МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 2019 р.

МАГІСТЕРСЬКА РОБОТА
НА ТЕМУ:

МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ МЕРЕЖЕВОГО ЗВ'ЯЗКУ В ПУБЛІЧНОМУ ПРОСТОРІ МІСТА

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 – "Комп'ютерна інженерія"

Науковий керівник роботи:	_____ (підпис)	І.С. Скарга-Бандурова (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	З.С. Татарченко (ініціали, прізвище)
Група:		КІ-17ДМ

Сєвєродонецьк 2019

ЗМІСТ

ВСТУП

В даний час все більшої актуальності набувають питання реконструкції середовища міських публічних просторів - фрагментів міського середовища, що мають важливий містобудівний, інформаційний статус і призначених для соціального, політичного, економічного спілкування городян. Однак, в теорії і практиці, відсутній системний підхід до проектування даних міських територій з позицій сталого розвитку їхнього середовища. Складові елементи міських публічних просторів розглядаються як окремо взяті об'єкти. Результатом цього стала дискомфортність громадських, публічних просторів, сучасних міст (невідповідність сформованої ІТ-структури функціональному використанню та вимогам створення сприятливих умов для людини; непродуманість рішень експлуатації в різні пори року і доби різними віковими та соціальними групами населення), що знижує містобудівну і соціальну ефективність територій, і вимагає активного втручання, а також розробки способів функціонального планування, технологічної зміни середовищних характеристик, з метою створення стабільних, саморегульованих систем публічних просторів.

Міські системи відрізняє особливо високий динамізм, який надає ІТ-тематиці більшої актуальності.

Інформаційна система — це система, призначена для зберігання, пошуку та обробки інформації. Відповідні організаційні ресурси, забезпечують і поширюють інформацію (людські, технічні, фінансові та т. п.). Вона призначена для своєчасного забезпечення належних людей належною інформацією, тобто для задоволення конкретних інформаційних потреб в рамках певної предметної області, при цьому результатом функціонування інформаційних систем є інформаційна продукція - документи, інформаційні масиви, бази даних та інформаційні послуги.

Велике значення має короткочасний відпочинок, під яким розуміється відновлення сил і всебічний гармонійний розвиток людини, не пов'язаний з відпусткою, проведеною поза місцем проживання, і що протікають за межами житла. На короткочасний відпочинок при п’ятиденному робочому тижню, на ділі, доводиться до 90% рекреаційного часу, але він проходить в основному неорганізовано, напівстихійно, що викликає необхідність пошуку можливостей управління.

Володіючи, таким чином, чіткою територіальністю — важливим стає підхід до локальної організації ІТ-послуг, спрямованої на задоволення потреб всіх громадян/жителів міста.

Особливістю публічних просторів є жвавість, людність, висока відвідуваність, доброзичлива соціальна атмосфера, що обумовлено їх головним функціональним змістом – бути осередком активності та обміну. У сучасних містах, в атмосфері хаосу, що панує в відкритих просторах (зокрема, сквери і парки), окупованій бездомними і «чужинцями», присутній особливий фактор не привабливості і небезпеки, що в свою чергу сприяє зменшенню ступеня зручності користування цими об'єктами. Дана обставина посилюється широкими можливостями, наданими досягненнями інформаційних технологій, коли міські жителі нудним, брудним паркам і площам, де повно несподіваних сюрпризів, вважають за краще домашній кінотеатр та Інтернет. Але ж це можна поєднати і отримати щось набагато більше, ніж звичайний простір — можна отримати комфортній, сучасний, безпечний, і дійсно — «публічний» IT-простір!

Зважаючи на це, виникає питання про доцільність вивчення і переосмислення принципів проектування даних об'єктів з урахуванням колективних переваг жителів міста і позицій сучасного етапу розвитку IT-структури.

Публічні IT-простори можуть виникати і успішно функціонувати тільки при більш уважному ставленню до них з боку міської адміністрації, соціально відповідального бізнесу і самих городян, тоді як ефективність роботи може бути досягнута тільки їх спільними зусиллями.

Актуальність дослідження визначається незадовільним станом публічних IT-просторів сучасних міст. Крім того, незадовільна технологічна обстановка потребує рекомендаційного підходу до міських територій з позицій концепції сталого розвитку, інфраструктури, що в сучасних умовах потребує перегляду принципів подальшої взаємодії технологічний й інформаційних пріоритетів у розвитку середовища публічних просторів як територій з підвищеною концентрацією активності городян, з урахуванням необхідності створення сприятливих умов індивідуалізації і безпеки міського середовища.

Мета роботи - обґрунтувати особливості формування інформаційних мереж публічних просторів, для створення комфортного, розвиненого міського середовища.

Відповідно до цього визначені завдання дослідження:

- аналіз публічного простору міста;
- аналіз способів організації зв’язку в публічному просторі;
- збір матеріалу про сформовані, сучасні, мережі Інтернет;
- аналіз можливих рішень, для вдосконалення каналів зв’язку Інтернет;
- розробка рекомендацій щодо покращення стану сучасних мереж Інтернет;
- розробка рекомендацій з правил охорони праці.

Об’єкт дослідження – процеси формування IT-мереж публічних просторів.

Предмет дослідження – сучасні мережі Інтернет.

Практична значимість роботи. Визначений комплексний підхід до формування нових мереж Інтернет в публічних просторах міста як методологічна основа перетворення їх середовища. Запропоновано підходи до реконструкції існуючих мереж Інтернет, з урахуванням ролі і можливостей розподілених мереж Інтернет, як способу й засобу гармонізації середовища проживання городянина. Виконано моделювання оптимального розташування контролера в локальній мережі публічного простору міста.

Методи дослідження. Орієнтуючись на поставлені мету і завдання, а також на можливості в зборі матеріалів, ми спиралися в своїй роботі на літературний, порівняльний, статистичний методи, використовували методи, засновані на системному підході: системно-структурний аналіз, програмно-цільове планування, інформаційне і математичне моделювання.

Публікації. За темою роботи з викладенням її основних результатів опубліковані 2 тез в наукових виданнях України.

Структура та обсяг магістерської роботи. Магістерська робота містить анотацію, вступ, 4 розділи, перелік використаної літератури, додаток. Пояснювальна записка містить 120 сторінок, 4 таблиць та 37 рисунків.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ОРГАНІЗАЦІЇ МЕРЕЖ ЗВ'ЯЗКУ В ПУБЛІЧНОМУ ПРОСТОРІ МІСТА

1.1 Публічний простір міста

У числі актуальних питань, що розглядаються як в соціології міста, так і в міському адмініструванні виділяється проблема соціальної взаємодії і громадського впливу в умовах міста.

У вигляді зростаючої ролі відкритих і загальнодоступних міських просторів, в організації і структуруванні соціального життя - вивчення публічних просторів, їх сприйняття і використання городянами, а також соціальних функцій є актуальним і необхідним питанням.

У зв'язку з цим набуває необхідність розгляду соціальної ролі публічних просторів в підтримці міського життя. Під публічним простором слід розуміти загальнодоступні місця, пристосовані для перебування людей, в межах яких відбувається переважна більшість соціальних взаємодій людей. Серед таких виступають парки, сквери, площі, вулиці, торгові доми - місця масового скупчення людей і т.п.

Виділяють три типи соціальних відносин, які можуть існувати в міському просторі:

– Особисті (в родині, серед друзів);

– Публічні (незнайомі люди спілкуються як категорії: продавець, покупець, водій таксі, пасажир і т.п.);

– Місцево-локальні (відносини людей, які знайомі один з одним, але не так близько і інтимно, як в родині, а скоріше функціонально: це відносини колег по роботі, членів клубів за інтересами, сусідів і т.п.).

Можливість перетворення і території з одного статусу в інший залежить від чисто кількісного фактора: публічна сфера перетвориться в локальну, якщо в громадському місці прийде певна кількість людей, пов'язаних певним відтінком їх відносин (знайомства). Так, якщо під час автобусної екскурсії половину салону зайняв шкільний клас, то автобус виявився, як би захоплений цими підлітками, навіть якщо інші пасажири — випадкові люди з вулиці. Публічний простір перетворилося в локальне. Відносини до місця є похідними від соціальних відносин і в якійсь мірі закріплюють їх.

Виділяють три типи таких «місць»:

– пам'ятні (здатні фіксувати моменти колективної пам'яті, як, наприклад, храм або публічний парк);

– Знайомі місця (місцевий продуктовий магазинчик, бар, забігайлівка, до яких ти звик);

– Домашні території, або місця для тусовки (місця, де люди живуть і відчувають себе «як вдома», тобто відчувають свободу вести себе так, як вони хочуть).

Публічні простори напівфункціональні і є важливою складовою життя міста. У соціальних науках під функціями розуміються деякі стійкі характеристики об'єкта, сукупність яких дає загальне уявлення про місце того чи іншого об'єкта або процесу в походженні, існуванні, розвитку глобального цілого, а також про взаємозв'язок і залежності його складових.

Отже, відкриті простори покликані служити досягненню явних соціально-значущих цілей — організації дозвілля та забезпечення ефективного проведення часу, безпеки городян, з одного боку — інтеграції і формуванню почуття ідентичності, що дозволяє мобілізувати їх на соціально значущі позитивні заходи, а з іншого — соціалізації жителів міста.

Перш за все, слід відзначити соціалізуючу роль простору, в якому городяни спостерігають один за одним, показують себе, що дуже важливо для процесів самоідентифікації — як особистої, так і групової. Соціальна взаємодія здійснюється в соціальних ситуаціях. Будь-які контакти індивідів, соціальні, власне, результатами контактів індивідів визначається більшою мірою стан суспільства.

Проте, буде помилкою вважати, що учасники публічного простору перетворяться в тісне співтовариство громадян. Перш за все, слід відзначити социализирующую роль простору, в якому городяни спостерігають один за одним, показують себе, що дуже важливо для процесів само ідентифікації — і особистої, і груповий. Соціальна взаємодія здійснюється в соціальних ситуаціях. Будь-які контакти індивідів, соціальні, власне, результатами контактів індивідів визначається більшою мірою стан суспільства.

Однією з ключових характеристик публічного простору є безпека. Безпека при цьому забезпечується самими людьми, а не відповідними правоохоронними органами. Люди доглядають один за одним, за дітьми, таким чином, починає працювати соціальний контроль публічного простору, відсутність якого часто і підвищує ризики міського життя.

В умовах відсутності інформації про інших жителів міста публічні простору стають каналом передачі інформації, знижують властиві місту страхи, деякі негативні ефекти міської анонімності, і тим самим виконують інформаційну та комунікативну функції. У відкритих і загальнодоступних просторах люди вивчають і спостерігають один за одним, набувають соціальний досвід, освоюють зразки поведінки, усвідомлюють почуття приналежності до міського товариства і т.п.

На сьогоднішній день величезною популярністю серед населення, особливо серед молоді набуває так зване третє місце — «third place» — публічний простір, що використовується одночасно в якості території спілкування, зони відпочинку, і місця роботи («перше місце» — це житло, «друге »- робота). В основному такі картини ми спостерігаємо в залах мереж кав'ярень, піцерій, приєднаних до бездротових каналах виходу в Інтернет-Wi-Fi і насичених комунікаціями.

Зручність, приємний імідж, різноманітність використання простору і занять, задоволення від інтеракції, спостереження за людьми, «карнавальність» — можливість гри, фестивалю, позбавлення від своєї істинної ідентичності, придбання нових масок — базові умови успішного функціонування публічного місця, визначені Л. Лофландом.

Вищеназвані елементи присутні в житті наших міст — площі використовуються для проведення культурно-масових і спортивних заходів в рамках відзначення державних, національних свят, також як і те, що для підтримки інтересу жителів у відкритих просторах встановлюються скульптури, фонтани різних форм і розмірів. Однак учасниками і глядачами такого роду заходів стають не самі жителі міста, а в більшості випадків гості і мігранти, перебування яких носить тимчасовий і проміжний характер. З цієї причини створення привабливою міського середовища стає найважливішим елементом політики міської влади, в реалізації якої повинні брати участь головні ініціатори і безпосередні учасники процесу - самі жителі міста.

Особливістю публічних просторів є жвавість, людність, висока відвідуваність, доброзичлива соціальна атмосфера, що обумовлено їх головним функціональним змістом — бути осередком активності та обміну. У сучасних містах в умовах екологічної занедбаності і в атмосфері хаосу, що панує в відкритих просторах (зокрема, сквери і парки), окупованій бездомними і чужинцями, присутній особливий фактор не привабливості і небезпеки, що в свою чергу сприяє зменшенню ступеня зручності користування цими об'єктами. Дана обставина посилюється широкими можливостями, наданими досягненнями інформаційних технологій, коли міські жителі нудним, брудним паркам і площами, де повно несподіваних сюрпризів, вважають за краще домашній кінотеатр та Інтернет.

В ідеальному варіанті відкритий простір, що стикається з найбільш жвавими районами міста, що викликає безліч асоціацій, доступно кожному представнику різних соціальних, вікових, етнічних груп, які відчувають себе там цілком комфортно і безпечно. Проте, значущою тенденцією в розвитку громадських просторів міста є їх комерціалізація і деградація: все менша кількість територій залишається відкритим і загальнодоступним, оскільки їх поступово займають відкриваються заклади громадського харчування,

дозвілля та торгівлі. Деякі з відкритих просторів, наприклад як спортивні та ігрові майданчики втрачають свій публічний статус, огороджуються і замикаються, «приватизуються». Сквери та алеї, парки які цілком повноцінно можуть виконувати функції публічного простору, перетворюються в осередок злочинності, залишені без освітлення і нагляду — вони таять в собі небезпеку, як в денний час, так і після настання темряви.

Зважаючи на це, виникає питання про доцільність вивчення і переосмислення принципів проектування даних об'єктів з урахуванням колективних переваг жителів міста і позицій сучасного етапу розвитку суспільства.

Публічні простору можуть виникати і успішно функціонувати тільки при більш уважному ставленні до них з боку міської адміністрації, соціально відповідального бізнесу і самих городян, тоді як ефективність роботи може бути досягнута тільки їх спільними зусиллями.

1.2 Способи організації зв’язку в публічному просторі

На відміну від більшості областей техніки, промисловість побудови комп'ютерних мереж за останні двадцять років практично не зазнала істотних змін, основна парадигма архітектури комп'ютерних мереж залишається практично незмінною. В результаті, мережі все ще занадто дорогі, складні і ними важко керувати.

Цей незадовільний стан справ може змінитися через дві революційні події:

– поява на ринку надзвичайно ускладненого, пропрієтарного, мережевого обладнання;

– поява принципово нового підходу, званого програмно-конфігуованими мережами (ПКМ - SoftwareDefinedNetworks).

ПКМ-підхід обіцяє зробити всі мережі дешевше і простіше в управлінні.

«Інфраструктура як код (IaC)» - цей напрямок швидко розвивається, в основі якого лежить використання скриптів для налаштування інфраструктури обчислень замість налаштування комп'ютерів вручну.

Модель «Інфраструктура як код (IaC)», яку іноді називають «програмованою інфраструктурою», - це модель, в якій процес налаштування інфраструктури аналогічний процесу програмування програмного забезпечення. По суті, вона поклала початок усунення кордонів між написанням додатків і створенням середовищ для цих додатків.

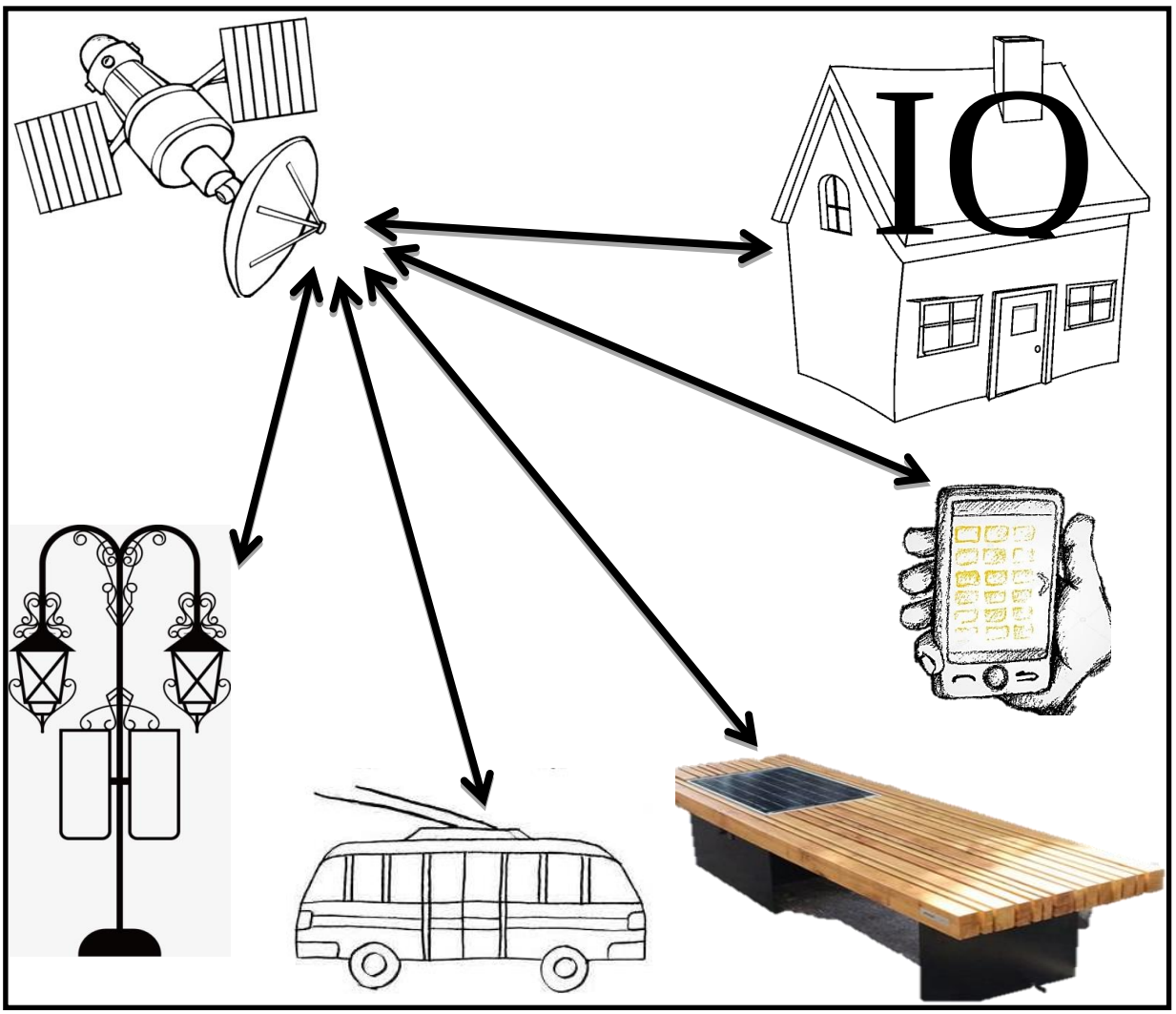


Рисунок 1.1. Споживачі Інтернет в публічному просторі

Додатки можуть містити скрипти, які створюють свої власні віртуальні машини і керують ними. Це основа хмарних обчислень і невід'ємна частина DevOps, набору практик, націлених на активну взаємодію фахівців з розробки з фахівцями з інформаційно-технологічного обслуговування і взаємну інтеграцію їх робочих процесів один в одного. Базується на ідеї про тісну взаємозалежність розробки та експлуатації програмного забезпечення і націлений на те, щоб допомагати організаціям швидше створювати і оновлювати програмні продукти і послуги.

«Інфраструктура як код (IaC)» - це процес управління і надання комп'ютерних центрів обробки даних за допомогою машиночитаємих файлів визначень, а не фізичної апаратної конфігурації або інструментів інтерактивного налаштування. Керована цим IT-інфраструктура включає в себе як фізичне устаткування, таке як сервери з білим металом, так і віртуальні машини і пов'язані з ними ресурси конфігурації. Визначення можуть бути в системі управління версіями. Він може використовувати або скрипти, які декларативні

визначення, а не ручні процеси, але цей термін частіше використовується для просування декларативних підходів.

Підходи IaC просуваються для хмарних обчислень, які іноді продаються як інфраструктура як послуга (IaaS). IaC підтримує IaaS, але не слід плутати його.

Однак, концепція SDN унікальна тим, що основна її ідея не просто централізувати інтелект мережі на виділеному пристрої - контролері, а управляти безпосередньо площиною передачі даних (data plane) з єдиного, спільного для всієї мережі, центру на базі спеціальних протоколів.

Комунікаційна мережа - система фізичних каналів зв'язку і комутаційного обладнання, що реалізує той чи інший низькорівневий протокол передачі даних. Існують провідні, бездротові (використовують радіохвилі) і волоконно-оптичні канали зв'язку. За типом переноситься сигналу виділяють цифрові і аналогові мережі. Призначенням комунікаційних мереж є передача даних з мінімальною кількістю помилок і спотворень. На основі комунікаційної мережі може будуватися інформаційна мережа, наприклад на основі мереж Ethernet як правило будуються мережі TCP / IP, які в свою чергу утворюють глобальну мережу Інтернет. Прикладами комунікаційних мереж є:

- комп'ютерні мережі;
- телефонні мережі;
- мережі стільникового зв'язку;
- мережі кабельного телебачення.

Якщо звернути увагу на програмно-визначаємі мережі (Software-defined Network - SDN), ми виявимо, що керуючий рівень повністю або частково переноситься взагалі на виділеній пристрій.

Програмно-визначаєма мережа (SDN) являє собою мережеву архітектуру, яка дозволяє грамотно і централізовано контролювати (тобто програмувати) мережу за допомогою програмного забезпечення.

Підприємства, оператори і постачальники послуг оточені рядом конкуруючих сил. Істотне зростання обсягу мультимедійного контенту, бурхливий розвиток хмарних обчислень, збільшення використання мобільних пристроїв і постійна вимога скоротити витрати.

У загальному плані кожна телекомунікаційна мережа складається з трьох частин, іноді званих площинами, тому що їх можна розглядати як окремі накладені один на одного мережі:

Керуюча площина - призначена для обміну інформацією, що керує, перш за все, сигналізацією, необхідною для встановлення з'єднань, їх роз'єднання і, іноді, для управління з'єднаннями під час уже встановленого сеансу зв'язку;

Площина даних, площина користувача - відповідає за передачу призначеного для користувача трафіку;

Адміністративна площину - здійснює обмін трафіком техобслуговування мережі зв'язку.

1.2.2 Поділ control і data plane в мережевому обладнанні

В роботі мережевого пристрою можна виділити дві абстракції - керуючий рівень (control plane) і рівень передачі (data plane). Control plane відповідає за логіку роботи мережевого пристрою для забезпечення в подальшому можливості передачі пакетів (заповнення різних таблиць, наприклад, маршрутизації, відпрацювання різних службових протоколів ARP / STP / та ін.). Data plane в свою чергу відповідає безпосередньо за передачу корисного трафіку через наш мережевий пристрій. Тобто, control plane нам надає інформацію куди і як слати мережевий трафік, а data plane вже виконує поставлені перед ним завдання. Дані абстракції можуть бути виділені як на логічному, так і на фізичному рівні. Але чи завжди на мережевому обладнанні присутній такий поділ і де саме виконуються функції кожної з абстракцій? Давайте спробуємо в цьому розібратися.

Цей поділ з'явився досить давно, з метою підвищення ефективності мережевих пристроїв. Стало зрозуміло, що використання однієї абстракції для управління і передачі мережевого трафіку неефективно. Керуючий рівень має досить складну логіку роботи і не виконує величезну кількість операцій в секунду. Передавальний рівень, навпаки, виконує одноманітні операції, але при цьому їх дуже багато. Таким чином, для керуючого рівня потрібно інтелектуальне залізо, а для передавального - високопродуктивне. Так як досягти обох параметрів в одній мікросхемі складно і часто дорого, логіку роботи мережевих пристроїв вирішили розділити. Це дозволило б реалізовувати складну логіку, наприклад, на базі процесорів загального призначення, а високу продуктивність отримати на спеціалізованих мікросхемах.

Перед виробниками мережевого устаткування на одній чаші ваг знаходиться функціональність і продуктивність, а на другий - вартість рішення. Пропонується розглянути робочі місця керуючого і передавального рівнів.

1.3 Mininet

Mininet - це емулятор комп'ютерної мережі. Під комп'ютерною мережею розуміються прості комп'ютери - хости, комутатори і OpenFlow-контролери. За допомогою найпростішого синтаксису в примітивному інтерпретаторі команд можна розгортати мережі з довільної кількості хостів, комутаторів в різних топологіях і все це в рамках однієї віртуальної машини (ВМ). На всіх хостах можна змінювати мережеву конфігурацію, користуватися стандартними утилітами (ipconfig, ping) і навіть отримувати доступ до терміналу. На комутатори можна додавати різні правила і маршрутизировать трафік. Загалом, виходить досить цікава річ, що дозволяє познайомитися з пристроєм і функціонуванням комп'ютерних мереж без необхідності використання будь-якого мережевого обладнання.

Починаючи з версії 2.6.24, ядром Linux підтримуються механізми віртуалізації і ізоляції - Cgroups, які дозволяють забезпечити мережевими інтерфейсами, таблицями маршрутизації і ARP-табло процеси в рамках однієї операційної системи. Це один з видів віртуалізації на рівні ОС, що дозволяє запустити безліч однотипних процесів в ізольованому і обмеженому по ресурсів оточенні. Подібні техніки дозволяють Mininet створювати в просторі ядра або користувача комутатори, OpenFlow-контролери і хости, і взаємодіяти в рамках модельованої мережі. Як віртуальних комутаторів використовується адаптована реалізація Open vSwitch'a. Основна функціональність Mininet реалізована на Python, за винятком деяких утиліт написаних на Сі. Практично будь-яка довільна топологія може бути описана за допомогою спеціального синтаксису на Python. В інтернеті можна знайти безліч цікавих лабораторних робіт на базі mininet, що вирішують різні завдання. Наприклад реалізація простого маршрутизатора.

При стандартних налаштуваннях всі об'єкти мережі mininet з'єднуються віртуальними гігабітними каналами.

Проте, тест показує трохи завищені результати. Це пов'язано з особливостями віртуального середовища. Тому що комутатор, що працює в просторі користувача, а не в просторі ядра, виконується значно повільніше.

Можна обмежити пропускну здатність каналів до довільних значень. А також, є можливість вказати затримки в каналі (latency).

Відповідно, починаючи від класичної серверної і закінчуючи віртуальними Ethernet-портами, в сучасних блейд-системах все віртуалізовано (Блейд-сервер — комп'ютерний сервер з компонентами, винесеними і узагальненими в кошику для зменшення займаного простору. Кошик — шасі для блейд-серверів, що надає їм доступ до

загальних компонентів, наприклад, блоків живлення і мережним контролерам. Блейд-сервери називають також ультракомпактними серверами.).

Віртуалізується все, і mininet - добрийий тому приклад. Реалізація цікава і це рішення зможе послужити інструментом моделювання, а різні експерименти допоможуть розібратися в принципах роботи обчислювальних мереж.

1.4 Групи, протоколів, їх призначення

Транспортні протоколи управляють передачею даних між двома машинами.

– TCP (Transmission Control Protocol). Протокол, що підтримує передачу даних, основану на логічному поєднанні між комп'ютерами, що посилають і приймають інформацію.

– UDP (User Datagram Protocol). Протокол, що підтримує передачу даних без встановлення логічного з'єднання. Це означає, що дані надсилаються без попереднього встановлення з'єднання між комп'ютерами одержувача і відправника. Можна провести аналогію з відправленням пошти по якомусь адресою, коли немає ніякої гарантії, що це повідомлення прибуде до адресата, якщо він взагалі існує. (Дві машини з'єднані в тому сенсі, що обидві підключені до Internet, але вони не підтримують зв'язок між собою через логічне з'єднання.)

Протоколи маршрутизації обробляють адресацію даних і визначають найкращі шляхи до адресата. Вони також можуть забезпечувати розбиття великих повідомлень на кілька повідомлень меншої довжини, які потім послідовно передаються і компонуються в єдине ціле на комп'ютері-адресата.

– IP (Internet Protocol). Забезпечує фактичну передачу даних.

– ICMP (Internet Control Message Protocol). Обробляє повідомлення стану для IP, наприклад, помилки і зміни в мережевих апаратних засобах, які впливають на маршрутизацію.

– RIP (Routing Information Protocol). Один з декількох протоколів, які визначають найкращий маршрут доставки повідомлення.

– OSPF (Open Shortest Path First). Альтернативний протокол для визначення маршрутів.

Підтримка мережевої адреси - це спосіб ідентифікації машини з унікальним номером і ім'ям.

– ARP (Address Resolution Protocol). Визначає унікальні числові адреси машин в мережі.

– DNS (Domain Name System). Визначає числові адреси за іменами машин.

– RARP (Reverse Address Resolution Protocol). Визначає адреси машин в мережі, але способом, зворотнім ARP.

Прикладні сервіси - це програми, які користувач (або комп'ютер) використовує для отримання доступу до різноманітних послуг.

– BOOTP (Boot Protocol) завантажує мережеву машину, читаючи інформацію для початкового завантаження з сервера.

– FTP (File Transfer Protocol) передає файли між комп'ютерами.

– TELNET забезпечує віддалений термінальний доступ до системи, тобто, користувач одного комп'ютера може з'єднуватися з іншим комп'ютером і відчувати себе так, як ніби він працює за клавіатурою віддаленої машини.

Шлюзові протоколи допомагають передавати по мережі повідомлення про маршрутизації та інформацію про стан мережі, а також обробляти дані для локальних мереж.

– EGP (Exterior Gateway Protocol) служить для передачі маршрутизаційної інформації для зовнішніх мереж.

– GGP (Gateway-to-Gateway Protocol) служить для передачі маршрутизаційної інформації між шлюзами.

– IGP (Interior Gateway Protocol) служить для передачі маршрутизаційної інформації для внутрішніх мереж.

Інші протоколи не належать до категорій, згаданих вище, але відіграють важливу роль в мережі.

– NFS (Network File System) дозволяє використовувати каталоги і файли віддаленого комп'ютера так, якщо б вони існували на локальній машині.

– NIS (Network Information Service) підтримує в мережі інформацію про користувачів декількох комп'ютерів, спрощуючи вхід в систему і перевірку паролів.

– RPC (Remote Procedure Call) дозволяє віддаленим прикладним програмам зв'язуватися один з одним простим і ефективним способом.

– SMTP (Simple Mail Transfer Protocol) - це протокол, який переносить електронні листи між машинами.

– SNMP (Simple Network Management Protocol) - протокол для адміністрування, який посилає повідомлення про стан мережі і підключених до неї пристроїв.

Всі ці види сервісу в сукупності складають TCP / IP - потужне і ефективне сімейство мережевих протоколів.

РОЗДІЛ 2. АНАЛІЗ РОЗПОДІЛЬНИХ МЕРЕЖ ЗВ'ЯЗКУ

2.1 Динамічна маршрутизація

Динамічна маршрутизація - вид маршрутизації, при якому таблиця маршрутизації редагується програмно. У разі UNIX-систем демонами маршрутизації; в інших системах - службовими програмами, які називаються інакше, але фактично грають ту ж роль.

Демони маршрутизації обмінюються між собою інформацією, яка дозволяє їм заповнити таблицю маршрутизації найбільш оптимальними маршрутами. Протоколи, за допомогою яких проводиться обмін інформацією між демонами, називається протоколами динамічної маршрутизації.

Дворівнева модель, в рамках якої розглядається все безліч машин Internet. В рамках цієї моделі весь Internet розглядають як безліч автономних систем (autonomous system - AS). Автономна система - це безліч комп'ютерів, які утворюють досить щільне співтовариство, де існує безліч маршрутів між двома комп'ютерами, що належать цієї спільноти. В рамках цієї спільноти можна говорити про оптимізацію маршрутів з метою досягнення максимальної швидкості передачі інформації. На противагу цьому щільному конгломерату, автономні системи пов'язані між собою не так тісно як комп'ютери всередині автономної системи. При цьому і вибір маршруту з однієї автономної системи може грунтуватися не на швидкості обміну інформацією, а надійності, безвідмовності і т.п.

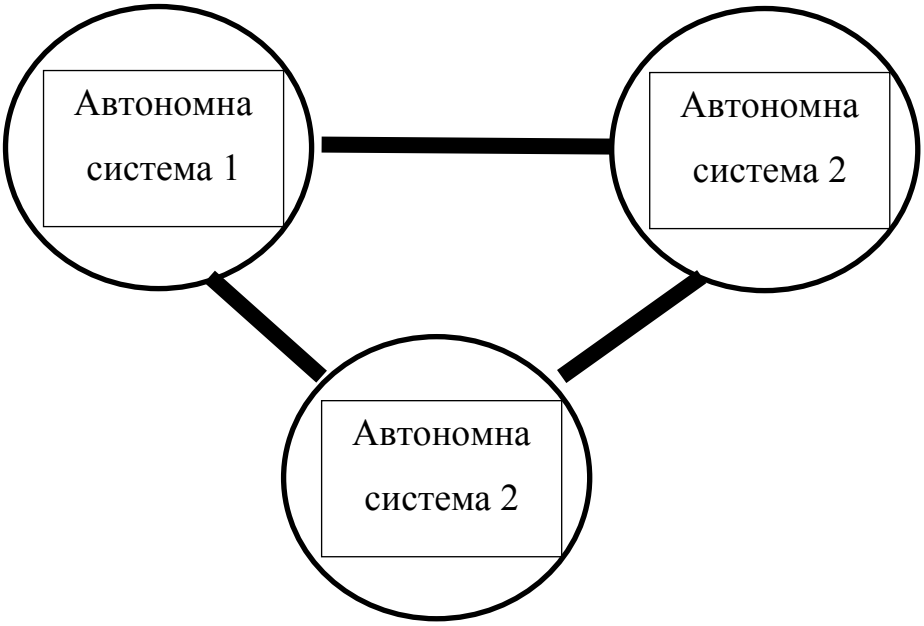


Рис. 2.1. Схема взаємодії автономних систем

Сама ідеологія автономних систем виникла в той період, коли ARPANET представляла ієрархічну систему. У той час було ядро системи, до якого підключалися зовнішні автономні системи. Інформація з однієї автономної системи в іншу могла потрапити тільки через маршрутизатори ядра. Така структура досі зберігається в MILNET. На малюнку 1.1 автономні системи пов'язані тільки однією лінією зв'язку, що більше відповідає тому, як сектор більшості країн СНД підключений до Internet. У класичних публікаціях по Internet взаємодія автономних частин частіше позначають пересічними колами, підкреслюючи той факт, що маршрутів з однієї автономної системи в іншу може бути кілька. Обговорення цієї моделі Internet необхідно тільки для того, щоб пояснити наявність двох типів протоколів динамічної маршрутизації: зовнішніх і внутрішніх.

Зовнішні протоколи служать для обміну інформацією про маршрути між автономними системами. Внутрішні протоколи служать для обміну інформацією про маршрути усередині автономної системи.

У реальній практиці побудови локальних мереж, корпоративних мереж та їх підключення до провайдерів потрібно знати, головним чином, тільки внутрішні протоколи динамічної маршрутизації. Зовнішні протоколи динамічної маршрутизації необхідні тільки тоді, коли слід побудувати закриту велику систему, яка із зовнішнім світом буде з'єднана тільки невеликим числом захищених каналів даних.

2.1.1 Алгоритми протоколів динамічної маршрутизації

Незважаючи на гадану складність і різноманіття, протоколи маршрутизації базуються всього на двох простих алгоритмах, відомих уже кілька десятиліть.

Для виконання своєї основної функції - перемикання трафіку - кожен маршрутизатор використовує таблицю, в якій відображена топологія мережі на даний момент часу. У найзагальнішому випадку таблиця маршрутизації містить адресу мережі призначення, адреса наступного вузла на шляху до цієї мережі і метрику (вартість) шляху. Створення та подальше оновлення таблиці маршрутизації при зміні топології мережі здійснюється за допомогою протоколів маршрутизації. Найбільшою популярністю користуються протоколи динамічної маршрутизації.

Алгоритм Беллмана-Форда (також відомий як алгоритм Форда-Фулкерсона) був покладений в основу першого протоколу маршрутизації, створеного для мережі ARPANET. Так звані протоколи вектора відстані (distance vector protocols), такі, як RIP, IGRP, BGP, використовують ті ж принципи. У 1979 році на зміну протоколу вектора

відстаней прийшов протокол стану каналу (link state protocol), що став основним в ARPANET. Сучасні протоколи стану каналу включають OSPF, IS-IS, NLSP і ін.

В даний час обидва типи протоколів знайшли собі застосування, так як у кожного з них є свої переваги і недоліки.

2.1.2 Протоколи векторів відстаней

Основна перевага алгоритму вектора відстаней - його простота. Дійсно, в процесі роботи маршрутизатор спілкується тільки з сусідами, періодично обмінюючись з ними копіями своїх таблиць маршрутизації. Отримавши інформацію про можливі маршрути від всіх сусідніх вузлів, маршрутизатор вибирає шлях з найменшою вартістю і вносить його в свою таблицю.

Гідність цього елегантного алгоритму - швидка реакція на хороші новини (поява в мережі нового маршрутизатора), а недолік - дуже повільна реакція на погані звістки (зникнення одного з сусідів). Як приклад ми розглянемо мережу (див. Малюнок 1.2) з декількох послідовно з'єднаних маршрутизаторів, де метрикою є число транзитних вузлів на шляху до точки призначення (як в протоколі RIP).

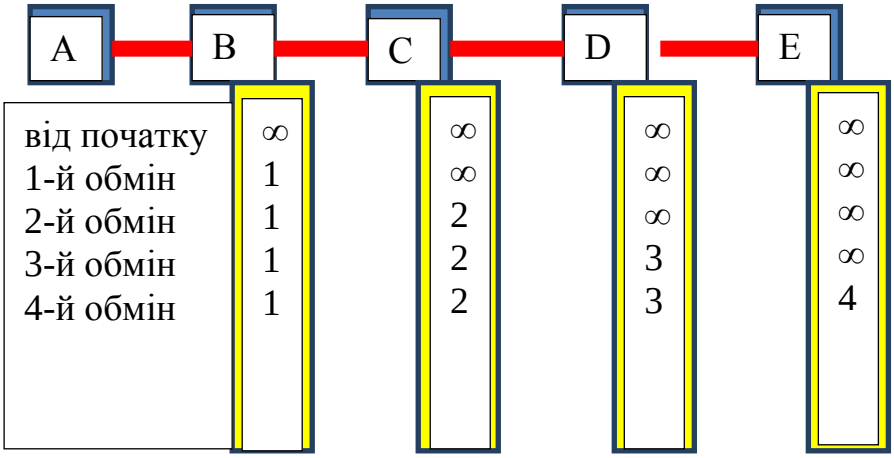


Рисунок 2.2. Поширення «доброї» новини в мережі. Таблиця маршрутизації (до вузла А)

Нехай в початковий момент часу маршрутизатор А не був доступний, т. Е. Відстань до нього в усіх таблицях - нескінченність. При включенні А пошле повідомлення своєму сусідові - вузлу В. Всі інші маршрутизатори дізнаються про це через послідовний обмін повідомленнями (для простоти будемо вважати, що обмін між усіма сусідніми вузлами відбувається синхронно кожні кілька секунд).

Під час першого обміну вузол B дізнається, що A заробив і вносить в свою таблицю маршрутизації «1» як відстань до A; всі інші вузли в цей момент як і раніше вважають A недоступним. При наступному обміні, через кілька секунд, вузол C також дізнається про появу маршрутизатора A. В результаті послідовності таких обмінів інформація досягне і вузла E, для якого вартість маршруту до A буде «4».

Таким чином, для мережі з максимальною довжиною маршруту N повідомлення про новий маршрутизатор дійде до самого віддаленого вузла в мережі через N-1 циклів обміну таблицями маршрутизації. На цьому етапі ніяких проблем не виникає. Тепер ми розглянемо зворотний випадок (див. Малюнок 1.3), коли вузол A перестає працювати внаслідок збою. При черговому обміні (ми будемо вважати його першим в цій серії) вузол B не отримує ніякого повідомлення від мовчазного маршрутизатора A. Це вірний сигнал про те, що у A виникли проблеми, і інформацію про нього необхідно видалити з таблиці. Однак в той же самий час вузол C повідомляє, що йому відомий шлях до A і вартість цього шляху «2». Той факт, що шлях до A, оголошений вузлом C, проходить через сам B (т. Е. Утворюється петля), залишається поза увагою маршрутизатора, і він заносить в таблицю шлях до непрацюючого A вартістю «3».

Під час наступного обміну C зауважує, що обидва його сусіда рекламують шлях до A вартістю «3», і негайно робить поправки в своїй таблиці. Тепер довжина шляху від З до A – «4». Якщо цей процес не зупинити, то він може продовжуватись до нескінченності, і ніхто так і не дізнається, що маршрутизатор A давно вийшов з ладу. Відповідно дані до A будуть надсилатися і далі.

Ця проблема алгоритму вектора відстаней отримала назву проблеми зростання до нескінченності (count-to-infinity problem). Вона є основною причиною завдання обмежень на максимальну довжину шляху в усіх протоколах вектора відстані. Протокол RIP, наприклад, вважає маршрут довжиною більше ніж в 15 транзитних вузлів нескінченним. Такий шлях буде негайно вилучений з таблиці маршрутизації. Т. е. В останньому прикладі вузол B зрозуміє, що вузол A недоступний, коли отримає оголошення шляху до A з вартістю «15». На жаль, така процедура займає занадто багато часу.

Для запобігання утворенню помилкових маршрутів використовується кілька методів, один з них - метод розщеплення горизонту (split-horizon). Це правило не так складно, як може здатися з назви: «Якщо відомо, що шлях до вузла X лежить через сусідній вузол Y, то вузлу Y не треба посилати оголошення маршруту до X».

Розглянемо той же приклад, що і на рисунку 2.3, але в умовах, коли діє правило розщеплення горизонту.

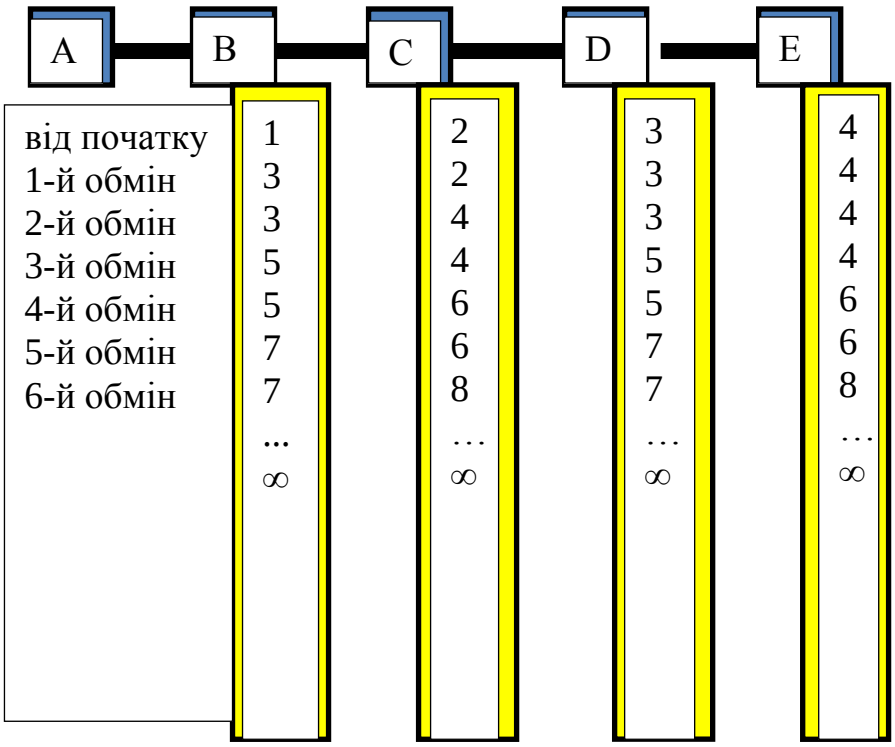


Рисунок 2.3 Проблема зростання до нескінченності

Після виходу з ладу маршрутизатора A вузол B дізнається про недієздатність A при першому ж обміні. Вузлу З правило розщеплення горизонту забороняє надсилати інформацію про A на B, так як шлях до A лежить через B. Таким чином, вузол C не може тепер (ненавмисно) обманювати свого сусіда зліва, і вузол B тут же позначає маршрутизатор A як недоступний. Після наступного обміну вже З дізнається від B про недоступність A, разом з тим помилкова інформація від вузла D, який все ще вважає маршрутизатор A чинним, на C не надійде.

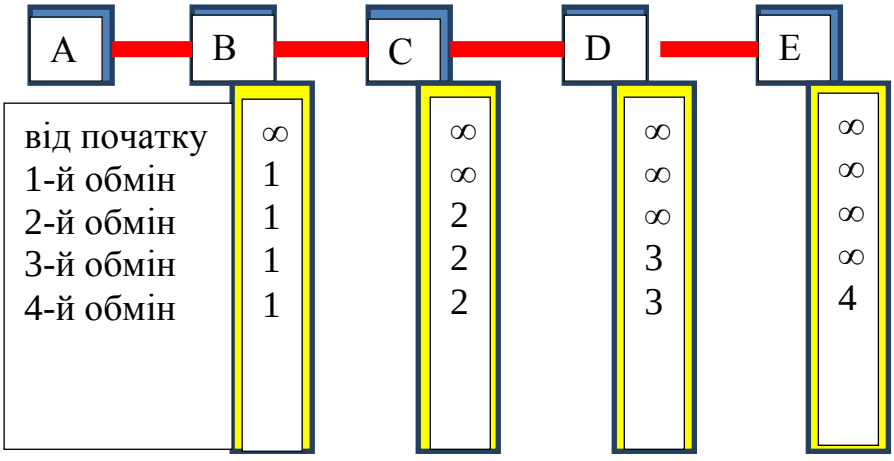


Рисунок 2.2. Поширення «доброї» новини в мережі.

Дані маршрутизації (до вузла A) надані у табл. 2.1.

Таблиця 2.1. Значення поля TOS для різних додатків

Додаток	Мінімальна затримка	Максимальна смуга	Максимальна надійність	Мінімальна вартість
Telnet/Rlogin	1	0	0	0
FTP:				
Команди	1	0	0	0
Дані	0	1	0	0
SMTP:				
Команди	1	0	0	0
Дані	0	1	0	0
DNS:				
Запит TCP	0	0	0	0
Заприт UDP	1	0	0	0

Як бачимо, з введенням правила розщеплення горизонту погана новина поширюється в нашій мережі так само швидко, як і гарна. При цьому ніяких петель не виникає. На жаль, навіть при мінімальному ускладненні топології правило розщеплення горизонту перестає діяти.

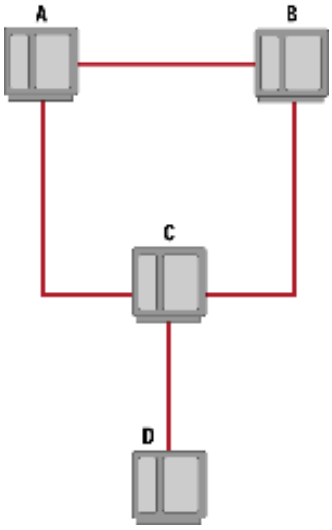


Рисунок 2.4. - Приклад ситуації, коли правило розщеплення горизонту не діє.

Розглянемо приклад мережі з надлишковою топологією (див. Малюнок 1.4). У початковий момент часу A і B знають, що відстань до вузла D одно «2». Після виходу D з ладу маршрутизатор C, не отримавши від D повідомлення, визначає, що вузол D

недоступний. A та B продовжують вважати D доступним, але правило розщеплення горизонту забороняє їм повідомляти цю неправдиву інформацію маршрутизатора C. При наступному обміні C повідомляє A і B про недоступність D. Але одночасно з цим вузол A отримує від B повідомлення про шляхи до D вартістю «2» , а вузол B отримує аналогічне повідомлення від A.

Інформація про аварію на D не почують його. Проблема зростання до нескінченності виникла знову.

У розглянутому вище прикладі маршрутизатори A і B не змогли коректно визначити відмова вузла D. Не допомогло і правило розщеплення горизонту. Подібну проблему допомагає вирішити метод тимчасової відмови від прийому повідомлень (hold-down), який використовується сучасними протоколами вектора відстаней.

Правило відмови від прийому забороняє маршрутизатора, який отримав повідомлення про відмову вузла, приймати оголошення маршруту до цього вузла протягом деякого часу. Отримавши від C повідомлення про недоступність D, маршрутизатор A не повинен довіряти повідомленням вузла B, так як в момент обміну той не мав достовірної інформації про D. Лише через деякий час, коли можна бути впевненим, що інформація про відмову D поширилася по всій мережі, маршрутизатор A може знову починати приймати оголошення про шляхи до D. (За цей час і A і B зітруть інформацію про маршрут до D, так як воно перевищує час зберігання записи в таблиці маршрутизації.)

З моменту появи алгоритму вектора відстаней наукові журнали періодично публікують опису різних, часто дуже складних, алгоритмів для вирішення проблеми зростання до нескінченності. На жаль, жоден такий метод не дозволяє повністю впоратися з названої завданням. Зловісний привид count-to-infinity продовжує бродити по мережах, які використовують у своїй роботі протоколи вектора відстаней. Якщо зациклення в мережі все ж сталося, то утворилася петля буде розірвана, коли метрика маршруту перевищить максимально допустиму. Цей процес може бути прискорений за допомогою механізму примусових оголошень (triggered updates).

Правило примусових оголошень звучить наступним чином: «Дізнавшись про зміну метрики маршруту, маршрутизатор зобов'язаний негайно повідомити про це сусідам». Дізнавшись про відмову маршрутизатора A (див. Малюнок 1.4), вузол B не чекатиме наступного обміну, а тут же повідомить про відмову вузла C. Вузол C, в свою чергу, негайно проінформує D. Вихід з ладу вузла A викликає швидко поширюється по мережі хвилю оголошень. В результаті адаптація мережі до нової топології відбудеться значно швидше.

Однак при виході з ладу одного з каналів мережі не всі оголошення дійдуть до одержувачів. У цьому випадку маршрутизатор, так і не дізнався про зміни, що відбулися, буде продовжувати рекламувати застарілі маршрути, а при відсутності механізму відмови від прийому проблема зростання до нескінченності знову сплутає таблиці маршрутизації. Сучасні протоколи вектора відстаней IGRP (Gateway Routing Protocol) і EIGRP (Enhanced Interior Gateway Routing Protocol) підтримуються, наприклад, маршрутизаторами Cisco. Вони мають таку корисну функцію, як метод коригування скасування маршруту (route-poisoning). Якщо правило розщеплення горизонту дозволяє запобігати утворенню петель між сусідніми маршрутизаторами, то метод коригування скасування маршруту здатний розпізнати і великі петлі, що охоплюють кілька вузлів. Відповідно до правила коригування значно зросла вартість маршруту розцінюється як ознака освіти петлі. Такий маршрут видаляється з таблиці маршрутизації. Яка зміна вартості маршруту розуміти як «значне», залежить від адміністратора. За замовчуванням маршрут, вартість якого раптом зросла більш ніж в 1,1 рази, розцінюється як недійсний.

Слабка сторона алгоритму вектора відстаней, як уже було сказано, - повільність реакції на негативні зміни в топології.

За повідомленням компанії Cisco, її фахівцям вдалося ліквідувати даний недолік. За швидкістю відновлення після аварії протокол EIGRP не поступається протоколам стану каналу. Цим він перш за все зобов'язаний алгоритму дифузійного поновлення DUAL (Distibuted Update Algorithm).

Маршрутизатор, що працює за алгоритмом DUAL, зберігає в таблиці маршрутизації не тільки адреса наступного вузла на шляху до мережі призначення, але і список сусідів, які знають таку ж коротку дорогу (feasible successors). У разі збоїв в мережі це дозволяє, не перераховуючи маршруту і не посилаючи оголошень по мережі, перемикати трафік на шлях з такою ж вартістю. Перераховування таблиць маршрутизації відбувається тільки при відсутності рівнозначного шляху. Оголошення маршрутів надсилаються тільки вузлів, яких зміна в топології стосується безпосередньо. Самий «літній» і заслужений представник сімейства протоколів вектора відстаней, поза всяким сумнівом, - протокол RIP. Він настільки простий і зручний в невеликих мережах, що йому прощають навіть відверті прояви старечого маразму (як відомо, RIP може запросто направити трафік через «напівживе» модемне з'єднання при наявності вільного волоконно-оптичного каналу - головне, щоб транзитних вузлів було поменше).

Вся справа в тому, що за часів створення RIP лінії зв'язку мали максималь-ву пропускну здатність 56 Кбіт / с, і протоколу маршрутизації не було потреби враховувати

швидкість каналу. Тому єдиний спосіб змусити RIP при визначенні маршруту віддавати перевагу швидким каналах - це призначити повільним лініях велику метрику вручну.

З'явився порівняно недавно протокол IGRP враховує багато характеристик каналів зв'язку. І RIP, і IGRP використовують функцію тимчасової відмови від прийому повідомлень для забезпечення більшої стабільності роботи в умовах мінливої топології. Ціна за таку стабільність - збільшення часу визначення нових маршрутів, так як, блокувавши зміна деякого маршруту внаслідок відмови будь-якого вузла з побоювання «дезінформації» з боку сусідів, маршрутизатор відкидає і коректні оголошення.

Багато реалізації протоколів дозволяють функцію відмови від прийому відключити. В цьому випадку, через поширення неправдивої інформації, петлі будуть виникати частіше, але ефективність роботи мережі може і підвищитися. При наявності механізму коригування (т. Е., Наприклад, якщо використовується IGRP) і при відсутності механізму відмови «дисципліну» в мережі слід посилити і змусити маршрутизатори ліквідувати маршрути навіть при збільшенні метрики на одиницю. В принципі, механізмів примусових оголошень і відмови від прийому достатньо для стабільної роботи мережі, однак нехтувати, наприклад, правилом розщеплення горизонту звичайно ж не варто. Розщеплення горизонту дозволяє щонайменше знизити обсяг розсилаються повідомлень.

На цьому розгляд протоколів вектора відстаней можна закінчити і перейти до іншої, не менш цікавою, групі протоколів маршрутизації - до протоколів стану каналу.

2.1.3 Протоколи стану каналу

Розвиток Internet привело до необхідності створення більш гнучкого і ефективного протоколу маршрутизації для обслуговування великих мереж. За задумом творців, протоколи стану каналу повинні були вирішити характерні для протоколів вектора відстаней проблеми. Однак, на відміну від протоколів вектора відстані, протоколи стану каналу складні і вимогливі до ресурсів маршрутизаторів. Основу протоколів стану каналу становить алгоритм переваги найкоротшого шляху, створений в 1978 році.

Формальний опис протоколів стану каналу досить заплутано і може зайняти не один десяток сторінок. У спрощеній формі принципи роботи маршрутизаторів в Відповідно до цього протоколу можна сформулювати у вигляді п'яти нескладних правил. Отже, кожен маршрутизатор в мережі повинен:

- при включенні в мережу отримати інформацію про своїх сусідів;
- дізнатися вартість шляху до кожного з сусідів (т. Е. Дізнатися про стан каналів);
- підготувати пакет-оголошення, що містить отриману інформацію;

- розіслати цей пакет всім сусідам;

- побудувати дерево найкоротших відстаней до всіх інших маршрутизаторів.

Іншими словами, маршрутизатора необхідно дізнатися всю інформацію про топології мережі, виміряти метрики каналів, що з'єднують власні фізичні інтерфейси з сусідами і далі, обчислити за допомогою алгоритму Дейкстри, найкоротші шляхи до всіх інших вузлів і внести отримані результати в таблицю маршрутизації.

При підключенні мережі, маршрутизатор насамперед повинен «познайомитися» зі своїми сусідами. Для цього він розсилає через всі свої фізичні інтерфейси спеціальні пакети з привітанням HELLO. Отримавши такий пакет, сусідній вузол повинен відповісти, повідомивши дані про себе.

Дізнавшись дані про сусідів, маршрутизатор приймається за другий пункт програми - тестування каналів зв'язку з метою з'ясування метрики кожного каналу. Під метрикою може розумітися пропускна здатність, час затримки, надійність (кількість помилок на одиницю переданої інформації), завантаження каналу.

Затримку каналу можна визначити, пославши спеціальний ECHO-пакет, який приймаюча сторона повинна негайно відправити назад. Розділивши час відгуку навпіл, маршрутизатор обчислює приблизну величину затримки каналу.

Завантаження каналу також нескладно виміряти. Однак відповідь на питання про те, як використовувати показник завантаженості каналу при обчисленні метрики, аж ніяк не однозначний. Розглянемо невеликий приклад. При наявності декількох альтернативних шляхів до точки призначення маршрутизатор, оцінивши завантаженість кожного з них, перемикає трафік на канал з меншим завантаженням. Тим самим він максимально використовує вільний канал, що цілком логічно. Під час наступного вимірювання метрик перевагу може бути віддано вже іншому каналу, через який трафік вже не йде і який, отже, тепер менш завантажений. В результаті трафік буде переключено на нього. Це призводить до того, що трафік постійно перекладається з одного каналу на інший, що, природно, не сприяє стабільності в роботі мережі.

Хороший протокол повинен вміти розподіляти навантаження по декількох каналах. Сучасні протоколи маршрутизації успішно справляються з цим завданням.

Крок номер три в програмі маршрутизатора полягає в повідомленні отриманих знань іншим. Інформація про каналах повинна бути розіслана сусідам. Однак пакети з оголошеннями про стан каналів (Link State Advertisement, LSA) можуть загубитися при транспортуванні або прибути в іншому порядку. Для того щоб одержувач міг розібратися в що прийшла інформації, кожен пакет з оголошенням про стан каналів забезпечується

полями source (адреса відправника), sequence number (номер пакета в послідовності відправлених повідомлень див. табл. 2.2) і age (вік) (див. Рис. 2.5).

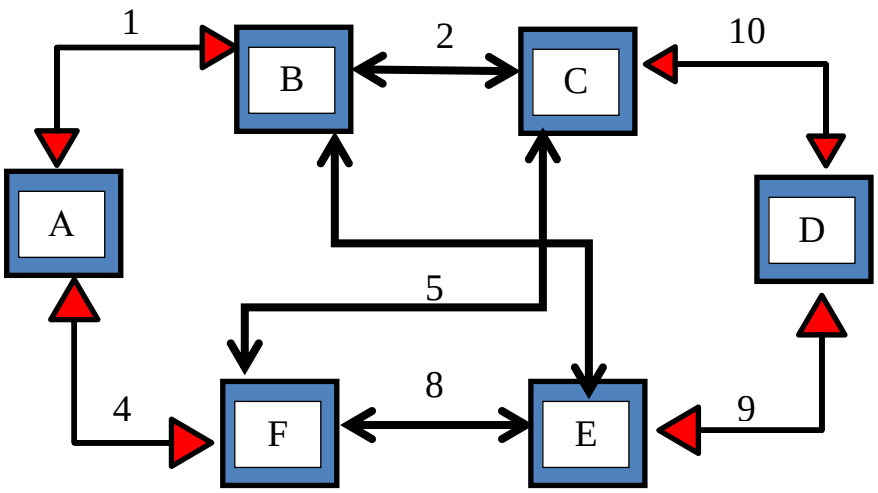


Рисунок 2.5. Обмін пакетами з оголошеннями про стан каналів.

Таблиця 2.2. Номер пакета в послідовності відправлених повідомлень

A		B		C		D		E		F	
Номер в послідовності		Номер в послідовності		Номер в послідовності		Номер в послідовності		Номер в послідовності		Номер в послідовності	
B	1	C	2	D	10	C	10	D	9	E	5
F	4	A	1	B	2	E	9	F	5	A	4
		E	8	F	1			B	8	C	1

В процесі роботи маршрутизатора пакети з оголошеннями маршрутів розсилаються зазвичай лише в разі будь-яких змін в мережі. В інший же час протоколи стану каналу мовчать і не завантажують канали службовою інформацією, лише зрідка обмінюючись невеликими HELLO-пакетами.

Обмін інформацією здійснюється за допомогою віялової розсилки (flooding), т. Е., Отримавши пакет, маршрутизатор LSA зберігає копію в своїй базі даних і посилає пакет далі всім іншим сусідам. У підсумку пакет, відправлений одним з вузлів мережі, обов'язково отримають всі інші маршрутизатори. У цьому ключова відмінність даного алгоритму від алгоритму вектора відстані, в якому кожен вузол міг спілкуватися тільки з безпосередньо підключеними до нього маршрутизаторами, що часто призводить до ефекту «зіпсованого телефону», коли, сам не розібравшись в топології, маршрутизатор збиває з пантелику сусідів. Протокол стану каналу дає можливість кожному вузлу самостійно обмінятися інформацією з усіма маршрутизаторами і отримати уявлення про

топологію мережі. Саме тому цього алгоритму не властиві проблеми зростання до нескінченності, а жорсткі обмеження на діаметр мережі відсутні. Вузьким місцем такого підходу є необхідність обов'язкової синхронізації баз даних всіх маршрутизаторів в межах автономної системи. Якщо різні вузли будуть по-різному уявляти собі топологію мережі, з якої вони працюють, то це призведе до утворення петель і до інших проблем. Отримавши пакет LSA, маршрутизатор перевіряє пару (source, sequence), що дозволяє відкинути застарілі та дубльовані оголошення. Поле age задає час, після закінчення якого не надіслав нових оголошень вузол вважається недоступним. У конкретних протоколах дані поля можуть носити інші назви, в протоколі OSPF, наприклад, поля age і sequence носять назви DeadInt і DD Sequence, а протокол IS-IS навіть використовує спеціальний тип пакета - порядковий пакет. Однак, незалежно від протоколу, наявність подібної інформації є обов'язковим для надійної роботи алгоритму переваги найкоротшого шляху.

Мережі з множинним доступом (наприклад, локальні мережі) відображаються вершинами для кожного вузла мережі і додаткової вершиною – «центром» цієї мережі. Дуги графа від «центру» до вузлів мережі не відображаються (див. рис. 2.6).

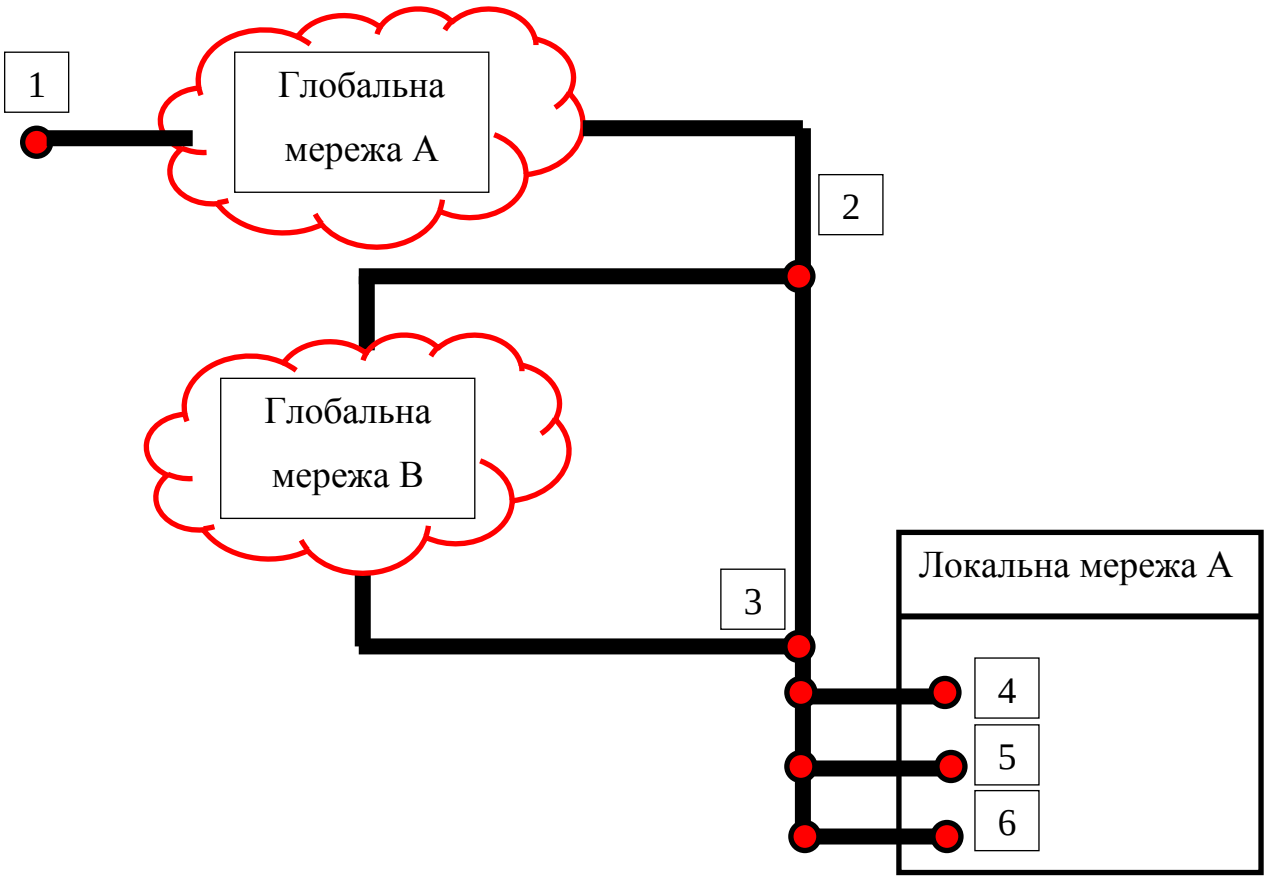


Рисунок 2.6. Мережа та її представлення у вигляді схеми.

Після отримання інформації від всіх вузлів маршрутизатор може побудувати «карту» мережі. Для цього він створює орієнтований граф, що відображає топологію мережі. З'єднання «точка-точка» між вузлами представляється на графі парою дуг (по одній в кожному напрямку), причому вартості цих дуг можуть відрізнятися один від одного.

Маючи в пам'яті такий граф, маршрутизатор застосовує алгоритм Дейкстри для вибору шляху з найменшою сумарною вартістю до кожної з вершин графа (т. Е. До кожного вузла мережі). За результатами цих обчислень і будується таблиця маршрутизації, яка використовується далі при перемиканні трафіку.

Найбільш популярні протоколи стану каналу - це IS-IS і OSPF. Протокол IS-IS спочатку створювався для мереж OSI, але згодом був адаптований і до інших протоколів мережного рівня, зокрема до IP. Наприклад, мережа NSFNet широко використовує IS-IS в своїй роботі. До основних переваг IS-IS прийнято відносити його «вроджену» здатність взаємодіяти з самими різними протоколами мережевого рівня, що робить його особливо корисним у великих багато протокольних мережах. У мережах TCP / IP, все ж, більш популярний протокол OSPF. Протоколи IS-IS і OSPF мають дуже багато спільного (OSPF, по суті, є покращеною версією IS-IS). Все сказане раніше про протоколах стану каналу в рівній мірі справедливо і для IS-IS, і для OSPF. Протоколом OSPF передбачена корисна можливість обчислення окремого набору маршрутів для кожного значення поля «тип сервісу» (Type-Of-Service, TOS) в заголовку протоколу IP. До створення OSPF жоден протокол не використав значення цього поля. Поле «тип сервісу» дозволяє запитувати для трафіку певний рівень сервісу. Довжина поля - чотири біта, з яких значущим може бути тільки один. Таким чином, ми маємо лише чотири можливих варіанти: мінімальна затримка, максимальна пропускна здатність, максимальна надійність, мінімальна вартість (в сенсі оплати). Кожна програма по-різному встановлює значення поля TOS.

В протоколах FTP і SMTP потрібно передавати команди з мінімальною затримкою, а для передачі даних їм необхідна велика пропускна здатність. Якщо запит DNS передається по протоколу UDP, то очевидно, що програма-resolver, що послала цей запит, бажає отримати відповідь якомога швидше, так як дейтаграми UDP не вимагають посилки підтверджень. Налаштувавши протокол OSPF для визначення маршрутів або з мінімальною затримкою, або з максимальною пропускною здатністю, в залежності від TOS, ми можемо ще більше прискорити роботу DNS, так само як FTP і SMTP.

Однак не варто забувати, що протоколи стану каналу дуже вимогливі до пам'яті. Зловживання багатими можливостями OSPF швидко призведе до переповнення пам'яті маршрутизатора і збоїв при обчисленнях маршрутів. В результаті весь трафік виявиться в стані хаосу, і ніякого заявленого типу сервісу він не отримає. Необхідно пам'ятати, що

абсолютно надійних протоколів маршрутизації не існує. При надмірному навантаженні відмовити може будь-який протокол. Якихось загальноприйнятих стандартів налаштування протоколів стану каналу немає. Однак зазвичай їх настройка проводиться з урахуванням наступних міркувань. Протоколах маршрутизації звичайно не подобаються «хмари» мереж X.25 і frame relay. Велике число повільних каналів, відповідно, вимагають розсилки великої кількості оголошень LSA, ускладнює роботу. Розсилка оголошень проводиться по «віялові» методу, тому повнозв'язна (fully-meshed) топологія мережі небажана. Мережі з частково зв'язковий (partial-meshed) топологією тут більш кращі. Незважаючи на відсутність суворого обмеження на максимальну кількість вузлів в мережі, можливості протоколів все ж не безмежні. Експерименти з протоколом OSPF показали, що 50 маршрутизаторів на зону (area) - це верхня межа, перевищення якого загрожує неприємними «сюрпризами» з боку мережі. При більшій кількості вузлів кращий вихід полягає в створенні нової зони.

Найсерйознішою проблемою може стати брак пам'яті. Для системи з n вузлів, кожен з яких має k сусідів, необхідний обсяг пам'яті пропорційний k * n. Зазвичай подібні проблеми проявляються в великих мережах, з дуже великою кількістю зовнішніх маршрутів. Визначення одного маршрутизатора (шлюзу) за замовчуванням для всіх зовнішніх шляхів може значно заощадити пам'ять. Взагалі, ретельне попереднє планування мережі здатне значно полегшити «життя» протоколам стану каналу.

2.2 Аналіз і вибір протоколу динамічної маршрутизації

2.2.1 Принципи динамічної маршрутизації

Протоколи динамічної маршрутизації можуть автоматично відстежувати зміни в топології мережі.

При використанні протоколів динамічної маршрутизації, адміністратор мережі конфігурує обраний протокол на кожному маршрутизаторі в мережі. Після цього маршрутизатори починають обмін інформацією про відомі їм мережах і їх станів. Причому маршрутизатори обмінюються інформацією тільки з тими маршрутизаторами, де запущений той же протокол динамічної маршрутизації. Коли відбувається зміна топології мережі, інформація про ці зміни автоматично поширюється по всьому маршрутизаторів, і кожен маршрутизатор вносить необхідні зміни в свою таблицю маршрутизації.

Показана на рисунку 2.7 мережу по-різному адаптується до змін топології, в залежності від того, який тип маршрутизації використовується: динамічна або статична.

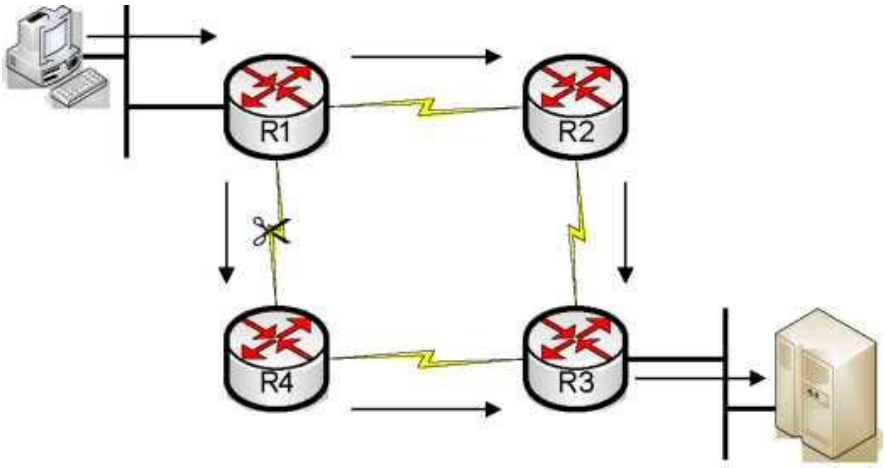


Рисунок 2.7. Динамічний маршрут

Статична маршрутизація дозволяє переслати пакет з однієї мережі в іншу, на основі вручну заданих маршрутів. В даному прикладі маршрутизатор R1 завжди пересилає потоки даних, призначені маршрутизатора R3, через маршрутизатор R4. Маршрутизатор звертається до своєї таблиці маршрутизації і відповідно розташованої в ній інформацією про статичному маршруті направляє пакет на вузол одержувач.

Якщо маршрут від маршрутизатора R1 до маршрутизатора R4 по якійсь причині ставати недоступним, то маршрутизатор R1 не може передавати пакет маршрутизатора R4 по ньому. Відповідно, до повторного ручного конфігурування маршрутизатора R1 на передачу пакетів через маршрутизатор R2 зв'язок з мережею одержувачем буде неможлива.

Динамічна маршрутизація забезпечує більшу гнучкість. У відповідно до таблицею маршрутизації, створеної на маршрутизаторі R1, пакет може бути доставлений до пункту призначення по більш кращого маршруту через маршрутизатор R4. Однак при цьому залишається доступним і другий шлях до пункту призначення - через маршрутизатор R2. Коли маршрутизатор R1 дізнається про те, що канал до маршрутизатора R4 вийшов з ладу, він відновить свою таблицю маршрутизації, роблячи маршрут через маршрутизатор R2 кращим маршрутом до пункту призначення. В цьому випадку маршрутизатори продовжують пересилання пакетів з резервного каналу.

Після того як маршрут між маршрутизаторами R1 і R4 відновитися, маршрутизатор R1 знову оновлює свою таблицю маршрутизації, віддаючи перевагу основним маршрутом через маршрутизатор R4.

Протоколи динамічної маршрутизації можуть також для підвищення ефективності роботи мережі застосовувати механізм балансування навантаження по декількох маршрутах.

2.2.2 Операції динамічної маршрутизації

Успішне функціонування динамічної маршрутизації залежить від виконання маршрутизатором двох його основних функцій при динамічної маршрутизації (рис. 2.8):

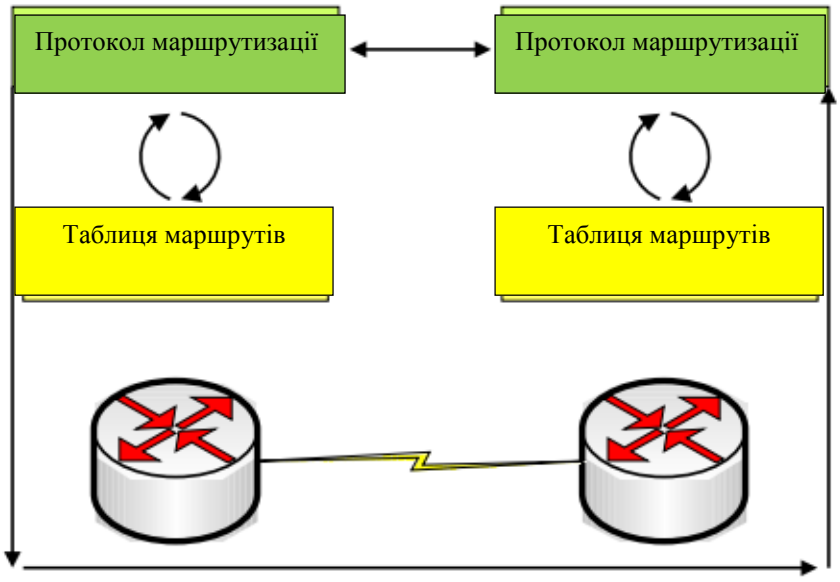


Рисунок 2.8. Протоколи маршрутизації підтримують інформацію про маршрути

Підтримка таблиці маршрутизації в актуальному стані;

- Своєчасне поширення інформації про відомі їм мережах і маршрутах серед інших маршрутизаторів.

При поширенні інформації про мережах механізм динамічної маршрутизації використовує один з протоколів маршрутизації. Такий протокол визначає набір правил, використовуваних маршрутизатором при здійсненні зв'язку з сусідніми маршрутизаторами. Протокол маршрутизації визначає:

- Яким чином поширюються поновлення маршрутів;
- Яка інформація міститься в оновленнях;
- Як часто розсилаються поновлення;
- Яким чином виконується пошук одержувачів оновлень.

Метрика маршруту або відстань до мережі також звана вартістю маршруту одна з головних складових інформації, що передається між маршрутизаторами про відомі їм маршрутах до мереж одержувачів. Кожен протокол маршрутизації має власні параметри і алгоритми розрахунку метрик маршрутів. Як параметри для розрахунку метрик маршрутів виступають: кількість переходів на шляху до мережі одержувача, швидкість передачі

даних по каналу зв'язку або більш складні метрики, в котрих беруться до уваги відразу кілька характеристик маршруту (Рисунок 2.9)

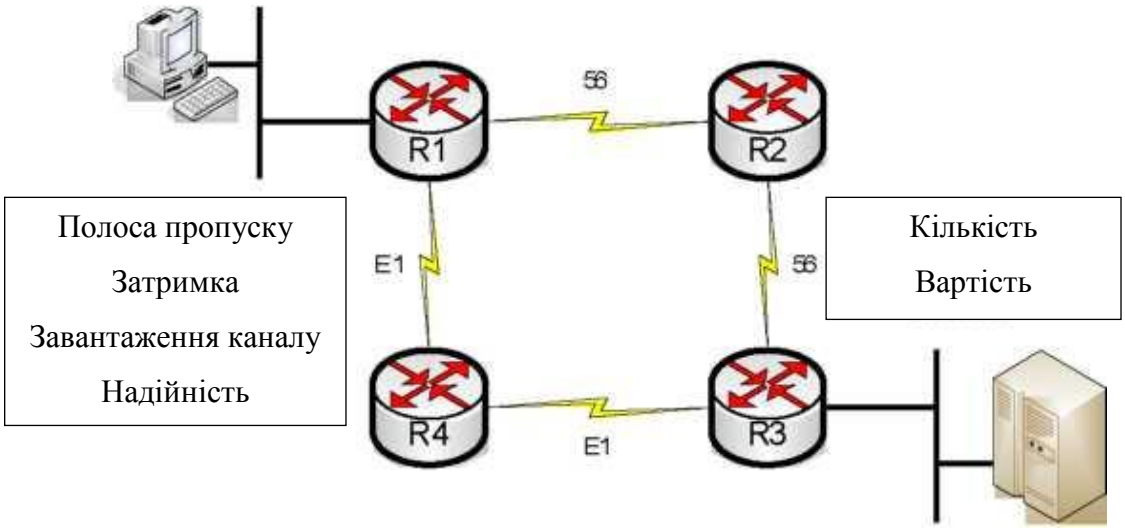


Рисунок 2.9. Метрики, що використовуються для визначення найкращого маршруту

Більшість протоколів маршрутизації ведуть бази даних про всі відомі їм мережах, а так само про всі відомі маршрутах до цих мереж. Якщо маршрутизатора відомо більше одного маршруту до мережі одержувача, то він порівнює метрики цих маршрутів і передає в таблицю маршрутизації маршрут з найменшою метрикою.

2.2.3 Вимоги мережі до протоколу маршрутизації

Як відомо, протоколи динамічної маршрутизації дозволяють маршрутизаторам IP-мереж автоматично створювати таблиці оптимальних (за обраним критерієм) маршрутів і динамічно модифікувати їх відповідно до змін, що відбуваються в топології мережі.

Вибір протоколу маршрутизації в значній мірі залежить від наступних факторів.

- Топологія і складність мережі.

Необхідно передбачити наявність резервних ліній зв'язку в мережі, що забезпечують її надійне функціонування (доступність серверів і мережевих сегментів) в разі відмов мережевого обладнання та основних ліній зв'язку. Наприклад, при деревовидної топології мережі з так званим «кореневим маршрутизатором», можливості динамічної маршрутизації зводяться до мінімуму.

- Розміри мережі і необхідність в її подальшому масштабування. Можливості деяких протоколів в цьому сенсі обмежені.

- Завантаженість мережі.

Для мереж з високим коефіцієнтом завантаженості ліній зв'язку має значення здатність протоколу до перерозподілу потоків даних.

- Вимоги до надійності мережі.

Допустимий час простоїв або нестабільності в роботі мережі через відмову її вузлів залежить від роду діяльності організації, і визначається можливими фінансові збитками або небезпекою порушення виробничого циклу.

- Вимоги до захисту інформації в мережі.

Ці вимоги визначаються ступенем ризику, пов'язаного з потраплянням інформації про адреси і маршрутах в мережі в руки зловмисників, що особливо важливо для мереж, що мають зовнішні канали зв'язку.

- Необхідність підключення маршрутизації сегмента до вже існуючої мережі.

В цьому випадку слід звернути увагу на сумісність протоколів маршрутизації і засобів їх реалізації.

- Можливість організації програмних маршрутизаторів.

При невеликому трафіку в мережі або на окремих її ділянках від маршрутизаторів не потрібна висока продуктивність. У таких випадках з економічної точки зору буває вигідніше використовувати замість апаратного маршрутизатора універсальний комп'ютер з декількома мережевими картами і програмним забезпеченням (ПЗ) з функціями протоколів маршрутизації. Однак не для всіх протоколів маршрутизації є відповідне ПО, а від складності протоколів залежить кількість споживаних обчислювальних ресурсів комп'ютера.

- Кваліфікація і суб'єктивні переваги обслуговуючого персоналу.

Складність налаштування маршрутизаторів і адміністрування мережі при використанні різних протоколів суттєво відрізняються. При наявності необхідних можливостей в декількох протоколах важливо врахувати зручність і наявність досвіду роботи з одним з протоколів в адміністратора мережі.

2.2.4 Аналіз протоколу RIP

Протокол RIP заснований на дистанційно-векторному алгоритмі і в більшості реалізацій використовує найпростішу метрику - кількість проміжних маршрутизаторів до мережі призначення. Головним достоїнством протоколу є легкість конфігурування, що не вимагає високої кваліфікації обслуговуючого персоналу. Протокол є відкритим і підтримується практично всіма виробниками мережевого обладнання. Також є реалізації

протоколу в ПО (наприклад, для Unix- подібних ОС - пакети Zebra, Quagga і ін.) І підтримка в ряді ОС (наприклад, в Windows, починаючи з Windows NT Server, в Unix-подібних, Cisco IOS). Основними недоліками протоколу є: повільна збіжність і великий обсяг службового трафіка (для адаптації до змін в топології мережі маршрутизатори періодично розсилають повні копії своїх таблиць). Це обмежило сферу застосування протоколу мережами з кількістю маршрутизаторів не більше п'ятнадцяти. В протокол RIP версії 2 добавлена підтримка маски змінної довжини, мультикастингова (багатоадресна) розсилка замість широкомовної і засоби захисту при обміні маршрутної інформацією у вигляді аутентифікації по ключу MD5 і відкритого (нешифрованого) тексту. Протокол досить поширений в не великих локальних мережах, які не прагнуть до розширення, з не високими вимогами до надійності мережі і відсутністю кваліфікованого персоналу мережевих адміністраторів. У новій версії протоколу Riping організована підтримка протоколу IPv6.

2.2.5 Аналіз протоколу IGRP

Закритий дистанційно-векторний протокол IGRP компанії Cisco Systems був спроектований для усунення ряду недоліків протокола RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з відмінними характеристики смуги пропускання і величини затримки. Протокол використовує комбіновану метрику, яка включає затримку, смугу пропускання, надійність і завантаженість маршруту. Вагові коефіцієнти, що визначають внесок цих характеристик в результуючу метрику, задаються користувачем, забезпечуючи гнучку адаптацію до його конкретним завданням. Показники затримки і смуги пропускання конфігуруються для кожної лінії зв'язку попередньо, а показники надійності і завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі. Для підтримки вимог QOS різних додатків можна підготувати кілька маршрутних таблиць, побудованих на основі метрик з різними значеннями вагових коефіцієнтів.

Протокол IGRP забезпечує швидшу збіжність, ніж RIP завдяки застосуванню пакетів оновлення з миттєвою розсилкою (інформація про зміни в мережі відправляється відразу, як тільки стає доступною, не чекаючи чергового часу поновлення). Протокол підтримує балансування навантаження між декількома маршрутами навіть в тому випадку, якщо їх метрики не рівні, але знаходяться в межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів відправлених по кожній колії даних буде пропорційно співвідношенню їх метрик.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини і можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні кошти аутентифікації при обміні маршрутною інформацією. Непрямим засобом захисту є можливість прийому повідомлень про оновлення маршрутів тільки від тих маршрутизаторів, які даний — визначає як «сусідні», а також можливість внесення змін в конфігурацію маршрутизатора тільки на підставі пароля, який зберігається в зашифрованому вигляді. Протокол сумісний з RIP.

2.2.6 Аналіз протоколу EIGRP

Протокол EIGRP компанії Cisco Systems є покращеною версією вихідного протоколу IGRP. Протокол є гібридним і заснований на алгоритмі поновлення Diffusing-Update Algorithm (DUAL). Він поєднує в собі кращі сторони дистанційно-векторних протоколів (простота алгоритму вибору оптимального маршруту) і протоколів стану каналів зв'язку (швидка збіжність і економія смуги пропускання мережі за рахунок повідомлень тільки про стан зв'язків і про їх зміни). Всі розсилки протоколу є мультикастними або індивідуальними. Таким чином, інформація розсилається тільки при змінах, і тільки тим маршрутизаторам, яких вона стосується. З метою підвищення масштабованості протоколу в нього додана підтримка масок підмереж змінної довжини і можливість об'єднання маршрутів. Маршрути діляться на внутрішні і зовнішні - отримані від інших протоко¬лов маршрутизації або записані в таблиці статично.

В останніх версіях EIGRP є засоби захисту, які не дозволяють зловмисникам дописувати елементи в таблицю маршрутизації, і аутентифікація по ключу MD5. Крім того, в даний час для EIGRP розробляють засоби підтримки IPv6, так що цей протокол буде розвиватись й надалі.

Основним недоліком EIGRP, як і його попередника, є закритість і реалізація тільки на обладнанні Cisco Systems.

Протокол добре сумісний з IGRP, а також з RIP.

2.2.7 Аналіз протоколу OSPF

Найбільш універсальним і гнучким у налаштуванні протоколом динамічної маршрутизації, в корпоративних мережах, на сьогодні, — є відкритий протокол вибору першого найкоротшого шляху (Open Shortest Path First Protocol - OSPF). Протокол

спочатку був орієнтований на роботу в великих мережах (до 65536 маршрутизаторів) зі складною топологією. Він заснований на алгоритмі стану каналів зв'язку і має високу стійкість до змін топології мережі і швидкої збіжністю. При виборі маршруту використовується метрика пропускної здатності складовою мережі (тобто передача даних по найбільш швидкісних каналів зв'язку). Протокол може підтримувати різні вимоги IP-пакетів на якість обслуговування (пропускна здатність, затримка і надійність) за допомогою побудови окремої таблиці маршрутизації для кожного з цих показників.

Протокол володіє і іншими достоїнствами, корисними в великих сучасних мережах. До них відносяться можливість балансування навантаження між каналами з рівними метриками і засоби аутентифікації як по нешифрований паролю, так і по шифрованому (шляхом додавання до пакету дайджесту ключа і тіла пакета за алгоритмом MD5). Нумерація пакетів виключає їх повторюваність і таким чином можливість повторної атаки. Відкритість протоколу визначає його підтримку практично всіма виробниками мережевого устаткування, реалізації в ПО під все популярні ОС (наприклад, для Unix-подібних ОС - пакети Zebra, Quagga і ін.), А також безпосередню інтеграцію в ряд ОС (наприклад, Windows 2000 Server і вище, OpenBSD, Cisco iOs, Solaris 10 і т.п.).

До недоліків проколу слід віднести високу обчислювальну складність і, отже, високі вимоги, що пред'являються до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає зі збільшенням розмірів мережі. Тому для збільшення масштабованості протоколу застосовується поділ мережи на логічні області, з'єднані магістральною областю. Внутрішня топологічна інформація між областямі не віддається. Скорочення обсягів таблиць маршрутизації і зниження службового трафіку при оновленні топологічної інформації служить можливість об'єднання декількох адрес мереж в один при виявленні у них загального префікса, і заміна широкомовних розсилок мульти-кастинговими. З метою економії IP-адрес в з'єднаннях типу «точка - точка» між маршрутизаторами призначати кінцевим точкам адреси не обов'язково. Платою за ці переваги є складність конфігурування і необхідність ретельного попереднього планування мережі для її оптимальної роботи (розбивка на області, виділення магістралі, розподіл функцій між маршрутизаторами з урахуванням їх обчислювальної потужності: рядові, виділені в зоні, прикордонні і т . п.).

В якості перспективних функцій OSPF слід назвати підтримку протоколу Ipv6 і можливість вибору маршруту на підставі поточного коефіцієнта завантаженості каналів зв'язку (розширена версія OSPF отримала назву Constrained Shortest Path First - CSPF).

Протокол сумісний з RIP.

2.2.8 Аналіз протоколу IS-IS

Протокол IS-IS заснований на алгоритмі стану каналів зв'язку і є попередником OSPF. В даний час цей протокол дуже рідко використовується в корпоративних мережах. Це викликано повною перевагою над ним протоколу OSPF, який, по суті, є вдосконаленим IS-IS. До недоліків протоколу відноситься його нездатність підтримувати маски підмереж змінної довжини, об'єднувати маршрути, а також широкомовний характер розсилок сусіднім маршрутизаторам. Все це негативно впливає на швидкість збіжності, навантаження маршрутизаторів і завантаженість ліній зв'язку.

2.2.9 Аналіз протоколу BGP

BGP-4. Протокол BGP розроблявся як зовнішній для організації маршрутизації між автономними системами в глобальній мережі Internet (максимальне число маршрутизаторів 65534 між AS). В даний час в Internet використовується 4-я версія протоколу BGP-4. Хоча протокол відноситься до зовнішніх протоколів маршрутизації, його іноді застосовують і для внутрішньої маршрутизації.

BGP є протоколом, що орієнтується на вектор відстані. Однак, на відміну від RIP і IGRP протокол BGP не вимагає періодичного оновлення всієї маршрутної таблиці. Обмін повними таблицями виконується між маршрутизаторами тільки при їх початковому підключенні. Надалі відсилаються тільки повідомлення про оновлення в таблицях, причому тільки тим маршрутизаторам, які явно вказані в якості сусідніх. В одному оновленні BGP-4 може бути оголошено про одне новий маршрут або анулювання декількох перестали існувати. Все це сприяє зниженню службового трафіку.

Метрика BGP є довільне число одиниць, характеризують ступінь переваги конкретного маршруту, і встановлюються адміністратором мережі, в основному виходячи з міркувань договірних і фінансових переваг, можливо, з обліку інших факторів (за замовчуванням на підставі мінімального числа проміжних AS). У раз¬них маршрутизаторів може використовуватися різна маршрутна політика.

Хоча BGP підтримує маршрутну таблицю всіх можливих шляхів до конкретної мережі, в своїх повідомленнях про коригування він оголошує тільки про оптимальні маршрути. Наявність в таблиці альтернативних маршрутів прискорює реакцію маршрутизатора на інформацію про недосяжність основного шляху, а також дозволяє підтримувати балансування навантаження. Оскільки протокол орієнтований на обмін даними між різними AS, де при виборі маршрутів переважають, як правило, не технічні, а

політичні міркування, то процес балансування навантаження на увазі осмислене розподіл маршрутів між альтернативними каналами за допомогою настройки відповідних параметрів протоколу.

Повідомлення BGP-4 про коригування містять послідовність AS, через які може бути досягнута зазначена мережа, її IP-адреса і довжина маски префікса (підтримується тільки безкласова адресація CIDR). Протокол дозволяє об'єднувати маршрути. Перелік AS використовується для поліпшення збіжності, швидкість якої у протоколу не висока.

Для забезпечення безпеки можуть застосовуватися різні способи аутентіфікаціі маршрутизаторів.

Протокол сумісний з RIP і OSPF.

У Додатку таблиці А.2 представлена порівняльна характеристика основних про-протоколі динамічної маршрутизації.

Важливою характеристикою протоколу маршрутизації є швидкість збіжності. Цей критерій не був включений в таблицю через відсутність чисельних даних коректно проведених експериментів для мереж різного масштабу. Виходячи з аналізу самих алгоритмів і заяв розробників компанії Cisco Systems, можна сказати, що дистанційно-векторний протокол RIP поступається за цим параметром вдосконаленому протоколу IGRP. Ще більшою швидкістю збіжності має комбінований протокол EIGRP, який наближається до найбільш швидкісним протоколам OSPF і IS-IS, заснованим на алгоритмі обліку стану каналів зв'язку. Протокол BGP не відноситься до числа швидкісних, як через дистанційно векторного алгоритму, так і з огляду на його особливостей, пов'язаних з роботою в якості зовнішнього протоколу (різна маршрутна політика маршрутизаторів, використання надійного транспортного протоколу TCP і т.п.).

2.2.10 Результати порівняльного аналізу

Порівняльна характеристика показує, що найбільш досконалими внутрішніми протоколами динамічної маршрутизації є OSPF і EIGRP. Протокол IS-IS по суті є більш ранній і менш функціональної версією протоколу OSPF, тому в даний час рідко використовується в корпоративних мережах. Переваги цих протоколів в повній мірі проявляються в складних великих мережах з сотнями і тисячами маршрутизаторів. Саме тут необхідна висока швидкість збіжності оптимальних маршрутів, гнучкість при виборі шляхів (з урахуванням різних характеристик, що складають маршрути каналів), підтримка вимог QoS для різних видів трафіку, економія смуги пропускання каналів (за рахунок зниження службового трафіку), зниження розмірів таблиць маршрутизації і швидкості

пошуку в них інформації. Ці вимоги виправдовують використання продуктивних апаратних маршрутизаторів з великими обсягами пам'яті і протоколів, що вимагають складної настройки. Однак такі великі мережі сьогодні є гетерогенними з точки зору виробників мережевого устаткування, тому лідируючі позиції тут займає відкритий протокол OSPF (EIGRP реалізується тільки на обладнанні Cisco Systems, і максимальну кількість маршрутизаторів не більше 255).

Для мереж середнього розміру (десятки маршрутизаторів) при наявності відповідних фінансових можливостей надійність і додаткові технічні переваги устаткування фірми Cisco Systems можуть зіграти вирішальну роль на користь побудови однорідної мережі. Тоді найбільший ефект дасть використання протоколу EIGRP. Оскільки лежить в його основі алгоритм DUAL піддається гнучкою налаштування (комбінована метрика, балансування навантаження шляхів з різними значеннями метрики), це дозволяє адміністратору мережі забезпечувати її максимальну продуктивність, оскільки добре відомо, що перед мережею можуть ставиться найрізноманітніші завдання, і тільки великі функціональні можливості і гнучкість їх використання допоможуть адміністратору вирішити будь-яке поставлене завдання. Хоча цілком можливо, що і можливостей більш простого в налаштуванні протоколу IGRP буде досить (наприклад, якщо не пред'являються високі вимоги до часу збіжності оптимальних маршрутів, зниження рівня службового трафіку і його безпеки, не потрібна підтримка масок підмереж змінної довжини і функції агрегування маршрутів).

Для гетерогенних мереж, особливо при наявності в них програмних маршрутизаторів, кращим вибором буде протокол OSPF. Оскільки при використанні EIGRP виникає проблема взаємодії обладнання, то маршрутизаторів від інших виробників залишається використовувати статичні маршрути, або мати справу з комбінацією RIP і EIGRP, що видається не дуже осмисленим.

Якщо відповідно до високих вимог до надійності, захищеності, продуктивності невеликої мережі (до десятка маршрутизаторів) для неї буде обрано обладнання Cisco, тоді, швидше за все, додаткові можливості EIGRP, пов'язані зі зменшенням часу збіжності і підвищенням масштабованості, не знадобляться. І прокол IGRP вирішить завдання такої мережі досить ефективно. Цей протокол найбільш зрозумілий мережевим адміністраторам, вже знайомим з RIP, а також для досягнення належної продуктивності вимагає від маршрутизаторів меншого обсягу оперативної пам'яті і менш потужний процесор.

Тут слід зазначити існування великої кількості організацій, для яких робота в мережі не є безпосереднім елементом їх основної діяльності, а є швидше за все засобом

комунікації. Рівень трафіку в таких мережах зазвичай не високий, тому можливості протоколу, пов'язані з балансуванням навантаження, зниженням службового трафіку за рахунок ієрархічної організації та розсилки тільки оновлень швидше за все виявляться незатребуваними. Такі організації зазвичай не пред'являють високі вимоги до мережі, тобто не вимагають високої швидкості збіжності, підтримки QoS, обліку в метриці характеристик різнорідних каналів (як правило, всі канали типу Fast Ethernet), часто використовують програмні маршрутизатори на не надто продуктивних ПК, і не бажають утримувати високооплачувані кадри кваліфікованих адміністраторів. У цих випадках найпростіший протокол RIPv2 буде цілком достатнім рішенням.

Протокол BGP розроблявся як протокол взаємодії між автономними системами Internet. Він має довільну метрику і невисоку швидкість збіжності. Його впровадження в корпоративну мережу в більшості випадків не виправдається. Розподіл мережі на автономні системи не дає істотної переваги. Прикордонні протоколи зазвичай потрібні тільки в тому випадку, коли мережа організації пов'язана з однією і тією ж зовнішньою мережею (наприклад Internet) декількома каналами або, коли вона працює як проміжна ланка між двома або більше мережами, причому необхідно забезпечити резервні канали зв'язку (типова ситуація для сервіс-провайдера Internet).

Таким чином, вибір конкретного протоколу динамічної маршрутизації залежить від розмірів і вимог, які висуваються конкретною корпоративною мережею. Грунтуючись на даних таблиці, можна з упевненістю сказати, що на сьогоднішній день найбільш досконалими внутрішніми протоколами динамічної маршрутизації є OSPF і EIGRP. Їх перспективність підтверджує і впровадження підтримки перспективного протоколу IPv6. І, якщо OSPF вже став фактично стандартним внутрішнім протоколом Internet, то з ростом ринку обладнання фірми Cisco Systems позиції EIGRP в однорідних корпоративних мережах будуть зміцнюватися. Протокол IGRP, мабуть, також поступиться йому своє місце. Проте, переваги простоти протоколу RIP для невеликих мереж продовжують залишатися затребуваними, про що, наприклад, свідчить поява нової версії протоколу Riping, в якій також передбачена підтримка протоколу IPv6.

2.3 OpenFlow

OpenFlow - протокол управління процесом обробки даних, що передаються по мережі передачі даних маршрутизаторами і комутаторами, який реалізує технологію програмно-конфігурується мережі.

Протокол використовується для управління мережевими комутаторами і маршрутизаторами з центрального пристрою - контролера мережі (наприклад, з сервера або навіть персонального комп'ютера). Це управління замінює або доповнює працюючу на комутаторі (маршрутизаторі) вбудовану програму, яка здійснює побудова маршруту, створення карти комутації і т. Д .. Контролер використовується для управління таблицями потоків комутаторів, на підставі яких приймається рішення про передачу прийнятого пакета на конкретний порт комутатора. Таким чином в мережі формуються прямі мережеві з'єднання з мінімальними затримками передачі даних і необхідними параметрами.

Версії мікропрограм з підтримкою Openflow розроблені для пристроїв багатьох виробників, включаючи Extreme Networks, Juniper, Cisco, HP, IBM, NEC.

Стандарт OpenFlow в першому промислово доступному варіанті, 1.0, став доступний в складі залізних свічів, але ця версія мала кілька архітектурних обмежень, які перешкоджали масовому впровадженню, і найбільш проблемне з них - відсутність множинних послідовних таблиць для обробки, тобто одне правило відповідало рівно одній парі взаимодействовавших кінцевих точок, без урахування додаткових збігів. Використання OpenFlow 1.0 проактивним чином (тобто зі створенням всіх необхідних правил заздалегідь) вело б до квадратичного росту числа правил від числа взаємодіючих хостів.

Частковим виходом із ситуації є використання механізму learning switch - тобто реактивної роботи OpenFlow свіча, коли правила запитуються кожен раз, коли вони не збігаються ні з одним, вже поміщеним в таблицю форвардинга свіча, а через певний TTL - видаляються з свіча. Стратегія видалення може бути як «жорсткої» - видалення через заданий проміжок часу після установки правила, так і «м'якої» - видалення відбувається тільки під час відсутності активності за заданий проміжок часу «всередині» конкретного потоку.

Модель learning switch виправдовує себе на значній кількості навантажень. Непереборною перешкодою для неї стають лише додатки, на зразок лічильників, які генерують сотні і тисячі унікальних запитів в секунду на рівні свіча. Також вона схильна до атаки швидкого спуфинга - клієнт, що генерує пакети з унікальними IP / MAC ідентифікаторами, як мінімум, здатний привести в неробочий стан свіч рівня обчислювальної Ноди, а якщо заздалегідь не подбати про обмеження PACKET_IN (повідомлень на обробку потоку для контролера), то і цілий сегмент мережі.

Підтримка сучасних стандартів OpenFlow виробниками доступного мережевого обладнання ToR в форматі whitebox на сьогоднішній день обмежується рішеннями на базі

Windriver (Intel), Cumulus (Dell) і Debian в Свіча Pica8, всі інші вендори або надають свічі більш високої цінової категорії, або зловживають своїми несумісними розширеннями / механізмами.

Сьогодні відкриті платформи Intel ONS або Dell (базовану на Trident II), при досить скромною ціною (<10 000 $ за 4 * 40G + 48 * 10G), дозволяють управляти трафіком декількох десятків тисяч віртуальних машин в масштабі однієї промислової стійки з 1-6 Тб пам'яті, використовуючи OpenFlow (1.3+).

2.3.1 Аналіз апаратних платформ

Bare-metal

Термін «Bare-metal» означає, що в комутаторі немає нічого, крім самого «заліза». На ньому не встановлено ніякої мережевої ОС, це просто коробка з набором Ethernet-портів. За замовчуванням, в таких комутаторах є лише boot loader (наприклад, Open Network Install Environment (ONIE)), за допомогою якого проводиться завантаження мережевий ОС.

Bare-metal обладнання, в основному, проводиться тайванськими виробниками, такими як Accton (Edge Core), Quanta QCT і Alpha Networks. Ці компанії часто називаються ODM (Original Device Manufacturer) виробниками. У список можна додати Corsa, Noviflow, Centec і Netronome.

Для кінцевого користувача Bare-metal комутатор - річ досить марна, адже його не вийде використовувати без софту.

White-box

White-box комутатор - Bare-metal комутатор з попередньо встановленою мережевий ОС. Подібні рішення в основному пропонують стартапи - Cumulus Networks, Big Switch Networks, Pica8 і ін. Ці компанії купують Bare-metal комутатори у ODM-виробників, завантажують на них свою ОС, наклеюють бирку з брендом і продають. Заробляють на продаж ПЗ і підтримки готового продукту - повнофункціонального комутатора.

Ось приклади мережевих ОС вищеназваних виробників:

Linux Operating System від Cumulus;

PicOS від Pica8;

SwitchLight OS від Big Switch.

Brite-box

Brite-box розшифровується як Branded white-box, тобто «Брендований» white-box. Термін придуманий Gartner і описує ще одну модель продажу white-box обладнання.

Наведемо приклад. Великі компанії HP і Dell пропонують white-box комутатори під своїми марками, але фактично - це те ж саме bare-metal обладнання плюс ПО від Cumulus, Pica8 і інших постачальників мережевих ОС. У випадку з Dell потрібно зробити невелику обмовку: вендор пропонує як сторонні мережеві ОС, так і власну - Dell OS10.

Купівля Brite-box комутатора - це всього лише більш комфортні умови для покупця, який отримує підтримку від великого вендора. Для простоти, далі ми будемо використовувати термін «white-box» для опису всіх трьох типів комутаторів.

2.3.2 Побудова системи мережевої безпеки на базі OpenFlow.

Контролер фактично централізує цю функцію теж (у вигляді спеціалізованого додатки) і, потенційно, забирає на себе весь інтелект firewall-ів, IPS-ів та інших традиційних систем мережевого захисту.

– У цьому плані ідеологія SDN, з точки зору мережевих пристроїв, цілком «диктаторська». «Чи думають» за комутатори і вирішують якісь пакети куди передавати SDN-контролери. Комутатора відводиться роль простого виконавця. Рішенням складних мережевих завдань (типу захисту від петель або забезпечення безпеки) займаються спеціалізовані додатки в централізованій контрольної площині на контролерах.

– ідеологія SDN дозволяє спростити самі мережеві пристрої до межі (фактично, до підтримки протоколу управління для зв'язку з контролером і базових функцій комутації), зробити їх слабкими, а значить і дешевими.

(Це, в кінцевому підсумку, може кардинально знизити OPEX, який не дає спокійно спати всім власникам IT бюджетів.)

Операційні витрати або операційні витрати (англ. OPEX, скор. Від operating expenses) - повсякденні витрати компанії для ведення бізнесу, виробництва товарів і послуг.

– Компанія HP була піонером у розробці SDN технологій і однією з перших вийшла на ринок з працюючим рішенням OpenFlow.

OpenFlow - протокол управління процесом обробки даних, передаю-трудящих через мережу передачі даних маршрутизаторами і комутаторами, який реалізує технологію програмно-конфігурується мережі.

Протокол використовується для управління мережевими комутаторами і маршрутизаторами з центрального пристрою - контролера мережі (наприклад, з сервера або навіть персонального комп'ютера). Це управління замінює або доповнює працюючу на

комутаторі (маршрутизаторі) вбудовану програму, яка здійснює побудова маршруту, створення карти комутації і т. п. Контролер використовується для управління таблицями потоків комутаторів, на підставі яких приймається рішення про передачу прийнятого пакета на конкретний порт комутатора. Таким чином в мережі формуються прямі мережеві з'єднання з мінімальними затримками передачі даних і необхідними параметрами.

HP одним з перших випустив комерційний продукт, що підтримує протокол OpenFlow. При цьому, комутатори HP, що підтримують OpenFlow, гібридні, тобто підтримують роботу одночасно в двох режимах - OpenFlow плюс традиційна комутація.

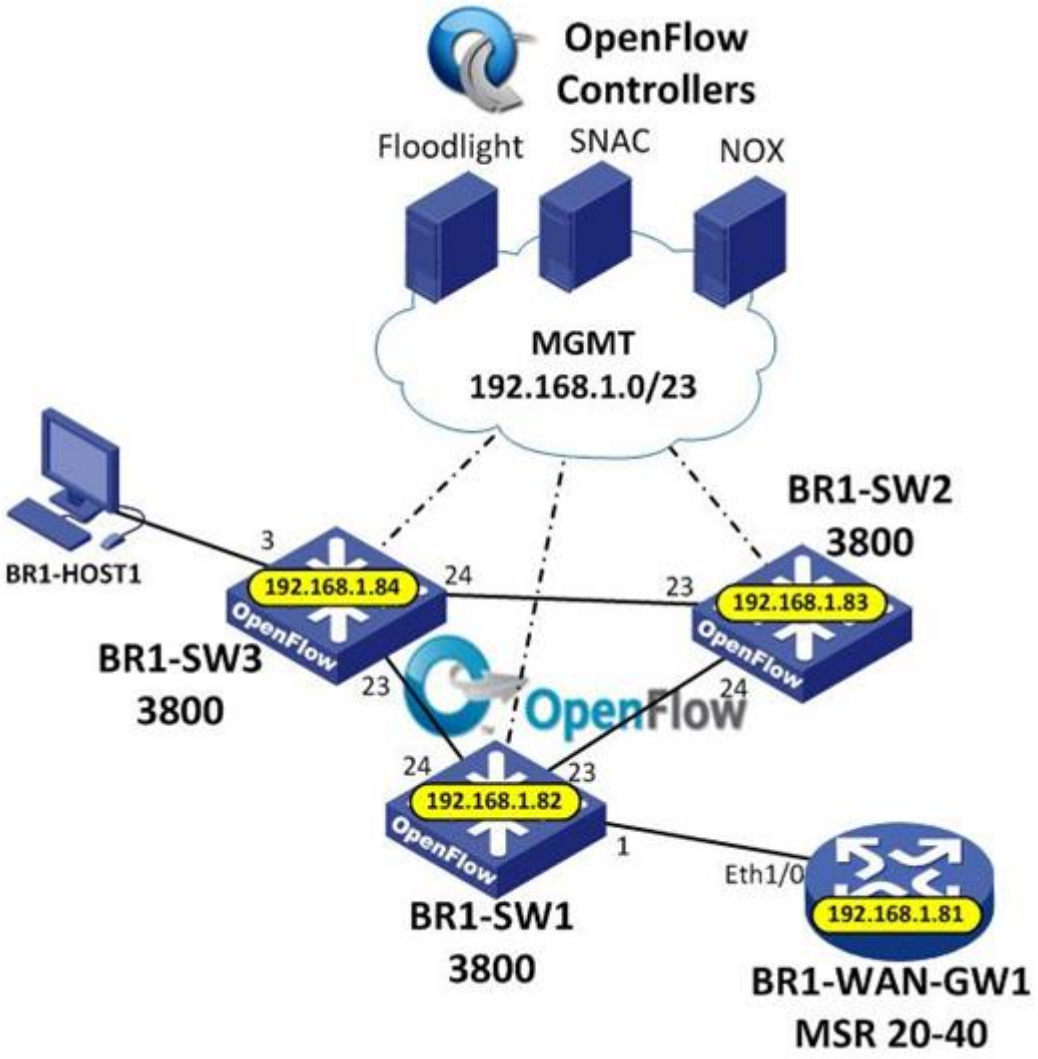


Рисунок 2.10. Приклад, трьох комутаторів HP серії 3800, об'єднаних в кільце.

В якості контролерів зібрані кілька варіантів - Floodlight, SNAC і NOX. У цьому прикладі на комутаторах налаштовані два контролера - SNAC і Floodlight, ось так:

```
openflow
enable
controller-id 1 ip 192.168.2.10 controller-interface oobm
```

```
controller-id 2 ip 192.168.2.11 controller-interface oobm
```

У OpenFlow налаштовані два instance-а, кожен з яких пов'язаний з окремим контролером, який управляє трафіком в окремому VLAN-е. У цьому прикладі контролер SNAC налаштований на управління трафіком в VLAN 3, контролер Floodlight налаштований на управління трафіком в VLAN 4, ось так:

```
instance "snac"
member vlan 3
controller-id 1
limit software-rate 10000
connection-interruption-mode fail-standalone
max-backoff-interval 10
enable
exit
instance "floodlight"
member vlan 4
controller-id 2
limit software-rate 10000
connection-interruption-mode fail-standalone
enable
exit
hardware-statistics refresh-rate 10
```

В керовані через OpenFlow VLAN-и заведені певні порти, ось так:

```
vlan 3
name "SNAC"
untagged 1/3,1/13
tagged 1/1,1/23-1/24
no ip address
exit
vlan 4
name "FLOODLIGHT"
untagged 1/4,1/14
tagged 1/1,1/23-1/24
no ip address
exit
```

Налаштування OpenFlow на комутаторах закінчено.

Далі можна побачити, що контролер визначив комутатори і ми можемо їх зареєструвати.

У веб-інтерфейсі SNAC-а це виглядає так:

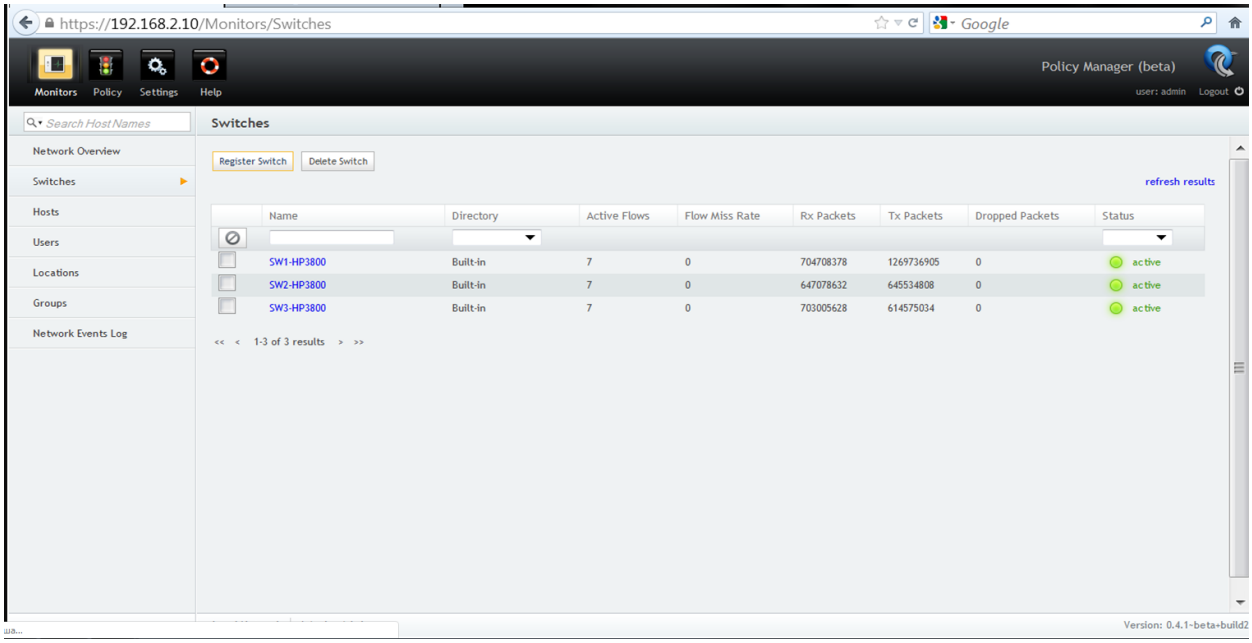


Рисунок 2.11. Вікно реєстрації контролерів

Потім, як тільки з'являється реальний трафік на портах, керованих через OpenFlow, контролер бачить джерела, з яких йде трафік:

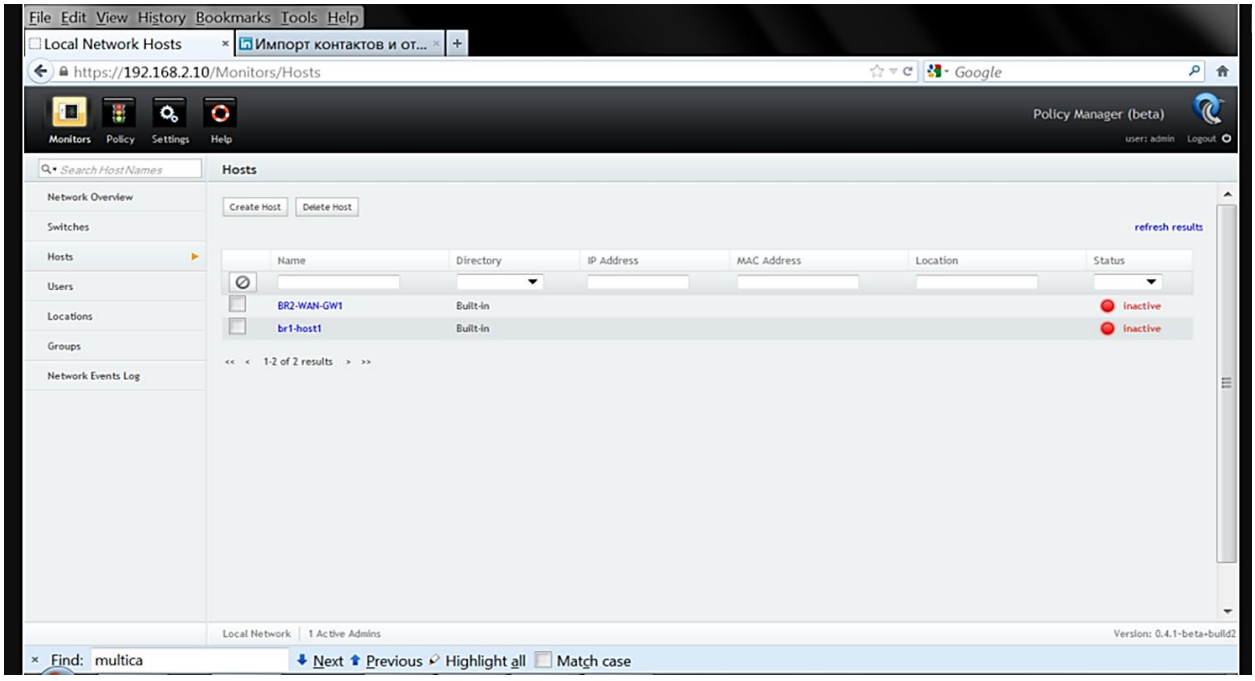


Рисунок 2.12. Джерела, з яких йде трафік

На основі зроблених налаштувань, контролер передасть в комутатор інформацію про потоках трафіку, які комутатор повинен обробляти. Віддані на комутатор потоки (flow) в CLI комутатора можна подивитися:

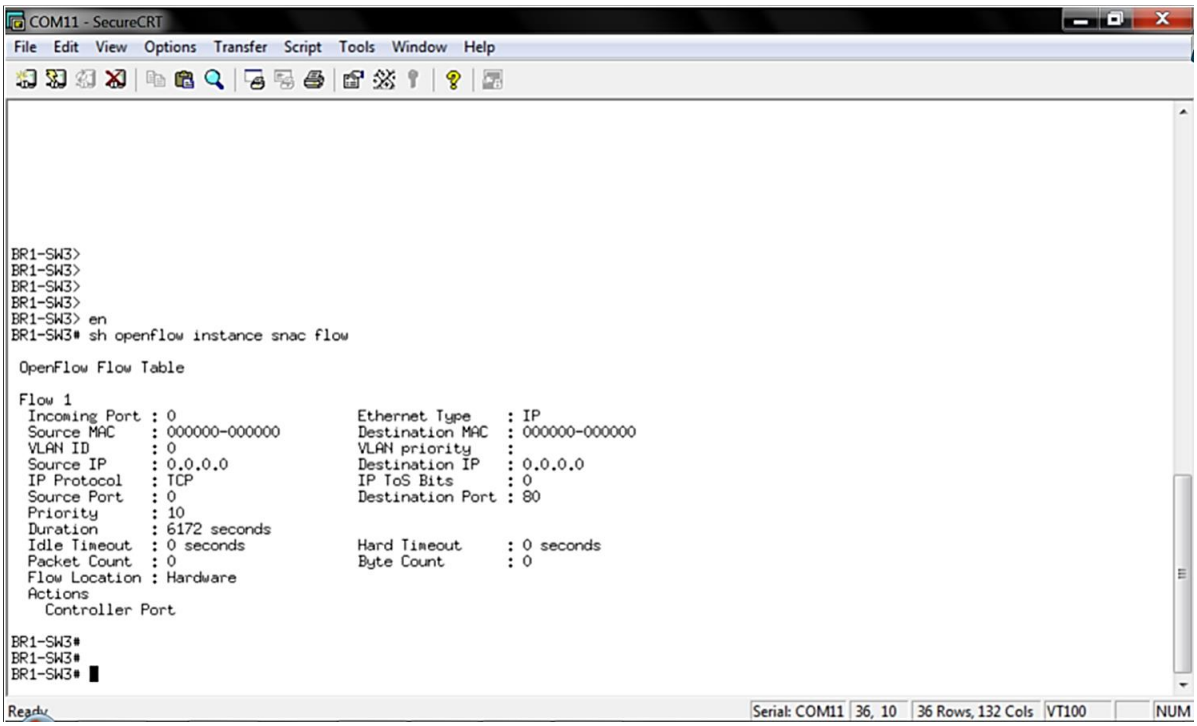


Рисунок 2.13. Віддані на комутатор потоки

Далі, до трафіку можна застосовувати різноманітні правила. Наприклад, в контролері SNAC є закладка, де можна застосовувати політики доступу за різними параметрами (src / dst MAC, src / dst IP, TCP порти, і т.п):

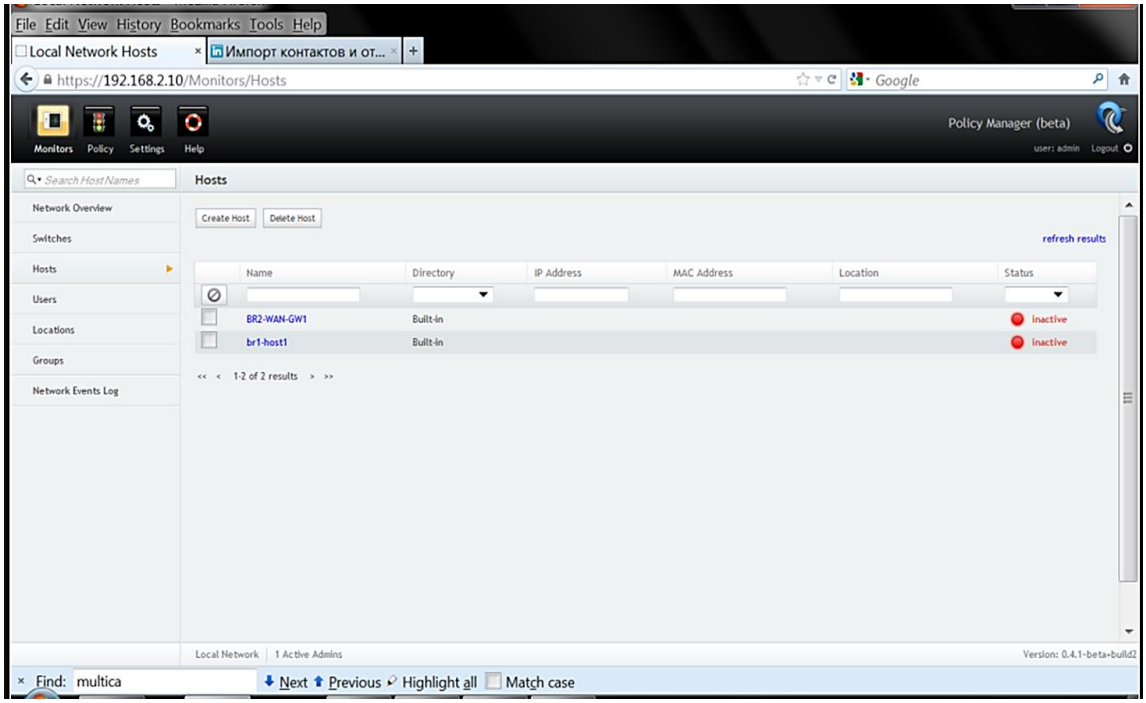


Рисунок 2.14.- Вікно налаштування політик

Можна подивитися топологію мережі, в Floodlight:

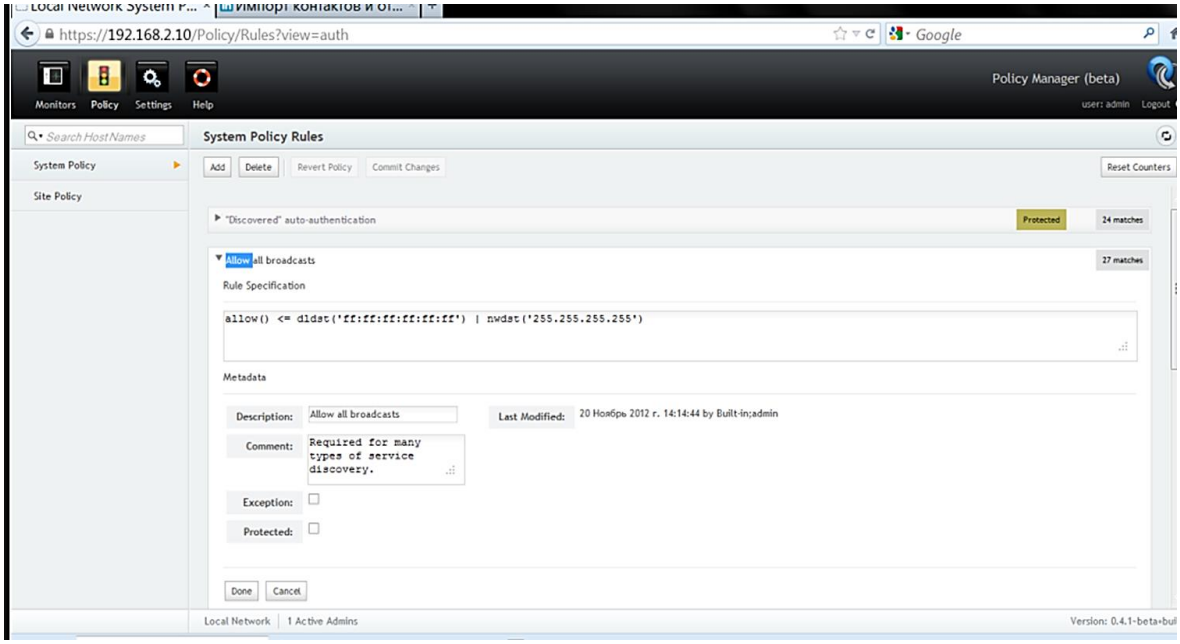


Рисунок 2.15. Інформація про топологію мережі

Можна подивитися різну статистику по потокам, історію подій, що відбувалися (хто реєструвався в мережі і т.п.), в SNAC ця закладка виглядає так:

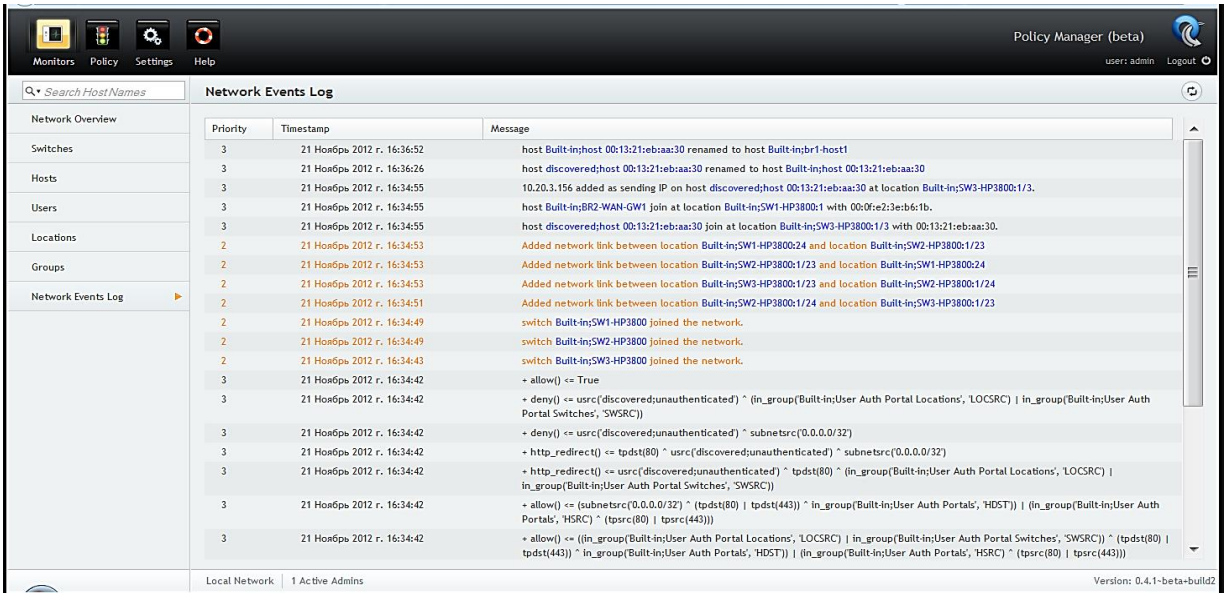


Рисунок 2.16. Статистика по потокам

Ми бачимо, що весь інтелект мережі, керованої через OpenFlow, розміщується тепер на контролерах, де і вирішується вся мережева політика.

2.4 Аналіз контролерів

Результати порівняння контрорлерів наведено у табл. 2.4.

Таблиця 2.4 - Коротке порівняння найчастіше використовуваних контролерів.

Постачальник	контролер	Устаткування для центрального офісу	Устаткування для філій	Особливості
ЦПІКС	Runos	Комутатори типу white box або комутатори на основі серверів x86		Вітчизняний контролер SDN
Brocade	Brocade SDN Controller (BSC)	Комутатори ICX 7750, ICX 7250; програмний маршрутизатор Brocade vRouter 5600	Комутатори ICX 7250; програмний маршрутизатор Brocade vRouter 5600	Архітектура SwitchPort Extender - «розподілене шасі»
Cisco	Cisco APIC-EM	Комутатори серії Cisco 2960 або 3650/3850; маршрутизатори Cisco ISR 4451	Комутатори серії Cisco 2960 або 3650/3850; маршрутизатори Cisco ISR 4431	Компанія планує поставляти APIC-EM безкоштовно з набором вбудованих мережевих додатків
Extreme Networks	One Controller	Комутатори Extreme Networks модельного ряду Summit і Black Diamond або будь-які інші комутатори з підтримкою протоколу Openflow v.1.0 і вище		Можливе використання будь-яких комутаторів з підтримкою протоколу Openflow v.1.0 і вище
HP Enterprise	HP VAN SDN Controller	Комутатори HP 5406R zl2, HP 3800, HP 5900CP; маршрутизатори HP MSR3044	Комутатори HP 2920 або HP 5406R zl2; маршрутизатори HP MSR3012	Широкий вибір SDN-додатків в HP SDN App Store
Huawei	Agile Controller	Комутатори S7700 і S5700; маршрутизатори AR2240	Комутатори S5700; маршрутизатори AR1200	Технології Super Virtual Fabric (SVF); Protocol Oblivious Forwarding (POF); процесори Ethernet Network Processor (ENP)
NEC	NEC PF6800	Комутатори NEC (серій PF52xx, PF53xx і PF54xx) або інших виробників, що відповідають стандартам OpenFlow 1.0 і / або OpenFlow 1.3		Прихильність стандартам OpenFlow, підтверджена сумісність з великим числом комутаторів інших виробників

2.4.1 «Сердце» SDN

Головним елементом будь-якого рішення SDN, безумовно, є контролер. З мережевою інфраструктурою контролер взаємодіє через «південні» інтерфейси, основний з них - OpenFlow. Шість з семи представлених контролерів підтримують зазначений протокол. Виняток становить тільки контролер APIC-EM компанії Cisco. На момент підготовки матеріалу в якості «південного» API на цьому контролері був доступний тільки Cisco CLI (відповідно, і працювати він міг тільки з комутаторами і маршрутизаторами Cisco). Однак уже в наступних версіях ПО APIC-EM запланована підтримка обладнання інших виробників або комутаторів без попередньо встановленою ОС (bare-metal switch) за рахунок використання OpenFlow і Cisco OnePK.

Загальний підхід Cisco полягає в поділі мережі замовника на логічні домени (ЦОД, WAN, кампус, сервісна інфраструктура і т. Д.) І використанні для кожного домена (або груп доменів) спеціалізованого SDN-контролера, найбільш ефективно вирішального стандартні для обраного домену завдання. Для забезпечення наскрізного сервісу, що вимагає взаємодії кількох інфраструктурних доменів, Cisco поставляє рішення по оркестрації (Network Service Orchestrator, NSO). Для поставленої задачі Cisco запропонувала контролер APIC-EM (Application Policy Infrastructure Controller - Enterprise Module), спеціально розроблений для корпоративних кампусних і розподілених (WAN) мереж. Це ідеологічний і технологічний спадкоємець контролера APIC, використовуваного в рамках архітектури Cisco Application Centric Infrastructure (ACI) для управління інфраструктурою ЦОДа.

Контролер APIC-EM реалізує функціональність управління мережевими елементами, залишаючи всі інші завдання зовнішнім системам управління і сторонніх додатків, які взаємодіють з APIC-EM через «північний» програмний інтерфейс REST.

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

Є підтримка протоколу OpenFlow і в компанії Huawei. При цьому Huawei створила розширення стандарту OpenFlow - технологію Protocol Oblivious Forwarding (POF), назад сумісну з OpenFlow. Цей підхід забезпечує можливість використовувати як OpenFlow, так і традиційні механізми маршрутизації для передачі і управління трафіком. Таким чином,

замовник може здійснити плавний перехід до SDN. Подібну міграцію пропонують і інші компанії (див. Нижче).

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

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

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

У контролерах Runos, відмітними особливостями, за твердженням представників ЦПІКС, є висока продуктивність (пропускна здатність 8 млн подій в секунду, затримка на обробку одного запиту 30 мкс) і зручність розробки. Проект Runos знаходиться у відкритому доступі на умовах ліцензії Apache 2.0, що має сприяти широкому поширенню контролера, його розвитку та доопрацювання сторонніми розробниками. У відкритому доступі знаходяться ядро контролера, базовий набір сервісів і додатків (визначення топології, побудова маршруту, статистика і моніторинг, інтерфейс REST, графічний інтерфейс). У комерційній версії контролер Runos володіє механізмами резервування, масштабованості і розподіленого управління.

Важливим моментом є резервування контролера. І всі постачальники забезпечили її - подробиці нижче в розділах, присвячених конкретним рішенням.

2.4.2 Вибір комутатору

Більшість постачальників віддали перевагу традиційному мережевому пристрою, але з підтримкою SDN. Huawei не пропонує в своїх рішеннях комутатори класу bare metal, однак, при впровадженні SDN важливо забезпечити спадкоємність архітектури і зберегти працездатність наявних додатків, а існуючі сервіси та протоколи орієнтовані на традиційні мережеві засоби. Представляючи свої SDN-рішення в цілому, компанія HP зазначила можливість побудови мережевої інфраструктури з комутаторами на базі відкритої платформи (white box), але рекомендувала їх використання в ЦОДах великих масштабів - від 200 ToR-комутаторів або від 10 000 портів. Такі інфраструктури можна реалізовувати на базі комутаторів HP серії Altoline. На думку фахівців HP, вони найбільш ефективні для Цодов, в яких в основному використовуються додатки Open Source, хмарні платформи OpenStack / CloudStack, рішення HPC на базі Hadoop, бази даних NoSQL (Cassandra / HBase) і т. П. Очевидно, що це не випадок нашого замовника.

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

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

2.4.3 Додатки SDN

Одне з важливих переваг SDN - можливість використання широкого набору додатків, що реалізують різні мережеві сервіси та функції. Такі додатки створюються в тому числі сторонніми розробниками і найчастіше надаються замовникам безкоштовно.

Більшість компаній для просування рішень SDN прагнуть сформувати екосистему SDN, важливою частиною якої є розробники програми. Відзначимо пропонований HP онлайн-магазин SDN-додатків HP SDN App Store (див. Врізку «SDN-додатки з магазину»). Як стверджують в HP, користувачі можуть буквально одним кліком мишки завантажувати SDN-додатки з магазину на контролер, відразу ж їх запускати і використовувати.

2.4.4 SDN-додатки з магазину

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

– SDN Privatizer - безкоштовний додаток, яке реалізує функціональність Private VLAN в масштабах всієї мережі, що дозволяє ізолювати один від одного різні групи користувачів, в тому числі, підключених до різних комутаторів або навіть розташованих в різних сегментах мережі.

BlueCat DNS Director - безкоштовний додаток, яке перехоплює DNS-запит користувача і, якою б IP-адреса сервера в ньому не був зазначений, замінює його на заданий адміністратором адресу корпоративного DNS, тим самим забезпечуючи додатковий рівень безпеки IT-інфраструктури

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

Фахівці NEC звертають увагу на переваги концепції сервісних ланцюжків (Service Chaining), коли різні необхідні користувачу функції можуть вибиратися і комбінуватися із загального пулу для конкретної віртуальної мережі VTN (див. Рис. 2.17). Це можуть бути класичні для IP-мереж L2 / L3 функції контролю доступу, приоритизации трафіку, управління політиками QoS і т. Д., А реалізовані вони можуть бути як у вигляді окремого SDN-додатки, так і на базі апаратного компонента. Такий підхід дозволяє власнику мережі

SDN створити набір VTN, архітектурно і функціонально оптимізованих відповідно до вимог користувачів, а також динамічно реагувати на штатні та позаштатні ситуації. Наприклад, система захисту від DDoS-атаки або пристрій фільтрації трафіку можуть включатися в структуру мережі і задіяні тільки у разі виявлення загрози.

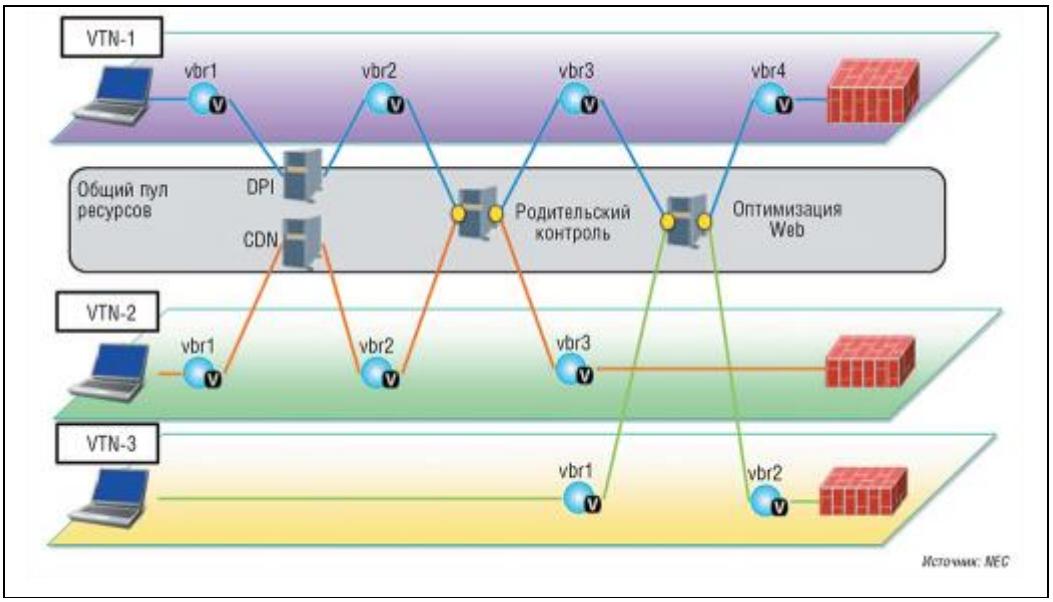


Рисунок 2.17. Приклади сервісних ланцюжків -Service Chaining

2.4.5 Особливості проектів ЦПІКС

Проект ЦПІКС, як уже говорилося, виділяється вибором комутаторів (пристрої white box або на основі серверів x86), в плані ж архітектури він більш-менш типовий. У центральному офісі кінцеві користувачі підключаються до шести граничним комутаторів, кожен з яких з метою резервування приєднується до двох центральних комутаторів 10G (див. Рис. 2.18).

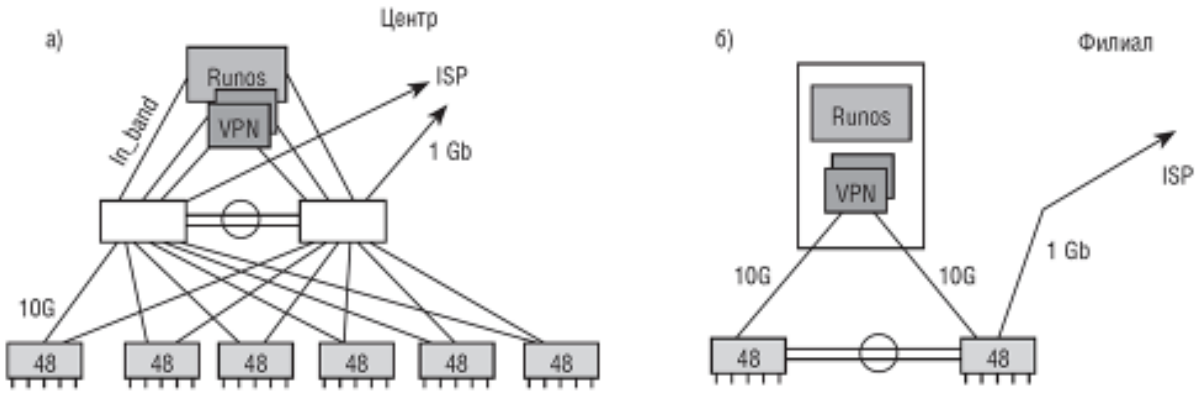


Рисунок 2.18. Структура мережі центрального офісу (а) і філії (б) в проекті ЦПІКС

На серверній фабриці функціонують необхідні замовнику мережеві сервіси, включаючи контролер Runos. Останній запускається в двох примірниках в режимі Active / Standby: в разі «падіння» першого примірника управління передається на резервний контролер.На відміну від центрального офісу, в філіях не потрібно великої кількості кінцевих портів, тому там досить двох комутаторів. Замість серверної фабрики розгортається один сервер віртуальних машин, на якому і будуть працювати необхідні мережеві сервіси.

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

У центральному офісі та філіях працюють свої екземпляри контролерів SDN. У разі втрати каналу до центрального офісу мережу філії продовжить функціонувати автономно.

Серед додаткових можливостей, які надає рішення ЦПІКС, - інтеграція з контролером Wi-Fi для безшовного роумінгу і можливість роботи по протоколу dot1x для аутентифікації користувачів без жорсткої прив'язки до порту комутатора. Остання функція дозволяє користувачам мігрувати між мережевими пристроями (включаючи точки доступу Wi-Fi), при цьому мережа буде автоматично підлаштовуватися під нове розташування користувача.

2.4.6 Brocade

Для вирішення завдання фахівці Brocade запропонували використовувати L3-комутатори сімейства ICX 7000, програмний маршрутизатор Brocade vRouter 5600 і контролер Brocade SDN Controller (далі BSC). У великому офісі передбачається розгорнути дворівневу мережу, в ядрі якої встановити пару високопродуктивних комутаторів ICX 7750 (вони ж можуть використовуватися для підключення серверів), пов'язаних твінаксіальнимі кабелями на швидкості nx40G. Рівень доступу реалізується на базі ICX 7250. Засоби управління всією мережею (включаючи порти доступу) консолідовані на рівні ядра (архітектура SwitchPort Extender) - вся локальна мережа, по суті, являє собою один комутатор («розподілене шасі»). На кордоні мережі встановлюється відмовостійка пара маршрутизаторів vRouter 5600, а в філіях - vRouter 5600 і 48-портовий ICX 7250.

Серед переваг комутаторів Brocade ICX з ОС FastIron (в порівнянні з комутаторами white box, а також пристроями ряду інших виробників) фахівці Brocade назвали підтримку вже згаданої архітектури Switch Port Extender і гібридних портів - один і той же порт

можна використовувати як для традиційної комутації / маршрутизації , так і для передачі трафіку відповідно до обумовленими контролером правилами. Комутатори можна об'єднати в стек за допомогою стандартних інтерфейсів 1/10 / 40G Ethernet, причому такий стек може бути розподіленим (до 10 км). Використовувана в комутаторах технологія PoE + / PoH дозволяє дистанційно (по локальній мережі) подавати електроживлення потужністю до 90Вт.

На базі BSC можна побудувати відмовостійкий кластер з трьох територіально розподілених вузлів. Як варіант можливе створення пулу контролерів, прихованих за одним віртуальним IP-адресою (VIP).

В якості опції в проект може бути включений продукт Brocade Flow Optimizer, який спільно з BSC використовується для інтелектуального управління потоками даних, виявлення аномалій і захисту від різних атак. У графічному інтерфейсі FlowOptimizer определяются профілі трафіку і які застосовуються до них правила, встановлені установки автоматично трансформуються в правила OpenFlow і за допомогою контролера в динамічному режимі передаються на мережеві пристрої.

2.4.7 Cisco

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

Можливості підключення центрального і віддалених офісів забезпечать маршрутизатори серії ISR 4000. У центральному офісі пропонується встановити отказоустойчивую пару маршрутизаторів Cisco ISR 4451, а у віддалених офісах (в залежності від вимог відмовостійкості і можливостей каналів глобальної мережі) - один або два маршрутизатора ISR 4431.

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

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

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

Cisco планує поставляти APIC-EM безкоштовно з набором вбудованих мережевих додатків (за нові спеціалізовані додатки буде, ймовірно, стягуватися додаткова плата).

2.4.8 Extreme networks

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

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

Запропоноване рішення дозволяє реалізувати ряд додаткових SDN-додатків і сервісів, включаючи автоматизацію створення віртуальних мереж, графічний інтерфейс управління трафіком, інжиніринг трафіку для бізнес-додатків, роботу систем безпеки на терабітних швидкостях і ін. Динамічному впровадженню нових сервісів допоможе можливість гнучкого перенаправлення трафіку (вибіркових потоків) на різні компоненти мережевої інфраструктури, такі як система аналітики і моніторингу додатків Purview, Captive-портали бездротових мереж Wi-Fi, з стеми записи IP-телефонії. Крім того, Extreme пропонує «SDN для Wireless»: повна підтримка концепції SDN та інтеграції сторонніх

додатків з бездротовими мережами Wi-Fi від Extreme Networks - IdentiFi (в тому числі пріоритизація трафіку VoIP, інтеграція з рішеннями MDM, BYOD).

2.4.9 HP

Представлений весь портфель продуктів SDN і, звичайно, деталізовано вирішення конкретного завдання. Згідно з пропозицією HP, ядро регіонального офісу складуть два модульних комутатора HP 5406R zl2, які забезпечать підключення комутаторів доступу (по 10G), а також комутаторів Цода, граничних маршрутизаторів і опціонального Wi-Fi-контролера HP Aruba. Для рівня доступу - підключення кінцевих пристроїв (ПК, ноутбуків, телефонів, опціональних Wi-Fi-точок HP Aruba) - призначаються сім 48-портових комутаторів HP 3800 з підтримкою PoE +, а для Цода - підключення серверів і СГД (по 10GbE / FCoE / iSCSI або 4 / 8G FC) - два конвергентних комутатора HP 5900CP (див. рис. 2.19).

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

Для формування територіально розподіленої мережі запропоновано використовувати маршрутизатори HP MSR3044 (в регіональному офісі) і HP MSR3012 (в філіях). Вони забезпечують контроль доступу і фільтрацію трафіку на кордоні мережі за допомогою вбудованого брандмауера. Для організації VPN-підключення рекомендована технологія HP ADVPN.

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

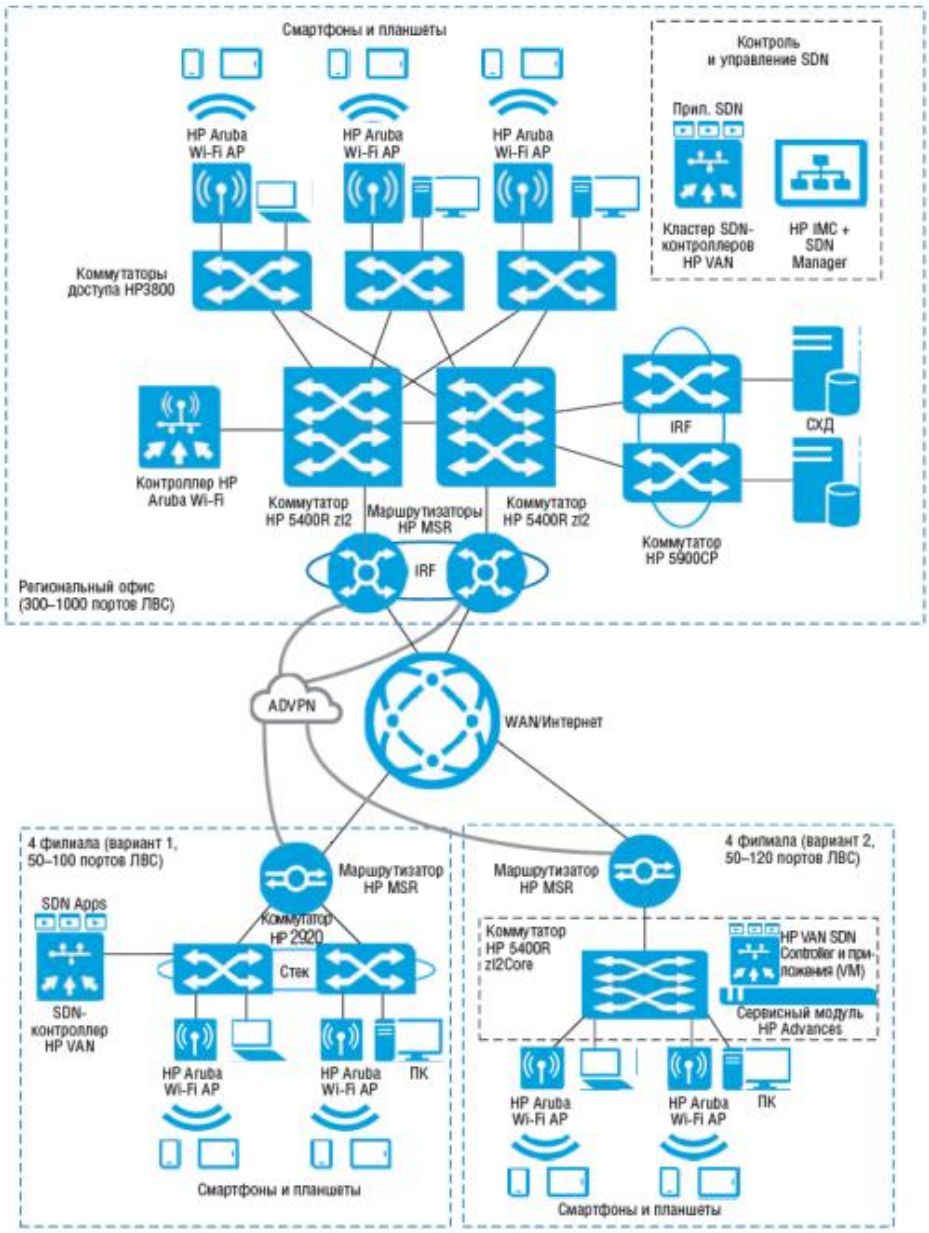


Рисунок 2.19. Структурна схема SDN-рішення HP для замовника

В якості основних HP запропонувала три SDN-додатки: HP Network Protector забезпечує безпеку в локальній мережі; HP Network Optimizer - управління QoS в ЛВС; HP Network Visualizer - моніторинг і діагностику ЛВС. Крім перерахованих, можна використовувати додаткові додатки з HP SDN App Store (див. «SDN-додатки з магазину»).

2.4.10 Huawei

За задумом архітекторів Huawei - ядром мережі регіонального офісу, повинен стати модульний комутатор S7706 з встановленими інтерфейсними платами з портами 10 Гбіт / с (для підключення серверів і комутаторів доступу) і 1 Гбіт / с (для підключення робочих

місць). Для рівня доступу запропоновані комутатори S5700-X-LI. Мережі філій будуть будуватися на базі комутаторів S5720-HI.

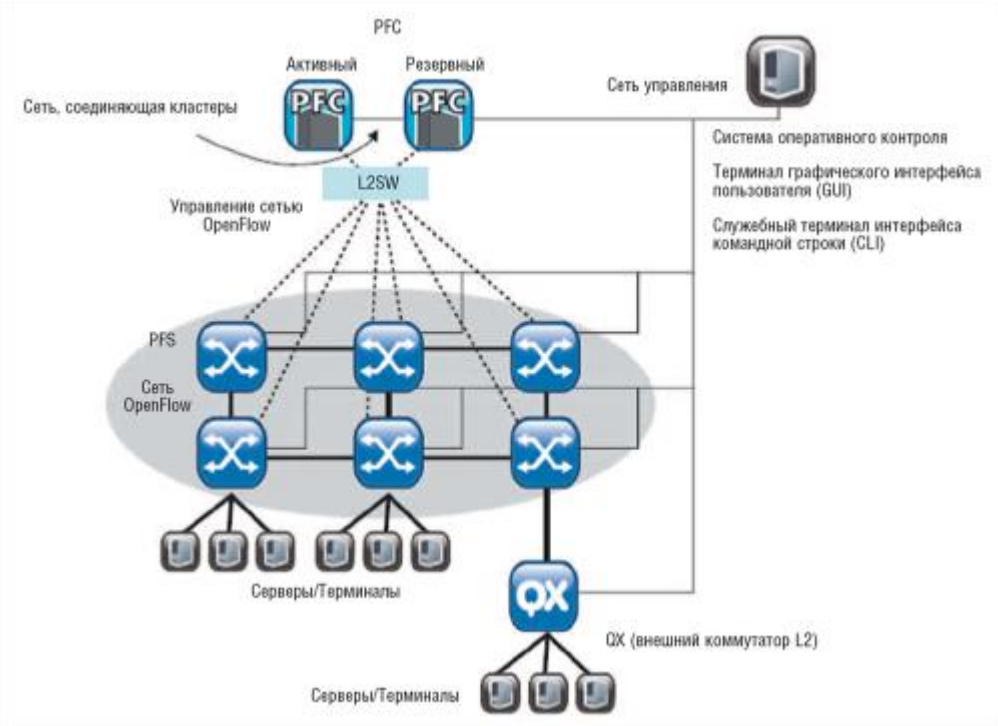
Важливим програмним компонентом рішення є Super Virtual Fabric (SVF). SVF - це технологія віртуалізації мережевої інфраструктури і уніфікованого управління мережевими елементами, користувачами і додатками. Завдяки SVF мережева інфраструктура буде представлена у вигляді єдиного віртуального комутатора з централізованим управлінням конфігураціями, QoS, правилами контролю доступу й аутентифікації користувачів. Крім провідної інфраструктури, SVF дозволяє віртуалізувати і бездротову мережу, при цьому обробка трафіку і аутентифікація будуть проводитися відповідно до загальних правил. Комутатор S7706 виступає в якості головного керуючого комутатора SVF-Parent, а комутатори S5700-X-LI і S5720-HI - як керовані SVF-Client, тому для останніх не потрібні індивідуальні конфігурація і управління. Для підключення до територіально розподіленої мережі, побудови тунелів і шифрування трафіку, забезпечення безпеки і надання голосових сервісів в регіональному офісі встановлюються маршрутизатори AR2240, а в філіях - AR1220E. Найближчим часом, згідно з концепцією Agile Branch, маршрутизаторами віддалених офісів також стане можливо управляти з централізованого контролера (спочатку заявлена робота через контролер Open Daylight, поряд з власним), так що їх не потрібно буде конфігурувати окремо. Розробляючи свій контролер SDN, Huawei передбачила підтримку кластеризації та модульну структуру ПО для забезпечення відмовостійкості і високої доступності. Agile Controller має ієрархічну структуру з декількома компонентами (Management Center (MC), Service Manager (SM), Service Controller (SC)) плюс зовнішні бази даних. Кожен з компонентів може бути зарезервований, а розподілений дизайн дозволяє розмістити частину компонентів безпосередньо в філіях.

Крім забезпечення базових функцій, Huawei пропонує ряд додаткових можливостей. Так, завдяки функції Free Mobility користувач отримає єдині політики безпеки, обслуговування та виділення ресурсів, а також сервісні політики, тобто обслуговування буде однаковим незалежно від місця, часу, типу терміналу або порту доступу. А технологія iPCA дозволить забезпечити наскрізний контроль якості на реальних потоках трафіку і визначити оптимальні шляхи передачі трафіку.

2.4.11 Nec

Для побудови SDN-мереж NEC пропонує платформу NEC ProgrammableFlow, що включає контролер NEC PF6800 і лінійку комутаторів P-Flow. Відмовостійкий контролер

PF6800 є ПО, який виконувався на кластері, який організований на базі двох окремих фізичних серверів або віртуальних машинах (див. Рис. 2.20). Як відзначають в NEC, її платформа SDN інтегрована з відкритими платформами SDN / NFV, що розвиваються в рамках проектів OpenStack і OpenDayLight.



Так як комутатори NEC P-Flow є гібридними (володіють можливістю настройки портів для роботи як в режимі IP, так і в режимі OpenFlow), мережа управління може бути поєднана з мережею управління OpenFlow і налаштована з використанням частини портів контролера PFS, перемикання в режим IP . При цьому мережа управління все одно використовує виділені фізичні канали, що дозволяє значно підвищити безпеку і захищеність мережі.

Рисунок 2.20. Архітектура мережі SDN на базі рішення NEC ProgrammableFlow

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

Основою SDN-рішення NEC є віртуалізація мережі VTN: в хмарі комутаторів OpenFlow створюється безліч незалежних мереж L2 / L3 IPv4 / IPv6, робота яких

підтримується автоматично при змінах у фізичній мережі. Користувач може створювати VTN, динамічно змінювати конфігурацію VTN в процесі експлуатації і застосовувати мережеві політики незалежно від інших VTN. При цьому для створення своїх VTN він може як скористатися пулом мережевих ресурсів, які надає оператор мережі SDN і вже інтегрованих з контролером SDN, так і задіяти свої унікальні фізичні пристрої або віртуалізовані (VNF) компоненти.

Серед переваг запропонованої мережі SDN фахівці NEC називають підвищення продуктивності мережі (стабільна робота забезпечується навіть при 100-відсотковому завантаженні каналів), можливість перебудови фізичної мережі без переривання обслуговування в віртуальних мережах, підвищення безпеки за рахунок повної ізоляції віртуальних мереж одного від одного, збільшення надійності мережі завдяки самовідновлення і автоматичного перерозподілу потоків трафіку відповідно до правил. Ефектною і водночас ефективною є візуалізація трафіку в фізичної і логічних мережах, що дозволяє спростити експлуатацію, прискорити виявлення і усунення несправностей, спростити моніторинг SLA.

2.4.12 Міграція (гібридні мережі)

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

Впровадження SDN не вимагає повної заміни існуючої IP-інфраструктури, а більшість переваг SDN стають доступні при повній або навіть часткової заміни ядра мережі або рівня агрегації. Запропоноване NEC рішення SDN може інтегруватися з IP-мережами на рівнях L2 (MCLAG) і L3 (VRRP / HSRP). При цьому один сегмент SDN може мати кілька підключень рівня L2 і / або L3 до мереж IP, і для всіх підключень може використовуватися єдиний пул мережевих сервісів (MCE, балансувальник, DPI, Proxy та ін.), Що значно спрощує завдання адміністрування. Для інтеграції декількох сегментів SDN фахівець NEC рекомендує організувати L2 VPN в існуючих мережах передачі даних.

Як зазначено у відповіді компанії Huawei, «негайний перехід до SDN може привести до втрати інвестицій, частина наявних функцій може бути втрачена або істотно спрощена (наприклад, функції балансувальника або оптимізатора трафіку)». Тому її комутатори Agile надають можливість саме міграції на SDN, а не радикального переходу до цієї технології. Вони здатні паралельно підтримувати два режими роботи: традиційна комутація / маршрутизація і SDN (див. рис. 2.21).

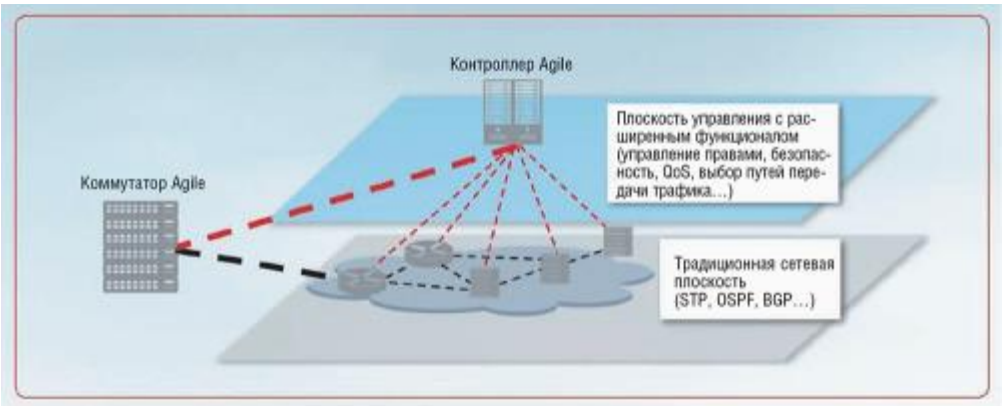


Рисунок 2.21. Комутатори Agile здатні паралельно підтримувати два режими роботи: традиційна комутація / маршрутизація і SDN

Фахівці Huawei особливо наголошують на тому, що в її комутаторах Agile використовуються мережеві процесори власної розробки (Ethernet Network Processor, ENP). Традиційні ASIC обробляють дані тільки зумовлених протоколів, а впровадження нових сервісів (наприклад, з нестандартною инкапсуляцией) тягне апаратні зміни (редизайн мікросхем). На відміну від ASIC, процесори ENP повністю програмовані, тому замовники можуть вже зараз почати фрагментарно впроваджувати «готові до SDN» пристрою в існуючу інфраструктуру і надалі, просто оновивши прошивку, підтримувати майбутні нові протоколи і сервіси.

За даними Cisco, в разі вибору її рішення інтеграція з традиційною мережею здійснюється прозоро і без застосування будь-яких додаткових технологій. Підключення до існуючої мережі рекомендується проводити через два опорних маршрутизатора Cisco ISR 4451, розташованих в центральному офісі. Незважаючи на те що ці маршрутизатори перебувають під контролем APIC-EM, для взаємодії з традиційною частиною мережі використовуються стандартні механізми - протоколи канального рівня (в залежності від типу ліній зв'язку) і протоколи комутації / маршрутизації відповідно до корпоративного стандарту.

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

В цілому, завдяки гібридній архітектурі, можна поетапно впроваджувати рішення SDN в існуючих мережах, при цьому дані рішення будуть тісно інтегруватися і

взаємодіяти з обладнанням, що не підтримують SDN та протокол OpenFlow. Це, зокрема, дозволяє використовувати переваги, які надають SDN-додатки, без необхідності повної заміни всього обладнання в мережі.

2.5 Комутатори

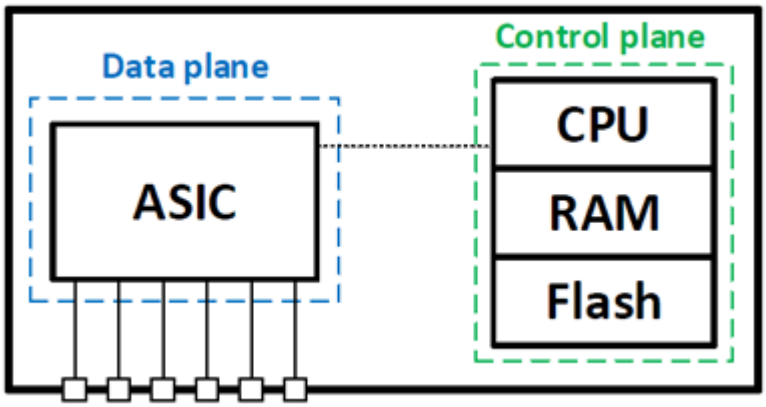
Головне для комутатора - швидкість передачі даних. Вся обробка пакетів повинна реалізуватися на швидкості порту, інакше комутатор буде гальмуючим елементом в нашій мережі. У зв'язку з цим, саме в комутаторах ми можемо виявити реалізацію передавального рівня на окремих мікросхемах - ASIC'ах (ASIC - інтегральна схема спеціального призначення). Фактично на комутаторі керуючий рівень виконується на базі процесора загального призначення, а передавальний рівень, як ми вже зазначили, на базі ASIC.

Процесори, які встановлюються в мережеве обладнання, часто мають відмінності від тих, які стоять в наших ПК і серверах. Це найчастіше спеціалізовані процесори, які розраховані на використання всередині різних пристроїв (мережевих, систем зберігання даних і ін.) І відносяться до класу вбудованих процесорів (embedded processors). Зазвичай вони мають невеликий розмір, споживають небагато енергії і є частиною однокристальної системи (System on a chip - SoC). SoC - практично повноцінний комп'ютер, виконаний на базі однієї мікросхеми (з (мікро) процесором, оперативною пам'яттю, контролером введення / виведення, інтерфейсами і ін.). Деякі з таких процесорів заточені на виконання операцій в мережевих пристроях, інші мають більш широкий спектр застосування. При цьому найчастіше на них можна запустити, наприклад, якісь рішення на базі Unix / Linux, так як вони все ж залишаються в першу чергу процесорами загального призначення.

Класичний ASIC має зумовлений набір функцій, які виконуються апаратно. Фактично загальна логіка обробки пакетів закладається в ASIC на етапі виробництва мікросхеми, змінити яку досить складно. У ASIC'е ми отримуємо прийнятний рівень логіки і при цьому високу швидкість обробки пакетів. Таким чином, висока продуктивність в комутаторі досягається за рахунок виконання функцій передавального рівня на ASIC'ах. І саме ASIC'і є причиною щодо обмеженою логіки роботи комутатора, яку складно надалі змінити. Можна було б замість ASIC використовувати мікросхеми FPGA (Field-Programmable Gate Array), які можна перепрограмувати. Але вони дороги і енергоємні. Тому виробники мережевого обладнання, щоб не збільшувати вартість своїх пристроїв, з одного боку, частина обробки пакетів намагаються перенести на процесор загального призначення (тобто туди де працює керуючий рівень), що не завжди добре

позначається на продуктивності пристрою. З іншого боку, намагаються модернізувати ASIC, зробивши їх більш функціональними і навіть програмованими (наприклад, ASIC UADP компанії Cisco).

Зазвичай в комутаторі варто один або кілька ASIC'ов. Наприклад, на кожні 12/24 порту ставиться свій ASIC. Програмування логіки роботи ASIC'а виконує керуючий рівень. Саме він заповнює всі таблиці всередині ASIC'а (маршрути, списки доступу та ін.). ASIC може мати достатній інтелект, щоб комутувати пакети всередині себе, або ж здійснювати комутацію пакетів через зовнішню шину / комутаційну фабрику. Така архітектура використовується в першу чергу в комутаторах фіксованою конфігурації (НЕ модульних). Прикладами таких комутаторів можуть бути Cisco Catalyst 2960/3650/3850.



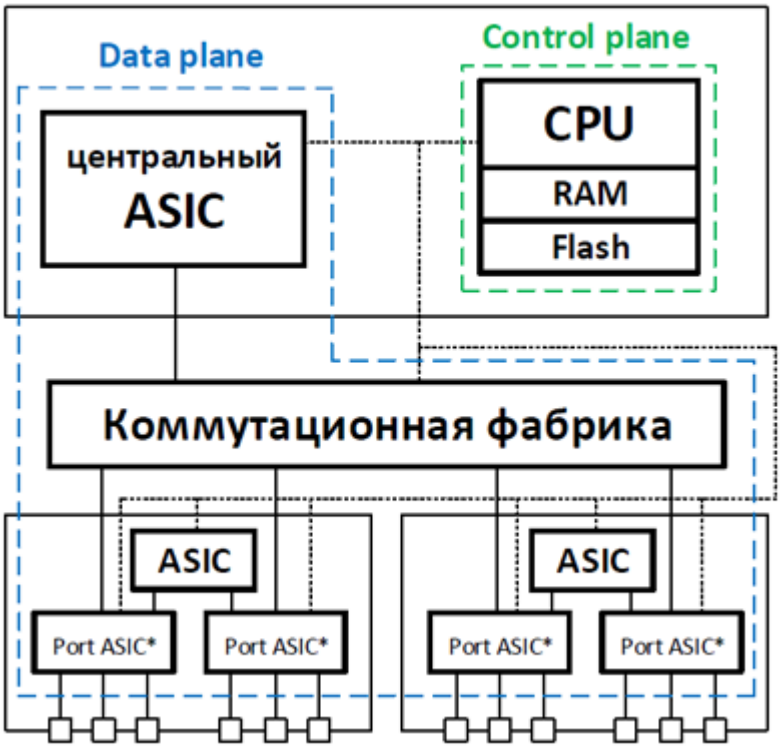
Структурні схеми комутаторів і маршрутизаторів є спрощеними для акцентування уваги в першу чергу на розташуванні керуючого і передавального рівнів. Вони не включають всі структурні елементи пристроїв.

Рисунок 2.22. Спрощена структурна схема комутатора

Якщо ми маємо справу з модульним комутатором (комутатор, в який можна встановлювати плати з різними типами портів), архітектура може бути більш складною. Більше портів, значить, потрібно більше продуктивність і більше ASIC'ов. Існує як мінімум два підходи в реалізації архітектури таких комутаторів.

У першому випадку, передає рівень виконується централізовано на виділених ASIC'ах, які розташовуються на окремій платі. В цьому випадку ASIC'і на лінійних картах є менш інтелектуальними і виконують вкрай обмежений набір функцій. Програмуванням логіки продовжує займатися керуючий рівень, якої в свою чергу запускається на своїх апаратних потужностях (використовується знову ж процесор загального призначення (причому їх може бути кілька), розташований на окремому модулі - супервізора).

Прикладом таких комутаторів можуть бути Cisco Catalyst 4500 і Cisco Catalyst6500 / 6800 (централізована комутація).



мікросхеми Port ASIC, встановлені на лінійних картах, що немає великий інтелектуальністю і виконують вкрай обмежений набір функцій

Рисунок 2.23. Структурна схема комутатора Cisco Catalyst 6500/6800.

Можливий варіант, де на кожному модулі з лінійними портами, варто своя спеціалізована плата передачі. У цьому випадку кожен модуль має свій передавальний рівень, що дозволяє підвищити продуктивність всієї «коробки». Можна сказати, що це проміжний варіант між першим і другим підходами реалізації архітектури модульних комутаторів. Прикладом таких комутаторів можуть бути Cisco Catalyst 6500/6800 (розподілена комутація).

Другий підхід - використовувати досить інтелектуальні ASIC'і на лінійних картах. У цьому випадку кожен ASIC може самостійно обробити мережевий трафік, виконуючи основний набір функцій. Тобто ми відразу маємо розподілене передає рівень. Це може виявитися більш дорогим рішенням, але при цьому часто більш продуктивним. Також ми мінімізуємо при такій архітектурі затримки під час передачі пакетів. Прикладом подібного комутатора може бути Cisco Nexus 9500.

Архітектура модульних комутаторів буває досить складною. Зокрема, для реалізації передавального рівня можуть використовуватися кілька різних ASIC'ов в рамках однієї лінійної карти. Кожен з них виконує свій спектр завдань або ж об'єднує

нижчестоящі ASIC'і. Комутаційна фабрика також може бути побудована на базі ASIC'ов, що виконують як функції зв'язку між лінійними картами, так і певні види обробки.

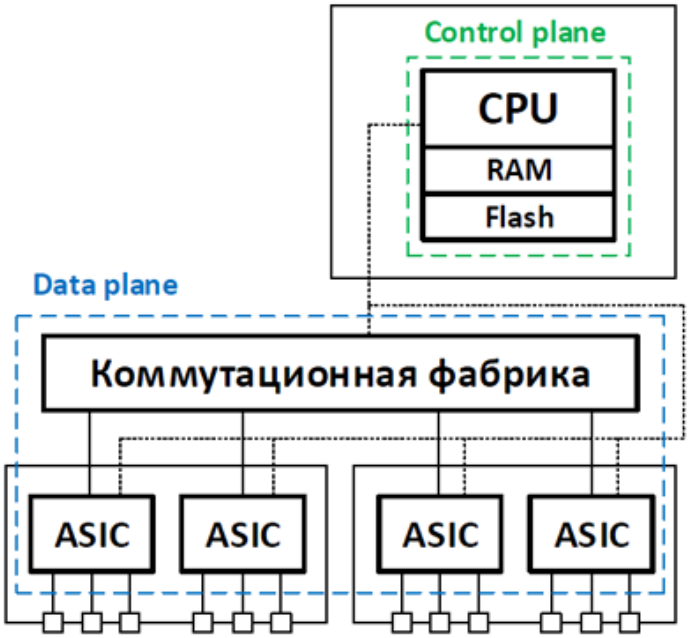


Рисунок 2.24. Структурна схема комутатора Cisco Nexus 9500

Відзначимо, що в комутаторах ми можемо мати розподіл рівня управління. Наприклад, в комутаторі Cisco Nexus 9500 керуючий рівень всередині одного пристрою рознесених: частина функцій виконуються на супервізора, а частина на платі лінійних портів (на кожній платі варто свій процесор загального призначення).

До цього моменту все розгляд йшло в рамках одного пристрою. Але багато комутатори вміють об'єднуватися в один логічний пристрій за коштами стекирования. У разі якщо у нас зібраний стек з комутаторів, зазвичай керуючий рівень запускається на основному комутаторі (його ще називають активним / майстром). А що передає рівень буде запущений окремо на кожному комутаторі в стеці. Тобто через стековий канал зв'язку керуючий рівень, розташований на основному комутаторі, роздає керуючу інформацію на всі комутатори в стеку для роботи передавального рівня локально. Прикладом такої моделі роботи може бути стек Cisco StackWise або HPE IRF.

2.5.1 Маршрутизатори

Давайте тепер подивимося, як йдуть справи з нашими абстракціями в маршрутизаторах. Якщо ми будемо розглядати щодо бюджетні маршрутизатори,

керуючий і передавальний рівні будуть виконуватися на одному і тому ж залозі - процесорі загального призначення (найчастіше в форматі SoC). Процесорний час розподілятиметься в цьому випадку між обома абстракціями. Ніяких спеціалізованих мікросхем для передавального рівня, як це було в комутаторах, ми там знайдемо. У зв'язку з цим ми отримаємо дуже гнучку логіку роботи пристрою, але не найвидатніші значення по продуктивності (десятки і сотні мегабіт в секунду). Причому різні Вендорний хитрощі (наприклад, Cisco Express Forwarding) є лише оптимізацією обробки пакетів на програмному рівні на базі стандартної апаратної бази. Прикладами таких пристроїв є, Cisco 800, 1900, 2900 та ін. Ситуація змінюється, якщо наш процесор загального призначення стає багатоядерним (наприклад, в Cisco ISR 4300), та ще таких процесорів може бути кілька (наприклад, в Cisco ISR 4400). У цьому випадку керуючий і передавальний рівні можуть виконуватися на різних ядрах і процесорах. Причому передавальному рівню виділяється відразу кілька ядер, щоб отримати паралельну обробку пакетів, а значить, підвищити продуктивність нашого пристрою. Варто зауважити, що деякі ядра можуть бути віддані взагалі під сторонні сервіси (звісно, якщо процесор це дозволяє зробити).

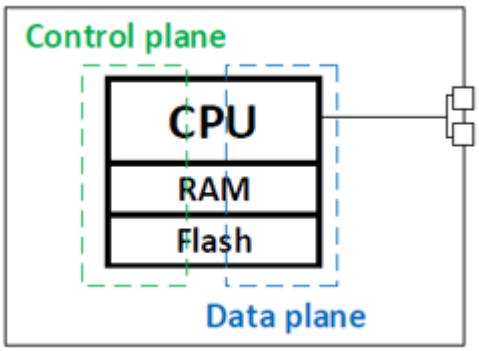


Рисунок 2.25. Структурна схема маршрутизатора.

Сучасні SoC мають багатоядерні процесори. 48 ядрами вже нікого не здивуєш. А укупі з інтегрованими в SoC акселіраторамі пакетної обробки, на базі одного SoC можна отримати дуже хорошу продуктивність: на ринку є рішення SoC, що дозволяють обробляти мережевий трафік на швидкостях до 40 Гбіт / с.

Окрема розмова - це високопродуктивні маршрутизатори. В цьому випадку звичайних процесорних потужностей загального призначення може не вистачати. Виробники мережного обладнання переносять передає рівень на окреме залізо, більш адаптоване для обробки великого потоку трафіку. Фактично ми йдемо до архітектури

комутаторів. Але так як маршрутизатор більш функціональний, звичайних ASIC'ов мало. У зв'язку з цим кожен виробник пропонує свої рішення.

Один з варіантів - використання спеціалізованих мережевих процесорів (Network Processor - NP або Network Processing Unit - NPU). Мережеві процесори істотно функціональніша, ніж ASIC'і, але при цьому більш продуктивні, ніж процесори загального призначення.

Як приклад розглянемо маршрутизатори Cisco ASR 1000, де основні функції передавального рівня виконується на окремій платі. На такій платі розміщується один або два спеціалізованих мережевих процесорів Cisco QuantumFlow Processor (QFP), які займаються безпосередньо обробкою трафіку. Даний процесор має архітектуру RISC і заточений саме під передачу трафіку. QFP другого покоління включає до 128 процесорних ядер, на кожному з яких може бути запущено чотири окремі процеси. Тобто ми маємо до 256 ядер на одній платі (у разі двох процесорів). Порівнявши з архітектурою простіших маршрутизаторів, де все виконується на декількох ядрах, можна відразу зробити висновок, що такі маршрутизатори є більш продуктивними.

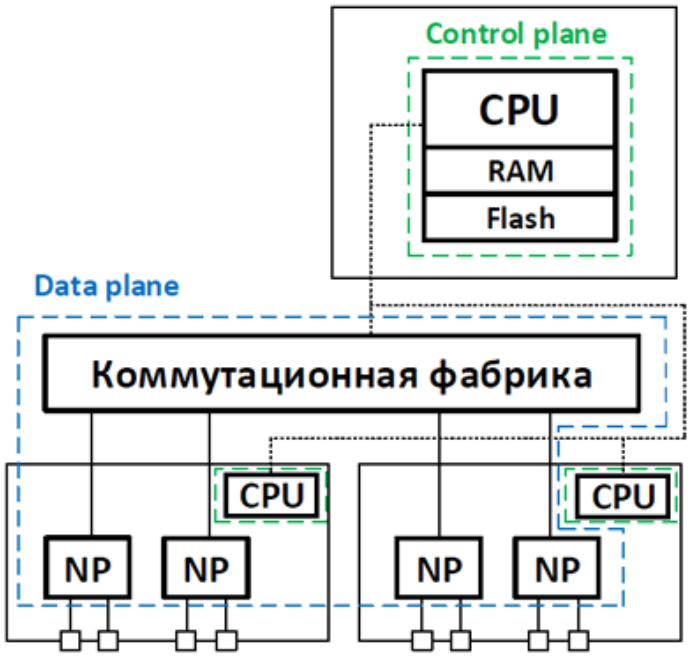


Рисунок 2.20. Структурна схема маршрутизатора Cisco ASR 1000

Мережеві процесори випускаються різними компаніями (Cisco, EZChip, Broadcom і ін.) І використовуються для виконання функцій передавального рівня багатьма виробниками мережевого устаткування. Наприклад, мережеві процесори

використовуються в обладнанні компаній Huawei (як в маршрутизаторах, наприклад, в NetEngine40E, так і в комутаторах S12700).

Крім мережевих процесорів, на ринку представлені спеціалізовані чіпсети, наприклад, Juniper Trio chipset. Вони позиціонуються між мережевими процесорами і ASIC'амі. За великим рахунком, загальний зміст зберігається - передає рівень виконується на спеціалізованому залозі, в даному випадку чіпсеті Trio Chipset. Відзначимо, що до виведення на ринок Trio chipset, компанія Juniper активно використовувала в своїх маршрутизаторах програмовані ASIC'і власної розробки (Internet Processor ASIC і I-Chip).

Варто відзначити, що в топових рішення, ми будемо мати не тільки рознесення рівнів управління і передачі між різними залізом, а й розподіл всередині кожного рівня. Наприклад, в маршрутизаторі Cisco ASR 9000 керуючий рівень всередині одного пристрою рознесених: частина функцій виконуються на процесорній платі, а частина на платі лінійних портів. Те ж саме стосується і передавального рівня: мережевих процесорів багато і вони розташовані безпосередньо на лінійних картах.

Так як реалізацій архітектур навіть у одного вендора досить багато, розглянути їх усі вкрай складно. Однак, якщо нам потрібна велика продуктивність, найчастіше передає рівень буде виконуватися на спеціалізованому залозі: будь то мережевий процесор, спеціалізований чіпсет, звичайний або програмований ASIC, або щось ще. У деяких пристроях ми зустрінемо навіть комбінацію цих мікросхем. Нерідко виробники мережевого обладнання в своєму обладнанні використовують мікросхеми сторонніх компаній (наприклад, ASIC'і або мережеві процесори).

SNMP (англ. Simple Network Management Protocol - простий протокол мережевого управління) - стандартний інтернет-протокол для управління пристроями в IP-мережах на основі архітектур TCP / UDP. До підтримуючих SNMP пристроїв відносяться маршрутизатори, комутатори, сервери, робочі станції, принтери, модемні стійки і інші. Протокол зазвичай використовується в системах мережного управління для контролю підключених до мережі пристроїв на предмет умов, які вимагають уваги адміністратора. SNMP визначено Інженерним радою інтернету (IETF) як компонент TCP / IP. Він складається з набору стандартів для мережевого управління, включаючи протокол прикладного рівня, схему баз даних і набір об'єктів даних.

Інтерфейс командного рядка (англ. Command line interface, CLI) - різновид текстового інтерфейсу (CUI) між людиною і комп'ютером, в якому інструкції комп'ютера даються в основному шляхом введення з клавіатури текстових рядків (команд), в UNIX-системах можливе застосування миші. Також відомий під назвою консоль. Інтерфейс командного рядка протиставляється системам управління програмою на основі меню, а

також різним реалізаціям графічного інтерфейсу. Формат виведення інформації в інтерфейсі командного рядка не регламентується; зазвичай це також простий текстовий висновок, але може бути і графічним, звуковим і т. п.

2.6 Хмарні системи

Поняття хмари нерозривно пов'язане з двома абстракціями - гарантована якість ресурсів і їх взаємна ізоляція. Розглянемо, як ці поняття застосовуються до пристрою мережі в хмарному вирішенні. Ізольованість ресурсів має на увазі наступне:

Антіспуфінг, виділення приватного сегмента мережі, фільтрація публічного сегмента для мінімізації впливів ззовні.

Гарантована якість ресурсів - це QoS в загальному розумінні, тобто забезпечення необхідної смуги і необхідного відгуку всередині мережі хмари.

QoS - технологія надання різних класів трафіку різних пріоритетів в обслуговуванні, також цим терміном в області комп'ютерних мереж називають ймовірність того, що мережа зв'язку відповідає заданому угодою про трафік, або ж, в ряді випадків, неформальне позначення ймовірності проходження пакета між двома точками мережі.

2.6.1 Ізоляція трафіку

Спуфінга - це підробка вихідного IP-адреси. Спуффінг може бути використаний зловмисником для обходу налаштувань міжмережевих екранів, а також для організації DoS-атак по відношенню до третіх осіб.

Антіспуфінг за допомогою iptables / ebtables або статичних правил в OpenVSwitch - це максимально дешеве рішення, але на практиці незручно. Якщо для linux bridge (мережевий міст) правила створюються за допомогою механізму nwfilter в libvirt і автоматично підтягуються при запуску віртуальної машини, для ovs оркестровці доведеться відстежувати момент старту і перевіряти чи оновлювати відповідні правила в свіч.

libvirt - це вільна реалізація API, демон і набір інструментів для управління віртуалізацією. Дозволяє управляти гіпервізорами Xen, KVM, а також VirtualBox, OpenVZ, LXC, VMware ESX / GSX / Workstation / Player, QEMU і іншими засобами віртуалізації, надає можливість контролювати віртуальні машини по мережі, розташовані

на інших комп'ютерах. Ці API широко використовуються в шарах гіпервізора при розробці хмарних рішень.

Додавання або видалення адреси або міграція віртуальної машини перетворюються в обох випадках в нетривіальну задачу, перекладають на логіку оркестровки. У момент запуску сервісу в публічне використання застосовували саме nwfilter, але були змушені перейти на OpenFlow 1.0 через недостатню гнучкість рішення в цілому.

Антіспуфінг за допомогою правил в свіч рівня стійки (ToR switch) при перенесенні в нього портів віртуальних машин за допомогою одного з механізмів тунелювання трафіку безпосередньо від інтерфейсів віртуальних машин. Як плюсів такого рішення можна відзначити зосередження логіки на свіч, відсутність необхідності її «розмазування» по програмним Свіча обчислювальних нод. Маршрут трафіку між машинами однієї обчислювальної Ноди завжди буде проходити через свіч, що може бути не завжди зручно.

top-of-rack (ToR) - це модель комутації, коли в кожній стійці стоїть комутатор, який обробляє трафік з серверів в цій стійці, і з'єднаний з комутатором ядра або з агрегують шаром (в залежності від кількості рівнів). Хоча і усталене назва top-of-rack - не затверджується, що саме у верхній частині стійки повинен фізично розташовуватися комутатор.

У такої схеми є ряд переваг - ймовірно основне - це скорочення кількості мідних кабелів. Кожна стійка з'єднується з наступним рівнем через комутатор, тому зникає потреба протягувати кабелі від окремих серверів далі стійки - всі кабелі залишаються в стійці. В цілому, вважається, що чим менше кабелів виходять зі стійки, тим краще, оскільки велика кількість мідних кабелів може ускладнювати перебіг повітря при охолодженні, складніше відстежити, який кабель куди йде, і вимагає додаткової інфраструктури для прокладки кабелів і з'єднань. Довгі «прокинути» кручений пари також можуть накладати обмеження на швидкість мережі.

У top-of-rack є і недоліки, які стануть помітними, коли кількість стійок в дата-центрі вашої компанії буде серйозно рости. Якщо припустити, що у вас скажімо 20 стійок, в кожній з яких коштує по 2 комутатора, то це 40 комутаторів, а з точки зору обслуговування - це вже не просто. Це 40 копій софта для комутатора для поновлення, 40 конфігураційних файлів, які треба створити і надійно архівувати, іншими словами - 40 місць, де «щось може піти не так».

Ще в такій архітектурі збільшуються вимоги до шару агрегації - зокрема щільність портів комутаторів на цьому шарі. Чим більше стійок підключені сюди через комутатор в своїй стійці, тим більше потенційно можливих проблем з масштабуванням.

Модель комутації end-of-row передбачає розташування комутатора, умовно, «в кінці ряду стійок» і обслуговування їм трафіку з усіх серверів з декількох стійок, розташованих в ряд. Знову ж фізично це не означає, що комутатор повинен бути чомусь саме в останній стійці. Таке розташування було прийнято для дублюючих комутаторів, які спочатку справді мали в різних кінцях ряду стійок, щоб наприклад якась раптова проблема типу протекшей даху в одному місці, не вирубала з роботи цілий ряд стійок.

У такій схемі сервери в стійці зазвичай з'єднуються щодо короткими RJ-45 кабелями з комутаційної панеллю в стійці, від якої йде щільний пучок кабелів, як правило через верх, над серверними стійками, до end-of-row комутатора.

End-of-row комутатор, це як правило рішення на базі модульного шасі, яке підтримує сотні серверних підключень. Таким чином, якщо у випадку з top-of-rack рішенням, кожна стійка була наче окремим модулем, то в даному випадку цілий ряд стійок умовно можна вважати за окремий модуль.

У попередньому прикладі, якщо ми умовно візьмемо по 10 стійок в ряд, то для 20 стійок знадобиться всього 4 end-of-row комутатора, на відміну від 40 комутаторів у випадку з top-of-rack конфігурацією. Тобто з точки зору підтримки - це в 10 разів менше потенційних турбот. Це, мабуть, головна перевага такої схеми.

Головний недолік такої схеми - це необхідність дуже уважно продумати кабельну схему для з'єднань, тому що кількість кабелів, необхідних для цього просто неймовірно, і все це може перетворитися в абсолютно некерований клубок.

У той же час невірно думати, що end-of-row дасть суттєву економію капітальних витрат. Наприклад 48-портова карта для end-of-row комутатора може коштувати приблизно стільки ж, скільки і 48-портовий комутатор, який Ви б поставили в стійку при top-of-rack вирішенні. Можлива економія може бути в обслуговуванні, оскільки обслуговувати істотно менша кількість end-of-row комутаторів виявиться все-таки простіше.

Антіспуфінг при перевірці полів в OpenFlow мережі - коли все свічі, фізичні та віртуальні, підключені до групи контролерів, які забезпечують, крім перенаправлення і трансформації полів трафіку всюди, його очищення на рівні програмного свіча обчислювальної (compute) Ноди. Це найскладніший і гнучкий з можливих варіантів, оскільки абсолютно вся логіка, починаючи від пересилання датаграмм всередині звичайного свічу, буде винесена в контролер. Неповні або неконсістентние правила можуть привести або до порушення зв'язності, або до порушення ізоляції, тому системи з великим відсотком реактивних (задаються динамічно за запитом від свіча) правил слід тестувати з допомогою, фреймворків на зразок NICE

Фреймворк - заготовки, шаблони для програмної платформи, що визначають структуру програмної системи; програмне забезпечення, що полегшує розробку і об'єднання різних модулів програмного проекту ..

Виділення сегмента мережі - рішення, що практикуються в великих гомогенних структурах, при цьому за групою віртуальних машин закріплюється або прив'язка до фізичних машинам (і портам фізичного свіча), або до тегу інкапсуляції (упаковка даних і функцій в єдиний компонент) будь-якого типу (vlan / vxlan / gre). Кордон фільтрації знаходиться на стику L2 сегмента, інакше кажучи, сегменту виділяється підмережа або набір підмереж і неможливість їх підміни обумовлюється роутингом у вищій інфраструктурі.

Як правило, фізичний сегмент мережі обмежений мережевим пристроєм, що забезпечує з'єднання вузлів сегмента з іншою мережею:

Комутатори (2-й рівень в моделі OSI)

Маршрутизатор (3-й рівень в моделі OSI)

2.6.2 Керування трафіком

Оптимізація маршрутів таким чином, щоб скористатися наявними можливостями мережевих лінків по-максимуму (інакше кажучи, знаходження максимуму Сума «min-cut» -разреза, який в деякому сенсі мінімальний, для всіх пар взаємодіючих кінцевих точок, з урахуванням їх ваг, тобто, пріоритетів QoS). IGP (протокол, який використовується для обміну інформацією про маршрутизації між спільно працюють маршрутизаторами в мережі Internet), покликані вирішувати цю проблему, в загальному випадку є недостатньо гнучкими - трафік може бути відсортований тільки на підставі заздалегідь виділених міток QoS і про динамічному аналізі та перерозподілі трафіку припадає не думати. Для OpenFlow, оскільки кошти аналізу окремих елементів трафіку є невід'ємною частиною протоколу, вирішити це завдання досить нескладно - достатньо побудувати коректно працює класифікатор окремих потоків. Ще один безперечний плюс OpenFlow, в цьому випадку, в централізованому підрахунку стратегії форвардинга можливо врахувати безліч додаткових параметрів, які просто не включені ні в один зі стандартів IGP.

Port Forwarding - це технологія, яка дозволяє звертатися з Інтернет до комп'ютера у внутрішній мережі за маршрутизатором, що використовують NAT (NAPT). Доступ здійснюється за допомогою перенаправлення трафіку певних портів з зовнішнього адреси маршрутизатора на адресу обраного комп'ютера в локальній мережі.

Проектування мережі навіть невеликого датацентру з гетерогенним наповненням (вміст одночасно безлічі роздрібних пользоватей без фізичної прив'язки групи машин до стійки), призводить до задачі побудови розподілених L2-over-L3 мереж (overlay networks) с допомогою одного з існуючих механізмів, через неможливість технічно помістити десятки тисяч віртуальних хостів в один широкомовний сегмент звичайними способами.

Overlay networks - загальний випадок логічної мережі, створюваної поверх іншої мережі. Вузли оверлейной мережі можуть бути пов'язані або фізичним з'єднанням, або логічним, для якого в основній мережі існують один або кілька відповідних маршрутів з фізичних з'єднань

Зазначені технології дозволяють «розвантажити» логіку форвардинга, оскільки обладнання тепер оперує мітками, відповідних груп хостів замість окремих адрес в приватних (і, можливо, публічних) сегментах користувальницьких мереж. За дешевизною і порівняльною простотою впровадження криється прив'язка як мінімум до виробника мережевого устаткування і кінцева недетерминированность - якщо відволіктися від деталізації, все оверлейні протоколи надають той, якого навчають свіч всередині окремої мітки, що може викликати труднощі при оптимізації трафіку всередині оверлейного сегмента, через «развязанностью» протоколів маршрутизації третього рівня і механізмів самого оверлею. Вибираючи OpenFlow, ми зводимо все управління трафіком до одного рівня прийняття рішень - мережевого контроллера. Оверлеї або заміщає їх власний механізм, безумовно, можуть виконувати ту ж роль щодо зменшення обсягу правил в Свіча-агрегатор, а оптимізація напрямки трафіку на ToR Свіча відбуватиметься, базуючись на довільному наборі метрик, на відміну від простої балансування.

РОЗДІЛ 3. ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО ПОЛОЖЕННЯ SDN-КОНТРОЛЕРА

3.1 Встановлення ОС

Спочатку треба встановити OracleVM, розгорнути зображення SDNHub. Запускаємо ОС. Оскільки ми використовуємо готовий образ системи, встановлюються майже всі необхідні пакети. Залишається лише налаштувати їх. Запускаємо командний рядок. Ми налаштуємо мережеву операційну систему.

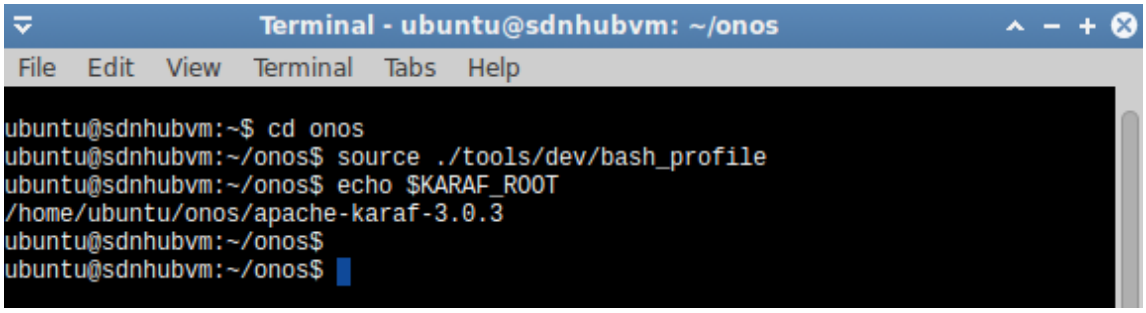


Рисунок 3.1. Вікно налаштування

Далі запускаємо ONOS з командою ok clean або karaf clean.

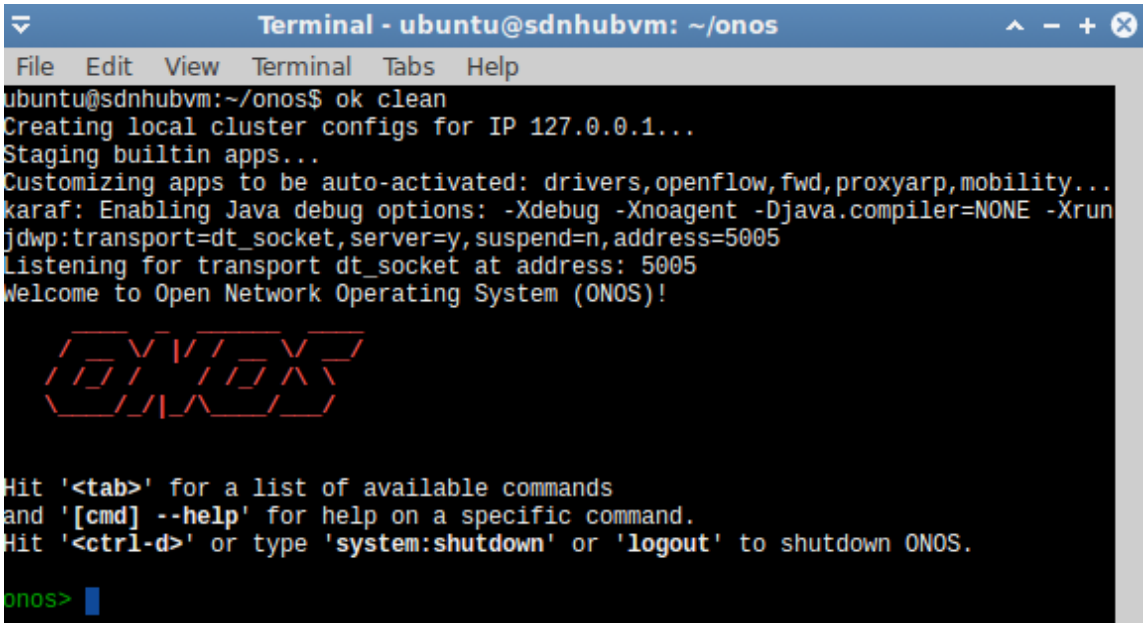


Рисунок 3.2. Вікно запуску ONOS

Повний список команд доступний за цим посиланням:
https://wiki.onosproject.org/display/ONOS/Appendix+A+%3A+CLI+commands
Або за допомогою базового підручника ONOS за наступним посиланням: https://wiki.onosproject.org/display/ONOS/Basic+ONOS+Tutorial

3.2 Моделювання оптимального положення SDN-контролера

Проводимо аналіз способів для розташування контролерів в програмно-визначених мережах, розраховуємо оптимальне розташування контролера з використанням методу оптимальності по Парето, Pareto-Optimal Resilient Controller Placement

Набір інструментів POCO-PLC, що полегшує аналіз і оптимізацію розміщення контролера в мережах SDN в динамічних умовах.

Для визначення оптимального маршруту було використано наступний алгоритм.

1. Завантажуємо POCO з https://github.com/lsinfo3/poco

2. Завантажуємо localbackup.zip з https://euros.informatik.uni-wuerzburg.de/public/localbackup.zip

3. З http://www.topology-zoo.org/dataset.html завантаження (вибераємо варіанти з багатьма мережевими пристроями) мережева модель (Format GraphML)

4. Запускаємо Matlab. Відкриваємо папку POCO (змінюємо призначення). Запускаємо poco_GUI.

6. У вікні провідника, який відкриється, вказуємо шлях до файлу.

7. Тепер ми можемо побачити свою мережу (Рис. GTS Poland network (Європа))

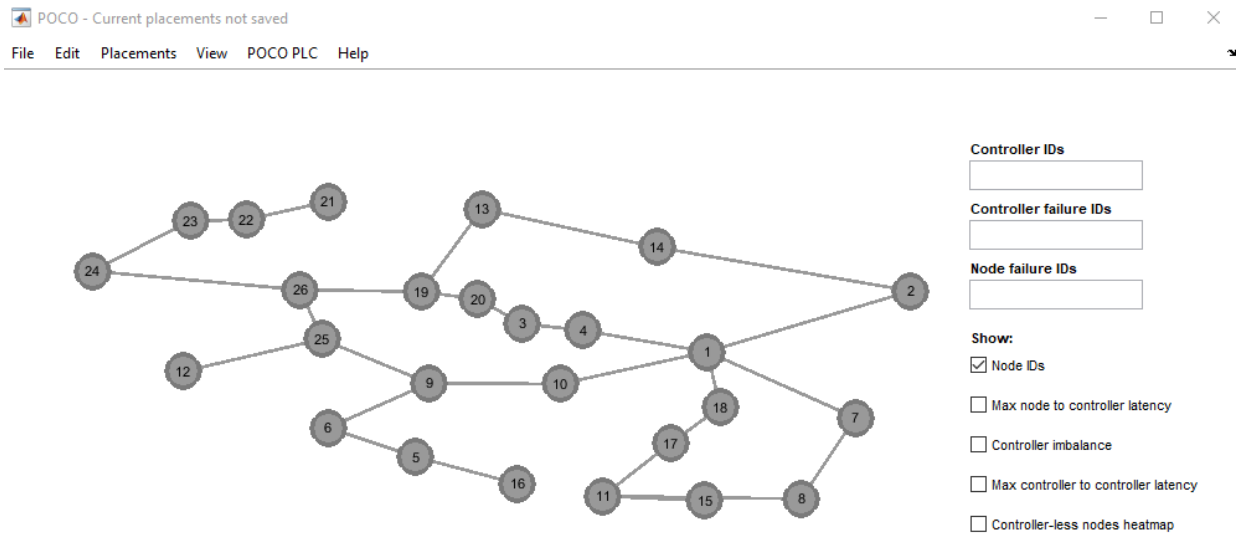
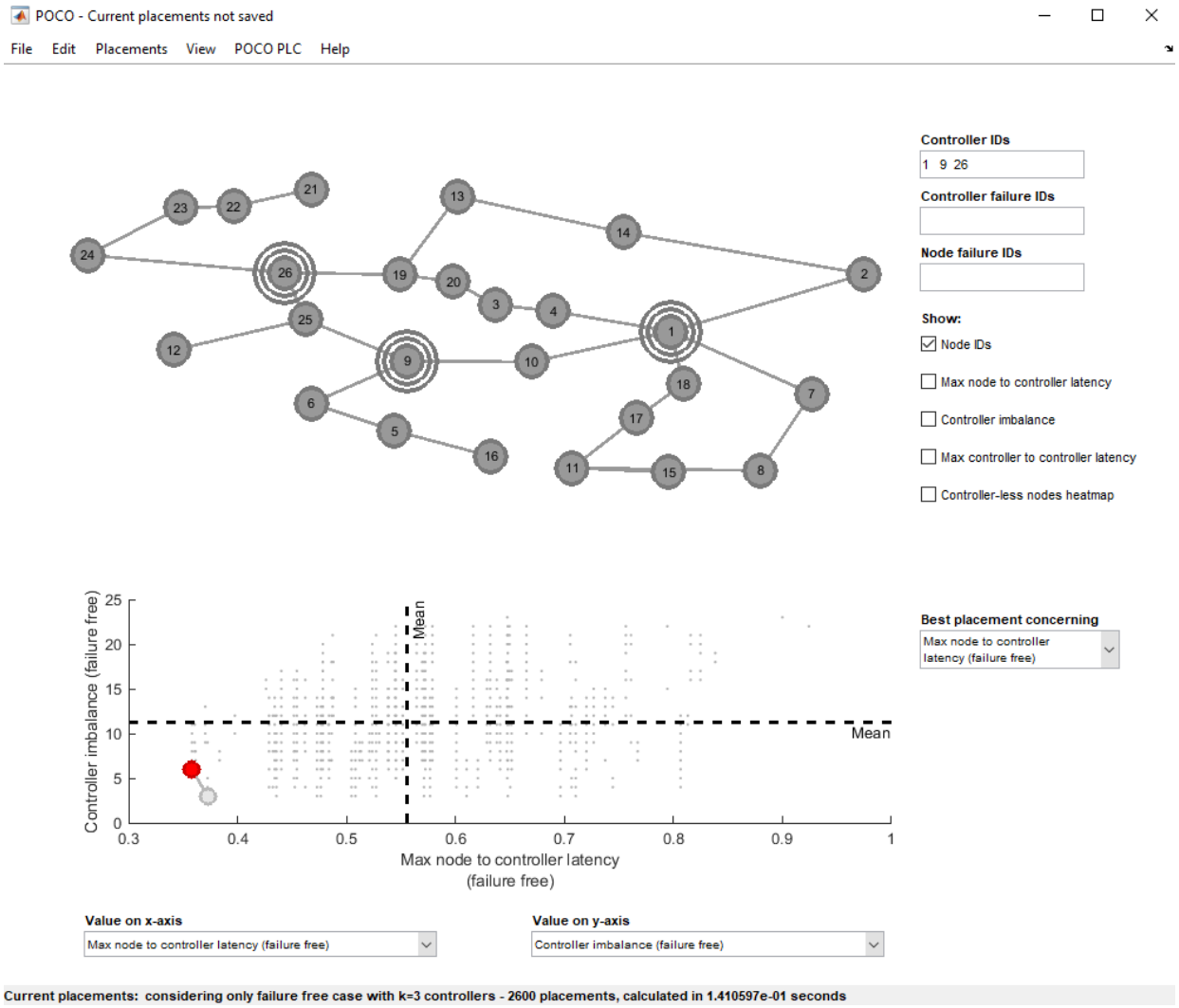


Рисунок 3.3. GTS Poland network (Європа)

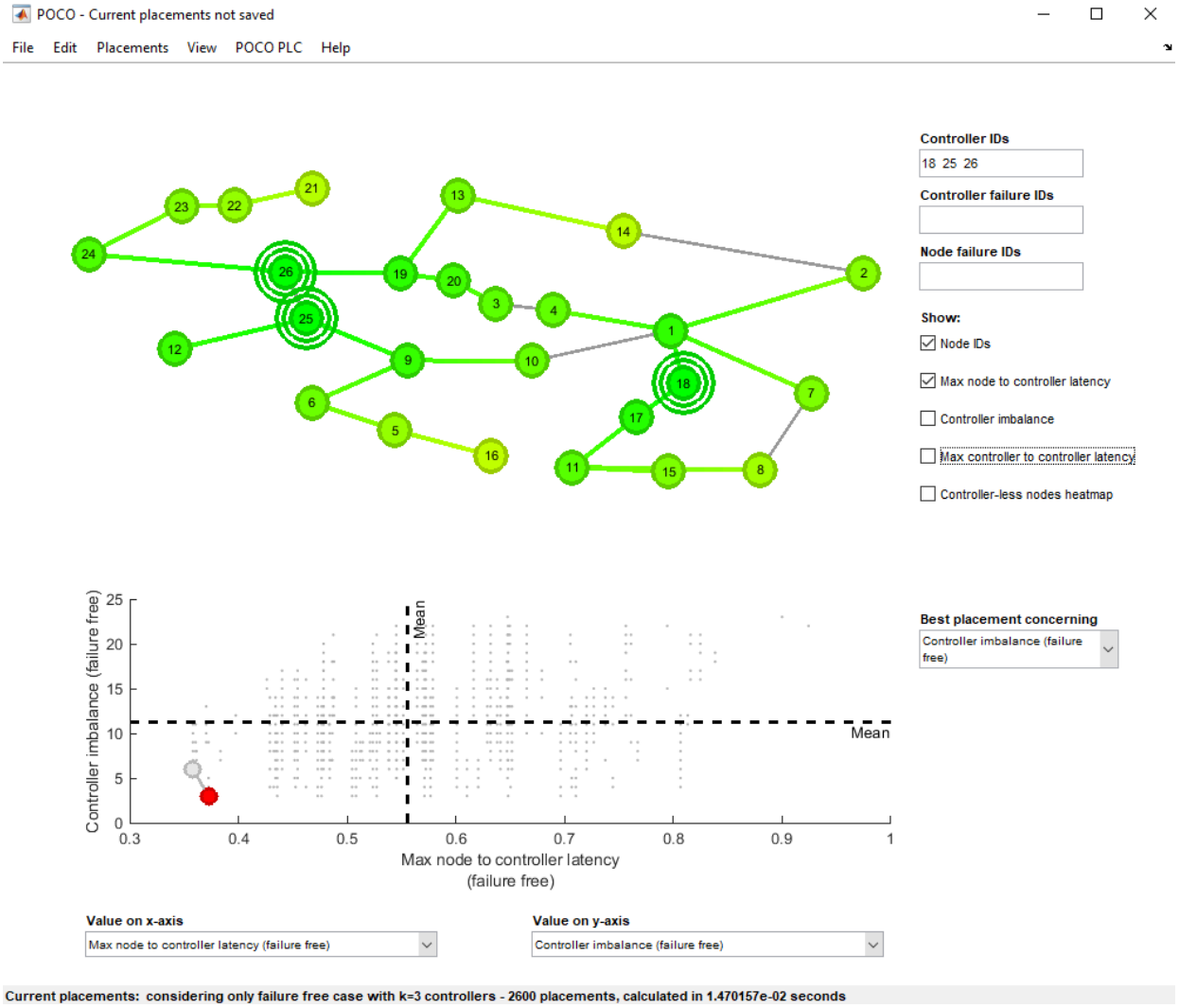
Тепер буде визначена конфігурація сценарію. Вона включає в себе кількість контролерів для дерева відмов. Натисніть Placemet -> Calculate placement -> дерево відмов -> k (1-5). У прикладі ми розміщуємо різні контролери номерів.



Натискаємо дисбаланс контролера (k = 3). Ми побачимо високо завантажені ділянки мережі (позначені червоним кольором)

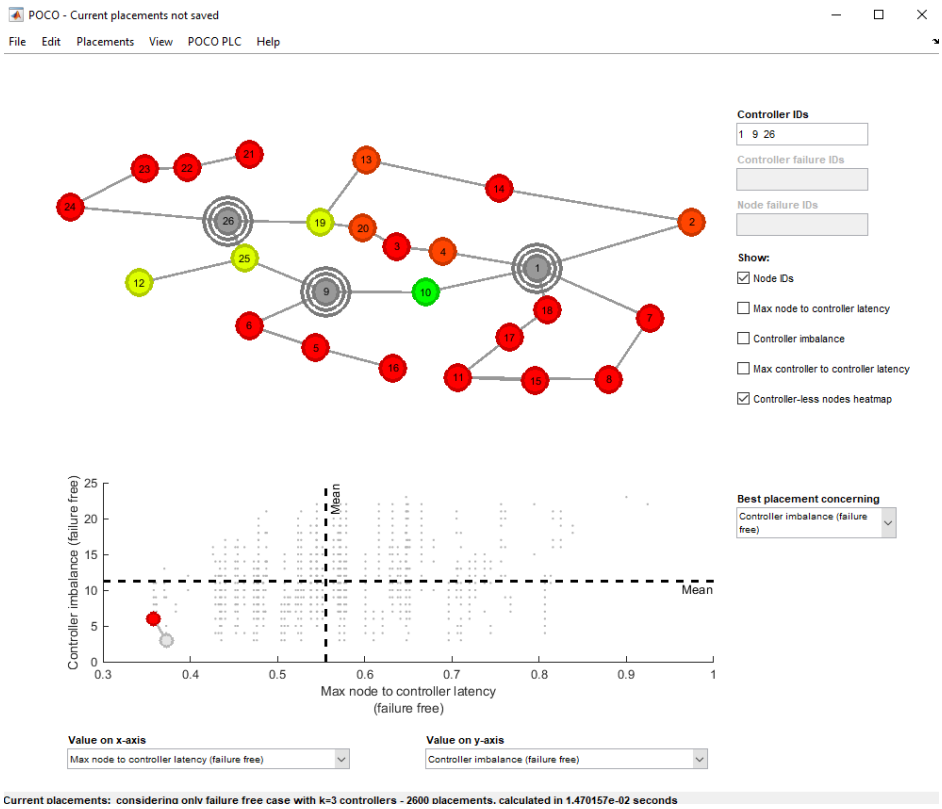
Чим більше вузлів контролює контролер, тим вища навантаження на цей контролер. Якщо кількість запитів вузла-контролера в мережі зростає, то ймовірність додаткових затримок через черги в системі контролера зростає. Таким чином, у сценаріях, коли вузли часто зв'язуються зі своїм контролером, необхідно, щоб призначення вузла-контролера було добре збалансованим.

Натискаємо «затримка контролера максимального вузла».



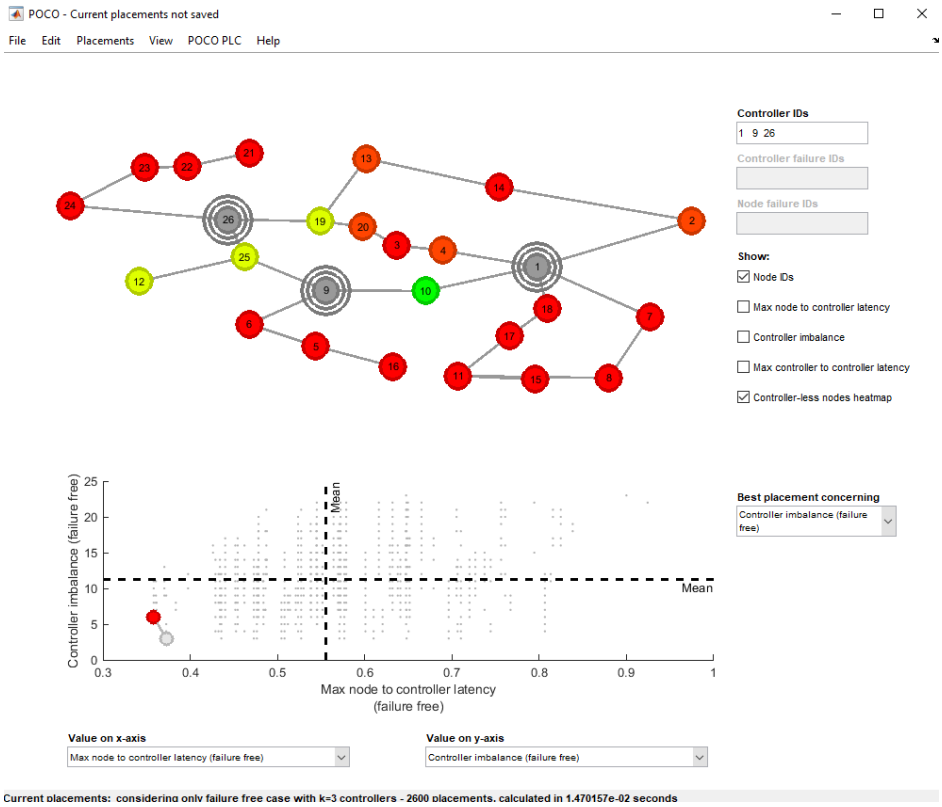
Коли розглядаються метрики затримки та надійності, як правило, не існує жодного найкращого рішення для розміщення контролера, а взагалі компроміс. Більшість схем розгортання, заснованих на затримці, в основному зосереджені на затримці передачі (TD) або затримці розповсюдження (PD)

Клацаємо «вузли теплообміну без контролерів». Вказує, чи є ризик без контролера вузлів.

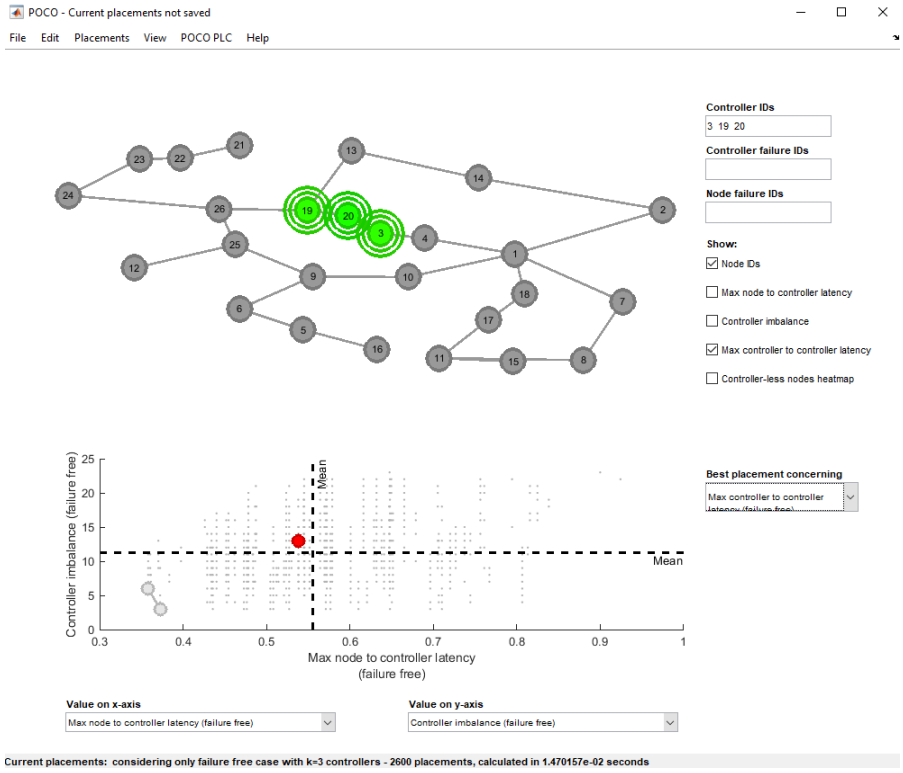


Обираємо «вузли теплообміну без контролерів». Нам вказують, чи є ризик без контролера вузлів.

На графіку внизу при виборі різних варіантів показана оптимальність. Вертикальне і горизонтальне сходження (пунктир) - і є найоптимальніший варіант. Як видно, на останньому рисунку, було змінено розташування на близьке до оптимального, і воно виявилося розташуванням контролерів поруч один з одним, але не були враховані інші параметри мережі, тому оптимальним воно і не є.



Натискаємо «Максимальний час затримки контролера».



4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було дослідження бездротових мереж з низьким енергоспоживанням та розробка з'єднання низько швидкісних периферійних компонентів з мікроконтролером в лабораторії екологічного призначення. Так як в процесі проектування використовувалося різне програмне забезпечення, то аналіз потенційно небезпечних виробничих чинників виконується для робочого місця, на якому використовується персональний комп'ютер.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

4.1.1 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 24.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [1].

Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та

перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [2].

4.2 Аналіз стану умов праці

Робота над створенням системи емоційної класифікації проходитиме в приміщенні багатоквартирного будинку. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об'єм, $м^3$	75

Згідно з [3] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [4] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Приміщення кабінету знаходиться на другому поверсі трьох поверхової будівлі і має об'єм 78 $м^3$, площу – 25 $м^2$. У цьому кабінеті обладнано три місця праці, з яких два укомплектовані ПК.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум в лабораторії знаходиться на рівні 50 дБА. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

4.2.3 Навантаження та напруженість процесу праці

Під час виконання магістерської роботи: за фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав’язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також профілактичних заходів.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших

приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є наступні:

– робоча напруга U = +220В ± 5%;
– робочий струм I = 2А;
– споживана потужність P = 350 Вт.

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання.

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

- застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

- застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

- виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно до [5] відносяться до пожежонебезпечної зони класу П-Iіа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа,

шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [6] і наведені в табл. 4.2:

Таблиця 4.2 – Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [6]. Рівні позитивних і негативних іонів у повітрі мають відповідати [6].

Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2015 [3]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН В.2.5-28:2015 [3] і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2+b^2}\cdot S_b = \left(1/8 \div 1/10\right)\cdot S_n \tag{4.1}$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$$S_n = a \cdot b = 5 \cdot 5 = 25 \text{ м}^2$$

$$S_{вік} = 1/8 \cdot 25 = 3{,}125 \text{ м}^2$$

Приймаємо 2 вікна площею $S = 1{,}6 \text{ м}^2$ кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типу ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *n* виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \tag{4.2}$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 25 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$\text{n} = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2.$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.4.3 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп’ютерів (зумовлений як роботою системних блоків, клавіатури, так і друкуванням на принтерах, а також зовнішніми чинниками), коливається у межах 50–65 дБА [7]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. У залах опрацювання інформації та комп’ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Віброізоляцію можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [7]. Допустимий рівень вібрацій

на робочому місці: для 1 ступеня шкідливості до 3 дБ; для 2-3 - 1-6 дБ; для 3 - більше 6 дБ.

4.4.4 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти) і установки в віконному отворі автономного кондиціонера БК-2000. Цей метод забезпечує приплив потрібної кількості свіжого повітря, що визначається в СНіП (30 $м^3$ на годину на одного працюючого).

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;
- експлуатацію сертифікованого обладнання;
- дотримання заходів електробезпеки;
- забезпечення оптимальних параметрів мікроклімату;
- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);
- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

- не залишати включені електроприлади без нагляду;

- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, спалахнути (канцелярські товари, сувенірну продукцію тощо).

Вимоги безпеки при надзвичайних ситуаціях:

1) При раптовому припиненні подачі електричної енергії вимкнути всі пристрої ПК в такій послідовності: периферійні пристрої, ВДТ, системний блок, стабілізатор (або блок безперервного живлення). Витягнути вилки з розеток. При наявності ознак горіння (дим, запах горілого) необхідно вимкнути всі пристрої ПК, знайти місце загоряння і виконати всі можливі заходи для його ліквідації, попередивши терміново про це керівництво.

2) При замиканні, перевантаженні електричного струму на електричному обладнанні, внаслідок ураження грозової блискавки та ймовірної небезпеки ураженням електричним струмом, приймають наступне:

- попередження замикання здійснюється правильним вибором, монтажем експлуатації мереж;

- застосування захисту схем у вигляді швидкодіючих реле, а також вимикачів, плавких запобіжників, автоматичних вимикачів.

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Загальний опір захисного заземлення визначається за формулою:

$$R_{ззп} = \frac{R_з \cdot R_п}{R_п \cdot n \cdot \eta_з + R_з \cdot \eta_п}, \qquad (4.3)$$

де Rз - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

Rш - опір опори, яке з'єднує заземлювачі, Ом;

n - кількість заземлювачів;

ηз - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; ηз = 0,7

ηш - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; ηш = 0,5;

Опір заземлення визначається за формулою:

$$R_з = \frac{\rho}{2\pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right), \quad (4.4)$$

де ρ - питомий опір ґрунту, залежить від типу грунту, Ом·м;

для піску - А00 ÷ 700 Ом·м; приймаємо ρ = А00 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3} \left(\ln \frac{2 \cdot 3}{0{,}05} + \frac{1}{2} \ln \frac{4 \cdot 2 + 3}{4 \cdot 2 - 3} \right) = 110 \text{, Ом}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_ш = \frac{\rho}{2\pi \cdot L} \cdot \ln \frac{2 \cdot L^2}{b \cdot t^1}, \quad (4.5)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; t_1 = 0,5 м.

$$R_п = \frac{400}{2 \cdot 3{,}14 \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0{,}03 \cdot 0{,}5} = 5{,}99 \text{, Ом}$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_з}{4 \cdot \eta_з}, \quad (4.6)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5{,}99}{5{,}99 \cdot 79 \cdot 0{,}7 + 110 \cdot 0{,}5} = 1{,}7 \text{ Ом}$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

- іскри і дуги коротких замикань;
- перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;
- іскри при розмиканні і розмиканні ланцюгів;
- розряди статичної електрики;
- необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

4.6 Охорона навколишнього природного середовища

4.4.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, а саме: аналіз математичних методів оцінки надійності БСМ і програмних продуктів для імітаційного моделювання БСМ, вибір найбільш підходящої системи для оцінки працездатності БСМ та оцінка впливу перешкод і потужності передачі радіосигналу на працездатність БСМ., процес виконання якої впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища» [8], Законом України «Про забезпечення санітарного та епідемічного благополуччя населення» [9], Законом України «Про відходи» [10], Законом України «Про охорону атмосферного повітря» [11], Законом України «Про захист населення і територій від

надзвичайних ситуацій техногенного та природного характеру» [12], Водний кодекс України[13].

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на знешкодження, утилізацію, тощо в ІТ галузі.

Вплив на атмосферне повітря при нормальних умовах праці не оказує, бо не має в приміщенні сканерів, принтерів та інших джерел викиду забруднюючих речовин в повітря робочої зони.

В процесі створення/розробки програми на робочому місці виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

— Відпрацьовані люмінесцентні лампи - I клас небезпеки

— Змінні носії інформації - IV клас небезпеки

— Макулатура - IV клас небезпеки

— Матеріали пакувальні пластмасові забруднені (ємності з-під тонеру, фарби, інш.) - IV клас небезпеки

— Побутові відходи - IV клас небезпеки

—

4.5 Висновки до розділу 4

Завдяки виконаній роботі був проведений аналіз умов праці, небезпечних та шкідливих чинників, з якими стикається робітник. Також було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі. Описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам, було комфортним і безпечним для робітника. Також впроваджені організаційні заходи з пожежної безпеки.

Було наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

4.6 Перелік посилань до розділу 4

1. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z0231-05 - 21.12.2017 р.

2. Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України (НАПБ Б.02.005-2003) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z1148-03 - 21.12.2017 р.

3. ДБН В.2.5-28:2015 Природнє і штучне освітлення [Електронний ресурс] / dbn.co.ua - Режим доступу: www.URL: http://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188

4. Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98) [Електронний ресурс] / Педрада - Режим доступу: www.URL: http://zakon.pedrada.com.ua/regulations/10637/478672/ - 22.12.2017 р.

5. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою (НАПБ Б.03.002-2007) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/32980/doc-НАПБ_Б.03.002.-2007 - 23.12.2017 р.

6. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.4.042-99) [Електронний ресурс] / UAinfo - Режим доступу: www.URL: http://ua-info.biz/legal/basetp/ua-zmptae.htm - 23.12.2017 р.

7. Санітарні норми виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.4.037-99) [Електронний ресурс] / Нормативно-директивні документи МОЗ України - Режим доступу: www.URL: http://mozdocs.kiev.ua/view.php?id=1789 - 23.12.2017 р.

8. Законом України «Про охорону навколишнього природного середовища» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/1264-12

9. Законом України «Про забезпечення санітарного та епідемічного благополуччя населення» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/4004-12

10. Законом України «Про відходи» [Електронний ресурс] / rada.gov.ua - Режим

доступу: www.URL:https://zakon.rada.gov.ua/laws/show/187/98-%D0%B2%D1%80

11. Законом України «Про охорону атмосферного повітря» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL:https://zakon.rada.gov.ua/laws/show/2707-12

12. Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/1809-14

13. Водний кодекс України [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80

14. ДСН 3.3.4.039-99 Санітарні норми виробничої та загальної вібрації

15. ГОСТ 12.1.006-84

16. ГОСТ 12.1.030-81 ССБТ. Электробезопасность. Защитное заземление. Зануление [16]

17. ГОСТ 13109-97. Електрична енергія. Сумісність технічних засобів. Норми якості електричної енергії в системах електропостачання загального призначення [17]

18. НПАОП 0.00-1.28-10. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин

ВИСНОВКИ

У магістерській роботі було досліджено стан публічних ІТ-просторів сучасних міст, надано аналіз публічного простору міста, способів організації зв’язку в публічному просторі.

Створено збір матеріалу про сформовані, сучасні, мережі Інтернет та проведено аналіз можливих рішень, для вдосконалення каналів зв’язку Інтернет.

Розроблені рекомендації щодо покращення стану сучасних мереж Інтернет, обґрунтуванні особливості формування інформаційних мереж публічних просторів, для створення комфортного, розвиненого міського середовища

Визначений комплексний підхід до формування нових мереж Інтернет в публічних просторах міста як методологічна основа перетворення їх середовища. Запропоновано підходи до реконструкції існуючих мереж Інтернет, з урахуванням ролі і можливостей розподілених мереж Інтернет, як способу й засобу гармонізації середовища проживання городянина.

Виконано моделювання оптимального розташування контролера локальних сітей у публічному просторі міста.

ЛІТЕРАТУРА

1. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z0231-05 - 21.12.2017 р.

2. Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України (НАПБ Б.02.005-2003) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z1148-03 - 21.12.2017 р.

3. ДБН В.2.5-28:2015 Природнє і штучне освітлення [Електронний ресурс] / dbn.co.ua - Режим доступу: www.URL: http://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188

4. Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98) [Електронний ресурс] / Педрада - Режим доступу: www.URL: http://zakon.pedrada.com.ua/regulations/10637/478672/ - 22.12.2017 р.

5. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою (НАПБ Б.03.002-2007) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/32980/doc-НАПБ_Б.03.002.-2007 - 23.12.2017 р.

6. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.4.042-99) [Електронний ресурс] / UAinfo - Режим доступу: www.URL: http://ua-info.biz/legal/basetp/ua-zmptae.htm - 23.12.2017 р.

7. Санітарні норми виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.4.037-99) [Електронний ресурс] / Нормативно-директивні документи МОЗ України - Режим доступу: www.URL: http://mozdocs.kiev.ua/view.php?id=1789 - 23.12.2017 р.

8. Законом України «Про охорону навколишнього природного середовища» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/1264-12

9. Законом України «Про забезпечення санітарного та епідемічного благополуччя населення» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/4004-12

10. Законом України «Про відходи» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL:https://zakon.rada.gov.ua/laws/show/187/98-%D0%B2%D1%80

11. Законом України «Про охорону атмосферного повітря» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL:https://zakon.rada.gov.ua/laws/show/2707-12

12. Законом України «Про захист населення і територій від надзвичайних ситуацій

техногенного та природного характеру» [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/1809-14

13. Водний кодекс України [Електронний ресурс] / rada.gov.ua - Режим доступу: www.URL: https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80

14. ДСН 3.3.4.039-99 Санітарні норми виробничої та загальної вібрації

15. ГОСТ 12.1.006-84

16. ГОСТ 12.1.030-81 ССБТ. Электробезопасность. Защитное заземление. Зануление [16]

17. ГОСТ 13109-97. Електрична енергія. Сумісність технічних засобів. Норми якості електричної енергії в системах електропостачання загального призначення [17]

18. НПАОП 0.00-1.28-10. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин

19. https://habr.com/company/hpe/blog/160531/

20. https://habr.com/company/hpe/blog/255363/

21. https://abc.vvsu.ru/books/gis_inet/page0006.asp

22. https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C

23. https://en.wikipedia.org/wiki/Infrastructure_as_Code

24. https://habr.com/company/cbs/blog/301000/

25. https://devops.com/automation-provisioning-configuration-management-puppet/

26. https://ru.wikipedia.org/wiki/SNMP

27. https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%BD%D0%BE%D0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%B8

28. https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B7%D0%B0%D1%82%D1%80%D0%B0%D1%82%D1%8B

29. https://ru.wikipedia.org/wiki/OpenFlow

30. https://sdnblog.ru/openflow-foundation-part1/

31. https://www.packetdesign.com/

32. https://www.ciena.ru/

33. http://www.donriver.com/

34. https://www.osp.ru/lan/2015/09/13046914/

35. https://docplayer.ru/26313075-Problemy-sovremennyh-kompyuternyh-setey.html

36. https://studme.org/54454/informatika/problemy_sovremennogo_interneta
37. https://dev.by/news/internet-challenges-by-tim-berners-lee
38. https://docs.microsoft.com
39. https://www.ciena.ru/insights/what-is/What-is-SDN_ru_RU.html
40. https://ru.wikipedia.org/wiki/QoS
41. https://ru.wikipedia.org/wiki/Libvirt
42. https://www.xelent.ru/blog/top-of-rack-i-end-of-row-kommutatoryi/
43. https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B5%D0%B9%D0%BC%D0%B2%D0%BE%D1%80%D0%BA
44. https://www.osp.ru/iz/rusnet/articles/13049937
45. http://www.xakep.ru/post/60886/\
46. http://ru.wikipedia.org/wiki/Cgroups
47. https://github.com/mininet/mininet/wiki/Simple-Router
48. http://pastebin.com/YS6aguDR
49. http://docs.openvswitch.org/en/latest/faq/configuration/
50. http://csie.nqu.edu.tw/smallko/sdn/vlc.htm
51. EGILMEZ, HILMI E., CIVANLAR, SEYHAN і TEKALP, A. MURAT, 2013, Оптимізаційні рамки для адаптованого відеопотоку з підтримкою QoS над OpenFlow Networks. IEEE транзакції з мультимедіа. 2013. Vol. 15, №. 3, с. 710-715. DOI 10.1109 / tmm.2012.2232645. Інститут інженерів електротехніки та електроніки (IEEE)
52. ІНСТРУМЕНТИ, SDN і РЕСУРСИ, SDN, 2018, ресурси SDN. Sdntutorials.com [онлайн]. 2018. [Доступ 4 лютого 2018 року]. Доступно з: http://sdntutorials.com/sdn-resources/
53. Hock D., Hartmann M., Gebert S., Jarschel M., Zinner T., Tran-Gia P. Pareto-Optimal Resilient Controller Placement in SDN-based Core Networks. Proceedings of the 2013 25th International Teletraffic Congress (ITC). 2013. pp.
54. Pareto efficiency. Enwikipediaorg. 2018. Available at: https://en.wikipedia.org/wiki/Pareto_optimality. Accessed February 4, 2018.
55. HOCK, DAVID, HARTMANN, MATTHIAS, GEBERT, STEFFEN, ZINNER, THOMAS and TRAN-GIA, PHUOC, 2014, POCO-PLC: Enabling dynamic pareto-optimal resilient controller placement in SDN networks. 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2014. DOI 10.1109/infcomw.2014.6849182. IEEE
56. Kshira Sagar Sahoo, Sampa Sahoo, Sambit Kumar Mishra, Sagarika Mohanty, Bibhudatta Sahoo. Analyzing Controller Placement in Software Defined Networks. National

Conference on Next Generation Computing and its Applications in Computer Science & Technology, 2016.

57. K-means and K-medoids. Mathleacuk. 2018. Available at: http://www.math.le.ac.uk/people/ag153/homepage/KmeansKmedoids/Kmeans_Kmedoids.html. Accessed February 4, 2018.

58. The Internet Topology Zoo. Topology-zooorg. 2018. Available at: http://www.topology-zoo.org/dataset.html. Accessed February 4, 2018.

59. POCO-Framework for Pareto-Optimal Resilient Controller Placement in SDN-based Core Networks

60. https://www.researchgate.net/publication/323974224_A_survey_and_classification_of_controller_placement_problem_in_SDN

61. https://github.com/lsinfo3/poco

62. https://euros.informatik.uni-wuerzburg.de/public/localbackup.zip

63. http://www.topology-zoo.org/dataset.html

64. http://www.topology-zoo.org/dataset.html

ДОДАТОК А

Порівняльна таблиця основних характеристик протоколів динамічної маршрутизації

Таблиця 2.3 Порівняльна таблиця основних характеристик протоколів динамічної маршрутизації

BGP v.4	різні методи аутентифікації	вектор відстані	Різні метрики (напівавтомат)	+	+
EIGRP	Аутентифікація за ключем MD5	комбіно ваний	різні метрики	+	+
OSPF	Відкритий пароль або аутентифікація по ключу MD5	стан каналів зв'язку	однакові метрики	+	+
IS-IS	-	стан каналів зв'язку	однакові метрики	-	-
IGRP	-	вектор відстані	різні метрики	-	-
RIP v.2	Відкритий пароль або аутентифікація по ключу MD5	вектор відстані	-	-	+
критерії / протоколи	Безпека	Тип алгоритму	балансування навантаження	об'єднання маршрутів	маски підмереж пере довжини

Продовження таблиці 2.3 Порівняльна таблиця основних характеристик протоколів динамічної маршрутизації						
65534	довільна	-	тільки зміни	Розбиття мережі на автономні системи і опис взаємодії між ними	відкритий	+
255	Комбінований	+	тільки зміни	-	Тільки на обладнанні Cisco Systems	+
65534	Одна основна і три додаткові	+	тільки зміни	Виділення центральної області і зв'язкових областей	відкритий	+
1024	Одна основна і три додаткові	+	тільки зміни	Виділення центральної області і зв'язкових областей	відкритий	-
255 (Реком. <50)	Комбінований	+	Вся таблиця	-	Тільки на обладнанні Cisco Systems	-
15	одна основна	-	Вся таблиця	-	відкритий	-
Максимальна кількість маршрутизаторів в мережі	Облік в метриці різних характеристик шляху	підтримка QoS	оновлення маршрутної інформації	необхідність логічної підготовки мережі	доступність реалізації	підтримка IPv6

ДОДАТОК Б

Аналіз небезпечних і шкідливих виробничих факторів

Таблиця Б- Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
nabqg•			
- підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	ДСН 3.3.4.042-99 [6]
- підвищений рівень шуму на робочому місці	-//-	2	ДСН 3.3.4.037-99 [7]
- підвищений рівень вібрації	-//-	2	ДСН 3.3.4.039-99 [14]
- підвищена або знижена вологість повітря	-//-	2	ДСН 3.3.4.042-99 [6]
- підвищена або знижена рухливість повітря	-//-	1	ДСН 3.3.4.042-99 [6]
- підвищений рівень іонізуючого випромінення в робочій зони	-//-	2	ДСН 3.3.4.042-99 [6] ГОСТ 12.1.006-84 [15]
- підвищений рівень електромагнітного випромінення	-//-	2	ГОСТ 12.1.006-84 [15]
- підвищений рівень напруги електричної	-//-	4	ГОСТ 12.1.030-81 [16]

мережі, замикання якої може відбутися через тіло людини			ГОСТ 13109-97 [17]
- підвищена напруженість електричного поля	-//-	2	ГОСТ 12.1.006-84 [15]
- підвищена напруженість магнітного поля	-//-	2	ГОСТ 12.1.006-84 [15]
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015 [3]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015 [3]
- підвищена яскравість світла	порушення умов праці (організації місця праці- налагодження моніторів)	1	ДСанПіН 3.3.2.007-98 [4]
- понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98 [4]
of•qg•			
ikbohnaheh]•qg•			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 [18] ДСанПіН 3.3.2.007-98 [4]
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	НПАОП 0.00-1.28-10 [18] ДСанПіН 3.3.2.007-98 [4]

ДОДАТОК В

Електронні матеріали презентації

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
Факультет інформаційних технологій та електроніки
Кафедра комп'ютерних наук та інженерії

кваліфікаційна робота освітнього ступеня магістр
123 «Комп'ютерна інженерія»

МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ МЕРЕЖЕВОГО ЗВ'ЯЗКУ В ПУБЛІЧНОМУ ПРОСТОРІ МІСТА

Виконав: студент групи КІ—17дм
Татарченко З.С.
Керівник: доц. Скарга-Бандурова
Інна Сергіївна.

Актуальність дослідження визначається незадовільним станом публічних ІТ-просторів сучасних міст. Крім того, незадовільна технологічна обстановка потребує рекомендаційного підходу до міських територій з позицій концепції сталого розвитку, інфраструктури, що в сучасних умовах потребує перепляду принципів подальшої взаємодії технологічний й інформаційних пріоритетів у розвитку середовища публічних просторів як територій з підвищеною концентрацією активності городян, з урахуванням необхідності створення сприятливих умов індивідуалізації і безпеки міського середовища.

Мета роботи - обґрунтувати особливості формування інформаційних мереж публічних просторів, для створення комфортного, розвиненого міського середовища.

Відповідно до цього визначені завдання дослідження:

- аналіз публічного простору міста;
- аналіз способів організації зв'язку в публічному просторі;
- збір матеріалу про сформовані, сучасні, мережі Інтернет;
- аналіз можливих рішень, для вдосконалення каналів зв'язку Інтернет;
- розробка рекомендацій щодо покращення стану сучасних мереж Інтернет;
- розробка рекомендацій з правил охорони праці.

Об'єкт дослідження – процеси формування ІТ-мереж публічних просторів.

Предмет дослідження – сучасні мережі Інтернет.

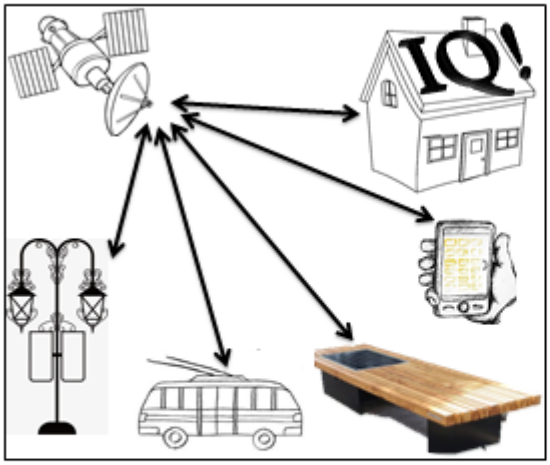
Практична значимість роботи

- ✓ Визначений комплексний підхід до формування нових мереж Інтернет в публічних просторах міста як методологічна основа перетворення їх середовища.
- ✓ Запропоновано підходи до реконструкції існуючих мереж Інтернет, з урахуванням ролі і можливостей розподілених мереж Інтернет, як способу й засобу гармонізації середовища проживання городянина.
- ✓ Виконано моделювання оптимального розташування контролера в публічному просторі міста.

Методи дослідження

Орієнтуючись на поставлені мету і завдання, а також на можливості в зборі матеріалів, ми спиралися в своїй роботі на літературний, порівняльний, статистичний методи, використовували методи, засновані на системному підході: системно-структурний аналіз, програмно-цільове планування, інформаційне і математичне моделювання.

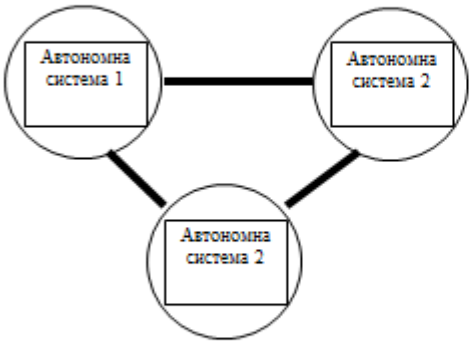
Способи організації зв'язку в публічному просторі



На відміну від більшості областей техніки, промисловість побудови комп'ютерних мереж за останні двадцять років практично не зазнала істотних змін.
В результаті, мережі все ще занадто дорогі, складні і ними важко керувати.

Під публічним простором слід розуміти загальнодоступні місця, пристосовані для перебування людей, в межах яких відбувається переважна більшість їх соціальних взаємодій. Серед таких виступають парки, сквери, площі, вулиці, торгові будинки - місця масового скупчення людей та ін.

Сучасні, мережі Інтернет



В даний час основу мережі Інтернет складають високошвидкісні магістральні мережі. Незалежні мережі підключаються до магістральної мережі через точки мережевого доступу NAP (Network Access Point).
Незалежні мережі розглядаються як автономні системи, тобто кожна з них має власне адміністративне управління і власні протоколи маршрутизації. Зміна протоколів маршрутизації всередині автономної системи не впливає на роботу інших систем. Розподіл мережі Інтернет на автономні системи дозволяє розподілити інформацію про топології всієї мережі і істотно спростити маршрутизацію

Автономна система повинна складатися не менше ніж з 32 менших за розміром мереж. Зазвичай в якості автономних систем виступають великі, незалежні, національні мережі.

Усередині автономної системи дані передаються від однієї мережі до іншої, поки не досягнуть точки сполучення з іншого автономною системою. Обмін даними можливий тільки в тому випадку, якщо між автономними системами існують угоди про надання транзиту. З цієї причини для користувачів різних автономних систем час доступу до одного і того ж ресурсу може мати відчутні відмінності

Аналіз можливих рішень, для вдосконалення каналів зв'язку Інтернет

Цей незадовільний стан справ може змінитися через дві революційні події:

• поява на ринку надзвичайно ускладненого, пропрієтарного, мережевого обладнання

• поява принципово нового підходу, званого програмно-конфігурованими мережами (ПКМ - SoftwareDefinedNetworks)

ПКМ-підхід обіцяє зробити всі мережі дешевше і простіше в управлінні

• «Інфраструктура як код (IaC)» - цей напрямок швидко розвивається, в основі якого лежить використання скриптів для налаштування інфраструктури обчислень замість налаштування комп'ютерів вручну.

• Модель «Інфраструктура як код (IaC)», яку іноді називають «програмованою інфраструктурою», - це модель, в якій процес налаштування інфраструктури аналогічний процесу програмування програмного забезпечення. По суті, вона поклала початок усунення кордонів між написанням додатків і створенням середовищ для цих додатків.

Аналіз можливих рішень, для вдосконалення каналів зв'язку Інтернет

Цей незадовільний стан справ може змінитися через дві революційні події:
• поява на ринку надзвичайно ускладненого, пропрієтарного, мережевого обладнання
• поява принципово нового підходу, званого програмно-конфігурованими мережами (ПКМ - SoftwareDefinedNetworks)

ПКМ-підхід обіцяє зробити всі мережі дешевше і простіше в управлінні

• «Інфраструктура як код (IaC)» - цей напрямок швидко розвивається, в основі якого лежить використання скриптів для налаштування інфраструктури обчислень замість налаштування комп'ютерів вручну.

• Модель «Інфраструктура як код (IaC)», яку іноді називають «програмованою інфраструктурою», - це модель, в якій процес налаштування інфраструктури аналогічний процесу програмування програмного забезпечення. По суті, вона поклала початок усунення кордонів між написанням додатків і створенням середовищ для цих додатків.

OpenFlow - протокол управління процесом обробки даних, що передаються по мережі передачі даних маршрутизаторами і комутаторами, який реалізує технологію програмно-конфігуруємої мережі

Протокол використовується для управління мережевими комутаторами і маршрутизаторами з центрального пристрою - контролера мережі (наприклад, з сервера або навіть персонального комп'ютера).

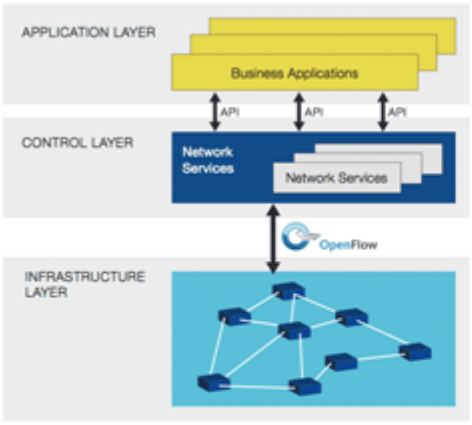
Це управління замінює або доповнює працюючу на комутаторі (маршрутизаторі) вбудовану програму, яка здійснює побудову маршруту, створення карти комутації і т. п.

Контролер використовується для управління таблицями потоків комутаторів, на підставі яких приймається рішення про передачу прийнятого пакета на конкретний порт комутатора.

Таким чином в мережі формуються прямі мережеві з'єднання з мінімальними затримками передачі даних і необхідними параметрами.

Тобто, в роботі мережевого пристрою можна виділити дві абстракції - керуючий рівень (control plane) і рівень передачі (data plane).

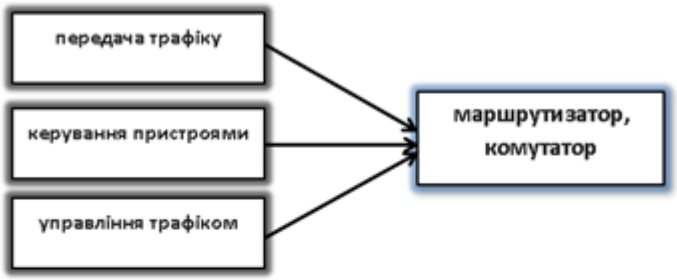
Розробка рекомендацій щодо покращення стану сучасних мереж Інтернет



SDN є результатом багаторічних технічних досліджень в даній області.

SDN - це мережі передачі даних, в яких рівень управління відділений від пристроїв передачі даних і реалізується програмно.

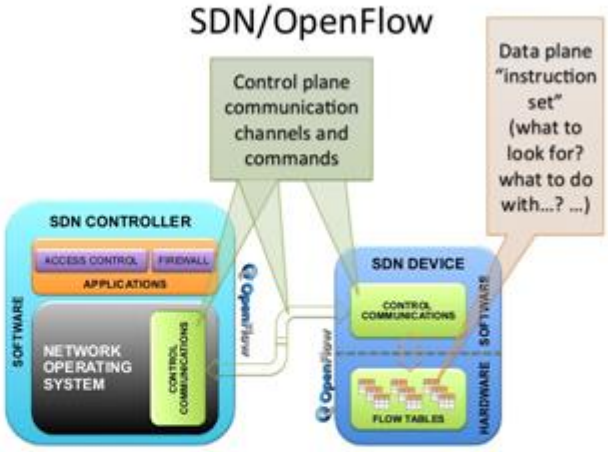
SDN-підхід розділяє рівень управління від рівня передачі трафіку за допомогою централізованого управління (замість звичайного розподіленого управління), а також дозволяє мережі бути програмно-визначаємою за допомогою відкритих і програмованих інтерфейсів.



відмінності від звичайної мережевої архітектури полягають у тому, що SDN за рахунок поділу апаратного і програмного забезпечення робить мережу віртуалізованою, на базі інформаційних технологій і програмного забезпечення.
Використання SDN спрощує конфігурацію пристроїв, управління і контролю, а також покращує коефіцієнт завантаження мережі і прискорює впровадження різних інновацій.

Оператори можуть використовувати SDN для швидкого уявлення і впровадження нових послуг, і в той же час, робити свою мережу видимою, керованою і контрольованою, а також покращуючи можливості управління і обслуговування.

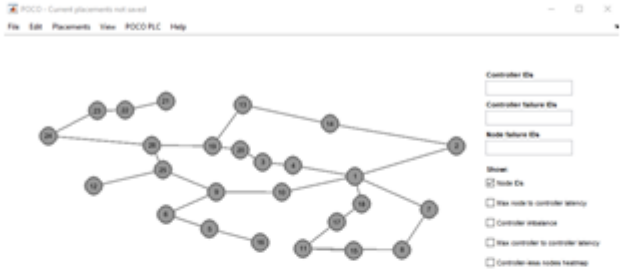
Відносно оптимізації мережі, SDN здійснює автоматичну оптимізацію мережевого трафіку в масштабі реального часу з урахуванням стану IP- і оптичних мереж. Це найбільш важливі аспекти SDN. На цьому етапі зниження витрат на пристрої більше не є головною турботою операторів. Замість цього оператори вважають, що SDN може більш ефективно використовувати мережеві ресурси, тим самим заощаджуючи витрати.



Відносно послуг, SDN здійснює швидке їх впровадження і автоматизацію обслуговування і автоматизоване виділення ресурсів для різних служб.

Відносно експлуатації та обслуговування, то SDN реалізує автоматизоване розгортання мережі, комплексне управління і контроль послугами та мережею.

Визначення оптимального положення sdn-контролера.



Проведено аналіз способів для розташування контролерів в програмно-визначених мережах.

Для визначення оптимального маршруту було використано наступний алгоритм.

1. Завантажуємо POCO з https://github.com/lsinfo3/poco
2. Завантажуємо localbackup.zip з https://euros.informatik.uni-wuerzburg.de/public/localbackup.zip
3. З http://www.topology-zoo.org/dataset.html завантаження (вибераємо варіанти з багатьма мережевими пристроями) мережева модель (Format GraphML)
4. Запускаємо Matlab. Відкриваємо папку POCO (змінюємо призначення). Запускаємо poco_GUI.
6. У вікні провідника, який відкриється, вказуємо шлях до файлу.
7. Тепер ми можемо побачити свою мережу (Рис. GTS Poland network (Європа))

Тепер буде визначена конфігурація сценарію. Вона включає в себе кількість контролерів для дерева відмов. Натисніть Placemet -> Calculate placement -> дерево відмов -> k (1-5). У прикладі ми розміщуємо різні контролери номерів.
Натискаємо дисбаланс контролера (k = 3). Ми побачимо високо завантажені ділянки мережі (позначені червоним кольором) Чим більше вузлів контролює контролер, тим вища навантаження на цей контролер. Якщо кількість запитів вузла-контролера в мережі зростає, то ймовірність додаткових затримок через черги в системі контролера зростає. Таким чином, у сценаріях, коли вузли часто зв'язуються зі своїм контролером, необхідно, щоб призначення вузла-контролера було добре збалансованим. Натискаємо «затримка контролера максимального вузла».

Коли розглядаються метрики затримки та надійності, як правило, не існує жодного найкращого рішення для розміщення контролера, а взагалі компроміс. Більшість схем розгортання, заснованих на затримці, в основному зосереджені на затримці передачі (TD) або затримці розповсюдження (PD). Клацаємо «вузли теплообміну без контролерів». Вказує, чи є ризик без контролера вузлів. Обираємо «вузли теплообміну без контролерів». Нам вказують, чи є ризик без контролера вузлів.

На графіку при виборі різних варіантів показана оптимальність. Вертикальне і горизонтальне сходження (пунктир) - і є найоптимальніший варіант. Як видно, на останньому рисунку, було змінено розташування на близьке до оптимального, і воно виявилося розташуванням контролерів поруч один з одним, але не були враховані інші параметри мережі, тому оптимальним воно і не є. Натискаємо «Максимальний час затримки контролера».

ВИСНОВКИ

✓ У магістерській роботі було досліджено стан публічних ІТ-просторів сучасних міст, надано аналіз публічного простору міста, способів організації зв'язку в публічному просторі.

✓ Створено збір матеріалу про сформовані, сучасні, мережі Інтернет та проведено аналіз можливих рішень, для вдосконалення каналів зв'язку Інтернет.

✓ Розроблені рекомендації щодо покращення стану сучасних мереж Інтернет, обґрунтуванні особливості формування інформаційних мереж публічних просторів, для створення комфортного, розвиненого міського середовища

✓ Визначений комплексний підхід до формування нових мереж Інтернет в публічних просторах міста як методологічна основа перетворення їх середовища. Запропоновано підходи до реконструкції існуючих мереж Інтернет, з урахуванням ролі і можливостей розподілених мереж Інтернет, як способу й засобу гармонізації середовища проживання городянина.

✓ Виконано моделювання оптимального розташування контролера локальних сітей у публічному просторі міста.