Journal of System & Technology
e-ISSN: XXXX-XXXX
Vol. 1, No. 1, Juni 2025

IMPLEMENTASI VIRTUAL LAN DAN ACCESS CONTROL LIST UNTUK SEGMENTASI AKSES PADA JARINGAN SEKOLAH: STUDI SIMULASI

Rakhmadi Rahman[1]*, Dwicki Herlambang[1], M Furqan Ramadhanu[1]
[1]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Parepare, South Sulawesi, Indonesia
rakhmadi.rahman@ith.ac.id, dwickyherlambang4@gmail.com, 0707furqan@gmail.com
*Corresponding author: rakhmadi.rahman@ith.ac.id

Abstract: Peningkatan kebutuhan jaringan komputer di lingkungan sekolah menimbulkan tantangan baru dalam hal keamanan, khususnya terkait kontrol akses dan segmentasi pengguna. Banyak institusi pendidikan masih menggunakan topologi jaringan datar (flat network), yang memungkinkan lalu lintas data terbuka tanpa pembatasan akses antar pengguna, sehingga rawan terhadap penyusupan dan kebocoran informasi. Penelitian ini bertujuan untuk merancang dan mensimulasikan arsitektur jaringan sekolah yang aman dan efisien dengan menerapkan teknologi Virtual Local Area Network (VLAN) dan Access Control List (ACL). Simulasi dilakukan menggunakan aplikasi Cisco Packet Tracer, dengan skenario jaringan terdiri dari tiga segmen utama: Lab Komputer (VLAN 10), Ruang Guru (VLAN 20), dan Ruang IT (VLAN 30). VLAN digunakan untuk memisahkan domain siar antar departemen, sedangkan ACL diterapkan pada router untuk mengatur hak akses berdasarkan kebijakan yang ditentukan. Hasil simulasi menunjukkan bahwa kombinasi VLAN dan extended ACL dapat membatasi komunikasi lintas segmen secara efektif; VLAN 10 tidak dapat mengakses VLAN 20 dan 30, VLAN 20 hanya dapat mengakses VLAN 10, dan VLAN 30 memiliki akses penuh. Simulasi ini membuktikan bahwa implementasi VLAN dan ACL dapat menjadi solusi praktis untuk meningkatkan keamanan jaringan lokal di sekolah tanpa memerlukan perubahan besar pada infrastruktur fisik yang ada.

Keywords—Access Control List, Cisco Packet Tracer, Jaringan Sekolah, Keamanan Jaringan, VLAN

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong institusi pendidikan, termasuk sekolah, untuk memanfaatkan jaringan komputer sebagai sarana utama dalam mendukung kegiatan belajar mengajar dan administrasi. Namun, di balik kemudahan tersebut, terdapat ancaman keamanan jaringan yang kian meningkat, seperti akses tidak sah, penyadapan data, hingga serangan internal dari pengguna jaringan itu sendiri. Permasalahan ini menjadi semakin krusial apabila sistem jaringan sekolah masih menggunakan topologi datar (flat network) tanpa adanya segmentasi atau pembatasan akses [1], [2].

Salah satu pendekatan yang dapat digunakan untuk meningkatkan keamanan jaringan adalah penerapan Virtual Local Area Network (VLAN) dan Access Control List (ACL). VLAN memungkinkan segmentasi jaringan berdasarkan fungsi atau departemen, sehingga lalu lintas data antar segmen dapat dipisahkan [3]. Sementara itu, ACL memberikan kontrol akses terhadap lalu lintas data, baik berdasarkan alamat IP, protokol, maupun port, sehingga dapat membatasi komunikasi antar VLAN sesuai dengan kebijakan yang ditetapkan [2], [4], [5].

Penelitian ini bertujuan untuk mensimulasikan penerapan keamanan jaringan berbasis VLAN dan ACL pada lingkungan sekolah menggunakan Cisco Packet Tracer. Berdasarkan survei Kementerian Pendidikan dan Kebudayaan tahun 2022, lebih dari **60%** sekolah di Indonesia masih menggunakan topologi jaringan datar (flat network) tanpa pengamanan segmentasi dan kontrol akses yang memadai. Hal ini menyebabkan tingginya risiko penyalahgunaan data, akses ilegal antarkomputer, serta sulitnya pengawasan trafik jaringan internal.

Beberapa penelitian sebelumnya telah mengkaji penerapan VLAN dan ACL secara terpisah, seperti pada studi [2] dan [5], namun masih terbatas pada konteks perusahaan atau kantor pemerintahan. Penelitian ini berbeda karena secara khusus mengkaji penerapan segmentasi jaringan berbasis VLAN dan ACL dalam konteks sekolah, yang memiliki kebutuhan dan struktur akses yang berbeda. Oleh karena itu, penelitian ini berkontribusi pada pendekatan yang lebih praktis dan terjangkau dalam meningkatkan keamanan jaringan pendidikan.

Melalui simulasi ini, diharapkan dapat diketahui sejauh mana efektivitas kombinasi VLAN dan ACL dalam meningkatkan keamanan jaringan serta mengurangi risiko akses yang tidak sah antar pengguna dari segmen jaringan yang berbeda [2], [6].

II. METODE PENELITIAN

Penelitian ini terdiri dari tujuh tahapan utama, yaitu studi pustaka, analisis kebutuhan jaringan, perancangan jaringan, pengembangan infrastruktur jaringan, konfigurasi perangkat jaringan, pengujian sistem jaringan, serta analisis terhadap hasil pengujian. Cisco Packet Tracer dipilih karena menyediakan fitur lengkap untuk simulasi VLAN dan ACL, mudah digunakan oleh pemula, dan banyak digunakan dalam pelatihan Cisco Networking Academy, sehingga cocok untuk skenario pendidikan Rangkaian tahapan penelitian ini ditampilkan pada Gambar 1.

Penelitian ini dimulai dengan tahap **studi literatur**, di mana dilakukan pengumpulan referensi dari buku, jurnal, dan artikel ilmiah yang relevan dengan topik keamanan jaringan, VLAN, dan Access Control List (ACL). Tujuan dari tahap ini adalah membangun dasar teori yang kuat serta memilih pendekatan konfigurasi yang tepat untuk

kebutuhan jaringan di lingkungan sekolah [2], [3], [4].

Gambar 1. Tahapan Penelitian

Selanjutnya, tahap **analisis jaringan** dilakukan untuk mengidentifikasi kebutuhan jaringan di sekolah, meliputi perangkat yang digunakan, fungsi tiap ruangan, serta pola akses pengguna terhadap layanan jaringan [1], [7].

Pada tahap **desain jaringan**, dirancang topologi jaringan menggunakan Cisco Packet Tracer. Desain ini meliputi pembagian VLAN berdasarkan fungsi ruangan (seperti ruang guru, ruang siswa, ruang administrasi, dan server), serta perencanaan konektivitas antar-VLAN [3], [5], [6].

Kemudian, masuk ke tahap **pengembangan jaringan**, di mana desain yang telah dibuat dikembangkan lebih lanjut dengan penambahan skema pengamanan menggunakan ACL. Tujuannya adalah untuk mendukung segmentasi jaringan serta pembatasan akses antar VLAN sesuai kebijakan [2], [4].

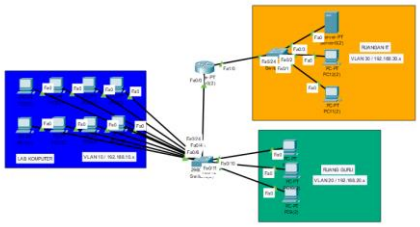
Setelah itu, dilakukan **konfigurasi jaringan** sesuai hasil desain dan pengembangan sebelumnya. Konfigurasi ini mencakup pembuatan VLAN di switch, pengaturan inter-VLAN routing pada router, serta penerapan ACL untuk mengatur hak akses antar jaringan [1], [3].

ahap berikutnya adalah **pengujian jaringan**, yang bertujuan untuk memastikan konektivitas antar perangkat dalam satu VLAN maupun antar VLAN. Pengujian dilakukan melalui fitur seperti *ping*, akses web, dan berbagi file di Cisco Packet Tracer. Jika hasil belum sesuai, konfigurasi akan diperbaiki dan diuji kembali [2], [5].

Terakhir, dilakukan **analisis hasil pengujian** untuk mengevaluasi efektivitas konfigurasi jaringan yang telah diterapkan. Pada tahap ini, dicatat perangkat mana yang berhasil atau gagal terhubung sesuai aturan ACL, guna menilai sejauh mana VLAN dan ACL berhasil meningkatkan keamanan jaringan di lingkungan sekolah [4], [6].

III. HASIL DAN PEMBAHASAN

Dalam simulasi ini dibuat sebuah sistem jaringan yang memanfaatkan VLAN dan Access Control List (ACL) sebagai filter untuk membatasi hak akses antar perangkat dalam jaringan. Topologi jaringan yang digunakan terdiri dari 1 router, 2 switch, dan 3 VLAN yaitu VLAN 10 (Lab Komputer), VLAN 20 (Ruang Guru), dan VLAN 30 (Ruang IT). Simulasi ini dirancang dan dikonfigurasi menggunakan aplikasi Cisco Packet Tracer versi terbaru.



Gambar 2. Rancangan Topologi Jaringan

Rancangan topologi jaringan dalam penelitian ini terdiri dari dua buah switch utama dan satu buah router sebagai pusat pengendali lalu lintas jaringan antar VLAN. **Switch 1** digunakan untuk mengakomodasi dua segmen VLAN, yaitu **VLAN 10** (Lab Komputer) dan **VLAN 20** (Ruang Guru). Sementara itu, **Switch 2** secara khusus digunakan untuk **VLAN 30** (Ruang IT), yang bertanggung jawab terhadap pengelolaan server dan kontrol jaringan.

Langkah selanjutnya adalah melakukan pemetaan alamat IP dan pengelompokan VLAN sebagai identitas setiap perangkat yang akan digunakan dalam jaringan komputer yang telah dirancang. Dengan cara ini, router dapat mengenali dan menjalankan aturan sesuai dengan protokol yang ditentukan. Pembagian VLAN dan IP dilakukan berdasarkan fungsi dari masing-masing ruangan di sekolah, yaitu Ruang IT, Ruang Guru, dan Laboratorium Komputer.

Tabel 1. aftar IP Address dan VLAN

Switch	VLAN	Nama Ruang	Range IP Address	Gateway	Network
Switch 1	30	Ruang IT	192.168.30.1 – 192.168.30.254	192.168.30.1	192.168.30.0/24
Switch 2	20	Ruang Guru	192.168.20.1 – 192.168.20.254	192.168.20.1	192.168.20.0/24
Switch 2	10	Lab Komputer	192.168.10.1 – 192.168.10.254	192.168.10.1	192.168.10.0/24

Pada Tabel 1 dijelaskan pembagian IP address dan jaringan VLAN pada masing-masing switch yang digunakan dalam simulasi. Pembagian ini dirancang untuk mengelompokkan perangkat berdasarkan fungsi dan kebutuhan aksesnya, sekaligus mempermudah pengaturan segmentasi jaringan dan pengamanan data.

Switch 1 digunakan untuk menghubungkan perangkat di **Ruang IT** dan ditempatkan pada **VLAN 30**, dengan alokasi IP address dari 192.168.30.1 hingga 192.168.30.254. IP gateway yang digunakan adalah 192.168.30.1, dengan network 192.168.30.0/24 dan netmask 255.255.255.0. **Switch 2** digunakan untuk mengakomodasi dua VLAN sekaligus, yaitu **VLAN 20** untuk **Ruang Guru** dan **VLAN 10** untuk **Laboratorium Komputer**. VLAN 20 menggunakan rentang IP 192.168.20.1 – 192.168.20.254, gateway 192.168.20.1, dan network 192.168.20.0/24. Sementara VLAN 10 menggunakan rentang IP 192.168.10.1 – 192.168.10.254, gateway 192.168.10.1, dan network 192.168.10.0/24.

Semua IP address yang digunakan merupakan kelas C yang umum digunakan dalam jaringan lokal skala kecil seperti lingkungan sekolah [2], [4]. Dengan pengelompokan ini, setiap segmen jaringan memiliki identitas sendiri, mempermudah pengaturan lalu lintas jaringan serta penerapan Access Control List (ACL) untuk membatasi hak akses antar VLAN [1], [3], [5]. Langkah berikutnya adalah menetapkan hak akses pada router untuk setiap VLAN yang digunakan. Tujuan dari tahap ini adalah untuk menentukan komputer mana yang diizinkan saling terhubung, serta perangkat mana yang memiliki akses ke layanan tertentu seperti web server dan FTP server dalam jaringan VLAN yang telah dibentuk [2], [6].

VLAN	Nama Ruangan	Network	Akses ke VLAN 10	Akses ke VLAN 20	Akses ke VLAN 30
10	Lab Komputer	192.168.10.0	V	X	X
20	Ruang Guru	192.168.20.0	V	V	X
30	Ruang IT	192.168.30.0	V	V	V

Keterangan: (v) diizinikan/permit (x) ditolak/deny

Tabel 2 menjelaskan pembagian hak akses antar VLAN. Komputer yang berada pada jaringan **VLAN 10 (Lab Komputer)** dengan alamat network 192.168.10.0 **tidak diizinkan** mengakses jaringan VLAN lain, yaitu VLAN 20 (Ruang Guru) dan VLAN 30 (Ruang IT). Komputer pada jaringan ini hanya dapat berkomunikasi dalam segmen yang sama. Sementara itu, **komputer pada VLAN 20 (Ruang Guru)** dengan alamat network 192.168.20.0 diizinkan mengakses VLAN 10, tetapi tidak diizinkan mengakses VLAN 30. Hal ini bertujuan untuk membatasi akses guru terhadap sumber daya yang sensitif atau teknis di jaringan IT.

Sedangkan **komputer yang berada pada VLAN 30 (Ruang IT)** dengan network 192.168.30.0 diberikan hak akses penuh untuk dapat mengakses seluruh VLAN, termasuk Lab dan Ruang Guru. Hal ini dikarenakan perangkat di VLAN 30 berfungsi sebagai pengelola sistem jaringan dan memerlukan kontrol penuh terhadap seluruh segmen.

Dengan konfigurasi ini, router akan bertindak sebagai pengontrol akses menggunakan **Extended Access Control List (ACL)** yang akan ditempatkan pada masing-masing sub-interface yang mewakili VLAN, guna membatasi atau mengizinkan lalu lintas jaringan sesuai dengan kebijakan yang telah ditentukan.

Selanjutnya dibuat konfigurasi VLAN pada tiap switch sebagai penghubung setiap komputer dengan jaringan. Switch pada jaringan ini ada tiga yaitu Switch Lab (VLAN 10), Switch Guru (VLAN 20), dan Switch IT (VLAN 30). Satu buah router digunakan sebagai penghubung antar VLAN menggunakan metode *router-on-a-stick*.

Konfigurasi Switch 1 – Ruang Guru Dan Ruangan Lab

```
Switch>en
Switch#conf t
witch(config)#vlan 10
Switch(config-vlan)#name LAB
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name GURU
Switch(config-vlan)#exit
Switch(config)#int range fa0/1 - 9
Switch(config-if-range)#swi mod access
Switch(config-if-range)#swi access vlan 10
Switch(config-if-range)#exit
Switch(config)#int range fa0/10 - 19
Switch(config-if-range)#swi mod access
Switch(config-if-range)#swi access vlan 20
Switch(config-if-range)#exit
Switch(config)#int fa0/24
Switch(config-if)#swi mod trunk
Switch(config-if)#exit
```

Konfigurasi Switch 2 – Ruang IT

```
Switch>en
Switch#conf t
Switch(config)#vlan 30
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#int range fa0/1 - 5
Switch(config-if-range)#swi mod access
Switch(config-if-range)#swi access vlan 30
Switch(config-if-range)#exit
Switch(config)#int fa0/24
Switch(config-if)#swi mod trunk
Switch(config-if)#exit
```

Konfigurasi Router – Konfigurasi VLAN

```
Router#en
Router#conf t
Router(config)#int g0/0.10
Router(config-subif)#enca dot1Q 10
Router(config-subif)#ip address 192.168.10.1
255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#int g0/0.20
Router(config-subif)#enca dot1Q 20
Router(config-subif)#ip address 192.168.20.1
255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#int g0/1.30
Router(config-subif)#enca dot1Q 30
Router(config-subif)#ip address 192.168.30.1
255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
```

Tahap terakhir adalah memasukkan konfigurasi extended ACL pada router untuk membatasi hak akses antar VLAN, khususnya untuk mencegah VLAN 10 mengakses VLAN 20 dan VLAN 30, serta mencegah VLAN 20 mengakses VLAN 30. Konfigurasi ini dilakukan untuk menghindari akses yang tidak diizinkan antar departemen jaringan dan memastikan segmentasi berjalan dengan baik.

Pada **Konfigurasi VLAN 10** dimasukkan konfigurasi extended ACL untuk **VLAN 10** agar setiap perangkat yang terhubung melalui jaringan Lab Komputer **tidak dapat mengakses** jaringan VLAN Guru maupun VLAN IT/Server. Konfigurasi ini menggunakan protokol ICMP sebagai dasar pengujian komunikasi antar perangkat.

Konfigurasi Router – Extended ACL untuk VLAN 10

```
Router#en
Router#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#ip access-list extended
BLOCK_VLAN10_TO_VLAN20_TO_VLAN30
Router(config-ext-nacl)#deny icmp 192.168.10.0
0.0.0.255 192.168.20.0 0.0.0.255 echo
Konfigurasi ini memblokir akses ICMP (ping) dari
VLAN 10 ke VLAN 20 dan VLAN 30, sehingga
komputer di Lab Komputer tidak dapat mengakses
departemen lain
Router(config-ext-nacl)#deny icmp 192.168.10.0
0.0.0.255 192.168.30.0 0.0.0.255 echo
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#int g0/0.10
Router(config-subif)#ip access-group
BLOCK_VLAN10_TO_VLAN20_TO_VLAN30 in
Router(config-subif)#exit
```

Pada **Konfigurasi VLAN 20** dilakukan konfigurasi extended ACL untuk **VLAN 20** agar perangkat yang terhubung dari jaringan Guru **tidak dapat mengakses VLAN 30**, namun tetap dapat berkomunikasi dengan VLAN 10. Konfigurasi ini juga menggunakan ICMP untuk membatasi akses antar jaringan.

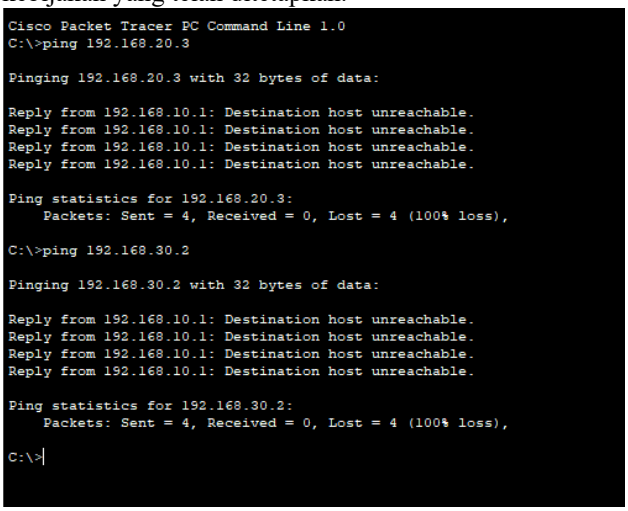
Konfigurasi Router – Extended ACL untuk VLAN 20

```
Router(config)#ip access-list extended
BLOCK_VLAN20_TO_VLAN30
Router(config-ext-nacl)#deny icmp 192.168.20.0
0.0.0.255 192.168.30.0 0.0.0.255 echo
Konfigurasi ini memblokir akses ICMP (ping) dari
VLAN 10 ke VLAN 20 dan VLAN 30, sehingga
komputer di Lab Komputer tidak dapat mengakses
departemen lain
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#int g0/0.20
Router(config-subif)#ip access-group
BLOCK_VLAN20_TO_VLAN30 in
Router(config-subif)#exit
Router(config)#
```

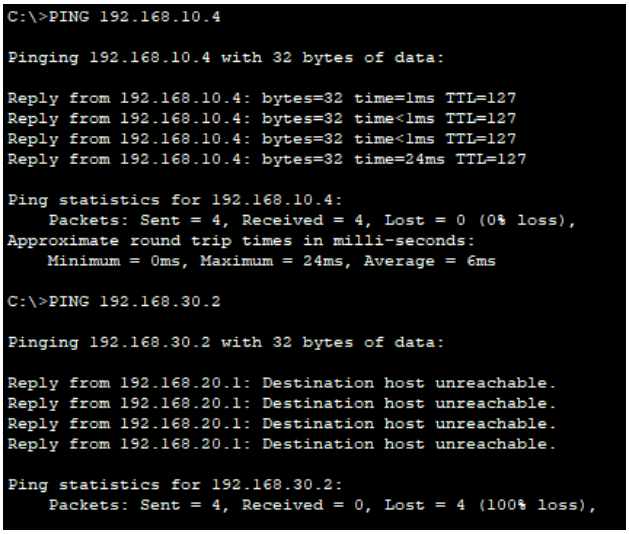
Pada konfigurasi **VLAN 30 tidak diberikan ACL tambahan** karena jaringan ini digunakan sebagai pusat IT yang memerlukan akses penuh ke semua jaringan untuk keperluan manajemen dan pengawasan sistem.

Dengan diterapkannya konfigurasi **extended ACL**, komunikasi antar jaringan VLAN hanya dapat dilakukan berdasarkan kebijakan yang telah ditentukan, sehingga keamanan jaringan sekolah dapat ditingkatkan dan potensi gangguan dari lalu lintas antar departemen dapat diminimalkan [2], [3], [5]. Hasil pengujian yang dilakukan menunjukkan bahwa perangkat dari **VLAN 10 gagal mengakses VLAN 20 dan VLAN 30**, sementara perangkat dari VLAN 20 hanya berhasil mengakses VLAN 10, sesuai dengan konfigurasi ACL yang telah diterapkan [1], [6].

Gambar 3 menunjukkan hasil pengujian konektivitas dari perangkat yang berada di **VLAN 10 (Lab Komputer)** ke perangkat pada **VLAN 20 (Ruang Guru)** dan **VLAN 30 (Ruang IT/Server)**. Berdasarkan hasil uji ping, ditampilkan pesan **"Request Timed Out"**, yang menandakan bahwa perangkat dari VLAN 10 **tidak dapat melakukan komunikasi ke VLAN lain**. Hal ini membuktikan bahwa konfigurasi extended ACL yang diterapkan pada interface `g0/0.10` berhasil **membatasi akses keluar dari VLAN 10** ke VLAN lainnya sesuai kebijakan yang telah ditetapkan.



Gambar 3. Hasil Uji Akses dari VLAN 10 ke VLAN 20 dan VLAN 30

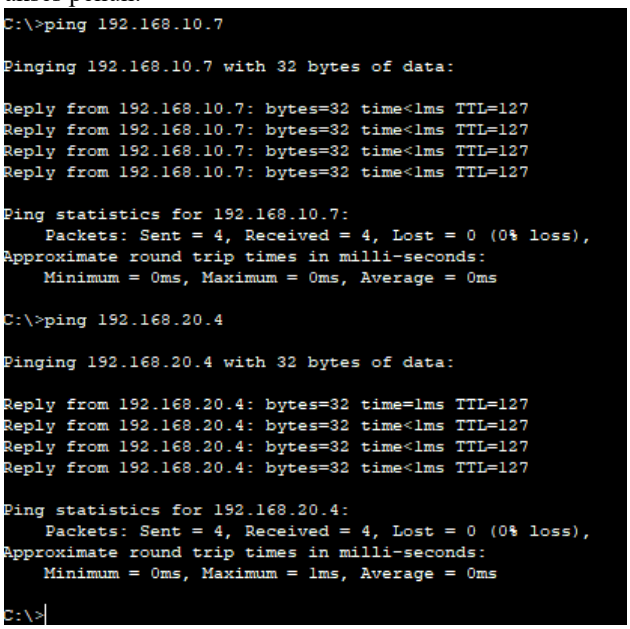


Gambar 4. Hasil Uji Akses dari VLAN 20 ke VLAN 10 dan VLAN 30

Gambar 4 memperlihatkan hasil pengujian dari perangkat **VLAN 20 (Ruang Guru)** ke perangkat pada **VLAN 10 (Lab Komputer)** dan **VLAN 30 (Server)**. Berdasarkan hasil uji ping, komunikasi ke VLAN 10 **berhasil dilakukan** ditunjukkan dengan balasan **"Reply from…"**, sementara akses ke VLAN 30 kembali menunjukkan pesan **"Request Timed Out"**. Hal ini menunjukkan bahwa **ACL pada interface `g0/0.20` berhasil membatasi akses dari VLAN 20 ke VLAN 30**, namun tetap mengizinkan akses ke VLAN 10.

Gambar 5 menunjukkan hasil pengujian dari perangkat yang berada di **VLAN 30 (Ruang IT)** ke perangkat-perangkat di **VLAN 10 dan VLAN 20**. Semua

pengujian berhasil dan menampilkan balasan **"Reply from…"**, yang menandakan bahwa perangkat VLAN 30 **dapat berkomunikasi dengan seluruh VLAN** tanpa hambatan. Hal ini sesuai dengan kebijakan bahwa VLAN 30 bertugas sebagai pusat pengelola jaringan dan diberikan akses penuh.



Gambar 5. Hasil Uji Akses dari VLAN 30 ke VLAN 10 dan VLAN 20

Hasil simulasi ini konsisten dengan penelitian [5] dan [6] yang menyatakan bahwa kombinasi VLAN dan ACL efektif dalam membatasi lalu lintas antar segmen. Namun, kelebihan penelitian ini adalah penerapan skenario pada konteks sekolah, yang menyesuaikan kebutuhan akses antara siswa, guru, dan pengelola IT. Solusi yang disimulasikan juga relatif sederhana dan ekonomis untuk diimplementasikan pada jaringan pendidikan skala kecil hingga menengah.

Hasil simulasi menunjukkan bahwa kombinasi VLAN dan extended ACL mampu mengatur lalu lintas jaringan secara selektif. Misalnya, siswa yang berada di VLAN 10 (Lab Komputer) tidak dapat mengakses VLAN 20 (Ruang Guru) maupun VLAN 30 (Ruang IT), sehingga mencegah potensi akses tidak sah terhadap data guru atau sistem administrasi. Sistem ini juga secara tidak langsung mengurangi risiko serangan internal seperti sniffing atau pemanfaatan kelemahan layanan jaringan karena trafik antar segmen sudah dibatasi.

Penerapan VLAN dengan ACL ini dapat mengurangi permukaan serangan dalam jaringan lokal. Jika terjadi serangan malware di satu VLAN, penyebarannya tidak bisa menyeberang ke VLAN lain. Selain itu, pendekatan ini sangat cocok diterapkan di sekolah karena tidak memerlukan perangkat tambahan—cukup dengan router dan switch yang sudah mendukung fitur VLAN dan ACL.

Simulasi ini juga dapat dijadikan acuan implementasi nyata, terutama pada sekolah menengah atau institusi pendidikan kecil-menengah yang memiliki keterbatasan anggaran dan tidak menggunakan perangkat firewall khusus.

IV. SIMPULAN

Berdasarkan hasil perancangan, konfigurasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan VLAN dan extended Access Control List (ACL) pada jaringan sekolah mampu meningkatkan keamanan dan segmentasi akses antar pengguna jaringan. Dalam simulasi menggunakan Cisco Packet Tracer, masing-masing VLAN berhasil dipisahkan secara logis berdasarkan fungsi ruangan, yaitu Lab Komputer (VLAN 10), Ruang Guru (VLAN 20), dan Ruang IT (VLAN 30).

Penerapan extended ACL pada router berhasil membatasi komunikasi antar VLAN sesuai kebijakan yang telah ditentukan. Hasil pengujian menunjukkan bahwa VLAN 10 tidak dapat mengakses VLAN 20 dan VLAN 30, VLAN 20 hanya dapat mengakses VLAN 10, dan VLAN 30 memiliki akses penuh ke semua VLAN. Hal ini membuktikan bahwa konfigurasi ACL yang diterapkan telah berjalan sesuai fungsi dan efektif dalam mengatur lalu lintas jaringan berdasarkan peran dan kebutuhan akses masing-masing bagian.

Dengan demikian, penerapan VLAN dan ACL dapat dijadikan solusi praktis dalam meningkatkan keamanan jaringan lokal di lingkungan sekolah, serta dapat menjadi acuan implementasi serupa pada institusi pendidikan lainnya dengan skala dan kebutuhan yang sebanding. Simulasi ini dapat diimplementasikan secara langsung pada jaringan sekolah dengan penyesuaian perangkat keras dan topologi jaringan yang sesuai, tanpa membutuhkan perangkat tambahan yang mahal.

Untuk pengembangan lebih lanjut, sistem ini dapat diintegrasikan dengan **DHCP Server** agar pengelolaan alamat IP lebih efisien, serta ditambahkan **sistem monitoring jaringan** seperti Zabbix atau PRTG guna memantau lalu lintas dan mendeteksi anomali lebih dini.

REFERENCES

[1] D. Pandu Agustio & E. R. Nainggolan, "Penerapan Virtual Local Area Network Pada Jaringan MAN dengan Metode Filtering Berbasis Access Control List di Dinas Komunikasi dan Informatika Kota Serang," *Jurnal Komputer Antartika*, vol. 1, no. 1, pp. 1–10, 2021. DOI: 10.70052/jka.v1i1.5

[2] F. W. Christanto, A. Nugroho, & W. A. Adhiwibowo, "Implementasi Keamanan Jaringan LAN Berbasis ACL dan VLAN," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 10, no. 2, pp. 45–52, 2021. Link

[3] W. Soetrisno, "Proteksi Jaringan Menggunakan Access Control List pada Local Area Network," *Techno Xplore: Jurnal Ilmu Komputer dan Teknologi Informasi*, vol. 8, no. 2, pp. 89–96, 2022. DOI: 10.36805/technoxplore.v8i2.3046

[4] N. A. Putra, V. Riyanto, G. Wijaya, & N. Herlinawati, "Firewall Design Using Access Control List Method As Data Filtering," *Jurnal Mantik*, vol. 5, no. 3, pp. 1684–1693, 2021. Link

[5] F. Firmansyah & M. Wahyudi, "Analisis Performa Access Control List Menggunakan Metode Firewall Policy Base," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 283–292, 2021. DOI: 10.30812/matrik.v20i2.1068

[6] Fahrizal & B. A. Candra, "Implementasi Access Control List dalam Perancangan Virtual Local Area Network pada PT Cakramedia Indocyber," *JEIS: Jurnal Elektro dan Informatika Swadharma*, vol. 2, no. 2, pp. 143–149, 2022. DOI: 10.56486/jeis.vol2no2.204

[7] S. Dewi, F. Firmansyah, & U. Hasan, "Penerapan Metode Access Control List Pada Jaringan VLAN Menggunakan Router Cisco," *IMTechno: Journal of Industrial Management and Technology*, vol. 3, no. 1, pp. 55–60, 2022. DOI: 10.31294/imtechno.v3i1.927

[8] S. Susilo, S. Hartono, K. Yunan, & B. A. Wardijono, "Implementasi

VLAN Cisco untuk Pengaturan Hak Akses pada Jaringan Komputer Sekolah," *Prosiding Seminar SeNTIK*, vol. 7, no. 1, pp. 273–284, 2023. Link

[9] F. Fatkhurrahman & A. Witanti, "Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik," *JEKIN - Jurnal Teknik Informatika*, vol. 4, no. 3, pp. 201–208, 2023. DOI: 10.58794/jekin.v4i3.904

[10] R. P. Prastiyo, "Perancangan dan Implementasi Jaringan VLAN untuk Meningkatkan Kinerja Jaringan di SMP Ad-Da'wah," *Journal of Industrial Engineering and Informatics*, vol. 1, no. 1, pp. 1–7, 2024. Link

[11] M. Z. Zulqifli, L. Lutfi, & M. A. Bahar, "Perancangan Sistem Jaringan VLAN pada SMP Negeri 2 Pasar Wajo," *Advances in Computer System Innovation Journal*, vol. 1, no. 1, pp. 55–62, 2023. DOI: 10.51577/acsijournal.v1i1.446

[12] I. Ramadhan & A. Junaidi, "Perancangan Jaringan VLAN Sekolah Menengah Atas Fatahillah," *Computer and Network Technology*, vol. 4, no. 1, pp. 32–40, 2024. DOI: 10.31294/conten.v4i1.4909

[13] A. D. Prasetya, "Simulasi ACL Standard pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer," *Jurnal Teknologi Komputer*, vol. 8, no. 2, pp. 112–118, 2022.

[14] A. Usior & E. Sediyono, "Simulasi Extended ACL pada Jaringan VLAN Menggunakan Cisco Packet Tracer," *AITI: Jurnal Teknologi Informasi*, vol. 20, no. 1, pp. 32–47, Feb. 2023.

[15] R. Kurniawan & S. Hidayat, "Penerapan Metode Access Control List Pada Jaringan VLAN Menggunakan Router Cisco," *Jurnal Informatika dan Sistem Komputer*, vol. 10, no. 1, pp. 55–60, 2021.

[16] S. N. Lestari & H. Wibowo, "Proteksi Jaringan Menggunakan Access Control List pada Local Area Network," *Jurnal Keamanan Jaringan dan Komunikasi*, vol. 7, no. 3, pp. 89–96, 2022.

[17] B. Cahyono, "Implementasi Access Control List dalam Perancangan Virtual Local Area Network pada PT Cakramedia Indocyber," *Jurnal Sistem dan Teknologi Informasi*, vol. 9, no. 2, pp. 143–149, 2021.