JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 3, SEPTEMBER, 2022, Pp. 143 – 162
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Pembatasan Akses Menggunakan MAC Address dengan Metode *Access Control List*

Muhammad Aditya Rabbani [(1)*], Martanto Martanto [(2)], Yudhistira Arie Wijaya [(3)]
[1] Teknik Informatika, STMIK IKMI, Cirebon
[2] Manajemen Informatika, STMIK IKMI, Cirebon
[3] Sistem Informasi, STMIK IKMI, Cirebon
e-mail : {adityarabbani10,martantomusijo,yudhistira010471}@gmail.com.
* Penulis korespondensi.
Artikel ini diajukan 26 Februari 2022, direvisi 29 Juni 2022, diterima 29 Juni 2022, dan dipublikasikan 25 September 2022.

Abstract

The Cangehgar Cyber Command Center of the 14th Arhanud/ PWY Battalion from Cirebon City is one of the offices with IT equipment to assist the job. The servers, like the office PCs, are connected via the local network. Due to the risk of leaking secret data from within, network security concerns must be handled so that unauthorized users cannot mistakenly access the server. It seeks to limit access when there are administrative customers and employees in each room by utilizing the access control list approach using a MAC address. Access to the server is restricted to the administrator's computer, while access to the employee's PC is disallowed. Then the questionnaire was distributed to find out the respondent's assessment of the access control list. According to the results of the study on security indicators, access control lists containing MAC addresses are useful in limiting access to server computers.

Keywords: Computer, Intranet Network, MAC Address, Access Control List, Security, Questionnaire

Abstrak

Setiap kantor memiliki peralatan komputer guna menunjang pekerjaan, seperti pada kantor Cangehgar *Cyber Operation Center* di Batalyon Arhanud 14/PWY, Cirebon. Komputer yang ada di kantor tersebut saling terhubung berkat adanya jaringan intranet, begitu pula dengan komputer server. Masalah keamanan jaringan perlu ditangani, sehingga pengguna yang tidak sah tidak bisa sengaja mengakses ke server, karena risiko kebocoran data rahasia dari bagian dalam. Menggunakan metode *access control list* dengan MAC *address*, bertujuan untuk melakukan batasan akses, di mana pada setiap ruangan memiliki komputer *client* admin dan juga staf. Hanya komputer admin yang dapat berkomunikasi dengan komputer server, sementara komputer staf aksesnya ditolak. Kemudian kuesioner disebarkan untuk mengetahui penilaian responden terhadap *access control list*. Hasil penelitian terhadap indikator keamanan cenderung setuju bahwa *access control list* dengan MAC *address* berguna membatasi akses ke komputer server.

Kata Kunci: Komputer, Jaringan Intranet, MAC *Address*, *Access Control List*, Keamanan, Kuesioner

1. PENDAHULUAN

Setiap departemen di suatu perusahaan, baik pemerintah maupun swasta memiliki perangkat komputer untuk menunjang pekerjaannya (Kartini & Eko, 2019). Bagian-bagian tersebut saling berhubungan dan dapat saling berkomunikasi (Gunawan & Agung, 2019). Komunikasi dapat beroperasi melalui sistem jaringan intranet. Jaringan intranet membutuhkan sistem pertahanan yang baik untuk mencegah dan memperkecil adanya pencurian informasi yang tidak diketahui (Ardiansyah & Yudiastuti, 2021). Keamanan jaringan merupakan bagian penting dalam menjaga informasi rahasia perusahaan (Munawar & Putri, 2020). Keamanan terhadap jaringan intranet adalah bentuk perlindungan dari kemungkinan terjadinya serangan pada sistem dan pencurian data pribadi serta perusahaan yang tidak boleh diketahui orang banyak (Sulaiman & Saripurna, 2021). Perusahaan yang menggunakan jaringan intranet perlu adanya perlindungan dari segi keamanan, karena banyaknya serangan dapat menyebabkan bocornya data yang sensitif milik

perusahaan (Bustami & Bahri, 2020). Terdapat beberapa indikator yang digunakan dalam menjaga aset perusahaan, di antaranya terdiri dari *confidentiality, integrity,* dan *availability* (Kelrey & Muzaki, 2019; Riskiyadi et al., 2021). Cara yang digunakan untuk menyelesaikan kasus tersebut adalah melakukan batasan akses terhadap komputer *client* menggunakan metode *Access Control List* (ACL). Penggunaan metode *access control list* mampu menentukan sebuah paket data yang dikirim atau diterima, diberi ijin untuk melewati *router* atau tidak (Sihotang et al., 2020) guna mencegah terjadinya kebocoran informasi data dari segi internal perusahaan, yang disebabkan oleh kelalaian karena tidak adanya batasan akses menuju komputer server.

Berdasarkan penelitian terdahulu yang membahas tentang *access control list* telah dilakukan oleh Dicky Novariansyah dan Irwansyah (Irwansyah & Novariansyah, 2019) terdapat permasalahan yang terjadi berupa belum maksimalnya keamanan secara keseluruhan, yang menyebabkan akses data dapat diakses oleh siapapun serta bisa menyebabkan kebocoran aset. Hasil riset tersebut berupa penyaringan terhadap akses LAN pada arsitektur VLAN berdasarkan alamat jaringan (IP). Penelitian yang dilakukan oleh Kurniati dan Rahmat Novrianda Dasmen (Kurniati & Dasmen, 2019) memiliki masalah berupa tingkat keamanan jaringan yang masih rendah dan diperlukan sebuah upaya untuk meningkatkan keamanan dengan membatasi akses pengguna terhadap komunikasi lalu lintas jaringan. Hasil dari penelitian tersebut adalah dengan menggunakan ACL dapat membatasi akses dan hanya pengguna terdaftar yang dapat masuk. Penelitian yang dilakukan oleh Umar Hasan dan kawan-kawan (Hasan & Dewi, 2022) menyajikan permasalahan berupa banyaknya instansi dan organisasi atau kelompok besar yang tidak memperhatikan keamanan pada jaringan komputer. Sebuah celah keamanan dapat dimanfaatkan oleh pihak ketiga sebagai peluang untuk melakukan serangan siber. Hasil dari riset ini adalah aplikasi *access control list* pada *router* Cisco mampu memantau paket data yang melewati *router*, yang merupakan peningkatan dalam industri keamanan karena memiliki proses otentikasi dan verifikasi.

Riset yang telah dilakukan oleh peneliti terdahulu mengenai keamanan jaringan menggunakan metode *access control list* memiliki dampak yang baik terhadap peningkatan keamanan. Riset yang dilakukan mempunyai kontribusi dan novelty berupa bentuk visualisasi yang diterapkan langsung menggunakan *routerboard* Mikrotik, yang sebelumnya hanya dilakukan secara simulasi menggunakan Cisco Packet Tracer, serta penelitian lebih berfokus pada jaringan intranet yang ada di lingkungan kantor Cangehgar *Cyber Operation Center*. Konfigurasi *access control list* pada *routerboard* Mikrotik dalam penelitian ini menggunakan *extended access list*, yang nantinya antara komputer server mampu berkomunikasi dengan komputer *client*, serta komputer *client* khususnya komputer admin mampu berkomunikasi balik ke komputer server, kecuali komputer staf, karena MAC *address* perangkat tersebut telah diatur untuk di-*drop* agar tidak bisa melakukan akses *ping* ke komputer server.

1.1 TINJAUAN PUSTAKA

1.1.1 *Access Control List*

Access control list mampu menyaring sebuah paket data pada lalu lintas jaringan yang menentukan agar paket data tersebut cocok untuk dilewati atau dihentikan (*drop*) (Purba, 2021).

1.1.2 Jenis *Access Control List*

Metode *access control list* terdapat 2 jenis, di antaranya adalah *standard access list* dan juga *extended access list*. Keduanya memiliki perbedaan, yaitu *standard access list* hanya memperhatikan IP sumber (*resource*) dari paket yang dikirim, sementara untuk *extended access list* mempertimbangkan IP sumber (*resource*), IP tujuan (*destination*) serta protokol dan jenis yang digunakan (Hafizhan et al., 2020).

1.1.3 Mikrotik

Mikrotik merupakan alat jaringan yang digunakan untuk melakukan konfigurasi dan mengontrol sebuah jaringan (Ahmad et al., 2020). Dalam penelitian ini Mikrotik digunakan sebagai visualisasi langsung untuk menerapkan konfigurasi *access control list* dengan MAC *address*.

1.1.4 Indikator Keamanan

Sebuah sistem dapat dikatakan aman apabila terdapat beberapa indikator, di antaranya adalah *confidentiality* (kerahasiaan) data dan informasi yang tidak boleh diketahui oleh pihak lain, *integrity* (keaslian) data agar tidak bisa diakses oleh pihak yang tidak memiliki izin, *availability* (ketersediaan) data dan informasi ketika sedang dibutuhkan serta *authentication* (autentikasi) terhadap *user* yang ingin melakukan akses ke jaringan intranet (Dianta & Zusrony, 2019; Sugawara & Nikaido, 2014).

2. METODE PENELITIAN

Riset kali ini menggunakan *Network Development Life Cycle* (NDLC) untuk metode penelitiannya. Metode ini memiliki 6 langkah, mulai dari analisis (*analysis*), perancangan (design), simulasi (*simulation prototyping*), implementasi (*implementation*), pemantauan (*monitoring*), hingga pengelolaan (*management*) (Nugroho & Daniarti, 2021). Metode ini sering digunakan untuk penelitian jaringan, karena sering digunakan untuk mengembangkan jaringan sebelumnya menjadi desain jaringan baru agar lebih efisien. Berikut rincian 6 langkah tersebut.

1) *Analysis*
   Tahap ini adalah tahapan pertama yang dilakukan dalam proses penelitian. Pada tahapan ini dilakukan analisis kebutuhan, mendefinisikan masalah yang ada, dan melakukan analisis jaringan yang digunakan.
2) *Design*
   Tahap perancangan atau desain adalah tahap menampilkan gambar sebagai rancangan topologi jaringan yang akan digunakan.
3) *Simulation Prototyping*
   Pada langkah *simulation prototyping* peneliti melakukan simulasi konfigurasi yang akan dilakukan, sebelum konfigurasi tersebut diimplementasikan langsung oleh alat jaringan yang akan digunakan. Hal ini penting untuk meminimalkan kesalahan saat konfigurasi langsung.
4) *Implementation*
   Pada tahap ini dilakukan konfigurasi langsung pada perangkat jaringan yang digunakan. Dalam penelitian ini digunakan *router* Mikrotik dalam implementasinya.
5) *Monitoring*
   Langkah ini merupakan langkah setelah menyelesaikan semua konfigurasi, juga langkah untuk memeriksa dan memonitor jaringan intranet yang digunakan.
6) *Management*
   Pada tahap *management* merupakan tahap akhir di mana hal tersebut dilakukan supaya mekanisme yang dibuat berjalan lancar dan dapat bertahan lama serta mempertahankan kinerja terbaiknya.

2.1 Sumber Data dan Teknik Pengumpulan Data

Sumber data dihasilkan dari data primer dan juga sekunder. Sumber data primer merupakan hasil dari observasi lapangan, wawancara mendalam, dan juga penyebaran kuesioner. Sumber data sekunder diperoleh dari jurnal-jurnal peneliti terdahulu, studi pustaka, serta buku-buku. Berikut teknik pengumpulan data yang dilakukan.

2.1.1 Observasi Lapangan

Observasi dilaksanakan di tempat penelitian guna memperoleh data riset melalui penglihatan secara langsung terhadap kondisi yang terjadi di lapangan. Dalam tahap ini diketahui desain topologi yang sedang digunakan, yaitu topologi *ring*.

2.1.2 Wawancara Mendalam

Wawancara dilakukan kepada narasumber terkait untuk memperoleh data tambahan mengenai topik yang kita teliti. Narasumber diajukan kepada koordinator, ketua tim, dan juga anggota tim. Contoh pertanyaan dengan unsur *why* dan *how* untuk mencari informasi tambahan dapat dilihat pada Tabel 1.

Tabel 1 Contoh Pertanyaan Wawancara

No.	Pertanyaan	Jawaban
1	Mengapa jaringan intranet begitu penting digunakan di kantor Cangehgar *Cyber Operation Center*?	Karena jaringan intranet termasuk ke dalam bagian dari *Local Area Network* yang batasannya hanya mencakup komunikasi antar ruangan. Adanya jaringan intranet pun berfungsi untuk melakukan pengiriman dan penerimaan data antar komputer server dengan komputer *client* yang ada.
2	Bagaimana keamanan jaringan intranet yang saat ini digunakan?	Keamanan jaringan intranet yang ada saat ini bisa dibilang masih kurang cukup, karena belum adanya konfigurasi lanjut, masih mengandalkan kepercayaan sesama pengguna *user* lainnya yang menggunakan jaringan tersebut.

2.1.3 Kuesioner

Kuesioner disebarkan kepada responden untuk dapat menjawab sebuah pernyataan mengenai bahasan yang sedang diteliti, khususnya yang menggunakan jaringan intranet dengan ketentuan kuesioner menggunakan skala Likert. Beberapa contoh pernyataan kuesioner tersebut dapat dilihat pada Tabel 2.

Tabel 2 Pernyataan Kuesioner

No.	Indikator	Pernyataan
1	*Confidentiality*	Kerahasiaan data (*confidentiality*) pada sebuah keamanan jaringan intranet sangat penting karena meliputi dengan asset informasi yang dimiliki.
2	*Integrity*	Keaslian data (*integrity*) dalam sebuah asset yang dimiliki tidak boleh diubah saat proses pengiriman data pada jaringan intranet oleh orang yang tidak memiliki kewenangan.
3	*Availability*	Ketersediaan data (*availability*) pada saat diakses dan bisa digunakan untuk transfer *file* antar perangkat komputer.
…		…

2.2 Populasi dan Sampel Penelitian

Populasi yang digunakan sebanyak 50 orang pengguna jaringan intranet. Dari jumlah populasi tersebut ditentukan jumlah sampelnya sebagai responden penelitian. Pemilihan uji coba sampel berdasarkan rumus Isaac dan Michael pada Pers. (1) ditunjukkan pada Tabel 3.

Tabel 3 Rumus Sampel Isaac Michael

N	S			N	S		
	1%	5%	10%		1%	5%	10%
10	10	10	10	35	33	32	31
15	15	14	14	40	38	36	35
20	19	19	19	45	42	40	39
...	...	...	...	**50**	47	44	**42**

$$s = \frac{\lambda^2.N.P.Q}{d^2(N-1)+\pi^2.P.Q} \qquad (1)$$

Di mana s merupakan ukuran sampel, λ^2 yaitu chi kuadrat yang nilainya tergantung derajat kebebasan (dk) dan taraf kesalahan; dengan dk = 1, taraf kesalahan 10%, nilai chi kuadrat sebesar 2,706 (tabel chi kuadrat), N adalah total populasi, P merupakan nilai probabilitas benar (0,5) sedangkan Q menunjukkan nilai probabilitas salah (0,5), dan d adalah perbedaan sampel dan rata-rata populasi, perbedaan mencakup 0,001; 0,005; dan 0,1.

Dengan batas toleransi 10% dan nilai d = 0,05. Perhitungannya seperti pada Pers. (2).

$$s = \frac{2{,}706 \times 50 \times 0{,}5 \times 0{,}5}{0{,}05^2 \times (50-1)+2{,}706 \times 0{,}5 \times 0{,}5} = \frac{33{,}825}{0{,}799} = 42{,}33 = 42 \text{ (dibulatkan)} \qquad (2)$$

2.3 Analisa Data

Analisa data dianggap sebagai kunci pada suatu riset, karena dapat memberikan hasil penelitian sebagai suatu laporan yang bisa diambil manfaatnya (Sugawara & Nikaido, 2014). Analisa data bertujuan untuk menemukan arti dari setiap data yang telah dikumpulkan, sehingga mampu menafsirkan hubungan satu dengan lainnya yang dapat diterima oleh logika. Analisa data sendiri dilakukan terhadap hasil data yang diperoleh dari observasi, wawancara, yang kemudian dirangkum dan dikategorikan karena data tersebut berupa sebuah teks atau narasi (Sugawara & Nikaido, 2014). Kemudian perolehan data dari kuesioner dianalisa menggunakan skala Likert dengan bantuan SPSS v.26 untuk mengetahui sebuah pendapat maupun persepsi responden terhadap fenomena yang terjadi.

3. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan mengulas tentang proses konfigurasi *access control list* sesuai dengan *Network Development Life Cycle (NDLC)*, mulai dari analisis, desain, simulasi, implementasi, *monitoring*, hingga manajemen. Serta menampilkan proses pengujian data yang diperoleh dari hasil kuesioner yang disebar kepada para responden, mengenai pernyataan yang berkaitan tentang *access control list* dengan MAC *address* sebagai metode keamanan jaringan intranet.

3.1 Konfigurasi Access Control List dengan MAC Address

Konfigurasi dilakukan menggunakan *routerboard* Mikrotik dengan bantuan *tool* Winbox. Proses konfigurasi mengacu pada metode *Network Development Life Cycle* (NDLC) sebagai metode yang biasa digunakan untuk perkembangan jaringan, baik dari desain sebelumnya ke desain jaringan yang baru. Berikut merupakan 6 tahap proses konfigurasi NDLC.

3.1.1 Analisis

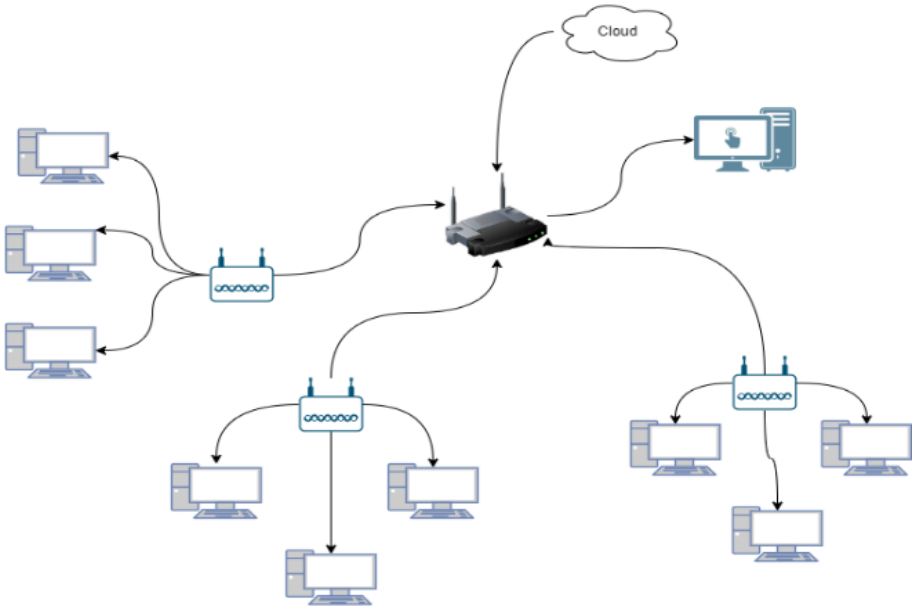
Pada tahap analisis, diperoleh hasil analisa terhadap jaringan intranet yang digunakan di lingkungan kantor cangehgar *cyber operation center* dengan detail topologi seperti yang ditunjukkan pada Gambar 1.

Hasil analisis diketahui topologi yang digunakan sebelumnya adalah topologi *ring*. Terdapat komputer server dan *access point* yang terhubung dengan *cloud*, serta memiliki perangkat *switch* pada setiap ruangan yang terhubung ke *access poin* utama yang ada di ruangan *cyber*.

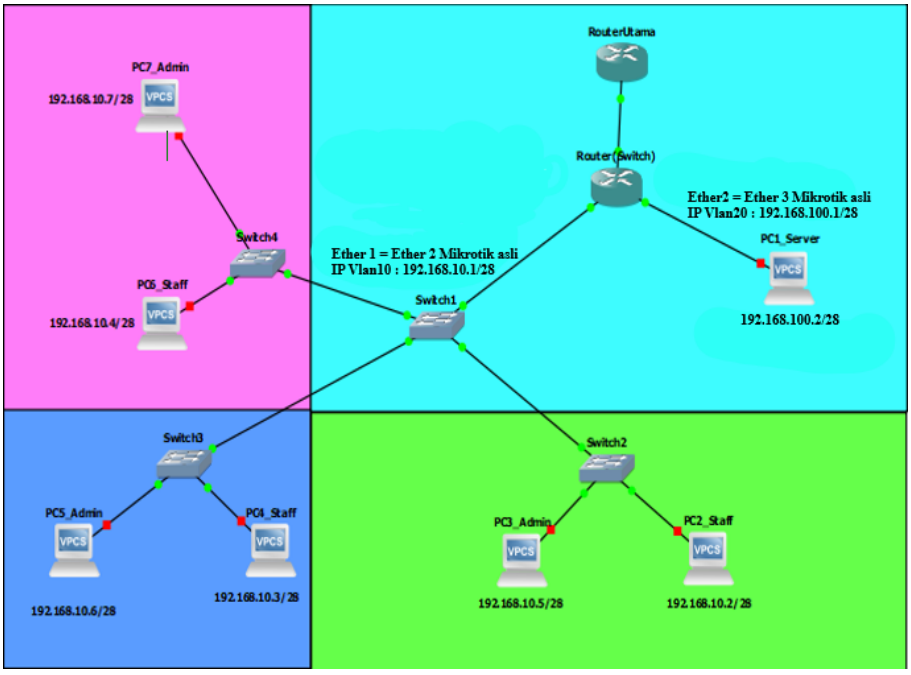
3.1.2 Desain

Dalam tahap desain ini, diusulkan sebuah jaringan baru dengan desain topologi *star*. Terdapat beberapa Mikrotik yang dijadikan sebagai pusat konfigurasi jaringan intranet. Pada topologi baru yaitu topologi *star*, terdapat Mikrotik yang digunakan sebagai pusat konfigurasi untuk jaringan intranet. Kemudian detail warna menunjukkan masing-masing divisi yang ada di lingkungan

kantor Cangehgar *Cyber Operation Center* seperti yang digambarkan pada Gambar 2. IP VLAN 20 dengan *address* 192.168.100.1/28 merupakan alamat untuk komputer server, sedangkan IP VLAN 10 dengan *address* 192.168.10.1/28 merupakan alamat untuk komputer *client,* yang terdiri dari komputer staf dan juga komputer admin.



Gambar 1 Topologi Sebelumnya



Gambar 2 Topologi Baru

3.1.3 Simulasi

Simulasi konfigurasi menggunakan *tools* jaringan yaitu GNS3, untuk konfigurasi Mikrotik. Tahap simulasi bertujuan untuk mencegah terjadinya kesalahan pada saat konfigurasi langsung

menggunakan *routerboard* Mikrotik. Contoh konfigurasi menggunakan GNS3 ditunjukkan pada Gambar 3 dan 4.

```
jan/26/2022 04:54:06 system,error,critical router was rebooted without proper shu
tdown

[admin@MikroTik] > system identity set name=RouterUtama
```

Gambar 3 Konfigurasi Identity RouterUtama

```
jan/26/2022 04:54:05 system,error,critical router was rebooted without proper shu
tdown

[admin@MikroTik] > system identity set name=RouterSwitch
[admin@RouterSwitch] >
```

Gambar 4 Konfigurasi Identity RouterSwitch

Proses konfigurasi Identity RouterUtama dan juga RouterSwitch bertujuan untuk membedakan antara kedua *router* yang saling terhubung tersebut. Pada RouterUtama lakukan setting VLAN 10 dan juga VLAN 20, dengan *address* 192.168.100.1/28 untuk VLAN 20 atau komputer server, serta 192.168.10.1/28 untuk VLAN 10 atau komputer *client.* Maka hasilnya seperti pada Gambar 5.

```
[admin@RouterUtama] > interface vlan add name=vlan10 interface=ether1 vlan-id=10
[admin@RouterUtama] > interface vlan add name=vlan20 interface=ether1 vlan-id=20
```

Gambar 5 Konfigurasi VLAN 10 dan VLAN 20

Untuk melihat *address* yang sudah terkonfigurasi, masukan perintah "*ip address print*", maka muncul *address* yang telah dikonfigurasi. Seperti ditunjukkan pada Gambar 6

```
[admin@RouterUtama] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.10.1/28    192.168.10.0    vlan10
 1   192.168.100.1/28   192.168.100.0   vlan20
[admin@RouterUtama] >
```

Gambar 6 Konfigurasi IP VLAN 10 dan VLAN 20

Pada *router* kedua atau RouterSwitch dilakukan konfigurasi *bridge*, kepada ether1, ether2, sampai ke ether3. Buat konfigurasi *trunk* untuk ether1 yang akan menyalurkan VLAN 10 ke ether2, dan VLAN 20 ke ether3. Hasilnya seperti pada Gambar 7 dan 8.

```
[admin@RouterSwitch] > interface bridge print
Flags: X - disabled, R - running
 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=0C:26:F1:AD:00:00
     protocol-mode=rstp fast-forward=yes igmp-snooping=no auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s
     forward-delay=15s transmit-hold-count=6 vlan-filtering=yes ether-type=0x8100 pvid=1 frame-types=admit-all
     ingress-filtering=no dhcp-snooping=no
[admin@RouterSwitch] >
```

Gambar 7 *Interface Bridge*

```
[admin@RouterSwitch] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload
 #     INTERFACE                  BRIDGE                 HW  PVID PRIORITY  PATH-COST INTERNAL-PATH-COST    HORIZON
 0     ether1                     bridge1                yes    1     0x80         10                 10       none
 1     ether2                     bridge1                yes   10     0x80         10                 10       none
 2     ether3                     bridge1                yes   20     0x80         10                 10       none
[admin@RouterSwitch] >
```

Gambar 8 *Interface Bridge Port*

Ether1, ether2, dan ether3 sudah tergabung kedalam *bridge1*, yang artinya semua ether sudah terhubung di dalam 1 *bridge.* Untuk melihat hasilnya ketikan perintah "*interface bridge VLAN print"*, maka hasilnya bahwa vlan10 dan vlan20 sudah berada dalam 1 *bridge*. Seperti yang ditunjukkan pada Gambar 9.

```
[admin@RouterSwitch] > interface bridge vlan print
Flags: X - disabled, D - dynamic
 #   BRIDGE                     VLAN-IDS  CURRENT-TAGGED                CURRENT-UNTAGGED
 0   bridge1                    10        ether1                        ether2
 1   bridge1                    20        ether1                        ether3
 2 D bridge1                    1                                       bridge1
                                                                        ether1
```

Gambar 9 *Interface Bridge* VLAN

Tagged adalah mode *trunk* di mana vlan-ids=10 disalurkan kepada *ports* Mikrotik ether2, serta vlan-ids=20 menyalurkan vlan20 dari *ports* ether1 kepada *ports* ether3. Hasil konfigurasi tersebut ditunjukkan pada Gambar 10.

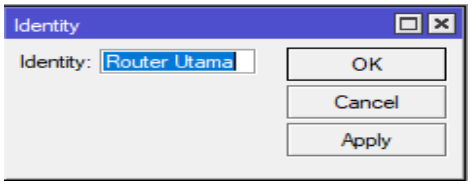
```
[admin@RouterSwitch] > interface bridge vlan add bridge=bridge1 vlan-ids=10 tagged=ether1 unta
gged=ether2
[admin@RouterSwitch] > interface bridge vlan add bridge=bridge1 vlan-id=20 tagged=ether1 untagged=ether3
[admin@RouterSwitch] > interface bridge set numbers=0 vlan-filtering=yes
```

Gambar 10 Konfigurasi *Trunk* VLAN

Pada proses yang ada di tahapan simulasi hanya sampai ke *setting* konfigurasi Mikrotiknya saja. Lebih detailnya ada pada tahapan implementasi di mana proses antar komputer *client* staf tidak bisa melakukan komunikasi *ping* (ICMP) ke komputer pusat atau server, sedangkan komputer *client* admin dapat melakukan komunikasi *ping* (ICMP) ke komputer server.

3.1.4 Implementasi

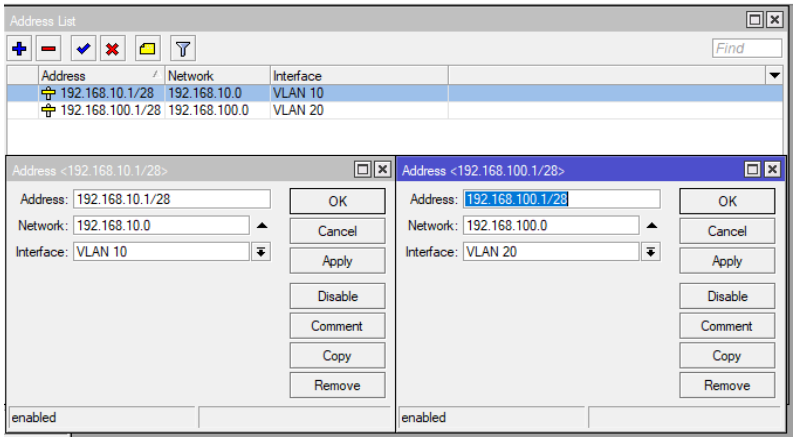
Tahap implementasi merupakan tahap implementasi langsung, di mana konfigurasi dilakukan langsung dengan menggunakan perangkat *routerboard* Mikrotik. Contoh konfigurasi *access control list* dengan MAC *address* pada Mikrotik ditunjukkan pada Gambar 11.



Gambar 11 Konfigurasi *Identity Router* Utama

Konfigurasi *identity* dilakukan untuk membedakan *router* utama dengan *router* (*switch).*

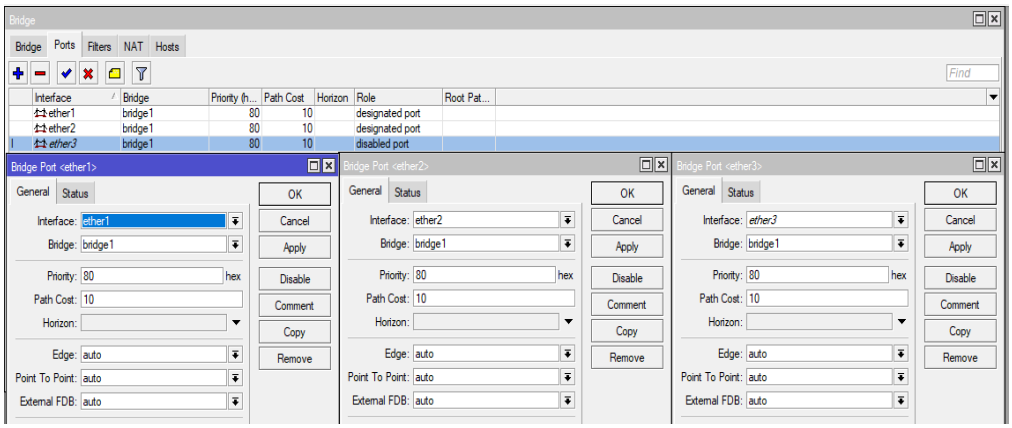
JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 3, SEPTEMBER, 2022: 143 – 162



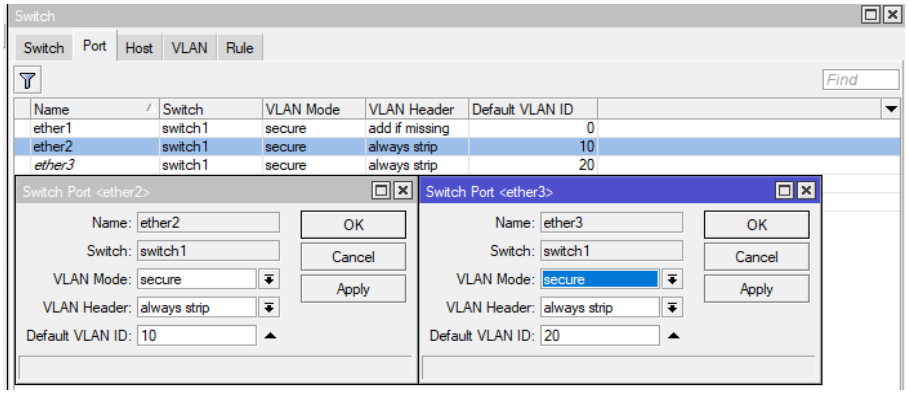
Gambar 12 Konfigurasi IP VLAN 10 dan VLAN 20

Konfigurasi *address* 192.168.10.1/28 untuk VLAN 10, seperti pada Gambar 12, yang nantinya dialokasinya untuk alamat komputer *client,* baik komputer staf maupun komputer admin. Alamat IP 192.168.100.1/28 dialokasikan untuk alamat komputer server.

Penambahan ether1 sampai dengan ether2 pada bridge1 agar dalam satu jalur atau satu jaringan seperti yang dapat dilihat pada Gambar 13 dan 14.

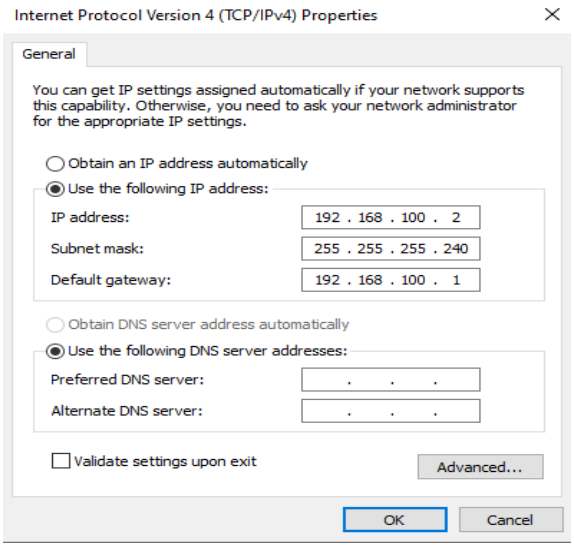


Gambar 13 Konfigurasi Bridge1 *Router* (*Switch*)

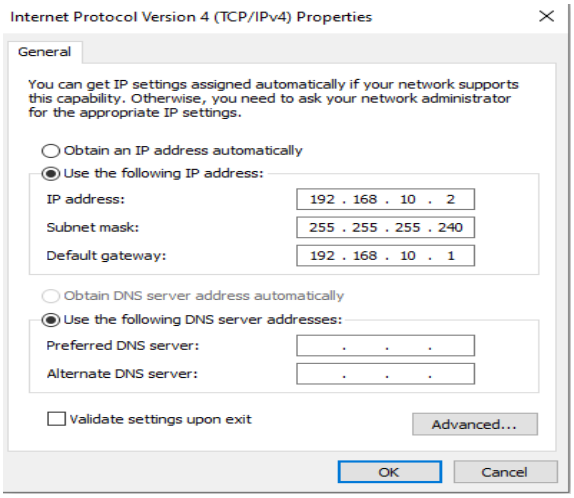


Gambar 14 Konfigurasi VLAN *Mode* dan VLAN *Header* Ether2 dan Ether3

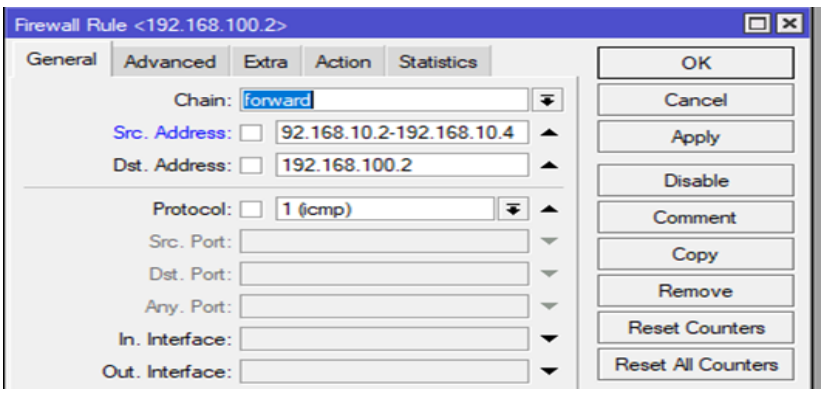
Pada bagian *IP Address* diisi dengan alamat 192.168.100.2 dengan *subnet mask* 255.255.255.240 karena menggunakan *prefix* 28 seperti yang dilakukan pada Gambar 15 dan 16.



Gambar 15 Konfigurasi IP Server



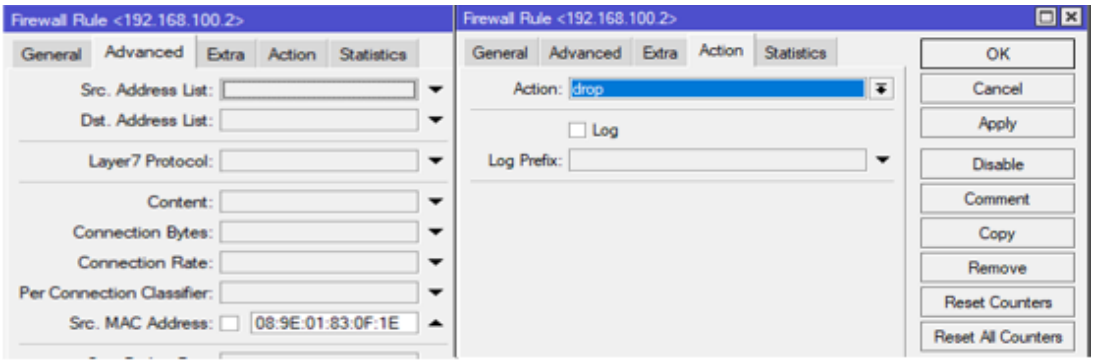
Gambar 16 Konfigurasi IP *Client* Staf



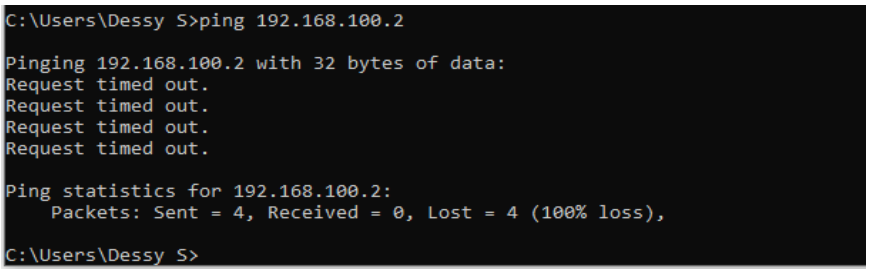
Gambar 17 Konfigurasi *Access Control List Client* Staf

JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 3, SEPTEMBER, 2022: 143 – 162

Pada bagian *Chain* pilih *forward* dengan *Src. Address* 192.168.10.2 – 192.168.10.4 sebagai alamat dari komputer *client* Staf dengan *Dst. Address* 192.168.100.2 sebagai alamat komputer server seperti pada Gambar 17.

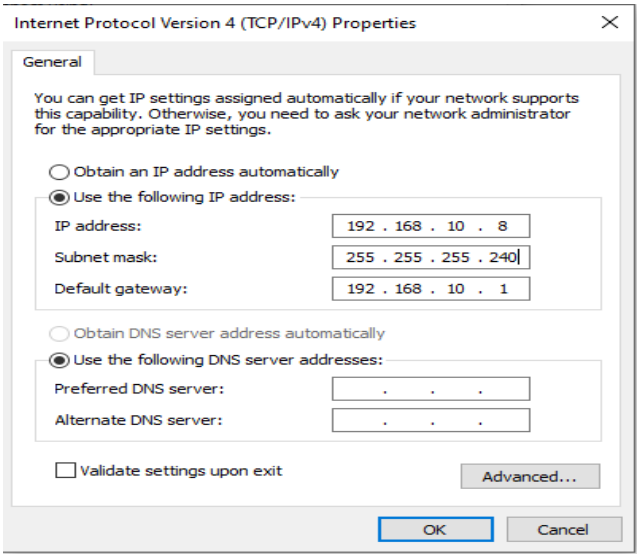


Gambar 18 Konfigurasi MAC *Address* dan *Action Drop*



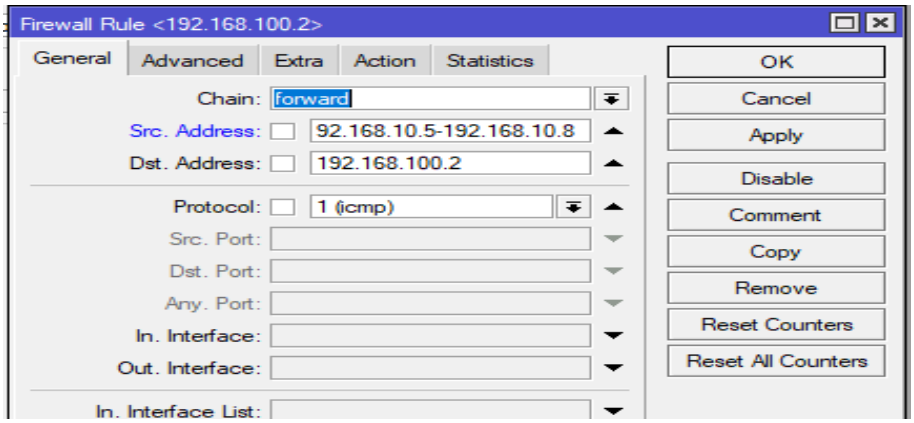
Gambar 19 Hasil Konfigurasi Setelah *Access Control List*

Komputer *client* staf tidak dapat melakukan akses kompunikasi *ping* ke komputer server, ditandai dengan *request timed out* seperti yang ditunjukkan pada Gambar 18 dan 19.



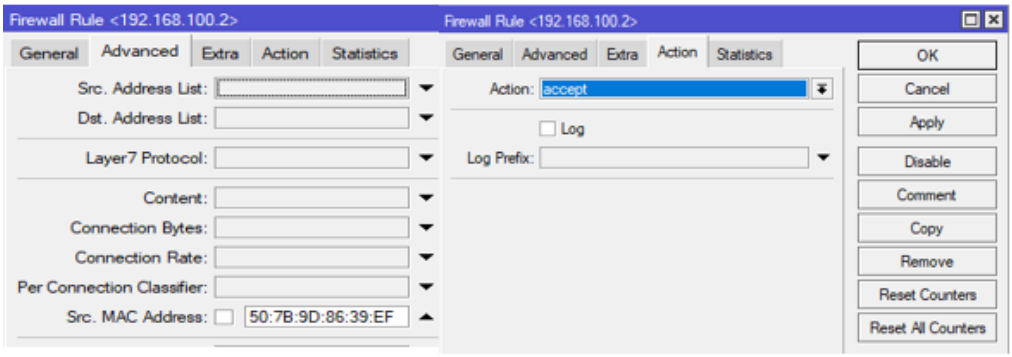
Gambar 20 Konfigurasi IP Komputer Admin

Sama dengan komputer staf, pada bagian IP *Address* diisi dengan 192.168.10.8 sebagai alamat komputer admin, dan *subnet mask* 255.255.255.240 karena menggunakan *prefix* 28 seperti pada Gambar 20.



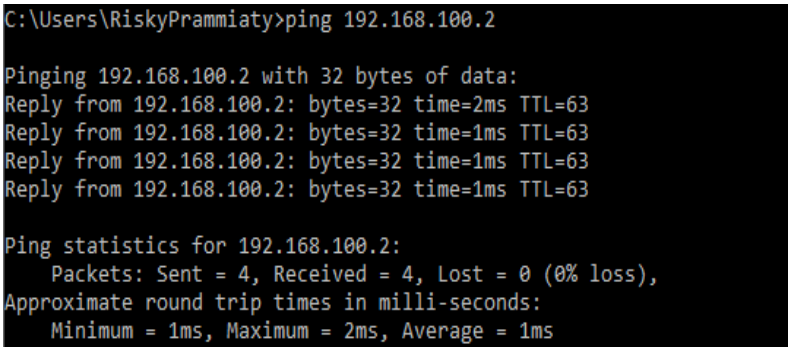
Gambar 21 Pengaturan IP *Access Control List Client* Admin

Pada bagian *Chain* pilih *forward* dengan *Src. Address* 192.168.10.5 – 192.168.10.8 sebagai alokasi alamat komputer admin, dan 192.168.100.2 sebagai alamat untuk komputer server seperti yang dicontohkan pada Gambar 21.



Gambar 22 Konfigurasi MAC *Address* dan *Action Access*

Pada bagian *Action* pilih *Accept* untuk mengizinkan komputer admin dapat melakukan komunikasi *ping* ke komputer server seperti konfigurasi yang dilakukan pada Gambar 22.



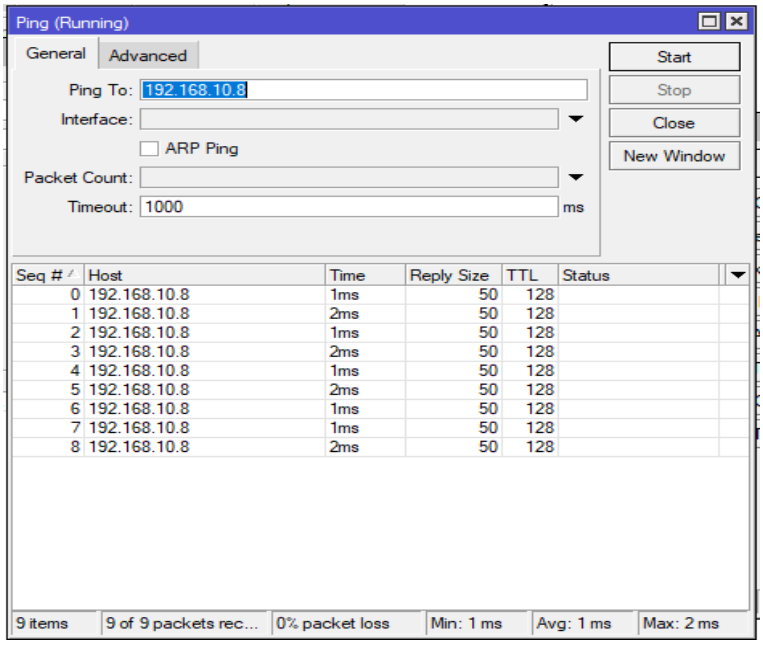
Gambar 23 Hasil *Access Control List* Komputer Admin

Hasil konfigurasi yang telah dilakukan, maka komputer *client* staf tidak dapat melakukan akses komunikasi *ping* ke komputer server, dan hanya komputer *client* admin yang dapat berkomunikasi *ping* dengan komputer server seperti hasil yang ditunjukkan pada Gambar 23. Dengan begitu pembatasan akses terhadap komputer server dapat dilakukan dan dapat meminimalkan

terjadinya kebocoran data dari pihak internal yang disebabkan oleh kelalaian anggota karena akses yang belum dibatasi.

3.1.5 *Monitoring*

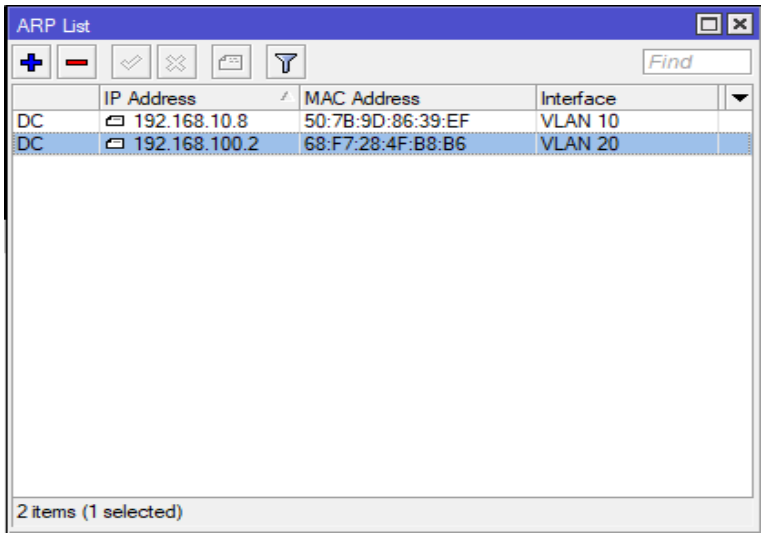
Riwayat *ping* yang dilakukan ke komputer server dapat dipantau seperti yang ditunjukkan pada Gambar 24.



Gambar 24 *Monitoring Ping* ke Komputer Server

3.1.6 Manajemen

Manajemen pada ARP (Address Resolution Protocol) List ditunjukkan pada Gambar 25.



Gambar 25 Manajemen pada ARP *List*

3.2 Proses Pengujian Data Kuesioner

Kuesioner terdiri dari total 10 pernyataan terhadap 42 responden. Pernyataan-pernyataan tersebut terdiri dari indikator keamanan, yaitu *confidentiality, integrity, accountability, availability, access control,* dan *authentication.* Hasil dari kuesioner tersebut ditunjukkan pada Tabel 4.

Tabel 4 Hasil Kuesioner Skala Likert

No. Responden	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10
1	4	4	4	5	5	5	4	5	3	4
2	5	4	4	5	5	5	3	5	4	5
3	3	3	3	1	1	4	1	3	3	3
4	4	4	4	4	4	4	4	3	4	4
…	…	…	…	…	…	…	…	…	…	…
40	4	4	4	4	2	4	4	4	4	4
41	4	4	4	4	3	4	4	4	4	4
42	4	4	4	4	3	4	4	4	3	4

3.2.1 Uji Validitas Data

Pengujian validitas bertujuan untuk menguji data yang diperoleh valid (sahih) atau tidak (Erliana et al., 2019). Pengujian tersebut memakai SPSS versi 26 dengan *Pearson Correlation.* Ketentuan pengujian validitasnya adalah r hitung > r tabel. Hasil dari uji validitas data, dengan ketentuan jumlah data (N) 42 responden dengan tingkat signifikan 0,05 dan rumusnya (N-2, 0,05) = (42-2, 0,05) = 0,3044 atau 0,304. Daftar pernyataan dari uji validitas data ditunjukkan pada Tabel 5 dan 6.

Tabel 5 Pernyataan Uji Validitas Data

Indikator		Pernyataan
Confidentiality	1)	Kerahasiaan data (*confidentiality)* pada sebuah keamanan jaringan intranet sangat penting karena meliputi dengan asset informasi yang dimiliki.
Integrity	2)	Keaslian data (*integrity)* dalam sebuah asset yang dimiliki tidak boleh diubah saat proses pengiriman data pada jaringan intranet oleh orang yang tidak memiliki kewenangan
Accountability	3)	Indikator *accountability* dalam sebuah system bermanfaat untuk mengetahui data *logged user* setiap melakukan kegiatan dalam sebuah jaringan.
Availability	4)	Jaringan intranet sangat berguna untuk melakukan komunikasi antar perangkat dalam satu jaringan.
	5)	Ketersediaan data (*availability)* pada saat diakses dan bisa digunakan untuk transfer *file* antar perangkat computer.
	6)	Manfaat dari penggunaan jaringan intranet dalam melakukan pekerjaan dirasa sangat efektif.
Access Control	7)	Keamanan jaringan intranet yang digunakan di lingkungan kantor Cangehgar *Cyber Operation Center* masih minim.
	8)	Peningkatan keamanan dengan *access control list* mampu membatasi akses terhadap paket data dan user dalam melakukan akses ke jaringan intranet serta ke komputer server
Authentication	9)	Akses komunikasi antara perangkat komputer *client* dan komputer server masih terbilang bebas tanpa adanya batasan akses.
	10)	Perlu dilakukan keamanan lebih pada jaringan intranet yang digunakan

Tabel 6 Hasil Uji Validitas Data

No.	Pertanyaan	R Hitung	R Tabel	Keterangan
1	*Confidentiality* (X1)	0,681	0,304	Valid
2	*Integrity* (X2)	0,536	0,304	Valid
3	*Accountability* (X3)	0,381	0,304	Valid
4	*Availability* (X4)	0,721	0,304	Valid
5	*Availability* (X5)	0,609	0,304	Valid
6	*Availability* (X6)	0,314	0,304	Valid
7	*Access Control* (X7)	0,661	0,304	Valid
8	*Access Control* (X8)	0,515	0,304	Valid
9	*Authentication* (X9)	0,377	0,304	Valid
10	*Authentication* (X10)	0,499	0,304	Valid

3.2.2 Uji Reliabilitas Data

Pengujian reliabilitas data menggunakan *Cronbach's Alpha* dengan total 10 pernyataan terhadap 42 responden dengan tingkat signfikansi 5% atau 0,304. pengujian reliabilitas bertujuan untuk menguji data tersebut reliabel, dapat dipercaya atau juga bisa disebut konsisten (Pairingan et al., 2018). Hasil pengujian menunjukkan angka 0,745 > 0,304 seperti yang ditunjukkan pada Gambar 26.

Reliability Statistics

Cronbach's Alpha	N of Items
.745	10

Gambar 26 Hasil Uji Reliabilitas Data

3.2.3 Uji Normalitas Data

Uji normalitas adalah uji terhadap data yang dimiliki apakah berdistribusi normal atau tidak (Prasetya & Harjanto, 2020). Ketentuan pengujian data tersebut apabila nilai signifikansi > 0,05 maka disebut normal. Hasil uji dengan nilai *Kolmogorov-Smirnov* 0,200 dan *Shapiro-Wilk* 0,369 seperti yang ditunjukkan pada Gambar 27.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Hasil Responden	.079	42	.200*	.971	42	.369

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Gambar 27 Hasil Normalitas Data

Guna memperkuat hasil normalitas data, dilakukan juga pengujian *Nonparametric Test* dengan *Legacy dialogs* menggunakan metode *exact test Asymtotic Only, Monte Carlo,* dan juga *Exact* dengan masing-masing hasil seperti yang ditunjukkan pada Gambar 28 sampai 30.

Hasil dari *Asymtotic Only* pada Gambar 28 menunjukkan nilai signifikasi 0,200, dan dapat dikatakan berdistribusi normal. Selanjutnya, hasil dari Monte Carlo pada Gambar 29 menunjukkan nilai signifikasi 0,938, dan dapat dikatakan berdistribuasi normal. Lalu, hasil dari *Exact* pada Gambar 30 menunjukkan nilai signifikasi 0,940, dan dapat dikatakan berdistribusi normal.

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		42
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	.41034226
Most Extreme Differences	Absolute	.079
	Positive	.079
	Negative	-.046
Test Statistic		.079
Asymp. Sig. (2-tailed)		.200[c,d]

a. Test distribution is Normal.
b. Calculated from data.
c. Lilliefors Significance Correction.
d. This is a lower bound of the true significance.

Gambar 28 Hasil *Asymtotic Only*

One-Sample Kolmogorov-Smirnov Test

			Unstandardized Residual
N			42
Normal Parameters[a,b]	Mean		.0000000
	Std. Deviation		.41034226
Most Extreme Differences	Absolute		.079
	Positive		.079
	Negative		-.046
Test Statistic			.079
Asymp. Sig. (2-tailed)			.200[c,d]
Monte Carlo Sig. (2-tailed)	Sig.		.938[e]
	99% Confidence Interval	Lower Bound	.932
		Upper Bound	.944

a. Test distribution is Normal.
b. Calculated from data.
c. Lilliefors Significance Correction.
d. This is a lower bound of the true significance.
e. Based on 10000 sampled tables with starting seed 334431365.

Gambar 29 Hasil Monte Carlo

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		42
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	.41034226
Most Extreme Differences	Absolute	.079
	Positive	.079
	Negative	-.046
Test Statistic		.079
Asymp. Sig. (2-tailed)		.200[c,d]
Exact Sig. (2-tailed)		.940
Point Probability		.000

a. Test distribution is Normal.
b. Calculated from data.
c. Lilliefors Significance Correction.
d. This is a lower bound of the true significance.

Gambar 30 Hasil Exact

JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 3, SEPTEMBER, 2022: 143 – 162

3.2.4 Uji Homogenitas Data

Pengujian homogenitas merupakan tahap di mana menguji sebuah data yang dimiliki homogen atau tidak (Dohot et al., 2020). Pengujian dilakukan terhadap variabel-variabel pernyataan. Contoh hasil akhir di mana nilai signifikan > 0,05 dan data tersebut dinyatakan homogen atau sejenis ditunjukkan pada Gambar 31.

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
Responden	Based on Mean	.452	1	37	.505
	Based on Median	.510	1	37	.480
	Based on Median and with adjusted df	.510	1	33.071	.480
	Based on trimmed mean	.440	1	37	.511

Gambar 31 Hasil Uji Homogenitas

3.2.5 Uji Anova

Pengujian anova dilakukan setelah melewati beberapa tahap uji sebelumnya. Pengujian data dengan uji anova dapat dilakukan apabila data sudah berdistribusi normal dan homogen (Herawati & Irwandi, 2019). Pengujian dilakukan kepada setiap variabel pernyataan yang diajukan kepada respoden, dan hasilnya rata-rata > 0,05 dan dinyatakan lulus uji anova. Hasil uji anova terhadap masing-masing variabel ditunjukkan pada Gambar 32 sampai 41.

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.318	2	8.159	1.332	.276
Within Groups	232.707	38	6.124		
Total	249.024	40			

Gambar 32 Uji Anova Variabel X1

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.343	2	2.171	.337	.716
Within Groups	244.682	38	6.439		
Total	249.024	40			

Gambar 33 Uji Anova Variabel X2

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	11.024	2	5.512	.880	.423
Within Groups	238.000	38	6.263		
Total	249.024	40			

Gambar 34 Uji Anova Variabel X3

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	41.338	3	13.779	2.455	.078
Within Groups	207.687	37	5.613		
Total	249.024	40			

Gambar 35 Uji Anova Variabel X4

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	14.262	3	4.754	.749	.530
Within Groups	234.762	37	6.345		
Total	249.024	40			

Gambar 36 Uji Anova Variabel X5

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.142	1	5.142	.822	.370
Within Groups	243.882	39	6.253		
Total	249.024	40			

Gambar 37 Uji Anova Variabel X6

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	10.127	3	3.376	.523	.669
Within Groups	238.897	37	6.457		
Total	249.024	40			

Gambar 38 Uji Anova Variabel X7

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	63.928	3	21.309	4.260	.011
Within Groups	185.096	37	5.003		
Total	249.024	40			

Gambar 39 Uji Anova Variabel X8

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8.167	2	4.084	.644	.531
Within Groups	240.857	38	6.338		
Total	249.024	40			

Gambar 40 Uji Anova Variabel X9

ANOVA

Responden

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	12.180	2	6.090	.977	.386
Within Groups	236.844	38	6.233		
Total	249.024	40			

Gambar 41 Uji Anova Variabel X10

Hasil pengujian data yang telah dilakukan, mulai dari uji validitas, uji reliabilitas, uji normalitas, uji homogen, hingga ke uji anova, memiliki hasil nilai akhir dengan tingkat signifikansi melebihi 0,05. Data-data tersebut bisa digunakan karena telah melewati tahapan-tahapan pengujian data.

4. KESIMPULAN

Konfigurasi keamanan jaringan intranet di kantor Cangehgar Cyber Operation Center berhasil dilakukan. Hal tersebut dapat dilihat dari proses konfigurasi yang telah dilakukan. Pembatasan akses menggunakan MAC *address* dengan metode *access control list*, mampu untuk membatasi akses perangkat komputer antara *client* staf dan *client* admin. Hanya komputer admin yang dapat melakukan akses komunikasi *ping* (ICMP) ke komputer server, sedangkan komputer staf tidak bisa berkomunikasi karena aksesnya di *drop.* Pembatasan tersebut berguna untuk menghindari sembarang akses dan kebocoran informasi dari segi internal. Sejalan dengan hasil konfigurasi yang berhasil, data-data dari kuesioner yang telah diolah melewati beberapa tahap pengujian mendapatkan tingkat akhir signifikansi diatas 0,05. Hasil tersebut menandakan bahwa responden cenderung setuju perihal *access control list* dengan MAC *address* berguna untuk membatasi hak akses. Saran peneliti untuk penelitian selanjutnya adalah membuat *access control list* menggunakan alat Switch Manageable dari Mikrotik, dengan sistem operasi SWOS untuk lebih mempermudah proses konfigurasi.

UCAPAN TERIMA KASIH

Terima kasih banyak kepada Divisi Cangehgar *Cyber Operation Center* yang telah mengizinkan penulis untuk melakukan riset di tempat tersebut.

DAFTAR PUSTAKA

Ahmad, T., Imtihan, K., & Wire, B. (2020). Implementasi Jaringan Inter-VLAN Routing Berbasis Mikrotik Rb260Gs Dan Mikrotik Rb1100Ahx4. *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, *3*(1), 77–84. https://doi.org/10.36595/jire.v3i1.221

Ardiansyah, A. H., & Yudiastuti, H. (2021). Perancangan Jaringan Intervlan Routing Dan Penerapan Acls Pada Pt. Sinar Alam Permai Dengan Simulasi Menggunakan Packet Tracer. *Prosiding Semhavok*, *3*(1), 210–218.

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review. *UNISTEK*, *7*(2), 59–70. https://doi.org/10.33592/unistek.v7i2.645

Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *3*(1), 1. https://doi.org/10.29407/intensif.v3i1.12125

Dohot, S., Khairina, N., & Robin. (2020). Pembuatan Media Pembelajaran Fisika Berbasis Hots Untuk Tingkat Smp. *Pendidikan Fisika*, *9*(1), 63–67. https://doi.org/10.22611/jpf.v9i1.18173

Erliana, H., Akos, M., & Priono, S. (2019). Pengaruh Disiplin Kerja Terhadap Kinerja Dengan Kepuasan Kerja Sebagai Variabel Intervening. *Administraus*, *3*(2), 31–58. https://doi.org/10.56662/administraus.v3i2.75

Gunawan, J., & Agung, H. (2019). Implementation of PPTP and BCP with Inter-VLAN on the Topology that Uses 2 ISP as Inter-Division Connectors (Case Study: PT Kenari Djaja Prima). *Jurnal Algoritma, Logika Dan Komputasi*, *2*(1), 138–150. https://doi.org/10.30813/j-

alu.v2i1.1574

Hafizhan, M., Wahyuddin, M. I., & Komalasari, R. T. (2020). Implementasi Packet Filtering Menggunakan Metode Extended Access Control List (ACL) Pada Protokol EIGRP. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(1), 185. https://doi.org/10.30865/mib.v4i1.1926

Hasan, U., & Dewi, S. (2022). Penerapan Metode Access Control List Pada Jaringan VLAN Menggunakan Router Cisco. *IMTechno: Journal of Industrial Management and Technology*, *3*(1), 37–41. https://doi.org/10.31294/imtechno.v3i1.927

Herawati, L., & Irwandi. (2019). Pengaruh Model Pembelajaran Kooperatif Tipe Jigsaw Terhadap Hasil Belajar dan Berpikir Kritis Siswa Pada Mata Pelajaran IPA di SMP Negeri 09 Lebong. *Prosiding Seminar Nasional Sains Dan Entrepreneunship Vi*, 1–9.

Irwansyah, I., & Novariansyah, D. (2019). Pengembangan Keamanan Jaringan Vlan Dan Acls Pt. Taspen (Persero) Palembang Menggunakan Simulasi Packet Tracer. *Prosiding Semhavok*, *1*(1), 95–102.

Kartini, D., & Eko, A. (2019). Upgrade Skill Komputer Perangkat Desa Pemakuan. *Jurnal Pengabdian Kepada Masyarakat MEDITEG*, *4*(2), 7–11. https://doi.org/10.34128/mediteg.v4i2.48

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Kurniati, K., & Dasmen, R. N. (2019). The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *10*(1), 49. https://doi.org/10.24843/LKJITI.2019.v10.i01.p06

Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer pada Era Big Data. *J-SIKA|Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14–20.

Nugroho, F. E., & Daniarti, Y. (2021). Rancang Bangun QoS (Quality of Service) Jaringan Wireless Local Area Network Menggunakan Metode NDLC (Network Development Life Cycle) di PT Trimitra Kolaborasi Mandiri (3KOM). *JIKA (Jurnal Informatika)*, *5*(1), 79. https://doi.org/10.31000/jika.v5i1.3970

Pairingan, A., Allo Layuk, P. K., & Pangayow, B. J. . (2018). Pengaruh Kompetensi, dan Independensi Terhadap Kualitas Audit dengan Motivasi Sebagai Variabel Pemoderasi. *Jurnal Akuntansi, Audit, Dan Aset*, *1*(1), 1–13. https://doi.org/10.52062/jurnal_aaa.v1i1.2

Prasetya, T. A., & Harjanto, C. T. (2020). Pengaruh Mutu Pembelajaran Online Dan Tingkat Kepuasan Mahasiswa Terhadap Hasil Belajar Saat Pandemi. *Jurnal Pendidikan Teknologi Dan Kejuruan*, *17*(2), 188–197. https://doi.org/10.23887/jptk-undiksha.v17i2.25286

Purba, G. C. (2021). Implementation Of Network Packet Filtering With Extended Acl Methods On Microtik In Securing Internet Connection Office AFD IV Butong Sulfur Unit. *Infokum*, *9*(2), 287–293.

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi*, *12*(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528

Sihotang, B. K., Sumarno, S., & Damanik, B. E. (2020). Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara. *JURIKOM (Jurnal Riset Komputer)*, *7*(2), 229. https://doi.org/10.30865/jurikom.v7i2.2010

Sugawara, E., & Nikaido, H. (2014). Properties of AdeABC and AdeIJK Efflux Systems of Acinetobacter baumannii Compared with Those of the AcrAB-TolC System of Escherichia coli. *Antimicrobial Agents and Chemotherapy*, *58*(12), 7250–7257. https://doi.org/10.1128/AAC.03728-14

Sulaiman, O. K., & Saripurna, D. (2021). Network Security System Analysis Using Access Control List (ACL). *International Journal of Information System & Technology Akreditasi*, *5*(2), 192–197. https://doi.org/10.30645/ijistech.v5i2.131