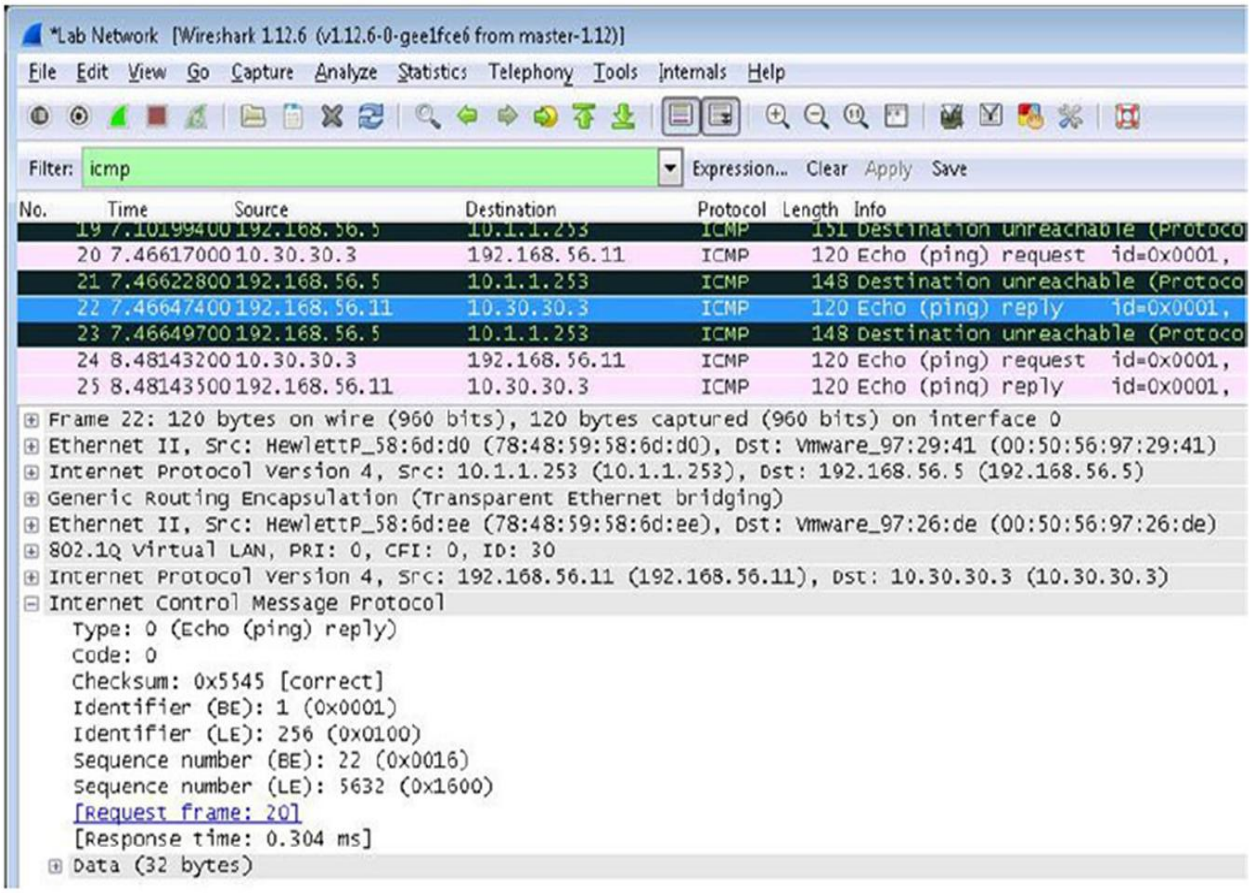


На малюнку вище можна побачити таке:

- Layer 2: Ethernet Frame with source MAC address of an HP switch and the destination a Vmware virtual machine (Jumphost)
- Layer 3: IP source of 10.1.1.253 (ProVision S1) and IP destination of 192.168.56.5 (Jumphost)
- Layer 4: GRE tunnel
- Encapsulated Layer 2: Source MAC address of VMware host (UserVM3) and destination MAC address of an HP switch (Comware switch 1)
- Encapsulated 802.1Q VLAN information
- Encapsulated Layer 3: Source IP address of 10.30.30.3 (UserVM4) and destination IP address of 192.168.56.11 (HP VAN SDN Controller)

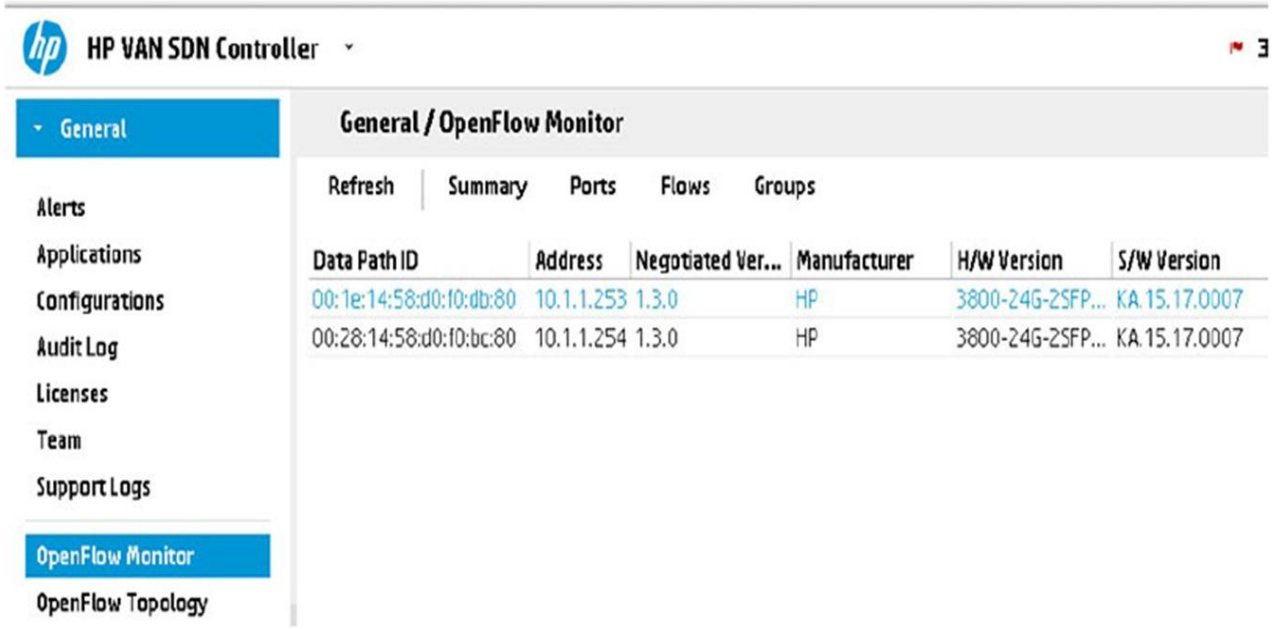
- Encapsulated Layer 4: ICMP echo request message

31. Знайдіть повідомлення *echo reply*

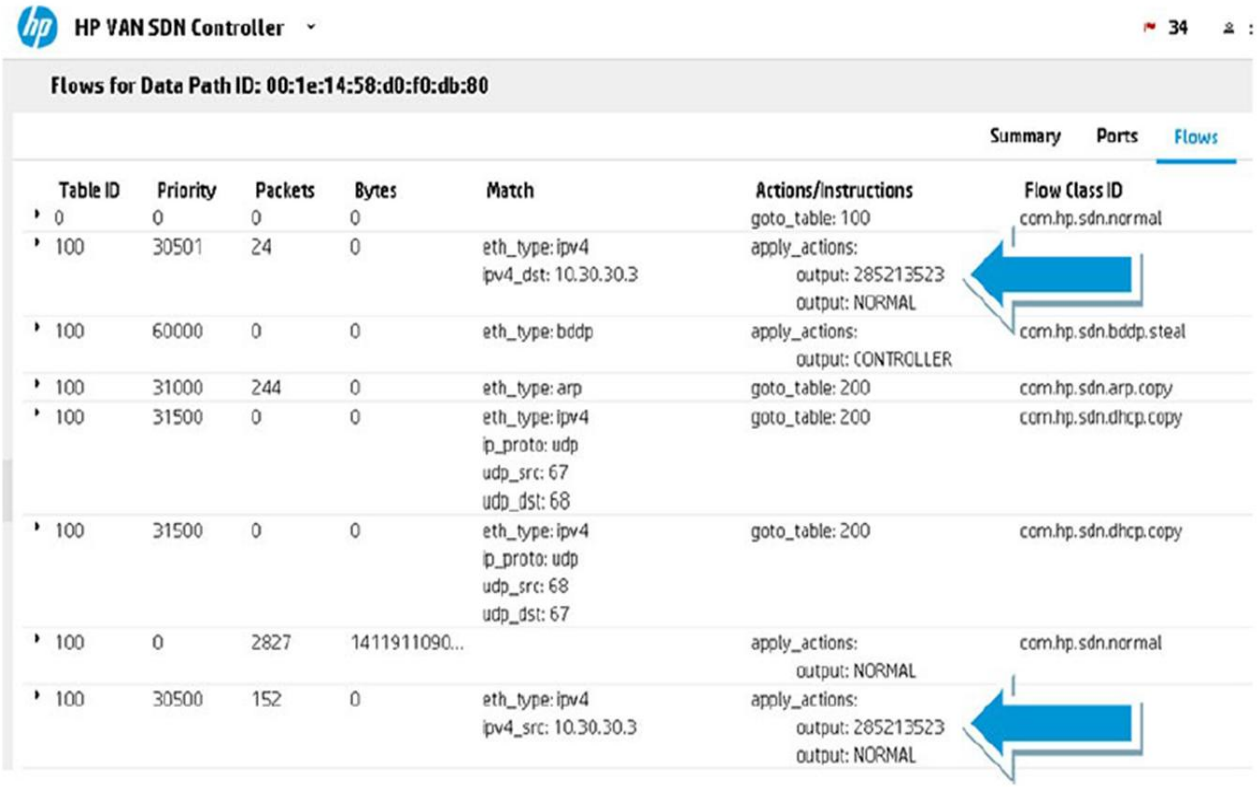


Result: Повідомлення echo reply з 192.168.56.11 на 10.30.30.3 можна побачити на малюнку вище. Пакет відображає оригінальний пакет echo reply, інкапсулізований у пакет GRE.

32. На графічному інтерфейсі HP Controller GUI, клікніть General і потім OpenFlow Monitor (дивись малюнок). Виберіть ProVision Switch 1 (10.1.1.253).



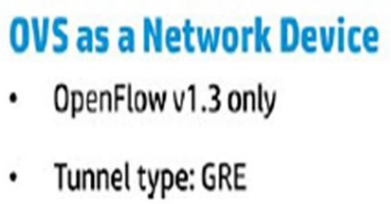
33. Клікніть Flows для перегляду таблиці потоку комутатора



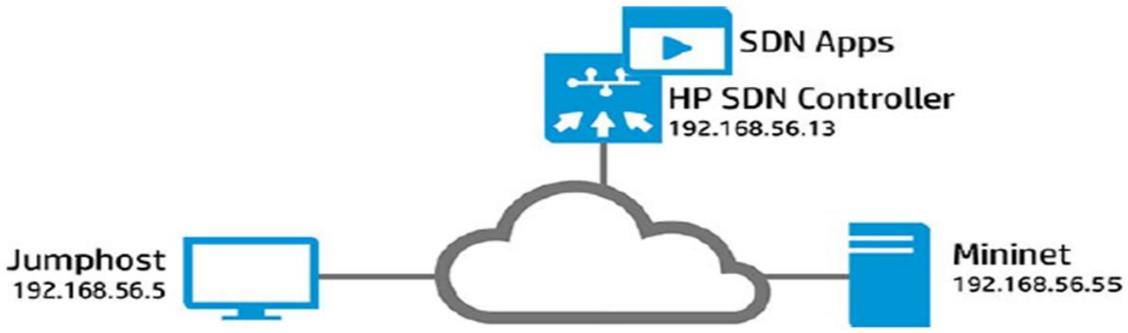
```
P1# show openflow instance vlan30 flows
Flow 2
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : Any
Destination IP Address : 10.30.30.3/32
 IP Protocol : Any
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30501 Duration : 2840 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 24
 Flow Table ID : 100 Controller ID : 3
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
 Output : ServiceTunnel18
 Normal
Flow 8
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : 10.30.30.3/32
 Destination IP Address : Any
 IP Protocol : Any
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30500 Duration : 3092 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 153
 Flow Table ID : 100 Controller ID : 3
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
Output : ServiceTunnel18
 Normal
```

4.5 Інтеграція HP Network Visualizer SDN з Open vSwitch

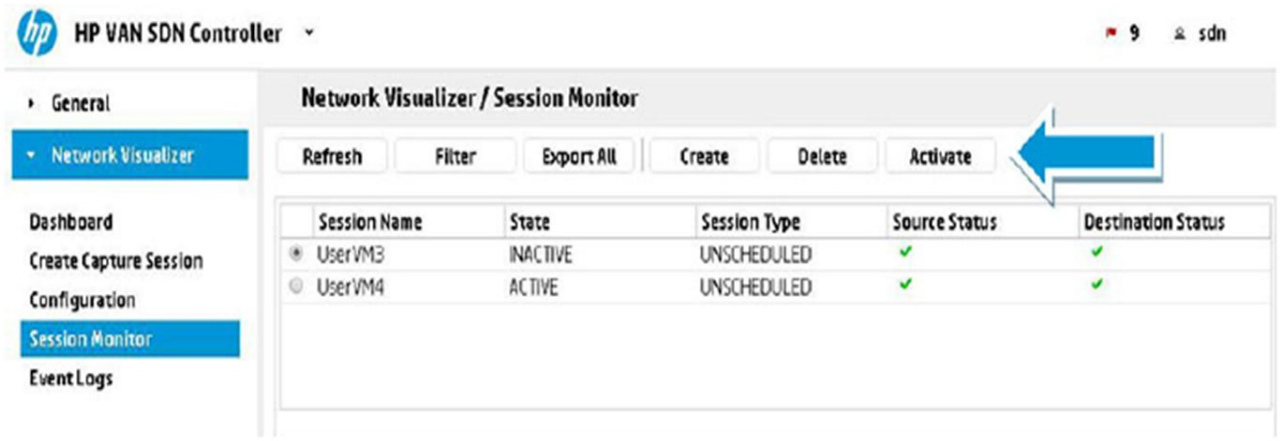
Окрім комутаторів HP, Network Visualizer підтримує Open vSwitches (дивись малюнок). Як було сказано раніше, Open vSwitch - це багаторівневий, з відкритим кодом, програмний комутатор.



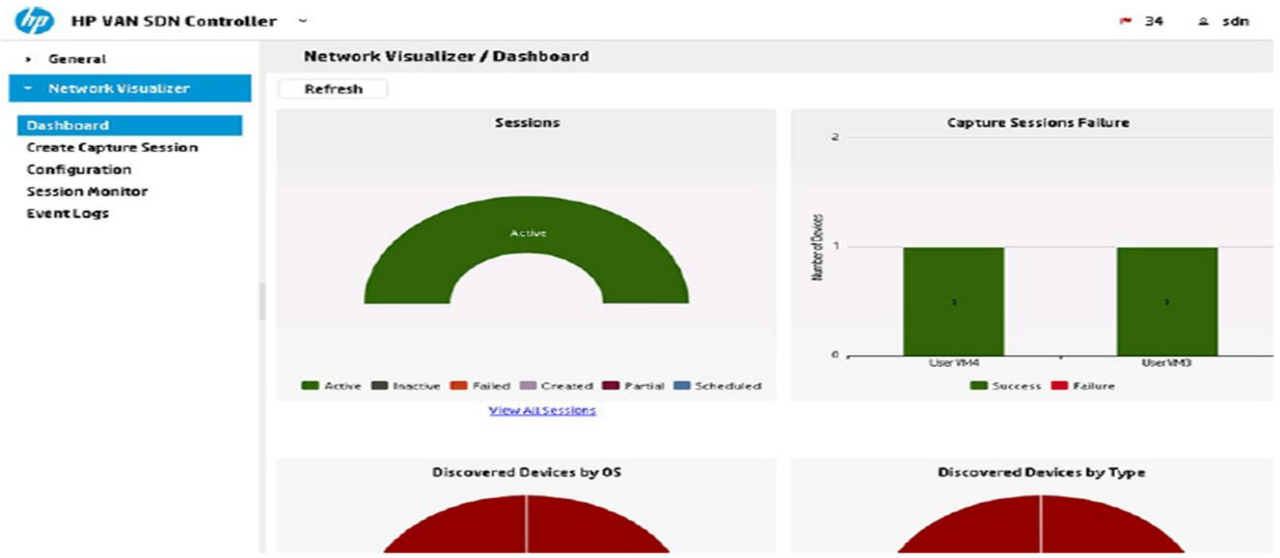
У цьому розділі наведено інструкції щодо інтеграції Network Visualizer із Open vSwitch у середовищі Mininet. Ви переглянете, як налаштувати сеанс захоплення та переадресацію захопленого трафіку на Jumphost на якому працює Wireshark. Ви також зможете переглянути потокові записи OpenFlow, створені Network Visualizer. Топологія, яка показана на малюнку, використовується для цього розділу. Ці інструкції вимагають комутаторів серії 3800.



1. На Network Visualizer, необхідно перевірити, що UserVM3 та UserVM4 сеанси активовані:

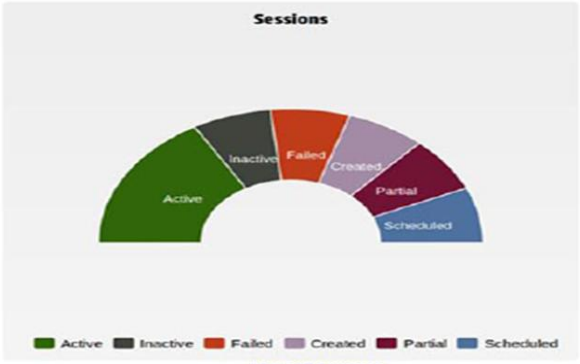


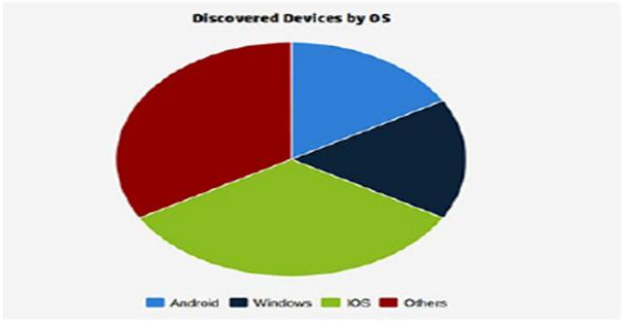
2. Клікніть Dashboard для перегляду активних сеансів та відкритих пристроїв.

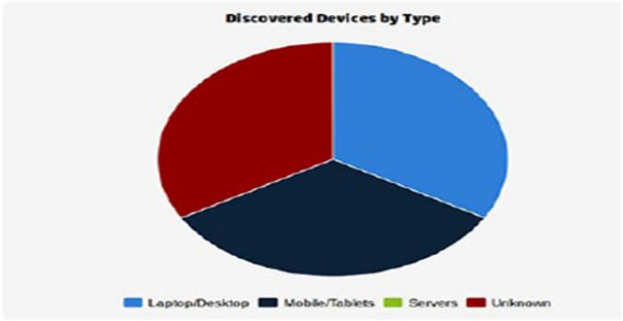


Result: На даний момент активні два сеанси (UserVM3 та UserVM4). Жодного iOS або Android пристрою не відкрито.

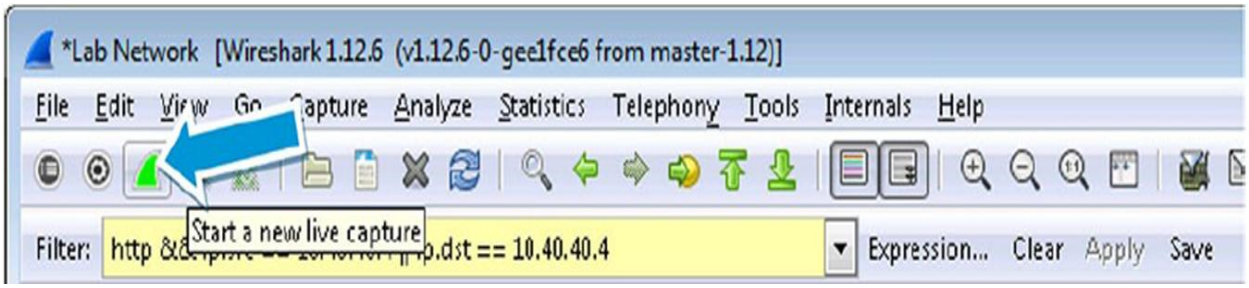
Вигляд мережі може бути таким, як показано на малюнку.



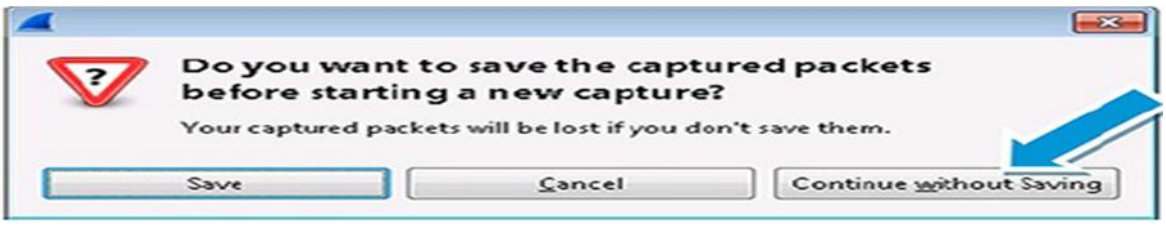




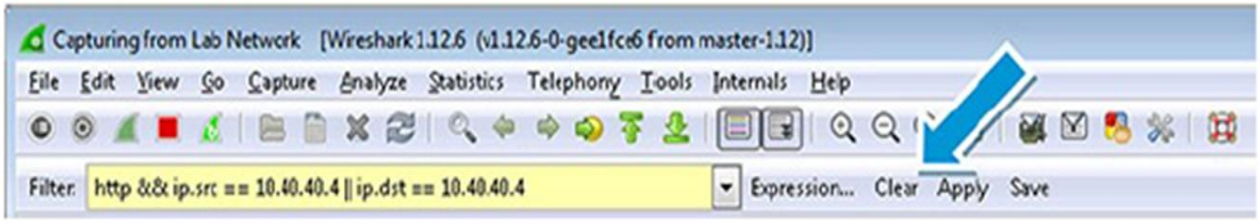
3. Запустіть захоплення Wireshark.



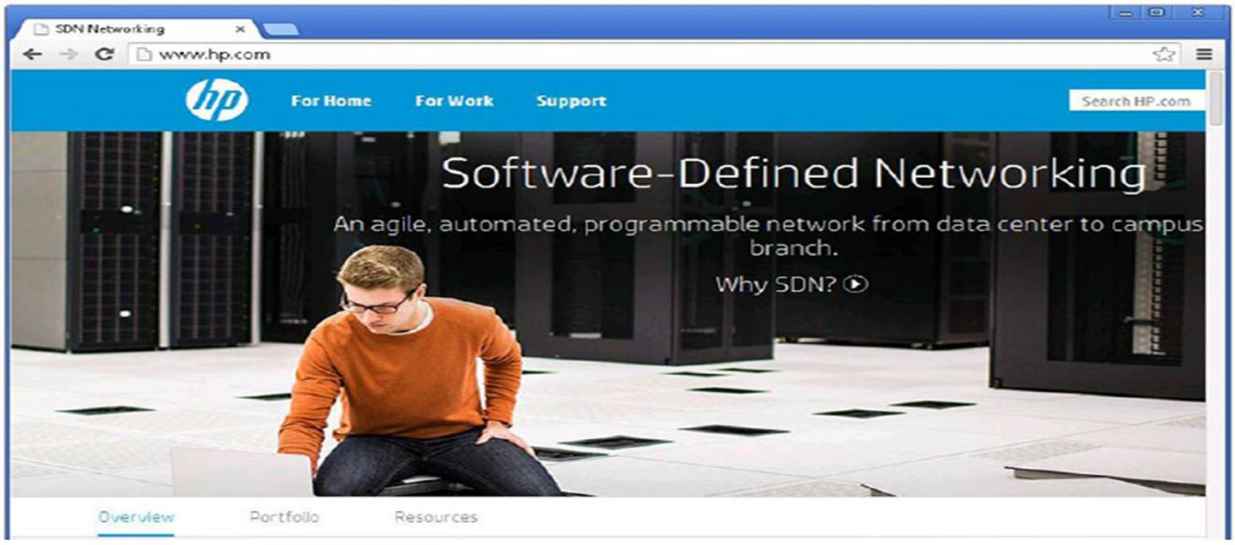
4. Клікніть *Continue without Saving*



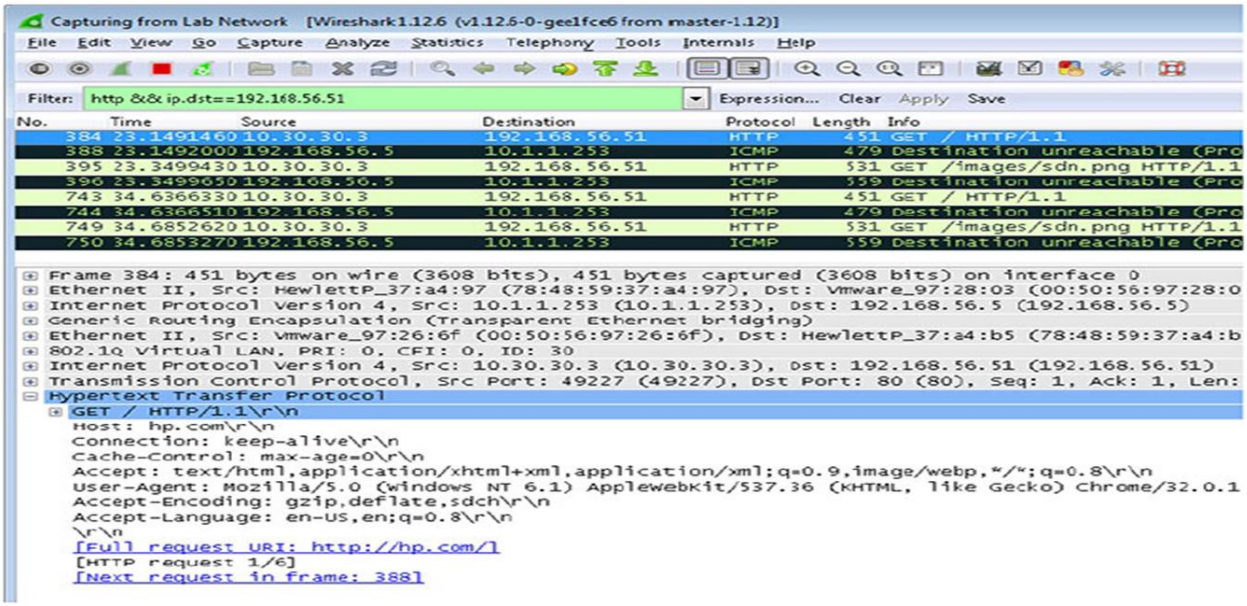
5. Очистіть фільтр Wireshark

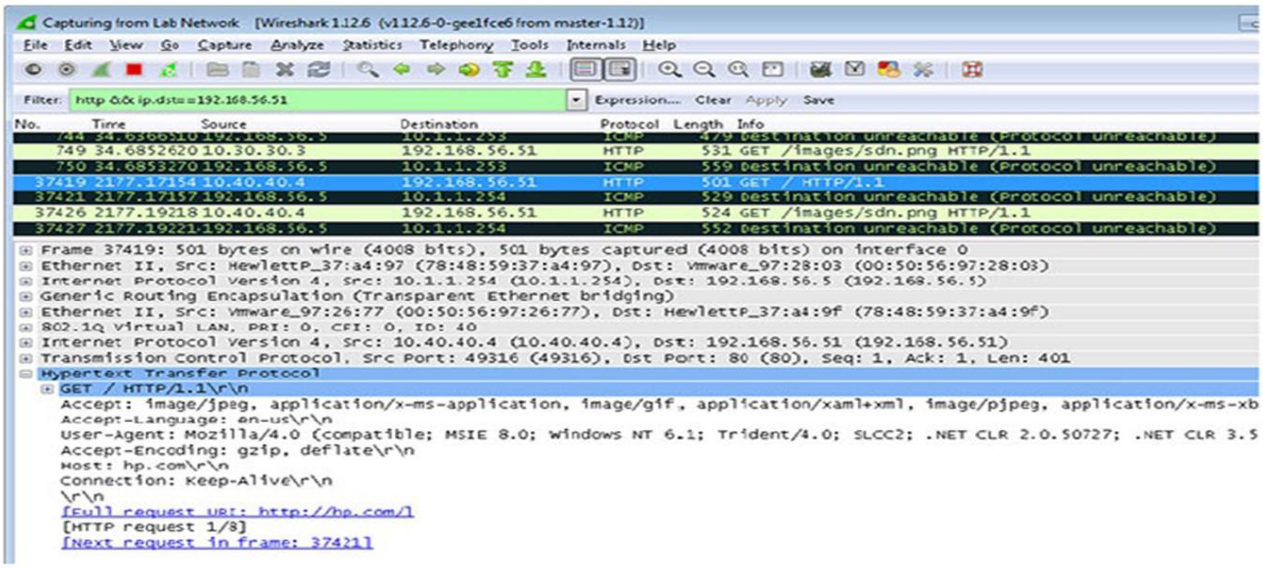


6. На UserVM3 (10.30.30.3), перейдіть до hp.com
7. На UserVM4 (10.40.40.4), перейдіть до hp.com



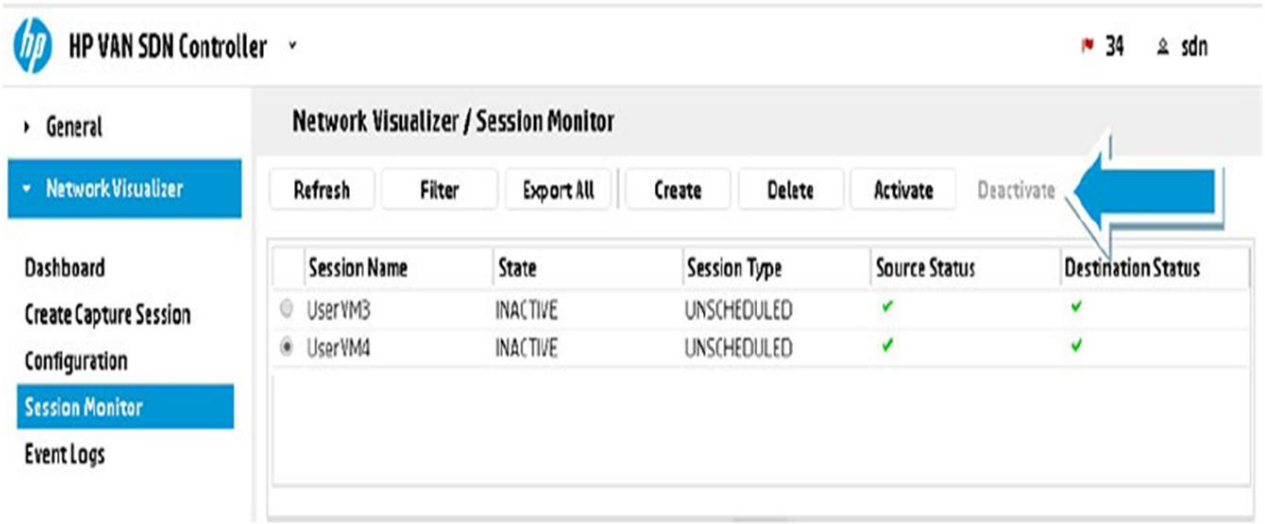
8. Змініть фільтр Wireshark на http && ip.dst==192.168.56.51.
9. Виберіть захоплений пакет з 10.30.30.3 та 10.40.40.4 (дивись малюнок).





Result: HTTP-трафік із 10.30.30.3 та 10.40.40.4 може бути захоплений одночасно. Цей трафік захоплено в різних точках мережі (комутатори ProVision P1 і P2) і пересилаються через service insertion tunnels на Windows ПК, що використовує Wireshark.

10. На Network Visualizer дезактивуйте обидва сеанси, вибравши кожен сеанс та клікнувши Deactivate (дивись малюнок).



Висновки.

У цьому розділі ви дізналися про програму HP Network Visualizer SDN Application. Це одна з комерційних, корпоративних SDN додатків, доступних від HP. Програма використовує мережу з підтримкою OpenFlow для покращення характеристик мережі та функціональності.

Network Visualizer забезпечує видимість в мережі та пропонує гнучке рішення для отримання копії мережевих пакетів для перевірки, верифікації та динамічного вирішення проблем. Ви можете отримати копію мережевих

пакетів з декількох вихідних пристроїв і пересилати захоплені пакети на моніторинг пристроїв в іншому місці.

У цьому розділі ви дізналися, як встановити, ліцензувати та налаштувати HP Network Visualizer. Ви також навчались реалізовувати та використовувати різні функції, зокрема:

- Capture Session wizard
- Monitor and analyze network traffic
- Network visibility
- Event logs

Література

1. Wim Groeneveld, Gerhard Roets, Antonio Mingrone, Peter Kilgour. Creating HPE Software-defined Networks. Hewlett Packard Enterprise Press 660 4th Street, #802 San Francisco, CA 94107

2. ONF, ”Open Networking Foundation,” 2015. [Online]. Available: https://www.opennetworking.org/

3. ODL, ”OpenDaylight,” 2015. [Online]. Available: https://www.opendaylight.org/