***Єфіменко А.А., к.т.н.,***
***Венгловська А.В., студ. 3-го курсу,***
*Житомирський державний технологічний університет*
***Ліпінська А.В., студ. 4-го курсу,***
*Національний авіаційний університет*

# ПРОБЛЕМИ БЕЗПЕКИ ПРОТОКОЛІВ РЕЗЕРВУВАННЯ ЗВ'ЯЗКІВ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ETHERNET

Потреба забезпечення ефективного та безперебійного функціонування як локальних, так і глобальних комп'ютерних мереж призвела до розробки та широкого впровадження сукупності технологій та протоколів, що призначені для підвищення рівня надійності як окремих складових, так і всієї мережі в цілому. Одним з найбільш поширених рішень для підвищення рівня надійності локальних мереж Ethernet є використання одного з варіантів протоколу канального рівня STP: RSTP, PVST, PVST+, RPVST+, MSTP. Як відомо, комутована мережа Ethernet може бути побудована з використанням зіркоподібної або ієрархічної фізичної топологій. Просте встановлення додаткових фізичних зв'язків між комутаторами мережі призводить до появи петель комутації і, як наслідок, до широкомовного шторму – ситуації, коли передача широкомовних і групових повідомлень зациклюється. Широкомовний шторм призводить до виходу з ладу мережі в цілому. Протоколи сімейства STP призначені для усунення петлеподібними зв'язків за рахунок переведення їх у резервний стан, тобто приведення комутованої мережі Ethernet з множинними зв'язками до деревоподібної (активної) топології. В основі протоколу STP лежить алгоритм STA – алгоритм формування кістякового дерева. За алгоритмом STA у мережі автоматично обирається кореневий комутатор, решта комутаторів стають призначеними і формують оптимальні маршрути передачі трафіку. Надлишкові зв'язки між комутаторами переводяться у резервний стан.

При розробці протоколу STP проблемам безпеки пристроїв мережі та безпеки передачі трафіку приділяли мало уваги. Як наслідок, у протоколі наявні вразливості, які тісно пов'язані з принципами та особливостями його функціонування. Предметом атаки на протокол STP можуть бути будь-які параметри протоколу, які формуються у процесі виборів. Відповідно атаки можна згрупувати за методами їх проведення таким чином:

1. Атаки, які орієнтовані на ініціалізацію перевиборів кореневого комутатора для всієї мережі.
2. Атаки, які орієнтовані на ініціалізацію перевиборів призначеного комутатора для певного сегмента мережі.
3. Атаки, які орієнтовані на ініціалізацію перевиборів призначеного порту для певного сегмента мережі.

Всі вищезгадані атаки використовують підміну параметрів у повідомленнях (BPDU) протоколу. Часто ці атаки називають атаками типу BPDU-Spoofing. Різновид атак, які орієнтовані на керування величиною часу збереження інформації у таблицях комутації комутаторів, носить назву „Provocation Aging". Використання лише BPDU-Spoofing (як і „Provocation Aging") є малоефективним. Але зазначені атаки є ефективними складовими інших атак. У першу чергу це стосується атак, які орієнтовані на відмову в обслуговуванні (STP DoS-атаки), та атак, які орієнтовані на перехоплення трафіка (STP-Based Sniffing). Можна виділити такі різновиди STP DoS-атак: вічні (постійні) вибори (STP Eternal Elections); зникнення кореня (STP Disappearance of Root); локалізована відмова в обслуговуванні (STP Local Denial of Service); фільтр BPDU (STP BPDU Filter); зміни (сходження/розходження) у структурі покриваючого дерева (STP Merging-Splitting of the Trees). Серед атак, які орієнтовані на перехоплення трафіка, можна виділити такі їх різновиди: „звичайне" перехоплення (STP MiTM); спровоковане перехоплення (STP Provocated Sniffing). Основними методами виявлення атак на протокол STP є: спостереження за процесами передачі даних та процесами функціонування комутаторів та кінцевих вузлів мережі; систематичний аналіз службового мережного трафіка; відстеження та аналіз системних повідомлень ОС мережних пристроїв; використання систем виявлення атак.

Провідні виробники мережного обладнання у процесі тестової експлуатації мереж на основі комутаторів з підтримкою протоколу STP виявили як основні функціональні недоліки, так і певні проблеми безпеки протоколу. На основі отриманого досвіду були розроблені методи і засоби їх усунення, що орієнтовані на прискорення та стабілізацію роботи протоколу, а також на підвищення рівня захищеності побудованої активної топології. Для захисту від STP-атак в протокол були включені функції: BPDU Guard, Root Guard, BPDU Filtering, Loop Guard.

Необхідно зробити висновок, що при експлуатації мережі, яка побудована з використання протоколу STP проблемам безпеки необхідно приділяти значну увагу. Важливо використовувати не лише штатні функції захисту протоколу STP, а й інші наявні засоби підвищення рівня захищеності мережі, тобто використовувати комплексний підхід для вирішення проблем безпеки.