# BAB 5
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan terhadap keamanan jaringan Laboratorium Telekomunikasi Teknik Elektro UPN Veteran Jakarta berbasis *Virtual Local Area Network* (VLAN), maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Perancangan dan implementasi segmentasi jaringan menggunakan VLAN berhasil membagi jaringan laboratorium menjadi tiga segmen, yaitu VLAN 10 Dosen, VLAN 20 Mahasiswa, dan VLAN 30 *Server*, dengan pendekatan *Router-on-a-Stick*. Hasil pengujian konektivitas menunjukkan bahwa seluruh perangkat pada masing-masing *VLAN* berhasil terhubung ke gateway yang sesuai dan komunikasi internal dalam satu segmen berjalan dengan baik sesuai rancangan awal.
2. Penerapan *Access Control List* (ACL) terbukti efektif dalam membatasi komunikasi antar-*VLAN* sesuai kebijakan keamanan yang telah ditetapkan. Seluruh pengujian menghasilkan respons yang sesuai, sehingga ACL mampu mencegah *unauthorized access* antar segmen jaringan secara konsisten.
3. Implementasi *Port Security* berhasil membatasi akses fisik perangkat pada setiap *port access switch* berdasarkan MAC address yang terdaftar. Penerapan *mode violation Shutdown* pada VLAN 10 Dosen dan VLAN 30 *Server*, serta mode *Restrict* pada VLAN 20 Mahasiswa, terbukti mampu mendeteksi dan merespons perangkat tidak sah yang mencoba terhubung ke jaringan sesuai dengan kebijakan keamanan yang dirancang.
4. Kombinasi penerapan VLAN, ACL, dan *Port Security* secara bersama-sama memberikan perlindungan berlapis pada jaringan laboratorium. VLAN memisahkan segmen jaringan, ACL mengontrol komunikasi antar segmen pada level jaringan, dan *Port Security* mengamankan akses fisik pada level *switch*, sehingga keamanan jaringan laboratorium meningkat dibandingkan kondisi awal tanpa segmentasi.

## 5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran untuk pengembangan penelitian lebih lanjut, yakni:

1. Penelitian selanjutnya disarankan untuk menguji skalabilitas implementasi pada jumlah perangkat dan VLAN yang lebih besar guna mengevaluasi konsistensi performa ACL dan *Port Security* pada skala jaringan yang lebih kompleks.
2. Pengujian dapat dikembangkan dengan melibatkan skenario serangan yang lebih bervariasi, tidak terbatas pada *MAC spoofing*, guna memperoleh gambaran ketahanan sistem yang lebih komprehensif.
3. Penelitian dapat dikembangkan dengan menambahkan mekanisme pemantauan jaringan secara real-time menggunakan sistem syslog terpusat atau platform *Network Monitoring System* (NMS), sehingga setiap pelanggaran keamanan dapat terdeteksi dan ditindaklanjuti secara lebih cepat oleh administrator.
4. Penelitian dapat dikembangkan dengan menambahkan fitur keamanan layer 2 lainnya seperti *Dynamic ARP Inspection* (DAI) dan *DHCP Snooping* sebagai pelengkap Port Security, guna mencegah serangan *ARP spoofing* dan *DHCP starvation* yang belum tercakup dalam penelitian.