IJM: Indonesian Journal of Multidisciplinary
e-ISSN: 3025-5961
Volume 3 Nomor 1 Tahun 2025
https://ojs.csspublishing.com/index.php/ijm

Simulasi ACL Standard pada Jaringan VLAN Menggunakan Aplikasi *Cisco Packet Tracer*

Delfin Christofa[1*], Tamsir Ariyadi[2]
Universitas Bina Darma [1,2]
e-mail: delfinchristofa1@gmail.com

Abstract
This research explores the implementation of the standard Access Control List (ACL) on VLAN networks using Cisco Packet Tracer. VLAN technology is used to improve network efficiency and security by dividing a physical network into multiple logical networks. ACL serves to control data traffic in detail by applying specific rules, enhancing communication between VLANs. The research method involves six stages: network analysis, design, development, configuration, testing, and result analysis. The simulation results show that the implementation of VLAN and ACL can selectively restrict access, thereby strengthening network security and improving efficiency. The network topology in the simulation consists of two VLANs connected by routers and switches to support device communication. This study demonstrates that Cisco Packet Tracer is an effective and cost-efficient simulation tool for learning and testing network configurations. Overall, the study provides practical insights on how to manage secure and structured networks in modern environments.
Keywords: *VLAN, standard ACL, Cisco, Switch, Configuration.*

Abstrak
Penelitian ini mengeksplorasi implementasi standar Access Control List (ACL) pada jaringan VLAN menggunakan Cisco Packet Tracer. Teknologi VLAN digunakan untuk meningkatkan efisiensi dan keamanan jaringan dengan membagi jaringan fisik menjadi beberapa jaringan logis. ACL berfungsi untuk mengontrol lalu lintas data secara rinci dengan menerapkan aturan yang khusus, yang meningkatkan komunikasi antar VLAN. Metode penelitian yang digunakan meliputi enam tahap, yaitu analisis jaringan, desain, pengembangan, konfigurasi, pengujian, dan analisis hasil. Hasil simulasi menunjukkan bahwa implementasi VLAN dan ACL dapat membatasi akses secara selektif, sehingga memperkuat keamanan jaringan dan meningkatkan efisiensi. Topologi jaringan dalam simulasi terdiri dari dua VLAN yang terhubung dengan router dan switch untuk mendukung komunikasi antar perangkat. Penelitian ini membuktikan bahwa Cisco Packet Tracer merupakan alat simulasi yang efektif dan hemat biaya dalam mempelajari serta menguji konfigurasi jaringan. Secara keseluruhan, studi ini memberikan wawasan praktis tentang cara mengelola jaringan yang aman dan terstruktur dalam lingkungan modern.
Kata Kunci: VLAN, ACL standar, Cisco, Switch, Konfigurasi.

PENDAHULUAN

Kemajuan teknologi informasi yang pesat telah mendorong kebutuhan akan jaringan komputer yang andal, efisien, dan aman. Salah satu teknologi penting dalam pengelolaan jaringan adalah Virtual Local Area Network (VLAN). VLAN memungkinkan segmentasi jaringan secara logis untuk meningkatkan efisiensi dan keamanan komunikasi data. Teknologi ini sangat bermanfaat dalam lingkungan yang memerlukan pembagian jaringan, seperti kampus, kantor, atau organisasi multinasional (Ananda et.all, 2024). VLAN juga memungkinkan pembagian satu jaringan fisik menjadi beberapa jaringan logis yang terpisah. Pembagian ini bertujuan untuk meningkatkan efisiensi operasional, mengurangi domain broadcast, dan meningkatkan keamanan melalui isolasi lalu lintas antar segmen jaringan (Sumarni & Purnama, 2023).

Simulasi VLAN menggunakan aplikasi seperti Cisco Packet Tracer memberikan solusi praktis dalam memahami dan menguji konfigurasi jaringan tanpa memerlukan perangkat keras fisik (Usior & Sediyono, 2023). Packet Tracer, sebuah alat simulasi jaringan yang dikeluarkan oleh Cisco, memungkinkan pengguna untuk mengonfigurasi perangkat jaringan, mendesain topologi, dan mengimplementasikan protokol seperti Access Control List (ACL) untuk meningkatkan keamanan jaringan (Dhaka, 2019). Untuk mendukung segmentasi VLAN, penggunaan Access Control List (ACL) menjadi relevan. ACL adalah fitur keamanan yang memungkinkan administrator jaringan untuk mengatur aturan akses berdasarkan protokol, alamat IP, atau port tertentu, sehingga hanya lalu lintas yang sesuai dengan kriteria yang diizinkan untuk melewati jaringan (Laksono & Nasution, 2020). Implementasi ACL pada VLAN memberikan kontrol yang lebih rinci terhadap lalu lintas data, sekaligus meningkatkan keamanan jaringan secara keseluruhan (Ariyadi, 2022).

Implementasi VLAN dan ACL melalui Cisco Packet Tracer telah terbukti menjadi pendekatan yang efisien untuk mengelola lalu lintas jaringan, melindungi data, dan meminimalkan potensi ancaman keamanan. Studi menunjukkan bahwa simulasi berbasis Packet Tracer dapat mengurangi biaya laboratorium serta memberikan peluang pembelajaran praktis kepada siswa dan profesional (Hosain et.al., 2019). Pada konteks yang lebih luas, teknologi VLAN digunakan dalam berbagai skenario, seperti implementasi kampus pintar dan jaringan perkantoran yang aman. Misalnya, VLAN dikombinasikan dengan Internet of Things (IoT) untuk mendukung otomatisasi dan keamanan dalam bangunan pintar serta perkantoran. Kombinasi ini meningkatkan efisiensi, memberikan kontrol jarak jauh, dan mengurangi risiko kerentanan keamanan (Almalki, 2020); (Azhari et.al., 2021). Selain itu, desain dan simulasi jaringan kampus aman menggunakan VLAN dan ACL telah menunjukkan keberhasilan dalam mengoptimalkan kinerja jaringan, melindungi data, dan memastikan transfer informasi yang andal. Dengan memanfaatkan protokol keamanan

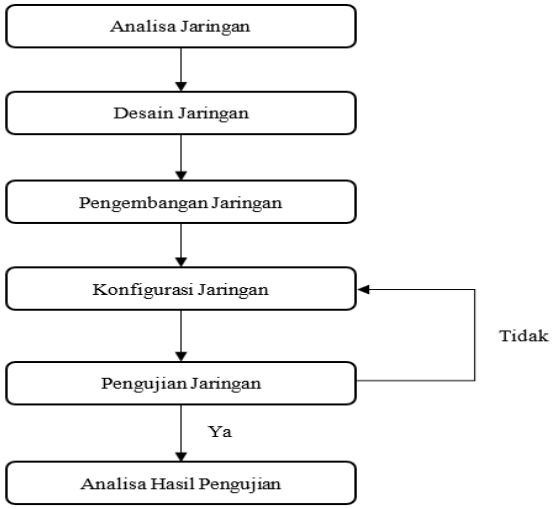
tingkat lanjut seperti Virtual Private Network (VPN) dan firewall, simulasi ini dapat diaplikasikan untuk mendukung kebutuhan institusi pendidikan modern (Ahmed & Hamdani, 2021).

Dalam konteks pembelajaran dan pengujian jaringan, Cisco Packet Tracer adalah salah satu perangkat lunak simulasi yang paling sering digunakan (Fahri, 2018). Aplikasi ini memungkinkan pengguna untuk merancang, mengonfigurasi, dan menganalisis jaringan secara virtual, memberikan solusi hemat biaya untuk eksperimen jaringan yang kompleks [13]. Cisco Packet Tracer mendukung berbagai fitur termasuk konfigurasi VLAN, ACL, dan protokol routing, sehingga mempermudah simulasi jaringan berskala besar yang mencakup berbagai elemen konfigurasi jaringan (Bangun et.all., 2020). Melalui pendekatan ini, Cisco Packet Tracer tidak hanya berfungsi sebagai alat pembelajaran, tetapi juga sebagai platform pengembangan teknologi jaringan yang lebih efisien. Hal ini relevan untuk memenuhi tantangan teknologi jaringan modern, baik untuk kebutuhan akademik maupun professional (Yadaf et.all., 2023). Penelitian ini bertujuan untuk mengeksplorasi implementasi ACL standar pada jaringan VLAN menggunakan Cisco Packet Tracer, sekaligus menganalisis dampaknya terhadap kinerja jaringan. Studi ini diharapkan dapat memberikan wawasan tentang strategi terbaik dalam mengonfigurasi ACL dan VLAN untuk memenuhi kebutuhan keamanan dan efisiensi jaringan modern.

METODE PENELITIAN

Ada enam tahapan yang dilakukan pada penelitian ini yaitu analisis jaringan, desain jaringan, pengembangan jaringan, konfigurasi jaringan, pengujian jaringan, dan analisis hasil pengujian. Adapun tahapan penelitian dapat dilihat pada Gambar 1.

Gambar 1
Tahap Penelitian



Sumber: Data diolah, 2024

Tahap pertama, analisis jaringan. Pada tahap ini dilakukan proses pengamatan dan pencarian berbagai sumber informasi dari literatur tentang sebuah konfigurasi yang akan diterapkan. Selain itu dilakukan pula pencarian informasi tentang kelebihan dan kekurangan dari konfigurasi yang akan dipakai. Tahap kedua, desain jaringan. Pada proses ini dibuat topologi jaringan VLAN pada aplikasi Cisco Packet Tracer sebagai simulator. Tahap ketiga, pengembangan jaringan. Pada tahap ini dilakukan proses penambahan konfigurasi keamanan jaringan yang sudah dibuat untuk dapat dipakai pada saat konfigurasi. Tahap selanjutnya yaitu konfigurasi jaringan. Pada tahap ini dilakukan konfigurasi sesuai dengan topologi jaringan yang dibuat dan memasukkan setiap komponen jaringan di dalam topologi tersebut, kemudian mengkonfigurasikan ACL Standart pada router melalui CLI pada router yang akan mengendalikan proses filtering paket data dalam jaringan. Tahap kelima, pengujian jaringan. Pada tahap ini diuji koneksi setiap device yang tersambung pada jaringan dan dilihat apakah konfigurasi ACL Strandart yang sudah dikonfigurasikan pada router berjalan atau tidak. Jika tidak berhasil, maka akan dilakukan konfigurasi lagi lalu kembali pada tahap pengujian. Tahap terakhir yaitu analisis hasil pengujian. Pada tahap ini dibuat suatu analisis hasil dari proses pengamatan pada proses-proses yang sudah dibuat dan dijalankan sehingga bisa menghasilkan prototipe jaringan yang digunakan.

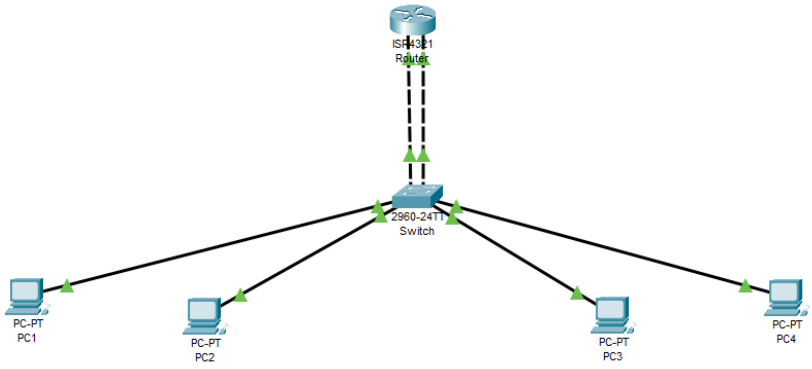
PEMBAHASAN

Topologi Jarigan

Dalam penelitian ini, telah dilakukan simulasi jaringan menggunakan VLAN dan Access Control List (ACL) standar pada perangkat Cisco Packet Tracer. Topologi jaringan yang dibangun terdiri dari perangkat-perangkat berikut:

1 Switch untuk menghubungkan perangkat di dalam jaringan.
1 Router untuk melakukan inter-VLAN routing.
4 PC, yang terbagi dalam dua VLAN terpisah: VLAN 10 dan VLAN 20.

Gambar 2
Rancangan Topologi



Sumber: Data diolah, 2024

Gambar 2 menggambarkan sebuah rancangan topologi yang dibuat untuk menerapkan konfigurasi dari ACL Standart pada suatu jaringan computer. Simulasi ini dibuat menggunakan aplikasi Cisco Packet Tracer versi 7.3.0. Dalam penerapannya berdasarkan topologi yang dibuat VLAN 10 digunakan untuk perangkat PC1 dan PC2, sementara VLAN 20 digunakan untuk perangkat PC3 dan PC4. Setiap perangkat dihubungkan ke switch melalui port yang sudah dikonfigurasi dengan mode akses (access mode) ke VLAN yang sesuai. Router menghubungkan kedua VLAN menggunakan dua interface fisik yang masing-masing terhubung ke VLAN 10 dan VLAN 20. Access Control List (ACL) diterapkan pada interface yang menghubungkan VLAN 10 untuk membatasi akses antara kedua VLAN.

Tabel 1
IP Address

Device	Interface	IP Address	Subnet mask	Default Gateway	VLAN
Router	Gigabitethernet0/0/0	192.168.10.1	255.255.255.0	-	VLAN 10
Router	Gigabitethernet0/0/1	192.168.20.1	255.255.255.0	-	VLAN 20
PC1	FastEthernet0/1	192.168.10.2	255.255.255.0	192.168.10.1	VLAN 10
PC2	FastEthernet0/2	192.168.10.3	255.255.255.0	192.168.10.1	VLAN 10
PC3	FastEthernet0/3	192.168.20.2	255.255.255.0	192.168.20.1	VLAN 20
PC4	Fast Ethernet0/4	192.168.20.3	255.255.255.0	192.168.20.1	VLAN 20

Sumber: Data diolah, 2024

Tabel IP Address yang disajikan menunjukkan konfigurasi alamat IP pada masing-masing perangkat dalam jaringan simulasi yang menggunakan VLAN dan ACL Standard. Router berfungsi sebagai penghubung antar VLAN (inter-VLAN routing) dengan dua interface fisik yang masing-masing dikonfigurasi untuk VLAN 10 dan VLAN 20. Interface GigabitEthernet0/0 pada router digunakan untuk VLAN 10 dengan IP Address 192.168.10.1 sebagai default gateway bagi perangkat di VLAN tersebut, sedangkan interface GigabitEthernet0/1 digunakan untuk VLAN 20 dengan IP Address 192.168.20.1 sebagai default gateway bagi perangkat di VLAN 20. Pada VLAN 10, PC1 dan PC2 memiliki IP Address 192.168.10.2 dan 192.168.10.3, yang berada dalam subnet 192.168.10.0/24 dengan default gateway 192.168.10.1. Sedangkan pada VLAN 20, PC3 dan PC4 memiliki IP Address 192.168.20.2 dan 192.168.20.3, yang

berada dalam subnet 192.168.20.0/24 dengan default gateway 192.168.20.1. Semua perangkat menggunakan subnet mask 255.255.255.0, sehingga perangkat dalam VLAN yang sama dapat saling berkomunikasi tanpa memerlukan bantuan router.

Segmentasi jaringan menggunakan VLAN memungkinkan pembagian perangkat secara logis sesuai dengan kebutuhan, sehingga meningkatkan efisiensi pengelolaan jaringan dan menambah tingkat keamanan. Router, selain memungkinkan komunikasi antar VLAN, juga memungkinkan penerapan kebijakan keamanan seperti Access Control List (ACL) untuk mengatur lalu lintas antar subnet. Dengan konfigurasi ini, setiap perangkat memiliki alamat IP yang terorganisasi dengan baik dan sesuai dengan topologi jaringan, sehingga mendukung komunikasi yang efisien dan terstruktur.

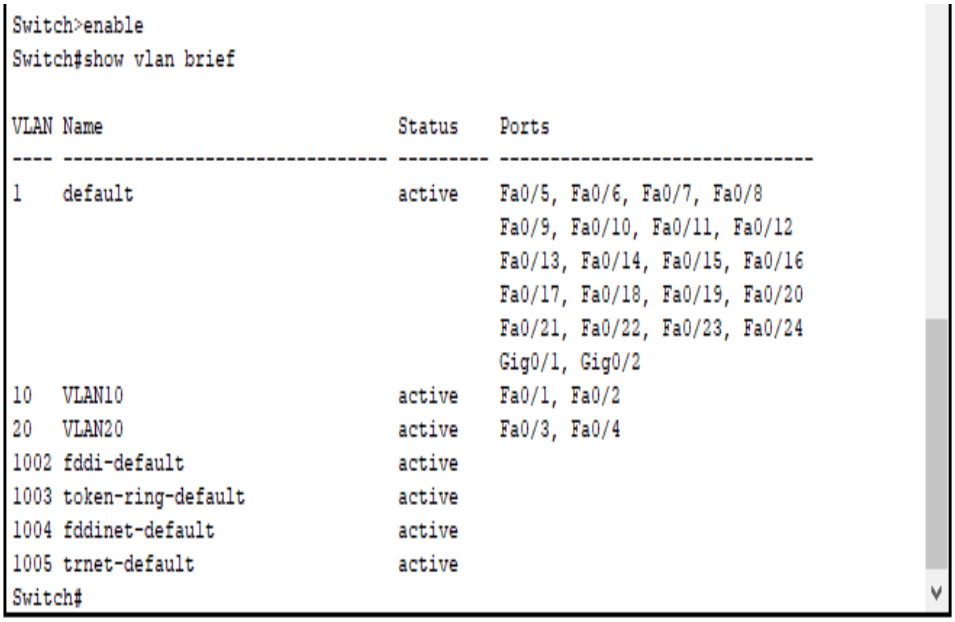
Konfigurasi Jaringan

3.2.1. konfigurasi Switch

```
Switch>enable
Switch#configure terminal

# Membuat VLAN
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#exit

# Port ke VLAN 10
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)#interface fastethernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

# Port ke VLAN 20
Switch(config)#interface fastethernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Switch(config)#interface fastethernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

Gambar 3
Hasil Konfigurasi Switch



```
Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   VLAN10                           active    Fa0/1, Fa0/2
20   VLAN20                           active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

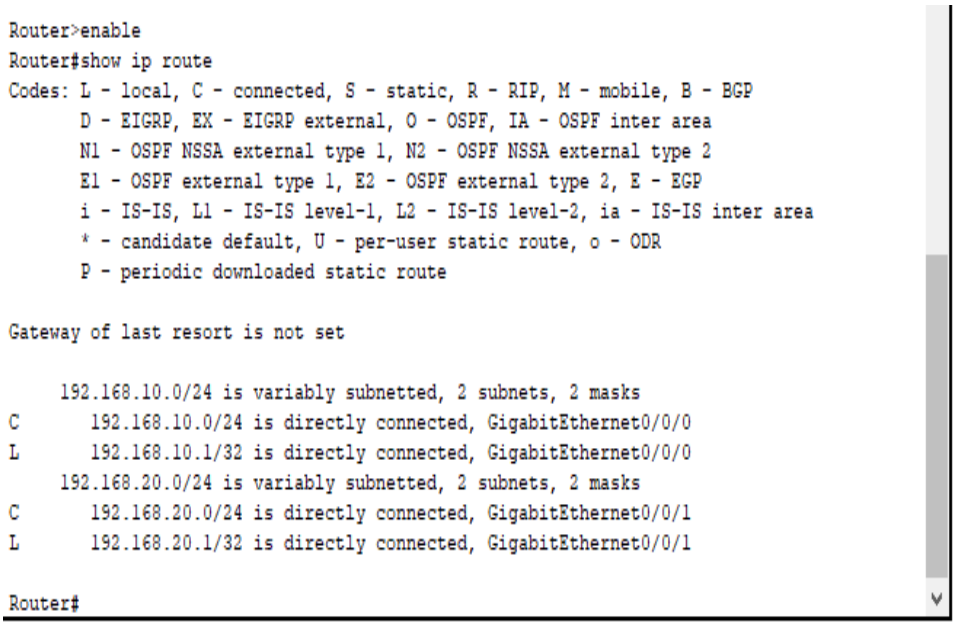
Sumber: Data diolah, 2024

Konfigurasi Router
Router>enable
Router#configure terminal

Interface untuk VLAN 10
Router(config)#interface gigabitethernet0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Interface untuk VLAN 20
Router(config)#interface gigabitethernet0/1
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Gambar 4
Hasil Konfigurasi Router



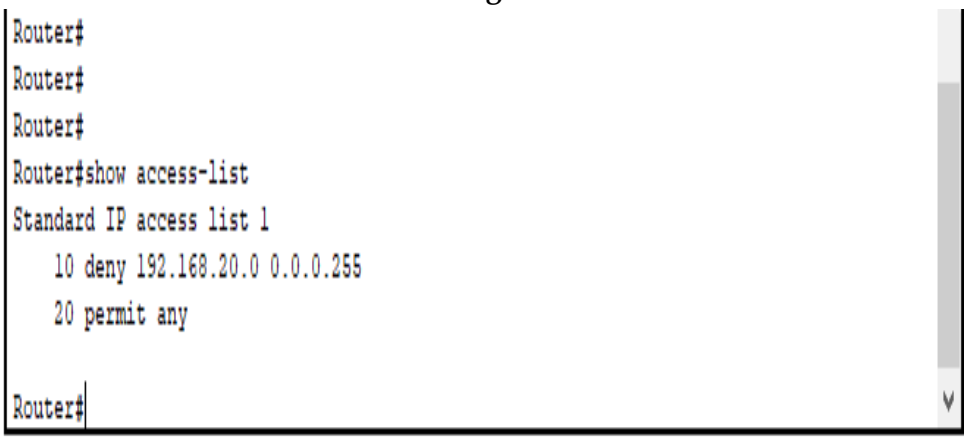
Sumber: Data diolah, 2024

Konfigurasi ACL

Router(config)#access-list 1 deny 192.168.20.0 0.0.0.255
Router(config)#access-list 1 permit any

Terapkan ACL pada interface VLAN 10
Router(config)#interface gigabitethernet0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#exit

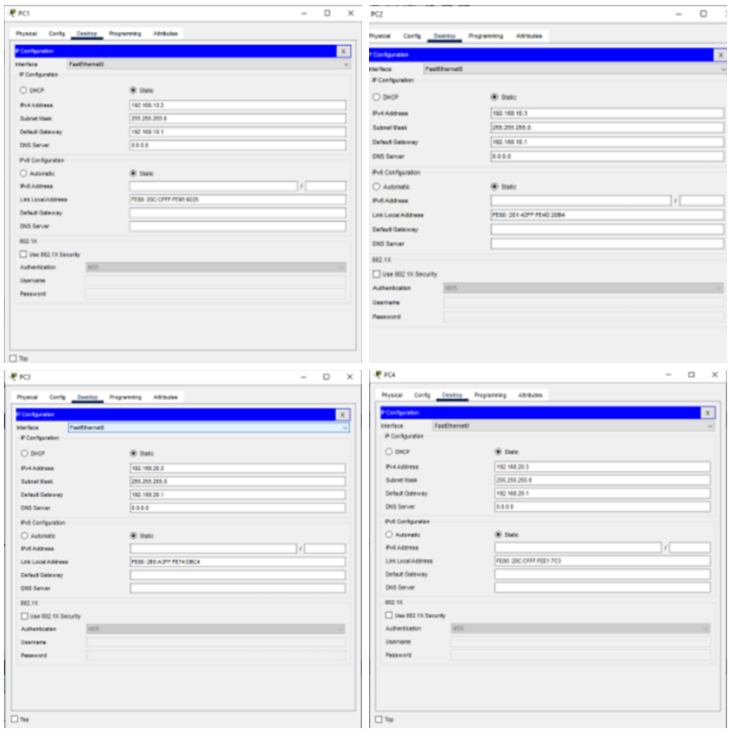
Gambar 5
Hasil Konfigurasi ACL



Sumber: Data diolah, 2024

Konfigurasi PC

Gambar 6
Konfigurasi PC



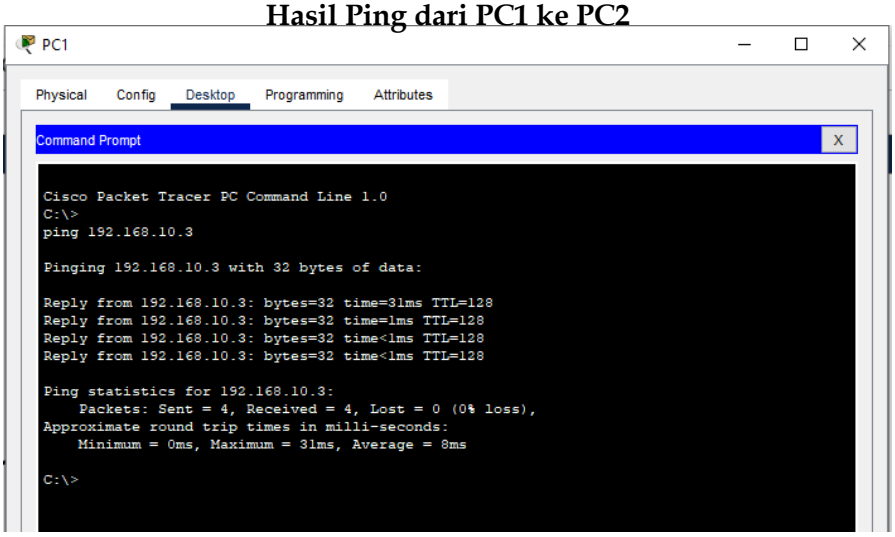
Sumber: Data diolah, 2024

Pengujian

Pengujian Ping dari PC1 ke PC 2

Pengujian dari PC1 dan PC dinyatakan Berhasil

Gambar 7
Hasil Ping dari PC1 ke PC2

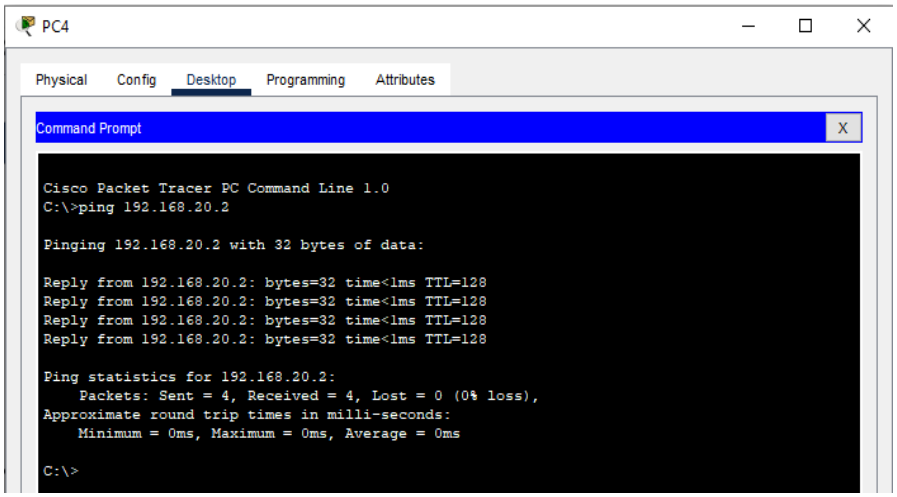


Sumber: Data diolah, 2024

Pengujian Ping dari PC4 ke PC3

Pengujian dari PC4 ke PC3 dinyatakan berhasi

Gambar 8
Hasil Ping dari PC4 ke PC3



Sumber: Data diolah, 2024

KESIMPULAN

Simulasi ini menunjukkan pentingnya penerapan VLAN dan Access Control List (ACL) dalam pengelolaan jaringan yang aman dan terstruktur. Dengan mengimplementasikan VLAN untuk memisahkan lalu lintas antar kelompok perangkat dan menggunakan ACL untuk mengontrol akses antar VLAN, keamanan dan kinerja jaringan dapat lebih terjamin. Penggunaan metode router-on-a-stick memungkinkan konfigurasi yang lebih sederhana dan efektif, meskipun hanya menggunakan interface fisik yang terbatas. Pengujian yang dilakukan membuktikan bahwa penerapan ACL Standard dapat membatasi akses secara selektif sesuai dengan kebijakan yang telah ditentukan, serta memastikan komunikasi yang diinginkan antara perangkat yang terhubung ke jaringan yang berbeda. Penelitian ini memberikan wawasan yang bermanfaat bagi pengelolaan jaringan, terutama dalam hal segmentasi dan pengaturan akses antar perangkat di jaringan yang lebih kompleks.

DAFTAR PUSTAKA

Aditya Ananda, W. Bagye, and S. Fadli, "Pelatihan Simulasi Dynamic Routing dan Virtual Lan Untuk Jaringan Menggunakan Cisco Packet Tracer Bagi Siswa Magang di PT. Jembatan Data Pangranggo (JDP) Lombok Timur Dynamic Routing And Virtual Lan Simulation Training For Networks Using Cisco Packet Tracer For Internship Students at PT. Pangranggo Data Bridge (JDP) East Lombok," Jurnal Hasil Kegiatan Sosialisasi Pengabdian kepada Masyarakat, vol. 2, no. 3, pp. 83–91, 2024, doi: 10.59841/bumi.v2i3.263.

Ahmed and M. N. A. Al-Hamadani, "Designing a secure campus network and

simulating it using Cisco packet tracer," Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 1, pp. 479–489, Jul. 2021, doi: 10.11591/ijeecs.v23.i1.pp479-489.

Almalki, "Implementation of 5G IoT Based Smart Buildings using VLAN Configuration via Cisco Packet Tracer," 2020.

Azhari, N. A. Sulaiman, and M. Kassim, "Secured Internet Office Network with the Internet of Things Using Packet Tracer Analysis," 2021 IEEE 11th International Conference on System Engineering and Technology, ICSET 2021 - Proceedings, pp. 200–205, 2021, doi: 10.1109/ICSET53708.2021.9612554.

Bangun, J. Vlan, D. Menggunakan, S. Cisco, P. Tracer, and R. Susanto, "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Attribution-NonCommercial 4.0 International. Some rights reserved," vol. 4, no. 2, 2020, doi: 10.30743/infotekjar.v4i2.2297.

Dhaka, "Traffic Management and Security in Wired Network," Communications in Computer and Information Science, vol. 835, pp. 17–30, 2019, doi: 10.1007/978-981-13-5992-7_2.

Fahri, A. Fiade, and H. B. Suseno, "Simulasi Jaringan Virtual Local Area Network (VLAN) Menggunakan Pox Controller," JURNAL TEKNIK INFORMATIKA, vol. 10, no. 1, pp. 85–90, Jan. 2018, doi: 10.15408/jti.v10i1.6821.

Laksono and M. A. H. Nasution, "Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X," Jurnal Sistem Komputer dan Informatika (JSON), vol. 1, no. 2, p. 83, Jan. 2020, doi: 10.30865/JSON.V1I2.1920.

Md Anwar Hossain, M. Zannat, M. Anwar Hossain α, and M. Zannat σ, "Simulation and Design of University Area Network Scenario (UANS) using Cisco Packet Tracer," 2019.

Midhun Krishna Yadav, A. Mummadi, V. Vardhan Ciripuram, R. Uma Mageswari, and A. Professor, "Secure Campus Area Network In Cisco Packet Tracer," 2023. [Online]. Available: www.ijcrt.org.

Sumarni and G. Purnama, "Perancangan Infrastruktur Jaringan Komputer Berbasis Cisco Packet Tracer dengan penerapan Metode NDLC Pada Lembaga Pendidikan (Studi Kasus SMK Pelayaran Malahayati)," 2023.

Tamsir Ariyadi, "Desain keamanan DHCP snooping untuk mengurangi serangan Local Area Network (LAN)," Desain Keamanan Dhcp Snooping Untuk Mengurangi Serangan Local Area Network (LAN), 2022.

Usior and E. Sediyono, "Simulasi Extended ACL pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer," AITI, vol. 20, no. 1, pp. 32–47, Mar. 2023, doi: 10.24246/AITI.V20I1.32-47).