Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Analisis Simulasi Mitigasi Ancaman ARP Dan *Round Trip Time* Pada Lalu Lintas DHCP VTP

Firmansyah[1*], Yusuf Hendra Pratama[2]
Program Studi Ilmu Komputer, Universitas Islam Al-Azhar, Mataram, Indonesia
*e-mail *Corresponding Author: firmanyasin@gmail.com*

Abstract

Round-Trip Time (RTT) is the total amount of time it takes to send the signal plus the total amount of time the signal acknowledges to receive. Communication between computers using a Local Area Network (LAN) computer network is still used today, but VLAN (Virtual Local Area Network) computer network technology can provide better results compared to LAN computer networks, but each data transmission uses the Address Resolution protocol. Protocol (ARP) that functions to find devices from origin to destination addresses. Testing the implementation of Static VTP (VLAN Trunking Protocol) and DHCP VTP was pinged 5 (five) times on Internet Protocol (IP) with the same host. On the DHCP VTP network, the maximum average time for sending data is 5.3ms, while on Static VTP, the average maximum time for sending data is 6.1ms, which means that the time for sending data on the DHCP VTP network is 0.8ms faster. ARP (Address Resolution Protocol) threat mitigation analysis results, that the established DHCP VTP network ensures that only valid ARP requests and responses will be forwarded.

Keyword: *Round-Trip Time; Address Resolution Protocol; Virtual Local Area Network; Dinamyc Host Configuration Protocol; Ping*

Abstrak

Round-Trip Time (RTT) adalah jumlah total waktu untuk mengirim sinyal ditambah jumlah total waktu yang diakui sinyal yang diterima. Komunikasi antar komputer menggunakan jaringan komputer *Local Area Network* (LAN) masih digunakan hingga saat ini, namun teknologi jaringan komputer VLAN (*Virtual Local Area Network*) dapat memberikan hasil yang lebih baik di bandingkan dengan jaringan komputer LAN, namun setiap pengiriman data menggunakan protokol *Address Resolution Protocol* (ARP) yang berfungsi untuk menemukan perangkat dari alamat asal ke tujuan. Pengujian penerapan *Static* VTP (*VLAN Trunking Protocol)* dan DHCP VTP dilakukan pinging sebanyak 5 (lima) kali pada *Internet Protocol* (IP) dengan *host* yang sama. Pada jaringan DHCP (*Dinamyc Host Configuration Protocol)* VTP menghasilkan rata-rata waktu maksimal pengiriman data adalah 5.3ms sedangkan pada *Static* VTP menghasilkan rata-rata waktu maksimal pengiriman data mencapai 6.1ms, yang artinya waktu untuk pengiriman data pada jaringan DHCP VTP lebih cepat 0.8ms. Analisis mitigasi ancaman ARP (*Address Resolution Protocol*) menghasilkan, bahwa jaringan DHCP VTP yang dibangun memastikan bahwa hanya permintaan dan respons ARP yang valid yang akan diteruskan.

Kata kunci: *Round-Trip Time; Address Resolution Protocol; Virtual Local Area Network; Dinamyc Host Configuration Protocol; Ping.*

1. Pendahuluan

Pada era digital tahun 2020, ilmu pengetahuan bidang teknologi terkhusus jaringan komputer sangat berkembang pesat, sehingga menjadi sangat canggih. Jaringan komputer ini bisa dikatakan sebagai tulang punggung sistem informasi, yang bisa menjadi salah satu ukuran kompetitif atau tidaknya perusahaan maupun perguruan tinggi. Membangun suatu jaringan komputer dengan mengimplementasikan VLAN, merupakan bagian dari perkembangan teknologi saat ini. Selanjutnya, rumusan masalah pada penelitian ini adalah bagaimana membuat perbandingan Jaringan komputer VLAN dan LAN menggunakan aplikasi simulasi jaringan Paket Tracer 6.0.1. Bagaimana membangun jaringan DHCP VTP, agar setiap pengiriman data tetap dilakukan inspeksi jaringan secara dinamis merupakan rumusan masalah lainnya. Broadcast merupakan pengiriman data dari lalu lintas jaringan komputer yang telah dibangun ke seluruh

komputer dalam host yang sama. Jika dalam jaringan terdapat 2 (dua) host, maka host akan dikirimi paket data sesuai dengan sumber host [1]. Penelitian tersebut belum memberikan penjelasan *tools* untuk mendeteksi serangan dan cara menangani pencegahan serangan ARP. Tujuan utama VTP adalah untuk membangun fasilitas agar *switch Cisco* dapat diatur sebagai grup. VTP adalah pengaturan fitur yang disediakan pada layer 2 di jajaran *Switch Cisco Catalyst* yang dapat memaksimalkan kinerja jaringan komputer [2]. Penelitian tersebut menggunakan VTP yang di konfigurasi pada *router*, solusi yang di tawarkan pada penelitian ini konfigurasi VTP menggunakan switch manageable. VLAN yaitu suatu objek jaringan yang memungkinkan akses komunikasi tanpa terbatas pada lokasi fisiknya, sehingga dapat merubah suatu jaringan dengan pengaturan secara virtual tanpa harus memikirkan lokasi fisik peralatan. Sebelum penggunaan teknologi VLAN, performa jaringan pada topologi yang dimaksud tidak baik [3]. Solusi pada penelitian tersebut untuk menggunakan VLAN sehingga performa jaringan menjadi lebih baik. *Internet Control Message Protocol* (ICMP) adalah salah satu protokol inti dari jaringan komputer, sehingga setiap alamat *Internet Protokol* (IP) dapat digunakan untuk mengontrol pesan dan informasi kesalahan pelaporan protokol antara jaringan dan gerbang untuk menuju ke internet. [4].

Tujuan penelitian ini adalah membandingkan dan mengkonfigurasi sebuah Jaringan komputer Statik VTP dan DHCP VTP dan melakukan analisis mitigasi ancaman ARP. Penelitian ini sangat penting dilakukan untuk keperluan perkembangan teknologi saat ini, jika di bandingkan dengan literatur singkat di atas, yang membahas aliran paket data dan forensik jaringan, namun belum adanya penelitian analisis mitigasi ancaman DHCP VTP. Harapan penulis, dengan adanya Analisis *Round Trip Time* (RTT) Dan Mitigasi Ancaman ARP Pada Lalu Lintas DHCP VTP dapat digunakan sebagai acuan untuk membuat jaringan VTP yang aman dan dapat memastikan setiap data yang dikirim telah divalidasi. Kelebihan ilmiah pada artikel ini yaitu penerapan DHCP VTP pada *switch manageable* yang memungkinkan lalu lintas data sudah ter validasi sehingga mitigasi ancaman ARP bukan lagi sebagai ancaman yang di takutkan. Penelitian yang dilakukan memperoleh beberapa manfaat, seperti mengetahui hasil perbandingan jaringan antara jaringan *Static* VTP dan Dinamik VTP.

2. Tinjauan Pustaka

2.1 Mitigasi Ancaman ARP

Fitur keamanan *Dynamic* ARP *Inspection* (DAI) diaktifkan dengan cara di konfigurasi untuk mengurangi *spoofing cache* ARP. Pengintaian DHCP melindungi jaringan dengan mengizinkan server untuk menerima pesan, respons inspeksi DHCP hanya dari server yang valid dan terhubung ke setiap interface. DAI membantu mencegah peracunan ARP dan serangan berbasis ARP lainnya dengan mencegat dan memverifikasi keaslian permintaan/balasan ARP atau ICMP apa pun, dan menghapus *spoofing* ARP apa pun yang berada di luar batas kecepatan yang dikonfigurasi pada *port* yang tidak terpercaya. [5]. Penelitian tersebut belum membuktikan adanya fitur keamanan DAI pada jaringan yang dirancang namun langsung pada tahap investigasi. Mitigasi ancaman terletak pada OSI Layer 2 (dua) karena dianggap sebagai sumber yang lemah dalam model OSI [6]. Solusi pada penelitian tersebut yaitu, manajemen protokol harus diamankan. Metode *Live Forensics* merupakan metode investigasi dengan cepat mendeteksi suatu serangan dan mengidentifikasi penyerang secara pemantauan langsung. Tanggal, waktu, MAC, IP, merupakan data yang diperlukan untuk proses investigasi sehingga dapat membantu investigator dalam mengambil keputusan pemotongan akses pada serangan yang terjadi [7]. Penelitian tersebut juga diharapkan dapat merekomendasi alat yang digunakan dalam deteksi dan identifikasi serangan dan penyerang. Penelitian selanjutnya akan mencari cara menangani dan mencegah serangan ARP Spoofing.

2.2 VLAN Trunking Protokol (VTP)

VTP memiliki fungsi utama yaitu penyederhanaan kerja pengembangan jaringan dalam implementasi VLAN. Implementasi VTP pada switch manageable, dapat berfungsi sebagai server, transparan, maupun *client* [8], juga menyatakan dalam penelitiannya, bahwa VLAN lebih memudahkan admin jaringan dalam menambah atau mengurangi *client* dan menyatakan VLAN aman apabila melakukan broadcast dibandingkan dengan LAN, namun belum ada pembuktian bahwa jaringan VLAN saja sudah cukup aman. *Round Trip Time* (RTT) adalah waktu pengiriman paket yang dibutuhkan untuk dikirim dari sumber ke tujuan kemudian kembali lagi ke sumber. Dalam konteks jaringan komputer RTT juga dikenal sebagai waktu pengiriman paket ICMP atau

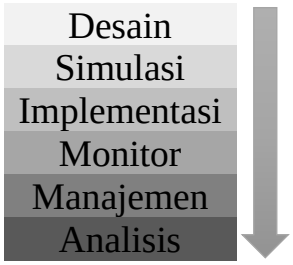
ping, sebagai percobaan pada koneksi internet. Pemanfaatan metode, koleksi, pemeriksaan, analisis dan pelaporan, yang dapat diulang dan dipertahankan merupakan salah satu metode forensik jaringan untuk pembuktian, dalam hal ini pembuktian pada lalu lintas virtual [9]. Berdasarkan dari percobaan dengan pengujian lalu lintas jaringan virtual, sistem yang dibangun berhasil mendapatkan bukti-bukti digital, baik dengan cara pengamatan secara langsung maupun pengamatan secara tidak langsung, namun jaringan yang di bangun menggunakan IP static bukan menggunakan IP DHCP.

2.3 Simulasi

Jaringan komputer akan terhubung apabila terdiri dari dua atau lebih komputer dengan satu jaringan yang sama. Simulasi jaringan ditunjukkan, dua jaringan yang berbeda, jika hanya alamat dikonfigurasi dalam satu jaringan yang sama, maka dapat menggunakan perangkat jaringan berupa switch. Hasil dan pembahasan simulasi jaringan telah berhasil dengan memanfaatkan aplikasi *software cisco packet tracer* 6.2, tentang pembangunan jaringan dijadikan informasi keadaan koneksi dalam satu jaringan, sehingga digunakan untuk penentuan biaya operasional perakitan jaringan komputer dan kerusakan jaringan komputer dengan tepat dan murah [10]. Simulasi keamanan jaringan menggunakan metode DHCP *snooping* dan VLAN telah berhasil membandingkan keamanan jaringan dengan melakukan penyaringan terhadap server yang tidak dipercaya sehingga jaringan komputer dan internet akan aman [11]. Penelitian tersebut di atas pada literatur simulasi belum meneliti analisis simulasi mitigasi ancaman ARP dan RTT pada lalu lintas DHCP VTP. Simulasi pengukuran RTT sudah diuji menggunakan algoritme yang sudah ada dan dikembangkan sebelumnya menggunakan aplikasi NS-3 [12]. Penelitian tersebut hanya meneliti Optimasi lalu lintas RTT, namun bukan pada jaringan virtual.

3. Metodologi

NDLC (*Network Development Life Cycle*) merupakan sebuah metode yang bergantung pada proses pembangunan perencanaan strategi bisnis pengembangan aplikasi, dan analisis pendistribusian data [13], [14], dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

Tahapan desain merupakan tahap pemetaan perangkat jaringan yang akan di tempatkan pada masing-masing ruangan. Tahapan simulation menggunakan alat simulasi jaringan *Cisco Packet Tracer* 8.2.0 (CPT). Tahap implementasi merupakan tahap pengujian jaringan komputer. Monitor jaringan adalah tahapan koneksi jaringan, jika berhasil terkoneksi, pada hal ini menggunakan CPT 8.2.0, indikator akan menyala berwarna hijau, namun jika berwarna merah, artinya belum ada koneksi jaringan. Tahapan manajemen merupakan tahapan konfigurasi jaringan VTP. Tahapan terakhir yaitu analisis untuk membuktikan kecepatan pengiriman data, antara VLAN dan VTP sekaligus analisis mitigasi ancaman ARP dan RTT pada lalu lintas DHCP VTP.

4. Hasil dan Pembahasan

4.1 Profil *Design*

Tahapan ini menentukan nama VLAN, VLAN ID, *Network* dan *Gateway* dapat dilihat pada Tabel 1 penetapan desain VLAN.

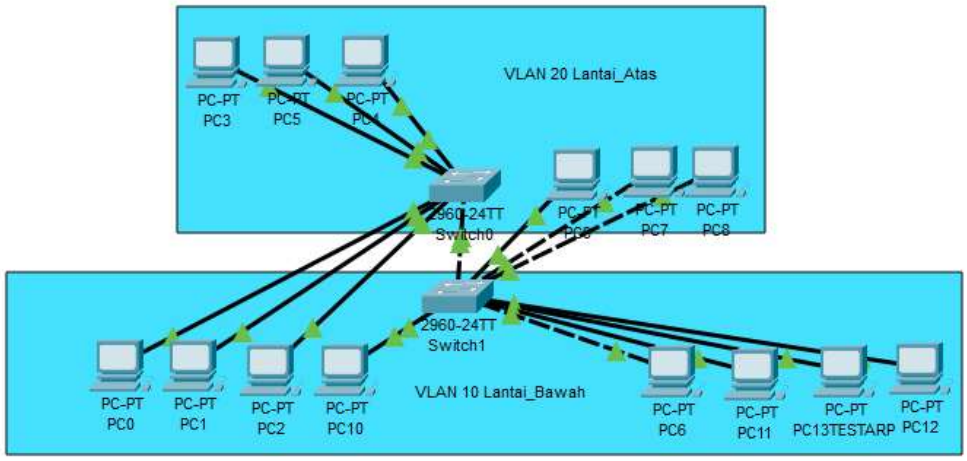
Tabel 1. Penetapan Desain VLAN

Nama VLAN	VLAN ID	NETWORK	GATEWAY
Lantai_Bawah	VLAN10	DHCP	192.168.10.1
Lantai_Atas	VLAN20	DHCP	192.168.20.1

Terlihat pada Tabel 1. bahwa VLAN yang akan di simulasikan yaitu VLAN10 dengan *gateway* 192.168.10.1 dan VLAN20 dengan *gateway* 192.168.20.1.

4.2 Monitor Jaringan

Seperti yang telah dijelaskan sebelumnya pada metode penelitian, bahwa monitor jaringan akan di tampilkan jika tahapan simulasi dan implementasi di jalankan, namun tahapan tersebut peneliti rangkum langsung pada langkah monitoring yang dapat dilihat pada gambar 2 Monitor Jaringan.



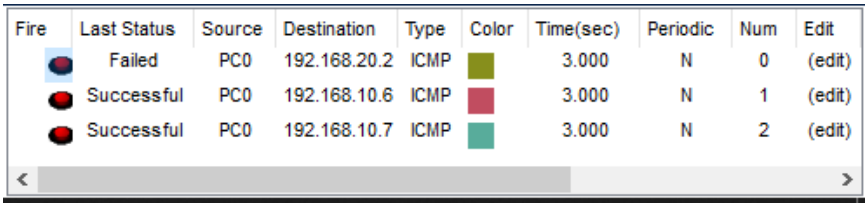
Gambar 2. Monitor jaringan

Pada gambar 2 terdapat 2 *Switch Manageable* dan 14 perangkat komputer yang telah di simulasi dengan VLAN ID masing-masing perangkat dan implementasi pengaturan VTP pada masing-masing *switch*, lebih jelas lihat pada tabel 2 VLAN ID.

Tabel 2. VLAN ID

VLAN ID	
VLAN10	**VLAN20**
PC0	PC3
PC1	PC5
PC2	PC4
PC10	PC6
PC6	PC7
PC11	PC8
PC13TESTARP	
PC12	

Pengaturan dilakukan pada *switch*0 sesuai desain menjadi 2 (dua) VLAN ID sebagai server, kemudian *switch*1 menjadi *client*. Penelitian di pusatkan pada perangkat yang berada pada VLAN10. Hasil pengaturan dapat dilihat pada gambar 3. Pengiriman data.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PC0	192.168.20.2	ICMP		3.000	N	0	(edit)
	Successful	PC0	192.168.10.6	ICMP		3.000	N	1	(edit)
	Successful	PC0	192.168.10.7	ICMP		3.000	N	2	(edit)

Gambar 3. Pengiriman Data

Berhasil dibuktikan bahwa pengaturan VLAN sesuai dengan desain, terlihat PC0 yang merupakan VLAN10 tidak dapat mengirimkan data menuju alamat 192.168.20.2 yang alamat tersebut merupakan VLAN20. Pengiriman data diatur dengan masing-masing menggunakan waktu atau *one shoot time/second* 3 (tiga) detik. Pengaturan DHCP VTP dapat dilihat pada gambar 4. DHCP *Binding*.

```
Switch#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.20.3     00E0.A3EA.785A           --                     Automatic
192.168.20.5     00E0.B0C5.8893           --                     Automatic
192.168.20.2     0060.3E0E.7328           --                     Automatic
192.168.20.6     0001.97EE.8B99           --                     Automatic
192.168.20.7     00E0.8FBA.5BA2           --                     Automatic
192.168.20.4     0006.2A9D.8E02           --                     Automatic
192.168.10.2     0060.2FA0.A0E5           --                     Automatic
192.168.10.5     00E0.F761.CB37           --                     Automatic
192.168.10.4     0001.421A.A960           --                     Automatic
192.168.10.6     0002.1761.C9C5           --                     Automatic
192.168.10.3     0007.EC26.024D           --                     Automatic
192.168.10.7     0002.1730.2279           --                     Automatic
192.168.10.9     0001.9717.942C           --                     Automatic
192.168.10.8     0090.21B2.5D10           --                     Automatic
```

Gambar 4. DHCP *Binding*

Berhasil melakukan pengaturan DHCP pada switch, yang di buktikan pada Gambar 4. DHCP *Binding,* terlihat bahwa ada 6 perangkat sebagai VLAN20 dan 8 perangkat sebagai VLAN10 dengan tipe otomatis atau DHCP.

4.3 Analisis Simulasi

Analisis pengujian RTT, dilakukan melalui pinging pada packet tracer 8.2.0 yang dapat menghasilkan perbedaan jaringan VLAN dan VTP DHCP. Pengujian dilakukan 3 (tiga) kali pinging dengan 5 (lima) perangkat yang berbeda. Hasil dapat dilihat pada Tabel 3. Pengujian RTT VLAN dan VTP DHCP.

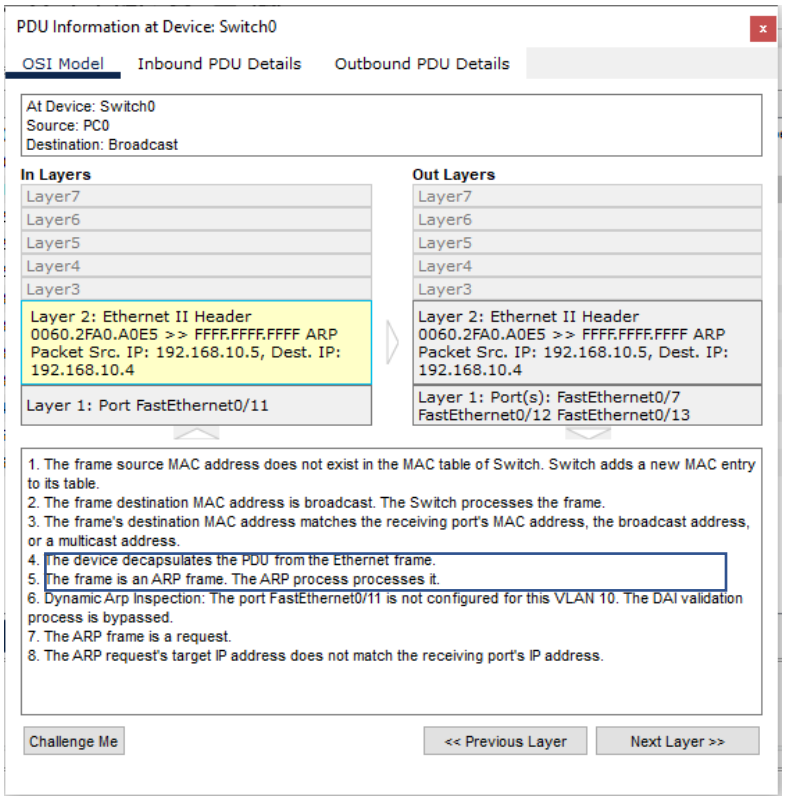
Tabel 3. Hasil Pengujian RTT

No	Jenis	DHCP VTP					STATIC VTP				
				Waktu					Waktu		
		Sumber	Tujuan	A	B	C	Sumber	Tujuan	A	B	C
1	PING	10.2	10.6	0	0	0	10.2	10.6	0	0	0
	PING			0	4	1			0	11	4
	PING			0	5	3			0	4	1
2	PING	10.2	10.7	0	0	0	10.2	10.7	0	10	3
	PING			0	3	0			0	10	2
	PING			0	5	1			0	0	0

No	Jenis	DHCP VTP					STATIC VTP				
				Waktu					Waktu		
		Sumber	Tujuan	A	B	C	Sumber	Tujuan	A	B	C
3	PING	10.2	10.9	0	5	2	10.2	10.9	0	29	7
	PING			0	5	3			0	10	3
	PING			0	1	0			0	10	5
4	PING	20.2	20.3	0	3	0	20.2	20.3	0	3	0
	PING			0	3	0			0	4	1
	PING			0	18	5			0	0	0
5	PING	20.2	20.6	0	1	0	20.2	20.6	0	0	0
	PING			0	4	1			0	0	0
	PING			0	22	5			0	0	0
Jumlah Waktu Rata-rata				0	5.3	1.4			0	6.1	1.7

Keterangan:
A: Minimal Waktu Tempuh dalam satuan *ms*
B: Maksimal Waktu Tempuh dalam satuan *ms*
C: *Average* dalam satuan *ms*

Terlihat pada tabel 3. Hasil pengujian RTT, bahwa waktu rata-rata yang ditempuh untuk mengirim data pada jaringan DHCP VTP lebih cepat dibandingkan dengan jaringan Static VTP. Pengujian selanjutnya akan dikirim paket data dengan bantuan protokol ARP, hasil dapat dilihat pada gambar 5. Pengiriman data ARP.



Gambar 5. Pengiriman Data ARP

Penelitian ini melihat efek penggunaan DHCP VTP pada jaringan VLAN menggunakan metode NDLC. Pengujian ini menganalisa protokol ARP pada OSI model layer 2, dimana terletak IP sumber dan IP tujuan. Hasil analisis ditemukan pada jaringan DHCP VTP, bahwa bingkai ARP di proses kemudian dilakukan inspeksi dinamis ARP dan langsung divalidasi. Dikatakan bahwa *FASTETHERNET 0/11* bukan termasuk bagian dari VLAN 10, namun tidak menjadi masalah, karena pengaturan DHCP pada penelitian ini menggunakan jangkauan *ethernet*, sehingga tetap akan dikirim. Teknik pemantauan ini mencakup bahan pembelajaran untuk pencegahan dan deteksi. Bahan pembelajaran deteksi menggunakan alat yang menangkap paket ARP. Ini dapat mengidentifikasi aktivitas mencurigakan di jaringan yang di bangun, dan setelah terdeteksi, pengintaian DHCP, dan teknik inspeksi ARP digunakan untuk mengurangi serangan guna mencapai jaringan yang lebih aman [15].

5. Simpulan

Peneliti menemukan hal yang baru bahwa dengan menggunakan alat simulasi jaringan *cisco packet tracer* 8.2.0, dapat membangun sebuah jaringan dengan metode NDLC, yang kemudian lalu lintas jaringan tersebut dapat dianalisa. Analisa RTT di butuhkan untuk menjamin setiap pengguna jaringan akan mendapatkan waktu akses atau pengiriman data antar jaringan yang cepat. Jaringan DHCP VTP terbukti lebih cepat dibandingkan dengan jaringan *static* VTP. Pengaturan mitigasi ancaman berhasil dilakukan sehingga memastikan bahwa jaringan DHCP VTP sangat aman dari serangan. Harapan penulis agar menjadikan pengaturan DHCP VTP menjadi aturan yang wajib digunakan pada jaringan komputer, sehingga penelitian selanjutnya yaitu bagaimana proses jaringan forensik untuk menemukan bukti jika adanya penyusupan atau serangan.

Daftar Referensi

[1] F. F. A. Firmansyah dan R. Umar, “Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien,” *Edu Komputika*, vol. 6, no. 2, pp. 54–59, 2019.

[2] M. Z. Rahmanzi, I. Fitri, dan A. Aningsih, “Kinerja Load Balancing pada Teknologi Etherchannel Menggunakan Metode VLAN Trunking Protocol (VTP),” *J I M P - Jurnal Informatika Merdeka Pasuruan*, vol. 5, no. 3, pp. 9-15, Mei 2021, doi: 10.37438/jimp.v5i3.236.

[3] K. B. Aditya Nurcahyo dan A. Prihanto, “Analisis Quality of Service (QoS) pada Jaringan VLAN (Virtual Local Area Network),” *Journal of Informatics and Computer Science (JINACS)*, vol. 3, no. 01, hlm. 62–70, Agu 2021, doi: 10.26740/jinacs.v3n01.p62-70.

[4] P. Purnomo, M. Nugroho, M. S. Kabes, S. P. Putra, dan J. Fathanah, “Sistem Pemantauan Jaringan Data Di Stasiun Bumi LAPAN,” *Format Jurnal Ilmiah Teknik Informatika*, vol. 11, no. 1, pp. 1-11, 2022, doi: 10.22441/10.22441/format.2022.v11.i1.004.

[5] H. A. Mangut, A. Al-Nemrat, C. B. Benza¨ıd, dan A.-R. H. Tawil, “ARP Cache Poisoning Mitigation and Forensics Investigation,” 2015, doi: 10.1109/Trustcom-BigDataSe-ISPA.2015.536.

[6] K. Nikolchev, K. Herasymenko, O. Starkova, dan M. Yastrebov, “Development of Recommendations for the Implementation of Integrated Security in the Corporate Network at the OSI Data Link Layer,” dalam *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, pp. 807–810, Okt 2020,. doi: 10.1109/PICST51311.2020.9468014.

[7] M. N. Hafizh, I. Riadi, dan A. Fadlil, “Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic,” *Jurnal Telekomunikasi dan Komputer*, vol. 10, no. 2, pp. 111-120, 2020, doi: 10.22441/incomtech.v10i2.8757.

[8] P. H. Sutanto, C. Sitasi, dan : Sutanto, “Perancangan Virtual Local Area Network Berbasis VTP Dan Inter-Vlan Routing,” *Jurnal Teknik Komputer*, no. 2, pp. 125–134, 2018, doi: 10.31294/jtk.v4i2.3662.

[9] F. Firmansyah, A. Fadlil, dan R. Umar, “Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 91–98, Feb 2021, doi: 10.29207/resti.v5i1.2784.

[10] I. C. R. Drajana dan A. Bode, “SIMULASI JARINGAN MENGGUNAKAN CISCO PACKET TRACER,” *Simtek : jurnal sistem informasi dan teknik komputer*, vol. 6, no. 1, pp. 24–27, Mei 2021, doi: 10.51876/simtek.v6i1.91.

[11] Z. Miftah, “SIMULASI KEAMANAN JARINGAN DENGAN METODE DHCP SNOOPING DAN VLAN,” *Faktor Exacta*, vol. 11, no. 2, pp. 167-178, 2018, doi: 10.30998/faktorexacta.v11i2.2456.

[12] H. Idwan dan I. Ihsanuddin, “Analisis Optimasi Round Trip Time (RTT) pada Jaringan Transmission Control Protocol (TCP) New Reno,” *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, vol. 4, no. 2, pp. 92-101, Okt 2020, doi: 10.35870/jtik.v4i2.143.

[13] J. D. Santoso, “Analisis Perbandingan Metode Queue Pada Mikrotik,” *Pseudocode*, vol. 7, no. 1, pp. 1-7, 2020, doi: 10.33369/pseudocode.7.1.1-7.

[14] N. M. A. Yalestia Chandrawaty dan I. P. Hariyadi, “Implementasi Ansible Playbook Untuk Mengotomatisasi Manajemen Konfigurasi VLAN Berbasis VTP Dan Layanan DHCP,” *Jurnal Bumigora Information Technology (BITe)*, vol. 3, no. 2, pp. 107-122, 2021, doi: 10.30812/bite.v3i2.1577.

[15] H. A. S. Adjei, M. T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah, dan E. S. A. Gyarteng, “SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection),” dalam *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, Feb 2021, vol. 2021-February, pp. 187–193. doi: 10.23919/ICACT51234.2021.9370460.