

ВИКОРИСТАННЯ СИМУЛЯТОРА GNS3 ДЛЯ АНАЛІЗУ ТРАФІКУ У МЕРЕЖІ

Проведення аналізу мережі є необхідним як на етапі проектування системи, так і на етапі супроводження. Для вирішення цієї задачі є доцільним використовувати симулятори та емулятори мереж. На даний час існує безліч симуляторів, таких як GNS3, Cisco Packet Tracer UNetLab, Huawei eNSP, Mininet, Line Network Emulator. Використання цих засобів дозволяє виявити допущені помилки у проектуванні ще до впровадження системи, також при необхідності внесення змін у вже існуючу мережу нададуть можливість від лагодити їх перед впровадженням. Одним з найпоширеніших є GNS3 – симулятор комп'ютерних мереж та мережевих пристроїв, які функціонують на базі процесорів з архітектурою MIPS. До таких мережевих пристроїв відносяться, в тому числі, більшість мережевих комутаторів та маршрутизаторів, вироблених компанією CISCO [1-4]. Даний засіб дозволяє підключити емульований сегмент до вже працюючої мережі, що дозволяє провести тестування змін у системі.

Також GNS3 надає можливість проводити аналіз трафіку, що генерується всіма мережевими пристроями моделі на всіх інтерфейсах з допомогою Wireshark, що було використано у роботі. Wireshark – широко поширений інструмент для захоплення і аналізу трафіку [5]. Wireshark має можливість детального розгляду структури пакета, відображаючи значення кожного поля протоколу будь-якого рівня, що робить його потужним засобом для перехоплення трафіку та його аналізу, може наочно відобразити докладну інформацію про трафік мережі. Використовується як всередині середовища GNS3, так і дозволяє аналізувати трафік з реальної комп'ютерної мережі (зчитуючи його з фізичних інтерфейсів за допомогою драйвера WinPCAP).

Використання GNS3 у роботі надало можливість провести дослідження мережевої топології та обладнання без внесення змін у вже працюючу мережу що дозволило провести необхідні дослідження та прийняти оптимальне рішення з мінімальними матеріальними затратами[6-8]. Також перевагою даних продуктів є те що вони розповсюджуються під вільною ліцензією GNU GPL, що дозволяє їх вільне використання та внесення необхідних змін у код продуктів.

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2011. – 944 с
2. Новиков Ю.В. Основы локальных сетей/Ю.В. Новиков. – М.: ЭКОМ, 2005. – 360 с.
3. Васин, Н.Н. Технологии пакетной коммутации. Часть 1. Основы построения сетей пакетной коммутации: учеб. пособие.- Самара: ПГУТИ, 2014. – 239 с.
4. Васин, Н.Н. Технологии пакетной коммутации. Часть 2. Маршрутизация и коммутация в сетях пакетной коммутации: учеб. пособие. – Самара: ПГУТИ, 2015. – 261 с.
5. Laura Chappell, Wireshark Network Analysis. Second Edition. - Protocol Analysis Institute, dba "Chappell University", 2012. – 461 с.
6. Д. Филлипс «Методы анализа сетей» / Д. Филлипс, А. Гарсия-Диас – Мир – 1984. 496 с.
7. Вишневський В.М. Теоретичні основи проектування комп'ютерних мереж. Навчальний посібник. / Вишневський В. М. – Техносфера, 2004.
8. Буров Є.М. Комп'ютерні мережі. / Буров Є.М. Вид. Львів: БаК, 2003. – 584 с.
9. Галушин С.Я. Сети ЭВМ и их защита. – Санкт-Петербург, 2000.