

## Кампусна мережа бізнес центру

Владислав Афанасьєв, студент<sup>1</sup>

<sup>1</sup> Київський національний університет будівництва і архітектури, Київ, Україна

### АНОТАЦІЯ

Враховуючи сучасні темпи глобалізації світу та його об'єднання в єдину систему за допомогою мережі Інтернет, створення нових то розширення вже існуючих мереж стало не від'ємною частиною розвитку. Забезпечення захисту мережі, а також підтримки відповідного рівня адміністрування для її ефективного функціонування та розширення за необхідності.

*Ключові слова:* мережа, топологія, модель, структура, критерії.

### 1. ВСТУП

На сьогоднішній день існує велика кількість вузлових пристроїв (комп'ютери, ноутбуки, принтери, планшети, мобільні прилади та інше), всі вони як правило об'єднані у мережі, які в свою чергу представлені від офісних (малих локальних мереж), до глобальних мереж таких як «Internet». Світова тенденція до повноцінного об'єднання ПК у відповідні мережі характеризується з ряду важливих причин, а саме прискорення передачі певних інформаційних повідомлень (даних), можливість швидкого обміну даними або ж інформацією між користувачами, одержання і передача повідомлень, можливість миттєвого одержання інформації з будь-якої точки світу, а також обмін даними між ПК різних виробників працюючих під різними програмним забезпеченням (далі - ПЗ). З цього слідує, що в найближчий час тенденція створення мереж різних типів не тільки не зменшиться, а й збільшиться через всесвітню глобалізацію, розповсюдження інтернет речей, та створення єдиного інформаційного простору.

### 2. МЕТА РОБОТИ

Створення мережі заданого типу її адміністрування, дослідження подальшого функціонування з заданими параметрами та властивостями, налаштування всіх її елементів. Моделювання мережі, перевірка її працездатності в емуляторі мережевого середовища Cisco Packet Tracer.

### 3. РОЗРОБКА МЕРЕЖІ

З метою відповідності вимогам користувачів навіть для невеликих мереж потрібне планування і проектування. На етапі планування розглядаються і враховуються всі вимоги, вартість та можливості впровадження. Важливими властивостями мережі є її надійність, масштабованість і доступність.

Щоб підтримувати і розвивати невелику мережу, необхідно добре розбиратися в протоколах і мережевих додатках, які запускаються по такій мережі. Аналізатори протоколів дозволяють фахівцям з мережних технологій швидко складати статистичні звіти про потоках трафіку в мережі. Інформація, зібрана аналізатором протоколів, оцінюється на основі даних про джерело і одержувача трафіку, а також з урахуванням типу відправляється трафіку. Результати аналізу фахівці з обслуговування

мереж можуть використовувати при прийнятті рішень про ефективне управління трафіком. До поширених мережевих протоколів відносяться протоколи DNS, Telnet, SMTP, POP, DHCP, HTTP і FTP. [1]

При плануванні впровадження мережі необхідно враховувати мережеві загрози і вразливості. Необхідно забезпечити безпеку всіх мережевих пристроїв. До таких пристроїв відносяться маршрутизатори, комутатори, призначені для користувача пристрої та пристрої забезпечення безпеки. Необхідно забезпечити захист мереж від шкідливого програмного забезпечення (віруси, трояни і черв'яки). Антивірусне ПЗ може виявити більшу частину вірусів і троянських програм, а також запобігти їх подальше поширення по мережі. Найбільш дієвий метод мінімізації наслідків атаки вірусу-хробака - завантажити оновлення для системи безпеки з сайту постачальника операційної системи і встановити відповідні поновлення на всі вразливі копії систем. [1]

Необхідно також забезпечити захист мереж від мережевих атак. Мережеві атаки можна розділити на три основні категорії: розвідувальна атака, атака доступу і атака типу «відмова в обслуговуванні» (DoS-атака). Існує кілька способів захисту мережі від подібних атак.

Такі служби по забезпеченню мережевої безпеки, як аутентифікація, авторизація та облік (Authentication, authorization, and accounting, AAA), є базовою інфраструктурою, яка встановлює засоби контролю доступу на будь-якому мережному пристрої. Послання служб аутентифікації, авторизації та обліку - це метод, що дозволяє контролювати вхід дозволених користувачів (аутентифікація), які дії вони можуть виконувати, перебуваючи в мережі (авторизація), а також стежити за їхніми діями під час доступу до мережі (облік).

Брандмауер - одне з найбільш ефективних засобів безпеки для захисту користувачів мережі від зовнішніх загроз. Брандмауер ставиться між двома (або більше) мережами та контролює трафік між ними, а також дозволяє запобігти несанкціонованому доступу.

Для захисту мережевих пристроїв необхідно використовувати надійні паролі. Крім того, при віддаленому доступі до мережевих пристроїв настійно рекомендується використовувати протокол SSH замість незахищеного протоколу Telnet. [1]

Після організації мережі адміністратор мережі повинен мати можливість здійснювати моніторинг і обслуговування мережевого підключення. Для цього доступний ряд команд. Для перевірки підключення по мережі до локальних і віддалених адресами призначення зазвичай використовуються такі команди, як ping, telnet і traceroute.

На пристроях Cisco IOS можна використовувати команду `show version` для перевірки і усунення неполадок базових програмних і апаратних компонентів, які використовуються під час завантаження. Щоб переглянути детальну інформацію про всі мережеві інтерфейси маршрутизатора використовується команда `show ip interface`. Також можна використовувати команду `show ip interface brief` для перегляду скорочених результатів виконання команди `show ip interface`. Протокол Cisco Discovery Protocol (CDP) - запатентований протокол Cisco, що функціонує на каналному рівні. Оскільки протокол CDP функціонує на каналному рівні, два (або більше) мережевих пристроїв Cisco, такі як маршрутизатори з підтримкою різних протоколів мережевого рівня, можуть отримати дані один про одного навіть в тому випадку, якщо з'єднання 3-го рівня не існує. [2]

Слід зберігати в архіві резервні копії файлів конфігурації Cisco IOS (наприклад `startup-config` або `running-config`). Їх можна зберегти в текстовий файл або на TFTP-сервер. Деякі моделі маршрутизаторів також оснащені портом USB, і резервну копію файлу можна зберегти на USB-накопичувач. При необхідності можна скопіювати ці файли з TFTP-сервера або USB-накопичувача на маршрутизатор і / або комутатор. [2]

Якщо мережу або частини мережі перестає працювати, то це може мати серйозний негативний вплив на бізнес. Мережеві адміністратори повинні використовувати системний підхід для усунення несправностей при виникненні мережевих проблем з метою максимально оперативного відновлення повної працездатності мережі.

Для того щоб адміністратори мереж могли забезпечувати спостереження за мережею, а також налагодження мережі, вони повинні мати повний набір точної і актуальної документації про мережі, включаючи файли настройки, діаграми фізичної і логічної топології і дані про вихідний рівень продуктивності.

Можна додати в мережу інструменти забезпечення якості обслуговування (QoS) і надати деяким типам трафіку, наприклад голосу і відео, пріоритет над трафіком, менш чутливим до затримок, таким як електронна пошта та перегляд веб-сторінок.

Трьома основними етапами процесу пошуку і усунення проблем є збір даних про симптоми, ізоляція проблеми і її усунення. У ряді випадків можна застосувати тимчасове рішення. Якщо виконану дію по виправленню не дозволило усунути проблему, то внесені зміни слід видалити. Адміністратор повинен документувати процес повністю на всіх етапах. Для кожного етапу повинна бути сформована політика усунення неполадок, включаючи процедури контролю змін. Після усунення проблеми важливо повідомити про це користувачам, всім співробітникам, які беруть участь в процесі усунення неполадок, а також іншим членам групи IT. [3]

До загальних програмних засобів, які можуть допомогти при пошуку і усунення неполадок, відносяться засоби системи управління мережами, бази знань, засоби формування базових показників, аналізатори протоколів на кінцевих пристроях і Cisco IOS EPC. У число засобів пошуку та усунення несправностей апаратного забезпечення входять NAM, цифрові мультиметри, тестери кабелів, аналізатори кабелів і портативні аналізатори мереж. Для виявлення потенційних проблем можна також використовувати інформацію з журналу Cisco IOS. [2]

Фізичний рівень, каналний рівень, мережевий рівень, транспортний рівень, а також рівень додатків мають характерні симптоми і проблеми, про які адміністраторам має бути відомо. Адміністратор може звертати особливу увагу на фізичну зв'язок, шлюзи за замовчуванням, таблиці MAC-адрес, перетворення NAT і дані про маршрутизацію.

#### 4. ВИСНОВКИ

Таким чином інформаційні мережі мають функціональну можливість передавати повідомлення голосові, дані, відео та зображення. В свою чергу, мережі для обміну даними побудовані з периферійних пристроїв, мережевих пристроїв, носіїв і різного роду вузлів. Для схематичної побудови логічної і фізичної мережі використовуються топологічні схеми які мають можливість зображаються у спеціальному середовищі проектування. Мережеві вузли мають функціональну можливість виконувати роль сервера, клієнта або разом взятих. Усі процеси, що приймають участь в обміні повідомленнями мають відповідно відправника, отримувача і канали передачі даних. Таким чином, обмін даними між відповідними комп'ютерами виконується спеціальним правилам, які мають назву - протокол. Протоколи в свою чергу аналізують особливості повідомлення, з можливим включенням шифрування, формату, розміру, інкапсулювання, синхронізації і відповідним способом розсилання.

Маршрутизатори з інтегрованими службами і інші мультифункціональні пристрої з'єднують мережу і мережі підприємств малого бізнесу з ціллю надання сумісного доступу до ресурсів і виходу в Інтернет на декілька вузлів.

В даній роботі дослідив класифікацію мереж за областю дії її географічного району, охоплення мережі та розмір мережі. Виділив такі типи:

- персональні мережі (Personal Area Networks)
- локальні мережі (Local Area Networks)
- кампусні мережі (Campus Area Network)
- глобальні мережі (Wide Area Networks)

В дипломній роботі представив кампусну мережу як мережу на стику LAN та WAN мереж.

З метою виконання дослідження моделювання кампусної мережі використав програмний емулятор Packet Tracer де й продемонстрував всі вище зазначені можливості мережі.

#### Список літератури

- [1] Джеймс Уезеролл & Ендрю Таненбаум (2016) Комп'ютерні мережі.
- [2] Wendell Odom & Sean Wilkins (2013), Cisco CCNA Routing and Switching 200-120 Official Cert Guide and Library Simulator.
- [3] Іван Горбатий & Андрій Бондарєв, (2016) Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи .

<sup>1</sup> Робота виконана під керівництвом к.т.н., доц. М.М.Делембовського