УДК 621.382

# МЕТОДИКА ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ОБЛАДНАННЯ JUNIPER

**Валуйський С.В., Кравчук І.В.**
*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: ilyukha.kravchuk@gmail.com*

## METHODOLOGY FOR BUILDING A SECURE NETWORK BASED ON JUNIPER EQUIPMENT

This article examines the possibility of building a secure and fault-tolerant network based on Juniper routers, with particular attention given to the LACP, VPN, RSTP, and TAP protocols. Their main advantages in network usage are identified.

Компанія Juniper вважається однією із провідних постачальників у світі. Вона була заснована о 1996 році і з того часу вона стала однією з провідних компаній у галузі мережевого обладнання. Тенденція її популярності змінювалася залежно від ринкових умов та конкуренції, проте загалом компанія зберегла свою популярність серед клієнтів, що шукають високоякісне та надійне мережеве обладнання.

У 2022 році аналітична компанія 650 Group дослідила та встановила, що протягом I кварталу 2022 року продаж технологій Juniper Mist AI збільшився на 117 %, що має найвищий відсоток росту прибутку в порівнянні з іншими конкурентами виробників засобів безпровідного зв’язку [1].

**Мета роботи.** Побудувати захищену та відмовостійку мережу на основі обладнання Juniper. Для забезпечення відмовостійкості буде використано протоколи LACP та RSTP. Для захисту мережі будуть використане налаштування VPN, TAP, а також стандартних профілів безпеки як ACL. Топологія цієї мережі буде побудована у вигляді кільця, буде використана віртуальна лабораторія GNS3 з використанням віртуального образу Juniper router, PC, а також додаткових комутаторів від вендора Cisco.

**Властивості та призначення протоколів, які будуть використанні в роботі.**

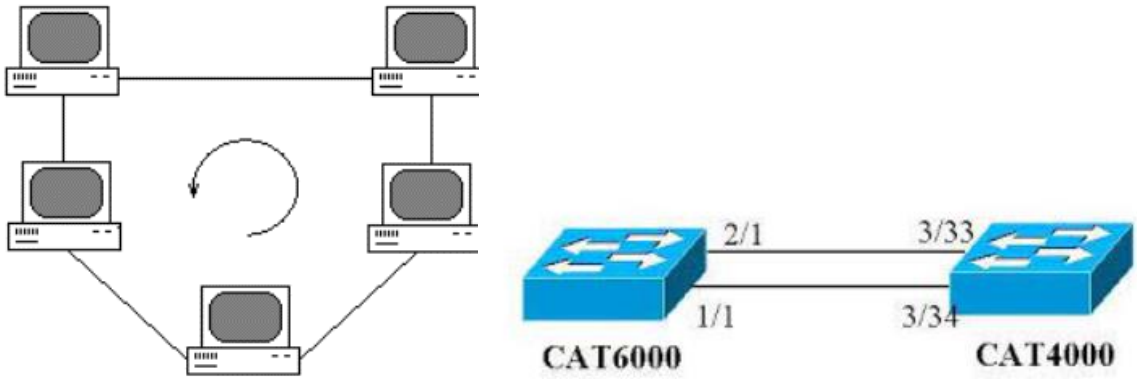
LACP – це протокол керування з'єднаннями, який використовується для об'єднання між собою кількох мережевих портів в один логічний канал, який називається Link Aggregation Group (LAG). LACP забезпечує створення та управління LAG між двома мережевими пристроями, зокрема між комутаторами, маршрутизаторами, серверами, забезпечуючи збільшення швидкості передачі даних, збільшення надійності та забезпечення балансування навантаження [2].

RSTP (Rapid Spanning Tree Protocol) є протоколом, який використовується для запобігання петель у мережах з топологією дерева. Цей протокол є удосконаленням протоколу Spanning Tree Protocol (STP), який був розроблений для запобігання петель у мережах з топологією дерева. RSTP відповідає за визначення шляху, який буде використовуватися для передачі даних в мережі. Він також забезпечує автоматичну реакцію на зміни топології мережі, що

дозволяє мережі бути більш масштабованою та надійною [3].

Налаштування політик безпеки для пропуску або відкидання трафіку – це процес налаштування правил та налаштувань в мережному обладнанні або програмному забезпеченні, які визначають, який трафік мережі повинен бути дозволений для проходження, а який повинен бути заблокований чи відкинутий. У Juniper налаштування політик безпеки для пропуску або відкидання трафіку зазвичай здійснюється за допомогою механізму Juniper Security Policies [4].

TAP – це тип мережевого інтерфейсу, який дозволяє передавати дані між комп'ютерами на різних рівнях мережевої моделі OSI. У контексті VPN, TAP використовується для передачі Ethernet-кадрів через тунель між двома або більше комп'ютерами, що знаходяться на різних кінцях VPN-підключення. Застосування TAP-адаптера у VPN дозволяє розширити мережевий доступ між комп'ютерами на різних фізичних мережах через інтернет-підключення [5].




а) б)

Рис. 1. Тополологія «кільце» (а) та приклад використання LACP (б).

На Рис.1б представлений приклад використання протоколу LACP. Якщо щось станеться з фізичним каналом 2/1 – 3/33, то мережа буде далі функціонувати, так як канал фізичний канал 1/1 – 3/34 буде далі працювати і навпаки. Цей протокол не тільки підвищує відмовостійкість мережі, а й збільшує її пропускну здатність. Тобто два фізичних каналу утворюють один логічний з вищою пропускною здатністю та відмовостійкістю.

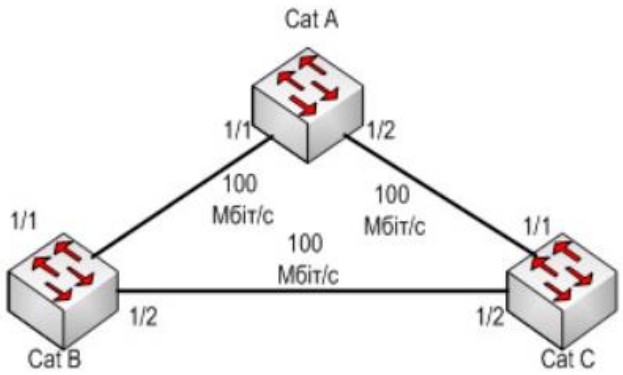



Рис. 2. Приклад використання RSTP.

На рис.2 представлене використання протоколу RSTP. Інтерфейси 1/2-1/2 між CatB – CatC знаходять у режимі DOWN, в той час як інтерфейси 1/1-1/1 між CatB – CatA та інтерфейси 1/2-1/1 між CatA – CatC знаходяться в режимі FRW. Якщо щось станеться наприклад з CatA, то вся мережа не впаде, а піднімуться інтерфейси 1/2-1/2 між CatB – CatC (перейдуть в режим FRW), тоді трафік зможе передаватись між ними.

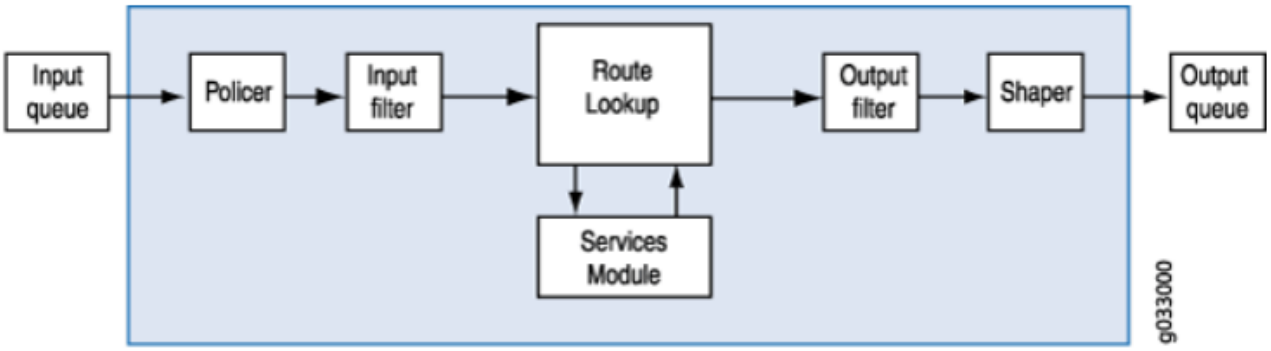



Рис. 3. Принцип роботи політик безпеки та протоколу TAP.

Як можемо бачити на рис.3, коли пакети надходять на пристрій, до них застосовуються класифікатори, фільтри та захисники. Далі визначається інтерфейс джерела пакета, виконавши пошук маршруту. Коли вихідний інтерфейс для пакета знайдено, застосовується фільтр, і пакет надсилається до вихідного інтерфейсу, де він ставиться в чергу та запланований для передачі. Пересилання на основі пакетів не потребує жодної інформації про попередній чи наступний пакет, що належить даному з'єднанню, будь-яке рішення щодо дозволу чи заборони трафіку залежить від пакету. Ця архітектура має перевагу масового масштабування, оскільки вона пересилає пакети без відстеження окремих потоків або станів.

**Висновок.** Отже враховуючи всі вище перераховані протоколи, техніки та особливості обладнання Juniper з його операційною системою Junos, можна побудувати захищену мережу від стороннього проникнення, а також бути впевненим, що у випадку непередбачуваних ситуацій мережа буде в робочому стані.

**Література**

1. Juniper Networks is recognized as a leading manufacturer of corporate and wireless local area networks. URL: https://itbiz.ua/news/kompaniya-juniper-networks-viznana-providnim-virobnikom-korporativnix-ta-bezprovidnix-lokalnix-merezh/ (the date of access: 24.03.2023).
2.802.1AX-2020 - IEEE Standard for Local and Metropolitan Area Networks--Link Aggregation. URL: https://ieeexplore.ieee.org/document/9105034 (the date of access: 24.03.2023).
3.Understand Rapid Spanning Tree Protocol (802.1w) URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html (the date of access: 24.03.2023).
4.Security Policies User Guide for Security Devices URL: https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-configuration.html (the date of access: 24.03.2023).
5.Flow-Based and Packet-Based Processing User Guide for Security Devices URL: https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-tap-mode-flow.html (the date of access: 24.03.2023).