JUMINTAL: Jurnal Manajemen Informatika dan Bisnis Digital
https://journal.literasisains.id/index.php/JUMINTAL
ISSN 2830-3016 (Media Online)
Vol. 5 No. 1 (Mei 2025) 15-28
DOI: 10.55123/jumintal.v5i1.6894

Optimasi Keamanan Jaringan Menggunakan Extended ACL pada Infrastruktur VLAN

Janeman Sumah[1], Robert Manaha[2], Wendel Selsily[3], Trientje Marlein Tamtelahitu[4], Marthevienty H.T. Soumokil[5]
[1,2,3,4,5]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Kristen Indonesia Maluku
Email: [1]yanno28@gmail.com, [2]ukimobet82@gmail.com, [3]wendelherman@gmail.com, [4]maerlientam@gmail.com, [5]marthevientyhts@gmail.com

Informasi Artikel
Diterima : 14-01-2026
Disetujui : 25-04-2026
Diterbitkan : 15-05-2026

ABSTRACT

Successful network scalability and management may not be immediately applicable to larger scales. As the network becomes more complex, VLAN and ACL management and administration can become a greater challenge, especially in terms of maintenance and troubleshooting. This study simulates the implementation of a VLAN network for the Faculty of Computer Science UKIM using a multilayer switch and Cisco Packet Tracer software. The network includes 3 IP servers and 4 VLANs. The configured servers include the Faculty server (192.168.10.10/24), Lab1 server (192.168.20.10/24), and Lab2 server (192.168.30.10/24), while the VLANs consist of MHS_FILKOM (ID 100), DOSEN_FILKOM (ID 200), PEGAWAI_FILKOM (ID 300), and ADMIN_FILKOM (ID 400). An extended ACL configuration is applied to regulate access on this network. The test results showed that HTTP access to the Faculty server was successfully blocked, thus protecting the server from unauthorized access via port 80. In addition, SSH access from the Admin network to all servers worked properly, allowing for secure server management. Communication between Lab1 and Lab2 servers was restricted to ICMP (ping) only, while other traffic was successfully blocked to maintain security between the servers. Internal traffic between VLANs and servers ran smoothly, ensuring smooth communication between the networks. Access to the Faculty server was also restricted to the Admin network (192.168.40.0/24), providing strict access control and improving overall network security. This configuration provides better security and allows for more effective network management.

Keyword: *Cisco Packet Tracer, ACL Extended, VLAN*

ABSTRAK

Skalabilitas dan pengelolaan jaringan yang berhasil dilakukan mungkin tidak langsung bisa diterapkan di skala yang lebih besar.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Ketika Jaringan bertambah kompleks, manajemen dan pengelolaan VLAN dan ACL bisa menjadi tantangan yang lebih besar, terutama dalam hal pemeliharaan dan troubleshooting. Penelitian ini mensimulasikan implementasi jaringan VLAN untuk Fakultas Ilmu Komputer UKIM dengan menggunakan multilayer switch dan perangkat lunak Cisco Packet Tracer. Jaringan tersebut mencakup 3 IP server dan 4 VLAN. Server yang dikonfigurasi meliputi server Fakultas (192.168.10.10/24), server Lab1 (192.168.20.10/24), dan server Lab2 (192.168.30.10/24), sementara VLAN terdiri dari MHS_FILKOM (ID 100), DOSEN_FILKOM (ID 200), PEGAWAI_FILKOM (ID 300), dan ADMIN_FILKOM (ID 400). Konfigurasi ACL extended diterapkan untuk mengatur akses pada jaringan ini. Hasil pengujian menunjukkan bahwa akses HTTP ke server Fakultas berhasil diblokir, sehingga server terlindungi dari akses tidak sah melalui port 80. Selain itu, akses SSH dari jaringan Admin ke semua server berfungsi dengan baik, memungkinkan pengelolaan server secara aman. Komunikasi antara server Lab1 dan Lab2 dibatasi hanya untuk ICMP (ping), sementara lalu lintas lainnya berhasil diblokir untuk menjaga keamanan antar server. Lalu lintas internal antar VLAN dan server berjalan tanpa hambatan, memastikan komunikasi antar jaringan berjalan lancar. Akses ke server Fakultas juga dibatasi hanya untuk jaringan Admin (192.168.40.0/24), memberikan kontrol akses yang ketat serta meningkatkan keamanan jaringan secara keseluruhan. Konfigurasi ini memberikan keamanan yang lebih baik dan memungkinkan manajemen jaringan yang lebih efektif.

Kata Kunci: Cisco Packet Tracer, ACL Diperluas, VLAN

1. PENDAHULUAN

Keamanan jaringan semakin menjadi prioritas utama dalam melindungi data dan informasi di era digital yang terus berkembang. Jaringan komputer kini memegang peran yang sangat vital dalam operasional bisnis digital dan institusi pendidikan, sehingga perlindungan terhadapnya menjadi suatu kebutuhan yang tidak dapat ditunda (Satria & Ramadhani, 2023). Penggunaan *Access Control List* (ACL), khususnya dalam platform Cisco Packet Tracer, adalah salah satu metode yang diterapkan untuk mengatur akses yang tidak sah dan menjaga integritas data dalam jaringan (Simanjuntak et al., 2017)(Wahyudi & Firmansyah, 2021)(Hafizhan et al., 2020). Keamanan dan kestabilan jaringan yang terjamin tidak hanya meningkatkan kinerja sistem tetapi juga memberikan dampak positif bagi para penggunanya, baik dalam sektor bisnis maupun pendidikan (Riva et al., 2024)(Tantangan et al., 2025).

Dalam konteks dunia digital, ancaman terhadap jaringan semakin beragam, mulai dari serangan malware, peretasan, hingga akses ilegal ke data. Oleh karena itu, penerapan sistem keamanan yang efektif menjadi sangat penting bagi organisasi, termasuk institusi pendidikan, yang mengelola data penting (Simulator et al., 2019). Router dengan kemampuan filtering, seperti penggunaan ACL, memungkinkan penyaringan lalu lintas jaringan, termasuk

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

memblokir akses yang tidak sah dengan menentukan aturan yang sesuai untuk traffic tertentu (Simanjuntak et al., 2017).

Beberapa studi menunjukkan bahwa Cisco Packet Tracer telah menjadi platform yang efektif untuk mensimulasikan konfigurasi ACL, baik itu ACL standar maupun extended, dalam mengelola dan mengontrol lalu lintas jaringan yang kompleks. Hal ini karena Packet Tracer menyediakan lingkungan yang interaktif dan mudah digunakan untuk mensimulasikan berbagai skenario, seperti pembatasan distribusi jaringan dan pengaturan proteksi terhadap akses ke alamat IP tertentu (Simulator et al., 2019)(Ts et al., 2021). Penggunaan ACL Extended, menurut penelitian oleh (Usior & Sediyono, 2023), sangat berguna dalam jaringan VLAN untuk menyaring jalur komunikasi dan memantau setiap aktivitas informasi yang masuk dan keluar. ACL Extended memungkinkan kontrol yang lebih rinci, mencegah potensi ancaman dengan hanya memblokir protokol atau port tertentu yang rentan terhadap eksploitasi, sambil tetap mengizinkan lalu lintas yang dianggap aman (Usior & Sediyono, 2023)(Ts et al., 2021).

Tidak hanya itu, penerapan ACL Extended terbukti efektif dalam meningkatkan efisiensi firewall yang digunakan untuk mengamankan perimeter jaringan, sebagaimana yang ditemukan dalam penelitian oleh (Sudarsan & Vasu, 2019), (Hafizhan et al., 2020), dan (Simanjuntak et al., 2017). Dengan memfilter paket dan membandingkannya dengan aturan yang telah ditentukan, ACL membantu menjaga keamanan jaringan sekaligus mempercepat pemrosesan data tanpa mengurangi kinerja jaringan secara keseluruhan.

Namun, selain pentingnya pengelolaan keamanan, kerugian yang ditimbulkan akibat kebocoran data dalam institusi pendidikan semakin meningkat. Penelitian oleh (Zhang et al., 2022) menunjukkan bahwa institusi pendidikan yang gagal mengamankan jaringan mereka mengalami kerugian ekonomi yang signifikan akibat pelanggaran data, yang dapat mencakup biaya hukum, reputasi yang tercemar, serta kehilangan kepercayaan dari mahasiswa dan pihak terkait. Hal ini mempertegas pentingnya penerapan sistem keamanan yang ketat untuk melindungi data akademik, finansial, dan informasi sensitif lainnya.

Berdasarkan tinjauan literatur yang ada, meskipun banyak penelitian yang telah membahas penggunaan ACL dalam mengamankan jaringan, belum banyak yang menguji penerapan ACL Extended secara spesifik pada segmentasi jaringan VLAN dalam skala institusi pendidikan. Metode simulasi yang digunakan dalam penelitian ini, melalui penggunaan Cisco Packet Tracer, memberikan keunggulan dibandingkan dengan metode manajemen jaringan konvensional yang digunakan sebelumnya di Fakultas Ilmu Komputer UKIM. Salah satu keunggulan utamanya adalah kemampuannya untuk melakukan simulasi secara interaktif dengan skenario jaringan yang lebih kompleks, yang sulit diterapkan dalam pengaturan nyata tanpa biaya dan sumber daya yang besar. Dengan menggunakan simulasi, peneliti dapat dengan mudah menguji berbagai aturan ACL dan melihat dampaknya terhadap keamanan dan kinerja jaringan secara langsung.

Selain itu, simulasi ini memungkinkan pengujian dalam kondisi yang terkontrol, sehingga memungkinkan evaluasi yang lebih mendalam tentang pengaruh ACL Extended dalam segmentasi VLAN. Hal ini memberikan solusi yang lebih efisien dan hemat biaya dibandingkan dengan implementasi langsung pada jaringan fisik yang memerlukan biaya

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

perangkat keras tambahan dan waktu yang lebih lama untuk konfigurasi dan pengujian. Dengan demikian, simulasi ini tidak hanya memberikan keunggulan dalam hal efisiensi waktu dan biaya, tetapi juga memungkinkan eksperimen dengan berbagai skenario yang tidak dapat dengan mudah diuji di lingkungan fisik.

Tabel 1. Fitur dan Jenis ACL

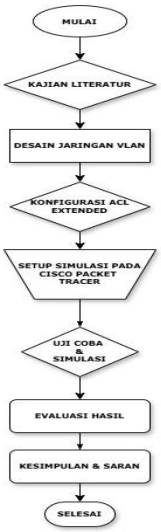
Feature	Standard	Extended	EtherType	WebVPN
Layer 2 packet filtering	No	No	Yes	No
Layer 3 packet filtering	No	Yes	No	Yes
Packet capture	No	Yes	Yes	No
AAA	No	Yes	No	No
Time range	No	Yes	No	Yes
Object grouping	No	Yes	No	No
NAT exemption	No	Yes	No	No
IPv6 support	No	Yes	No	Yes
Protocol Independent Multicast (PIM)	Yes	No	No	No
Application layer inspection	No	Yes	No	No
IPS inspection	No	Yes	No	No
VPN encryption	No	Yes	No	Yes'
Remarks	Yes	Yes	Yes	Yes
Line numbers	No	Yes	No	No
ACL logging	No	Yes	No	Yes
QoS	Yes	Yes	No	No
VPN split-tunneling	Yes	No	No	No
Policy NAT	No	Yes	No	No
OSPF route-map	Yes	Yes	No	No

Berdasarkan tinjauan literatur yang ada, meskipun banyak penelitian yang telah membahas penggunaan ACL dalam mengamankan jaringan, belum banyak yang menguji penerapan ACL Extended secara spesifik pada segmentasi jaringan VLAN dalam skala institusi pendidikan. Metode simulasi yang digunakan dalam penelitian ini, melalui penggunaan Cisco Packet Tracer, memberikan keunggulan dibandingkan dengan metode manajemen jaringan konvensional yang digunakan sebelumnya di Fakultas Ilmu Komputer UKIM. Salah satu keunggulan utamanya adalah kemampuannya untuk melakukan simulasi secara interaktif dengan skenario jaringan yang lebih kompleks, yang sulit diterapkan dalam pengaturan nyata tanpa biaya dan sumber daya yang besar. Dengan menggunakan simulasi, peneliti dapat dengan mudah menguji berbagai aturan ACL dan melihat dampaknya terhadap keamanan dan kinerja jaringan secara langsung.

Selain itu, simulasi ini memungkinkan pengujian dalam kondisi yang terkontrol, sehingga memungkinkan evaluasi yang lebih mendalam tentang pengaruh ACL Extended dalam segmentasi VLAN. Hal ini memberikan solusi yang lebih efisien dan hemat biaya dibandingkan dengan implementasi langsung pada jaringan fisik yang memerlukan biaya perangkat keras tambahan dan waktu yang lebih lama untuk konfigurasi dan pengujian. Dengan demikian, simulasi ini tidak hanya memberikan keunggulan dalam hal efisiensi waktu dan biaya, tetapi juga memungkinkan eksperimen dengan berbagai skenario yang tidak dapat dengan mudah diuji di lingkungan fisik.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

2. METODE



Gambar 1. Alur Penelitian

Tahap awal penelitian dimulai dengan menentukan topik, yaitu simulasi jaringan VLAN dengan ACL Extended pada lingkup Fakultas Ilmu Komputer UKIM. Kemudian dilakukan peninjauan terhadap penelitian dan literatur yang relevan. Tujuannya adalah untuk memahami teori yang mendasari VLAN dan ACL Extended serta mengidentifikasi gap atau kekurangan dalam penelitian sebelumnya yang dapat diisi oleh penelitian ini.

Langkah selanjutnya adalah merancang skema jaringan VLAN. Desain ini menentukan bagaimana VLAN akan diterapkan, termasuk pembagian jaringan menjadi beberapa segmen VLAN sesuai dengan kebutuhan. Kemudian, konfigurasi ACL Extended dibuat untuk mengontrol akses antar VLAN. ACL Extended digunakan untuk menentukan aturan spesifik yang membatasi atau mengizinkan lalu lintas berdasarkan alamat IP, protokol, dan port(Wahyudi & Firmansyah, 2021).

Setelah desain dan konfigurasi selesai, jaringan VLAN dan aturan ACL Extended disimulasikan menggunakan Cisco Packet Tracer v 8.2.1. Setup ini mencakup uji coba simulasi untuk memastikan bahwa konfigurasi berjalan sesuai dengan yang diharapkan. Pengujian ini meliputi pengujian konektivitas dan efektivitas ACL Extended dalam mengendalikan akses antar VLAN. Setelah uji coba, hasil simulasi dievaluasi untuk melihat apakah konfigurasi yang dilakukan telah sesuai dengan tujuan penelitian. Evaluasi ini juga membandingkan hasil dengan standar atau ekspektasi yang diinginkan.

Indikator Kinerja Utama (KPI)

Latency Jaringan (Network Latency):

1. Deskripsi**:** Latency mengukur waktu yang diperlukan oleh data untuk bergerak dari satu titik ke titik lainnya dalam jaringan. Dalam konteks ini, pengukuran latency dilakukan untuk

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

membandingkan waktu yang dibutuhkan untuk mentransfer data sebelum dan setelah penerapan ACL.

2. Tujuan**:** Mengukur dampak dari penerapan ACL terhadap kecepatan komunikasi antar server dan perangkat dalam VLAN.
3. Metode Pengukuran**:** Pengukuran dilakukan dengan menggunakan perintah ping dari satu perangkat ke perangkat lainnya di dalam jaringan, serta melakukan uji coba dengan berbagai jenis trafik (misalnya, HTTP, SSH).

Efektivitas Aturan ACL dalam Mencegah Unauthorized Access**:**

1. Deskripsi**:** Efektivitas aturan ACL diukur berdasarkan kemampuannya dalam memblokir akses yang tidak sah ke server atau port yang dilindungi.
2. Tujuan**:** Mengukur apakah aturan ACL yang diterapkan dapat mencegah akses yang tidak sah, seperti memblokir port 80 untuk HTTP atau membatasi akses SSH.
3. Metode Pengukuran**:** Pengujian dilakukan dengan mencoba mengakses server Fakultas menggunakan port yang diblokir (port 80 untuk HTTP) dan memverifikasi bahwa akses diblokir. Selain itu, pengujian dilakukan untuk memastikan bahwa akses SSH (port 22) ke server dari jaringan yang berwenang tetap diizinkan.

Keberhasilan Pengaturan Akses Antar VLAN:

1. Deskripsi**:** Mengukur sejauh mana ACL berhasil mengatur komunikasi antar VLAN sesuai dengan tujuan yang ditetapkan, seperti pembatasan akses hanya untuk protokol tertentu (misalnya, hanya mengizinkan ICMP antara Server Lab1 dan Server Lab2).
2. Tujuan**:** Memastikan bahwa ACL dapat memfilter lalu lintas antar VLAN berdasarkan protokol dan port yang diizinkan.
3. Metode Pengukuran**:** Pengujian dilakukan dengan mencoba berbagai jenis komunikasi antar server di VLAN yang berbeda, seperti ping, SSH, dan HTTP, untuk memastikan bahwa hanya lalu lintas yang diizinkan yang dapat diterima.

Langkah Pengujian

Konfigurasi dan Persiapan Jaringan:

1. Sebelum pengujian dilakukan, semua perangkat dalam jaringan disiapkan sesuai dengan konfigurasi yang telah ditentukan dalam simulasi VLAN dan ACL Extended.
2. Proses konfigurasi ini mencakup penetapan IP address untuk masing-masing server, konfigurasi VLAN pada switch, dan penerapan ACL pada router.

Pengujian Latency:

Dilakukan dengan mengirimkan paket data menggunakan perintah ping antar perangkat (server dan workstation) di dalam jaringan. Waktu respons dicatat untuk menganalisis perubahan latency setelah ACL diterapkan.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Pengujian Efektivitas ACL dalam Mencegah Akses Tidak Sah:

1. HTTP Access Block Test: Mencoba mengakses server Fakultas melalui port 80 (HTTP) dari jaringan yang tidak sah. Jika akses diblokir, maka aturan ACL dianggap efektif.
2. SSH Access Test: Mengakses server melalui port 22 (SSH) dari jaringan Admin untuk memastikan akses dapat dilakukan tanpa hambatan.
3. ICMP Test: Menguji komunikasi antar Server Lab1 dan Lab2 hanya untuk protokol ICMP (ping) dan memastikan bahwa lalu lintas lainnya diblokir sesuai aturan ACL.

Pengujian Akses Antar VLAN:

Menguji komunikasi antara server di VLAN yang berbeda untuk memastikan aturan ACL membatasi akses sesuai dengan yang diinginkan (misalnya, hanya mengizinkan komunikasi antar jaringan internal tertentu).

Hasil Pengujian

Setelah pengujian dilakukan, hasilnya dievaluasi untuk menentukan seberapa efektif penerapan ACL dalam mencapai tujuan penelitian. Beberapa hasil yang diharapkan adalah:

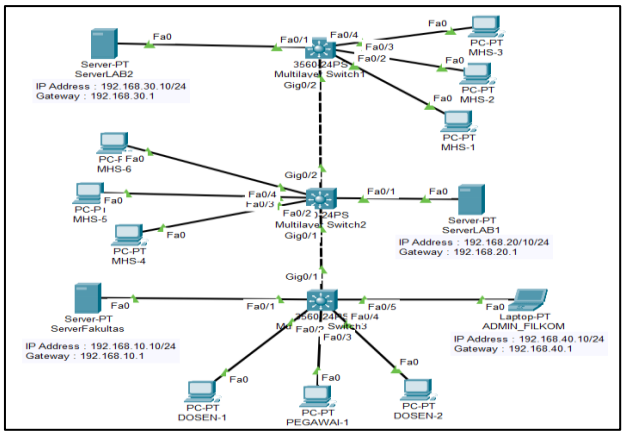
1. Latency yang minimal meskipun ada pembatasan akses.
2. Keberhasilan dalam memblokir akses yang tidak sah sesuai dengan aturan yang ditetapkan.
3. Pemisahan komunikasi antar VLAN yang efektif, dengan hanya lalu lintas yang diizinkan yang dapat berkomunikasi.

3. HASIL DAN PEMBAHASAN

Desain Jaringan

Skema Jaringan VLAN

Skenario jaringan VLAN yang akan disimulasikan, termasuk *switch*, *server*, dan perangkat lainnya pada Fakultas Ilmu Komputer UKIM terlihat pada gambar 2.



Gambar 2. Skema Jaringan VLAN

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Pemetaan VLAN

Proses penentuan VLAN yang akan dibuat dan tujuan masing-masing VLAN terlampir pada bagan tabel 2. Sedangkan pada tabel 3 menyajikan pemetaan *Server*, IP *Server*, & VLAN Id.

Tabel 2. Pemetaan Nama VLAN & Tujuan VLAN

Nama VLAN	Tujuan VLAN
MHS_FILKOM	Memisahkan akses untuk jaringan mahasiswa, dengan tujuan memberikan akses ke sumber daya akademik dan internet.
DOSEN_FILKOM	Memisahkan lalu lintas perangkat untuk dosen.
PEGAWAI_FILKOM	Memisahkan lalu lintas perangkat administrasi, seperti staf akademik fakultas
ADMIN_FILKOM	Memisahkan lalu lintas perangkat administrasi, seperti staf administrasi dan server manajemen.

Tabel 3. Pemetaan Server, IP Server, & VLAN Id

Server	IP Address	VLAN ID	VLAN Name
Server Fakultas	192.168.10.10/24	100	MHS_FILKOM
Server LAB1	192.168.10.20/24	200	DOSEN_FILKOM
Server LAB2	192.168.10.30/24	300	PEGAWAI_FILKOM
-		400	ADMIN_FILKOM

VLAN 400 (ADMIN_FILKOM) tidak terkait langsung dengan salah satu *server*, namun disertakan untuk keperluan pengelolaan jaringan administrasi.

Konfigurasi VLAN

Verifikasi konfigurasi Interface VLAN pada *Switch*.

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

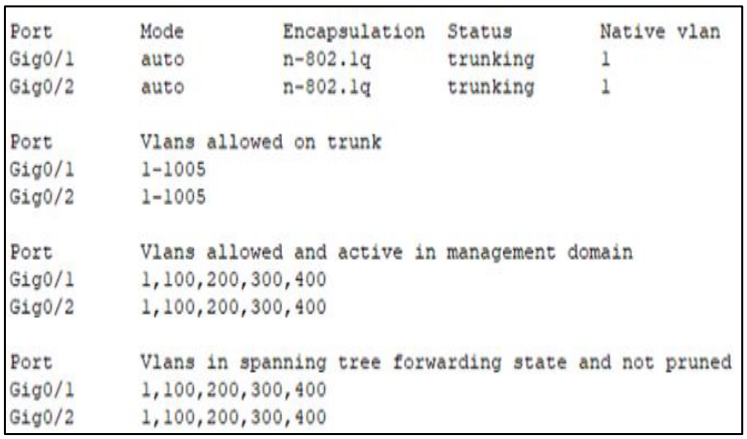
```
Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Vlan100
C    192.168.20.0/24 is directly connected, Vlan200
C    192.168.30.0/24 is directly connected, Vlan300
C    192.168.40.0/24 is directly connected, Vlan400
```

Gambar 3. Verifikasi Konfigurasi VLAN

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Konfigurasi *Switch Multilayer* Utama

Melakukan konfigurasi ke salah satu *switch multilayer* sebagai *multilayer switch* utama dengan mengonfigurasi semua VLAN di *switch* tersebut dan melakukan *routing* antar VLAN. Hasil konfigurasi terlihat pada gambar 5.



```
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1
Gig0/2      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,100,200,300,400
Gig0/2      1,100,200,300,400

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,100,200,300,400
Gig0/2      1,100,200,300,400
```

Gambar 4. Verifikasi *Switch Multilayer* Utama

Aturan Keamanan (*Security Rules Summary*)

Tabel 4. Ringkasan Aturan Keamanan (*Security Rules Summary*)

No	Nama Aturan	Deskripsi	Action (Izinkan/Blokir)	IP Address / Port Terkait
1	Blokir HTTP ke Server Fakultas	Memblokir akses HTTP (port 80) ke server Fakultas untuk meningkatkan keamanan	Blokir	192.168.10.10 (Port 80 - HTTP)
2	Izinkan SSH ke Semua Server dari Admin	Memungkinkan akses SSH (port 22) ke semua server dari jaringan Admin	Izinkan	192.168.40.0/24 (Port 22 - SSH)
3	Blokir Lalu Lintas Lab1 ke Lab2 (Kecuali ICMP)	Membatasi akses antara Server Lab1 dan Server Lab2 hanya untuk ICMP (ping)	Blokir (Selain ICMP)	192.168.20.10 - 192.168.30.10 (Port ICMP)
4	Izinkan Lalu Lintas dari Server Fakultas ke Lab1	Mengizinkan semua lalu lintas dari server Fakultas ke Lab1	Izinkan	192.168.10.10 → 192.168.20.10
5	Blokir Akses ke Server Fakultas (Kecuali dari Jaringan Admin)	Memblokir akses ke Server Fakultas kecuali dari jaringan Admin	Blokir (Selain Admin)	192.168.10.10 (Jaringan Admin: 192.168.40.0/24)

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Hasil Uji Coba (*Testing Results*)

Tabel 5. Hasil Uji Coba (*Testing Results*)

No	Uji Coba	Tujuan Pengujian	Hasil
1	Pengujian Blokir Akses HTTP ke Server Fakultas	Memverifikasi bahwa akses HTTP (port 80) diblokir ke server Fakultas	Akses HTTP diblokir dengan sukses (port 80)
2	Pengujian Akses SSH ke Semua Server dari Admin	Memastikan akses SSH ke server dapat dilakukan dari jaringan Admin	Akses SSH berhasil dilakukan dari jaringan Admin
3	Pengujian Akses antara Server Lab1 dan Lab2	Menguji komunikasi antara Server Lab1 dan Lab2 untuk memastikan hanya ICMP yang diizinkan	Hanya ICMP (ping) yang diizinkan, lalu lintas lainnya diblokir
4	Pengujian Lalu Lintas Antar Server	Memastikan Server Fakultas dapat mengakses Server Lab1	Semua protokol dan layanan berjalan tanpa hambatan
5	Pengujian Akses ke Server Fakultas dari Jaringan Admin	Memastikan hanya jaringan Admin yang dapat mengakses Server Fakultas	Akses hanya berhasil dari jaringan Admin (192.168.40.0/24)

Konfigurasi dan Verifikasi ACL Extended

Konfigurasi ACL *extended* sesuai dengan tujuan penelitian untuk mengontrol akses antar VLAN pada Fakultas Ilmu komputer UKIM. Pada pengaturan *Access Control List* (ACL) dilakukan pada *layer* 3 *switch* di *Cisco Packet Tracer* (Science, 2019).

Multilayer *switch* yang mendukung routing menggunakan Cisco 3560 untuk mengontrol lalu lintas antar VLAN dan melakukan *filtering* pada *ports* tertentu. Gambar 6 menyajikan hasil konfigurasi ACL *Extended* pada IP Access list 100.

```
Extended IP access list 100
    10 deny tcp any host 192.168.10.10 eq www
    20 permit tcp 192.168.40.0 0.0.0.255 host 192.168.10.10 eq 22
    30 permit tcp 192.168.40.0 0.0.0.255 host 192.168.20.10 eq 22
    40 permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.10 eq 22
    50 permit icmp host 192.168.20.10 host 192.168.30.10
    60 deny ip host 192.168.20.10 host 192.168.30.10
    70 permit ip host 192.168.10.10 host 192.168.20.10
    80 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
    90 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
    100 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
    110 deny ip any host 192.168.10.10
    120 permit ip 192.168.40.0 0.0.0.255 host 192.168.10.10
```

Gambar 6. Konfigurasi ACL *Extended* pada IP *Access list* 100

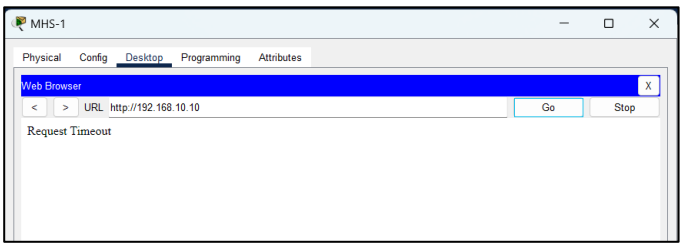
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Pengujian Dan Simulasi

Pengujian pada IP Access list 100 untuk mengevaluasi efektivitas VLAN dan ACL.

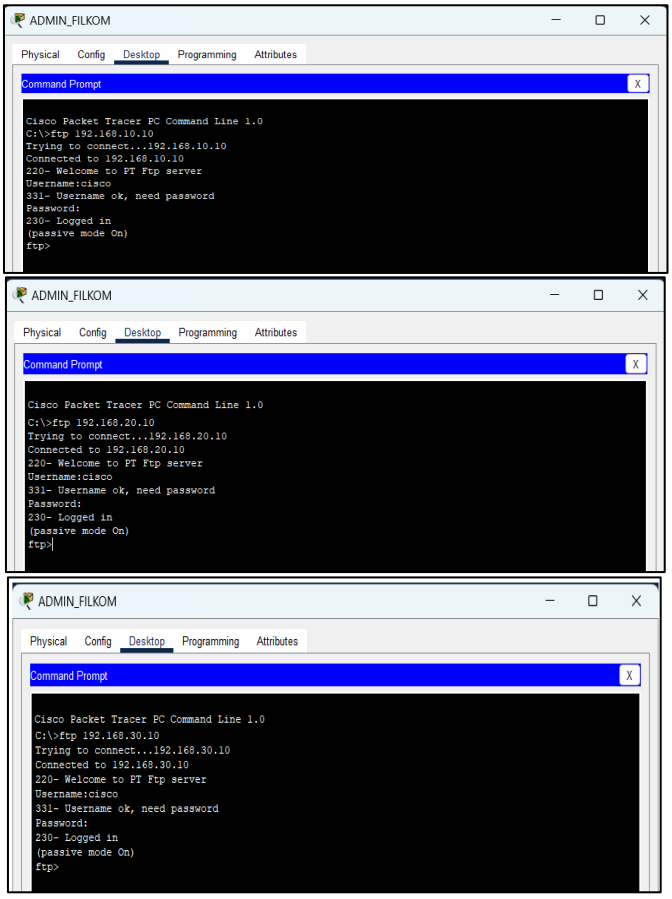
1. Blokir Akses HTTP ke Server Fakultas (192.168.10.10)

Blokir akses HTTP (port 80) ke server Fakultas untuk meningkatkan keamanan dan membatasi akses.



2. Izinkan Akses SSH ke Semua Server dari Jaringan Admin

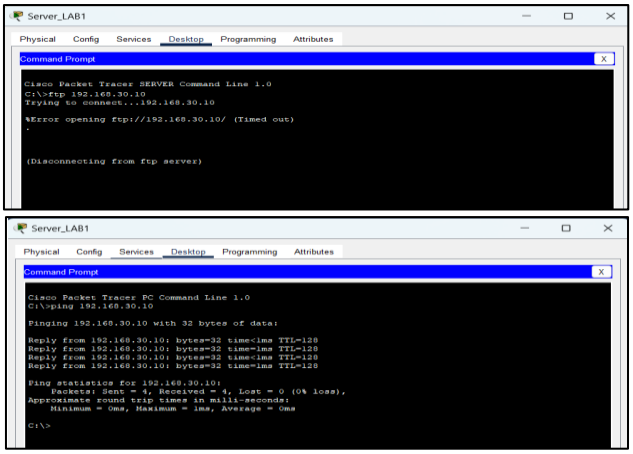
Izinkan akses SSH (port 22) ke semua server dari jaringan 192.168.40.0/24 (jaringan Admin) untuk manajemen server.



Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

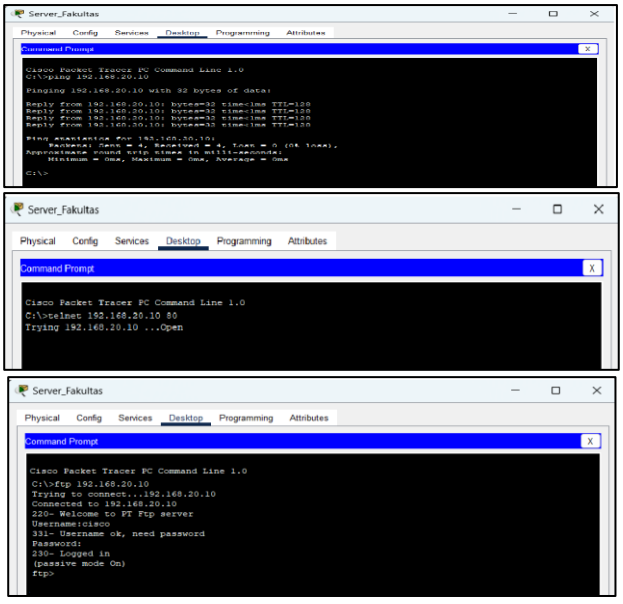
3. Blokir Semua Lalu Lintas dari Server Lab1 ke Server Lab2 Kecuali ICMP (Ping)

Batasi akses antara Server Lab1 dan Server Lab2 dengan hanya mengizinkan ping untuk tujuan pemantauan, dan blokir semua lalu lintas lainnya.



4. Izinkan Semua Lalu Lintas dari Server Fakultas ke Server Lab1

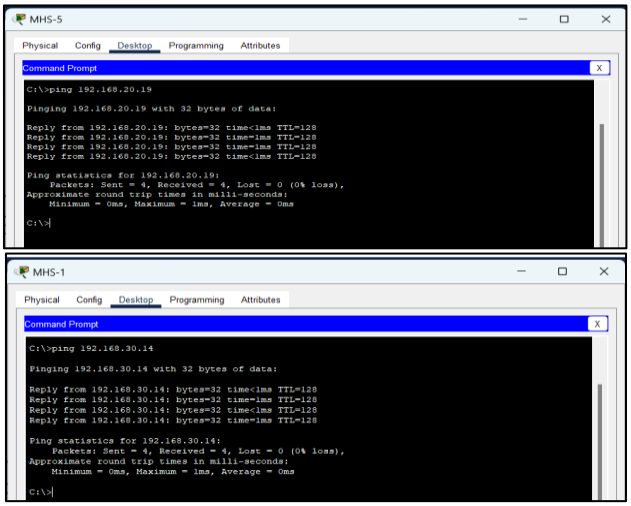
Izinkan server Fakultas mengakses server Lab1 untuk semua protokol dan layanan.



5. Izinkan Semua Akses Antar Jaringan Internal

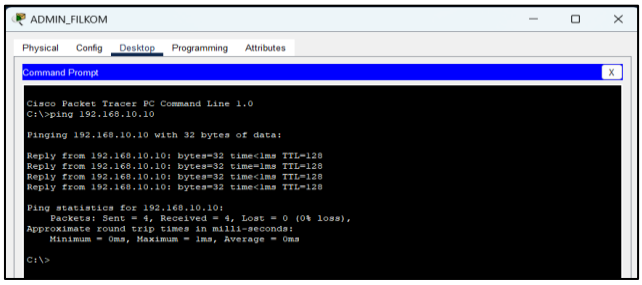
Pastikan semua lalu lintas antar subnet lain diizinkan untuk komunikasi umum dalam jaringan.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)



6. Blokir Akses ke Server Fakultas Kecuali dari Jaringan Admin

Blokir semua akses ke Server Fakultas kecuali dari jaringan 192.168.40.0/24.



4. PENUTUP

Kesimpulan

Berdasarkan hasil pengujian, konfigurasi yang diterapkan menunjukkan bahwa blokir akses HTTP ke Server Fakultas telah berhasil dilakukan, sehingga server terlindungi dari akses melalui port 80. Selain itu, akses SSH dari jaringan Admin ke semua server berfungsi dengan baik, memungkinkan administrasi server secara aman. Komunikasi antara Server Lab1 dan Lab2 telah berhasil dibatasi hanya untuk ICMP (ping), sementara lalu lintas lainnya secara efektif diblokir untuk menjaga keamanan jaringan antar server. Semua lalu lintas antar subnet internal, termasuk Server Fakultas, Lab1, dan Lab2, diizinkan, memastikan komunikasi antar jaringan berjalan lancar tanpa hambatan. Terakhir, Server Fakultas (192.168.10.10) hanya dapat diakses oleh jaringan Admin (192.168.40.0/24) sesuai dengan aturan yang ditetapkan, memberikan kontrol akses yang ketat dan meningkatkan keamanan jaringan.

Berdasarkan evaluasi, kesimpulan ditarik mengenai efektivitas konfigurasi VLAN dan ACL Extended dalam simulasi jaringan memberikan keamanan yang baik dengan membatasi akses antar server dan hanya mengizinkan Admin Fakultas dan lalu lintas jaringan yang diatur secara eksplisit.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

DAFTAR PUSTAKA

Hafizhan, M., Wahyuddin, M., & Titi, R. (2020). Implementasi Packet Filtering Menggunakan Metode Extended Access Control List (ACL) Pada Protokol EIGRP. JURNAL MEDIA INFORMATIKA BUDIDARMA, 4, 185. https://doi.org/10.30865/mib.v4i1.1926

Riva, A., Ahsyar, T., & Fronita, M. (2024). Analisis Kepuasan Pengguna Jaringan Internet Pada Kemenag Pekanbaru. JEKIN - Jurnal Teknik Informatika, 4, 625–637. https://doi.org/10.58794/jekin.v4i3.872

Satria, A., & Ramadhani, F. (2023). Analisis Keamanan Jaringan Komputer dengan Menggunakan Switch Port Security di Cisco Packet Tracer. Sudo Jurnal Teknik Informatika, 2(2), 52–60. https://doi.org/10.56211/sudo.v2i2.260

Science, C. (2019). 황성희 1 . 김현아 2 . 정현영 3 † 1. 25(4), 125–134.

Simanjuntak, P., Suharyanto, C. E., & Jamilah. (2017). Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan. Isd, 2(2), 122–128.

Simulator, T., Kumar, P. P., & Mudimela, P. R. (2019). Implementation of Smart College Network Using CISCO Packet. 16, 3871–3882.

Sudarsan, A., & Vasu, A. K. (2019). Performance Evaluation of Data Structures in Implementing Access Control Lists. August.

Tantangan, I., Jaringan, K., & Hidayat, T. (2025). Etika Profesi IT dalam Perspektif Filsafat Informatika Tantangan Keamanan Jaringan.

Ts, A., Parthasarathy, R., Preethy, A., Rajamanickam, L., Alias, S. B., Krishnan N, M., Perumal, I., & Ayyappan, P. (2021). Configuration of Access Control List Applications: Route Filtering and Traffic Control for Enterprise Network Design Using Cisco Packet Tracer Simulation Tool. Sci.Int.(Lahore), 33(3), 265–271. https://www.researchgate.net/publication/360088057

Usior, O. J., & Sediyono, E. (2023). Simulasi Extended ACL pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer. Aiti, 20(1), 32–47. https://doi.org/10.24246/aiti.v20i1.32-47

Wahyudi, M., & Firmansyah. (2021). Network Performance Optimization using Dynamic Enhanced Interior Routing Protocols Gateway Routing Protocol for IPv6 (EIGRPv6) and IPv6 Access Control List. Journal of Physics: Conference Series, 1830(1), 0–12. https://doi.org/10.1088/1742-6596/1830/1/012017

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. (2022). Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security, 19, 402. https://doi.org/10.1504/IJICS.2022.127169

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)