IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN LABORATORIUM TELEKOMUNIKASI UPN VETERAN JAKARTA BERBASIS VIRTUAL LOCAL AREA NETWORK (VLAN)

Muhammad Fahrurizqi Ilham

ABSTRAK

Keamanan jaringan penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data pada jaringan laboratorium multi-pengguna. Penelitian ini mengimplementasikan dan menganalisis kombinasi VLAN, *Access Control List* (ACL), *Port Security*, dan *Secure Shell* (SSH) pada jaringan berbasis *router-on-a-stick* menggunakan MikroTik RB750 dan Cisco Catalyst 2960 melalui *trunk* 802.1Q. Jaringan dibagi menjadi empat VLAN berbasis IPv4, VLAN 10 Dosen (192.168.10.0/29, Fa0/5–7), VLAN 20 Mahasiswa (192.168.20.0/29, Fa0/2/3/8/9), VLAN 30 Server (192.168.30.0/29, Fa0/4), dan VLAN 99 Management (Fa0/24). ACL diterapkan untuk membatasi komunikasi antar-VLAN, Port Security menggunakan metode *sticky MAC* dengan mode *shutdown* (VLAN 10, 30) dan *restrict* (VLAN 20), serta SSH mengamankan akses manajemen menggantikan Telnet. Pengujian meliputi *ping* 15 paket untuk konektivitas intra/antar-VLAN sebelum-sesudah ACL, simulasi *MAC spoofing* untuk mengukur status interface, *Violation Count*, dan *Response Time* pada Port Security, serta verifikasi autentikasi SSH dari VLAN 99 dengan RSA 1024-bit dan *strong-crypto*. Hasil menunjukkan VLAN berhasil memisahkan domain jaringan, ACL dan SSH mencapai efektivitas 100%, serta Port Security mendeteksi dan merespons perangkat tidak sah sesuai mode konfigurasi. Kombinasi mekanisme ini meningkatkan keamanan tanpa mengganggu komunikasi yang diizinkan.

Kata Kunci: *VLAN*, *Access Control List* (*ACL*), *Port Security*, *Secure Shell (SSH)*, Keamanan Jaringan.

IMPLEMENTATION OF VIRTUAL LOCAL AREA NETWORK (VLAN)-BASED NETWORK SEGMENTATION SECURITY IN THE TELECOMMUNICATIONS LABORATORY OF UPN VETERAN JAKARTA

Muhammad Fahrurizqi Ilham

ABSTRACT

Network security is essential for maintaining the confidentiality, integrity, and availability of data on multi-user laboratory networks. This research implements and analyzes a combination of VLAN, Access Control List (ACL), Port Security, and Secure Shell (SSH) mechanisms on a router-on-a-stick based network using a MikroTik RB750 router and Cisco Catalyst 2960 switch connected via 802.1Q trunk. The network is divided into four IPv4-based VLANs: VLAN 10 Lecturer (192.168.10.0/29, Fa0/5–7)*, VLAN 20 Student* (192.168.20.0/29, Fa0/2/3/8/9)*, VLAN 30 Server* (192.168.30.0/29, Fa0/4)*, and VLAN 99 Management (192.168.100.1/29, Fa0/24). ACL is applied to restrict inter-VLAN communication, Port Security uses the sticky MAC method with shutdown mode (VLAN 10, 30) and restrict mode (VLAN 20), while SSH secures management access in place of Telnet. Testing includes 15-packet ping tests for intra and inter-VLAN connectivity before and after ACL implementation, MAC spoofing simulation to measure interface status, Violation Count, and Response Time for Port Security, and SSH authentication verification from VLAN 99 using 1024-bit RSA keys and strong-crypto. Results show VLAN successfully segmented the network domains, ACL and SSH achieved 100% effectiveness, and Port Security successfully detected and responded to unauthorized devices according to configured modes. This combination of mechanisms enhances laboratory network security without disrupting authorized communication.*

Keywords: *VLAN*, *Access Control List* (*ACL*), *Port Security*, *Secure Shell (SSH)*, *Network Security*.