A Comparative Analysis of IoT Traffic Segregation Utilizing Dedicated and Distributed VLANs

Wason Futrakul[1], Chaknarin Koongcharoen[2, *]
[1] Wason Futrakul (Department of Electrical and Computer Engineering, Faculty of Science and Engineering, Kasetsart University, Chalermphrakiat Sakon Nakhon Province Campus 59/5 Moo1 Chiangkrua Muang Sakon Nakhon 47000. THAILAND.)
[2]Chaknarin Kongcharoen (Department of Computer and Information Science, Faculty of Science and Engineering, Kasetsart University, Chalermphrakiat Sakon Nakhon Province Campus 59/5 Moo1 Chiangkrua Muang Sakon Nakhon 47000. THAILAND.)

**Corresponding Author Email: chaknarin.k@ku.th*

Abstract

This study examines network performance by contrasting two VLAN configurations for IoT traffic isolation: a dedicated VLAN solely for IoT devices (VLAN 5) in conjunction with general-use VLANs (VLANs 1-4), and a distributed model wherein IoT devices are allocated across multiple VLANs (VLANs 1-4). The extensive implementation of IoT devices produced considerable network traffic, affecting overall performance. The experimental configuration employed MikroTik devices in the EVE-NG emulator, comprising one MikroTik CHR functioning as a Core Router and five MikroTik CHRs serving as Layer 2 Switches, overseeing five VLANs, each with five client machines. The results indicate that segregating IoT devices within a dedicated VLAN significantly improves the average transmission rate for general users, reaching 10.15 Mbps versus 8.875 Mbps in the distributed configuration. Furthermore, the dedicated VLAN configuration decreases the average Remote CPU Load to 63.25%, in contrast to 65.25% in the distributed configuration. These findings indicate that a dedicated IoT VLAN architecture enhances network efficiency by stabilizing CPU loads and optimizing traffic management.

Keyword: IoT VLAN Architecture, Network Performance, Traffic Isolation.