

Analisis Pengaruh Konfigurasi NAT Statik Berbasis Web Menggunakan Wire Shark

Hero Wintolo¹, Salam Aryanto², Muhamad Hafish³

^{1,2,3} Departemen Informatika
Institut Teknologi Dirgantara Adisutjipto
Jl.Janti, Blok-R, Lanud Adisucipto, Yogyakarta, Indonesia

e-mail: ¹herowintolo@itda.ac.id, ²salamori@yahoo.com, ³mhafish18@gmail.com

Informasi Artikel	Diterima: 19-02-2021	Direvisi: 12-03-2021	Disetujui: 19-03-2021
-------------------	----------------------	----------------------	-----------------------

Abstrak

Konfigurasi peralatan jaringan komputer yang digunakan untuk mengelola sebuah jaringan komputer banyak yang menggunakan *command line* atau berbasis teks meski ada beberapa merek dari peralatan jaringan komputer sudah menawarkan perangkat lunak untuk konfigurasi yang berbasis *Graphical User Interface*(GUI) dengan fungsi yang terbatas. Hal ini menjadi inspirasi untuk membuat perangkat lunak berbasis web untuk fungsi konfigurasi *Network Address Translator* (NAT) statik dan dinamik. Hasil perancangan perangkat lunak diujikan dalam *Local Area Network*(LAN) dan jaringan internet untuk layanan *server*. Perangkat lunak yang dibuat pada penelitian ini terbukti dapat bekerja untuk pembuatan NAT statik dan dinamik melalui perangkat lunak wireshark yang memperlihatkan proses penyalinan alamat IP *source* menjadi alamat IP router yang ada NAT statik dan dinamik sehingga dapat mengakses web *server* yang ada. Sebanyak 30 komputer dalam LAN dan komputer dari jaringan internet 100% dapat mengakses web *server* melalui NAT statik yang dikonfigurasi menggunakan *keyboard* dan *mouse*.

Kata Kunci: NAT, web, wireshark

Abstract

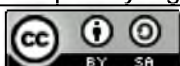
Many computer network equipment configurations used to manage a computer network use the command line or text-based although there are several brands of computer network equipment that offer software for configuration based on a Graphical User Interface (GUI) with limited functionality. This became the inspiration for creating web-based software for static and dynamic Network Address Translator (NAT) configuration functions. The results of the software design were tested in a Local Area Network (LAN) and internet network for server services. The software made in this research is proven to work for static and dynamic NAT creation through wire shark software which shows the process of copying the source IP address to the IP address of the router with static and dynamic NAT so that it can access the existing web server. As many as 30 computers on the LAN and computers from the internet network can 100% access the web server via static NAT configured using a keyboard and mouse.

Keywords: NAT; web; wire shark

1. Pendahuluan

Hubungan komputer dengan komputer yang lainnya pada jaringan komputer dapat terjadi ketika secara fisik antar komputer tersebut dihubungkan dengan media transmisi kabel atau non kabel atau *wireless* melalui peralatan jaringan komputer *switch* atau *router* dan secara non fisik komputer diberi alamat dengan menggunakan alamat *Internet Protocol* (IP). Komputer yang saling terhubung ini dapat berupa *personal komputer* atau *server* yang dihubungkan menggunakan peralatan jaringan komputer yang dikenal juga sebagai *end device*

berupa *switch* dan *router*. Pemilihan peralatan jaringan komputer yang akan digunakan sebagai penghubung antar komputer ini akibat dari Network Address (NA) atau dikenal juga sebagai alamat jaringan yang merupakan bagian dari alamat IP. Jika NA sama maka dibutuhkan peralatan jaringan komputer berupa *switch*, jika NA tidak sama maka membutuhkan peralatan jaringan komputer berupa *router*. Alamat IP yang diberikan pada komputer merupakan alamat IP versi 4 yang bersifat *private*, sehingga jika komputer ini digunakan untuk mengakses komputer lainnya dengan NA



yang berbeda dan IP versi 4 yang bersifat *public* maka dibutuhkan cara agar IP *private* dapat menggunakan IP *public* dari router untuk terhubung ke komputer yang memiliki IP *public* dengan menggunakan *routing* atau NAT (Fauzi, Nugroho, & Wahyudi, 2018). IP *public* hanya dikenal pada IP versi 4, sedangkan pada IP versi 6 tidak mengenal istilah IP *public*. NAT yang digunakan untuk menghubungkan komputer dengan komputer lainnya yang berbeda NA dan IP publiknya yang dikenal sebagai internet terdiri dari dua jenis, NAT statik dan NAT dinamik serta dapat mengamankan jaringan yang terhubung ke NAT dari ancaman *flooding* (Octafian, 2016). Dengan menggunakan NAT dinamik komputer dapat mengakses komputer lainnya pada jaringan internet tanpa menggunakan *routing* (Tujini & S, 2019) dan dapat menggunakan *poly base routing* (Pambudi & Muslim, 2017). Konfigurasi NAT dapat dilakukan secara langsung pada *router* atau tidak langsung menggunakan simulator packet tracer (Natali, Fajrillah, & Diansyah, 2016). Konfigurasi langsung pada peralatan jaringan komputer dapat dilakukan dengan mengakses peralatan melalui console atau menggunakan perangkat lunak Kerio Control (Tutang, Tutuko, & Rosyidin, 2015) atau GNS3 (Ginting, Suroso, & Hadi, 2020).

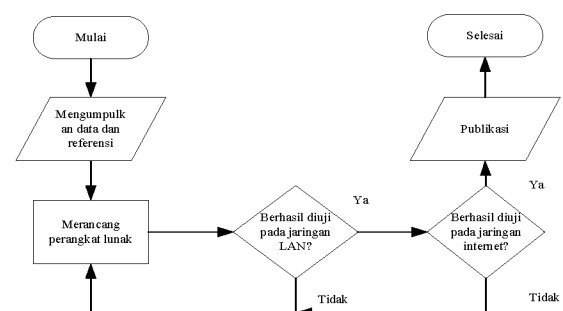
Peralatan jaringan komputer berupa *router* yang digunakan untuk menghubungkan komputer ke jaringan internet dapat dibuat menggunakan komputer dengan sistem operasi linux untuk konfigurasi NAT pada *routing protocol* (Fauzi et al., 2018), akan tetapi efisiensi dari pemakaian komputer untuk *router* tentu kurang efisien dibandingkan dengan peralatan jaringan komputer yang khusus untuk *router* yang berupa mikrotik (Ardianto, Alfaresi, & Darmadi, 2018; Rahman, Sumama, & Nurdin, 2020) atau cisco. Proses konfigurasi pada peralatan jaringan ini dapat menggunakan mekanisme *Command Line Interface* (CLI) pada saat melakukan console ke peralatan jaringan atau dengan menggunakan perangkat lunak yang dibuat menggunakan teknologi web (Ayuningtyas, Sudaryanto, & Cessara, 2020; Wiryawan & Rosyid, 2019). Sehingga dalam penelitian ini, proses pembuatan NAT statik dilakukan menggunakan perangkat lunak yang khusus dibuat untuk peralatan cisco *router* dengan teknologi web. Hasil konfigurasi diuji dan diamati menggunakan perangkat lunak *wireshark* (Diansyah, 2015). Penggunaan *wireshark* sebagai perangkat lunak untuk mendapatkan data aliran paket data pada jaringan komputer menggunakan teknik *sniffing* (Adriant & Mardianto, 2015). Aliran paket data dapat berupa teks, gambar, audio

dan video (Afrida & Rahmatia, 2018) dapat diamati menggunakan perangkat lunak ini.

Penggunaan NAT pada penelitian ini bertujuan untuk mengembangkan penelitian yang sebelumnya telah dilakukan terkait penggunaan *web server* yang dapat diakses melalui jaringan internet. *Web server* ini diletakkan pada jaringan lokal yang terhubung internet. Peningkatan kecepatan akses *web server* dapat dilakukan dengan menggunakan *load balancing* (Rachmawan, Irwan, & Argyawati, 2016). Dan akses publik melalui jaringan internet ke dalam jaringan lokal harus didukung dengan *domain name system* (Tedyana & Kurniati, 2016). Pengamatan aliran data pada jaringan lokal yang ada *web server* ini nantinya akan diamati menggunakan perangkat lunak *wireshark*.

2. Metode Penelitian

Penelitian ini didahului dengan mengumpulkan data yang digunakan untuk perancangan perangkat lunak. Data yang diperlukan berupa Application Programming Interface (API) milik peralatan cisco *router* yang akan dibuat perangkat lunaknya yang berbasis web. Ini sangat penting dalam menentukan kesuksesan dalam pembuatan perangkat lunak untuk konfigurasi NAT statik. Setelah perangkat lunak selesai dibuat, selanjutnya diadakan pengujian untuk proses konfigurasi NAT statik pada *router cisco* seri 2600 pada jaringan komputer dalam LAN dan jaringan *server* yang terhubung ke internet. Dalam pengujian ini ada perangkat lunak tambahan yang digunakan, yaitu *wire shark*. Perangkat lunak ini digunakan untuk monitoring data dari dan ke *web server* yang akan diakses komputer melalui *router* yang ada NAT statik. Hasil pengujian dalam bentuk data kualitatif dan digunakan untuk penyusunan laporan pada publikasi, Metode yang digunakan selengkapnya dapat dilihat pada gambar 1.



Gambar 1. Metode penelitian yang dilakukan

3. Hasil dan Pembahasan

Hasil perancangan perangkat lunak berbasis web untuk konfigurasi NAT Statik dapat dilihat pada gambar 2. Perangkat lunak

ini lebih mudah penggunaannya dibandingkan dengan menggunakan *Command Line Interface* (CLI) karena penggunaan klik *mouse*, untuk membuat NAT pilih tombol *create* dan untuk menghapus NAT pilih tombol *delete*. Saat memilih *Create* pengguna perangkat lunak ini harus mengisi dua alamat IP yaitu : *private* dan *public* . Setelah proses pemasukan alamat IP maka selanjutnya dapat menekan tombol *submit* untuk mengeksekusi perintah *Create*. Implementasi aktivitas *Delete* sama hal seperti yang dilakukan pada aktivitas *Create*. Yaitu memasukkan *IP private* dan *IP public*, lalu menekan tombol "*submit*" untuk mengeksekusi perintah *Delete*.



Gambar 2. Perangkat lunak hasil perancangan

Fungsi tambahan dari perangkat lunak ini berupa menu pengisian dan penghapusan alamat IP untuk *interface fast ethernet* yang ada pada peralatan jaringan komputer yang dikonfigurasi menggunakan perangkat lunak ini. Fungsi lainnya yang tidak kalah penting yaitu fungsi untuk menampilkan hasil konfigurasi NAT statik atau dinamik yang telah dilakukan pada peralatan jaringan komputer berupa *router* yang dapat dilihat pada gambar 3.

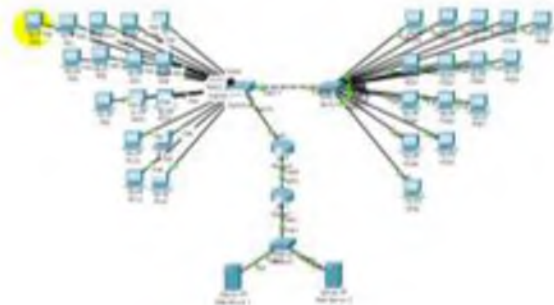


Gambar 3. Tampilan hasil pembuatan NAT yang digunakan pada *router*

3.1 Pengujian pada Jaringan LAN

Perangkat lunak hasil perancangan dalam penelitian ini diujikan pada jaringan komputer yang menggunakan *router* cisco seri 2600 untuk melayani dua buah *server* dan 30 komputer dalam jaringan LAN. Desain jaringan untuk pengujian dibuat menggunakan *packet tracer* yang sesuai dengan kondisi yang ada pada laboratorium komputer yang digunakan

dalam pengujian ini. Komputer yang didalamnya ada perangkat lunak hasil penelitian diletakan pada jaringan komputer seperti terlihat pada gambar 4 dengan diberi warna kuning.



Gambar 4. Jaringan komputer di laboratorium komputer yang digunakan untuk pengujian

Router 0 menggunakan dua alamat IP 30.30.30.1 untuk melayani 30 komputer dengan NA 30.30.30.0 dan alamat IP 10.10.10.30 untuk terhubung ke *router 1* yang memiliki alamat IP 10.10.10.40. Alamat IP yang lainnya pada *router 1* digunakan untuk terhubung ke *server* dengan NA 20.20.20.0. *Server 1* berupa *web server* memiliki alamat 20.20.20.5 dan *server 2* merupakan *web server* kedua yang memiliki alamat IP 20.20.20.10. Konfigurasi jaringan komputer dalam pengujian ini digunakan untuk membuktikan bahwa perangkat lunak hasil penelitian dalam konfigurasi NAT yang berhasil memberikan akses ke *server 1* dan 2 pada 30 komputer yang ada di laboratorium.

3.2 Pengujian pada Jaringan Internet

Pengujian selanjutnya yang dilakukan untuk menguji perangkat lunak hasil rancangan dengan menerapkannya pada jaringan komputer yang menempatkan komputer 1 dan 2 dapat diakses orang lain melalui jaringan internet. Peralatan yang digunakan dalam pengujian ini digambarkan menggunakan *packet tracer* seperti terlihat pada gambar 5. Web Server 1 merupakan komputer 1 memiliki alamat IP 11.11.11.88 dan Web Server 2 merupakan komputer 2 dengan alamat IP 11.11.11.80 melalui switch terhubung ke cisco *router 2600* series dengan alamat IP 11.11.11.2. Router ini terhubung ke router internet yang memiliki layanan koneksi internet dengan NA 10.10.10.0. PC0 merupakan komputer yang digunakan untuk mengakses web server 1 dan 2 melalui jaringan internet. Sedangkan PC1 yang diberi lingkaran kuning merupakan komputer yang didalamnya ada perangkat lunak yang hasil penelitian sekaligus beri perangkat lunak *wire shark* untuk pengamatan

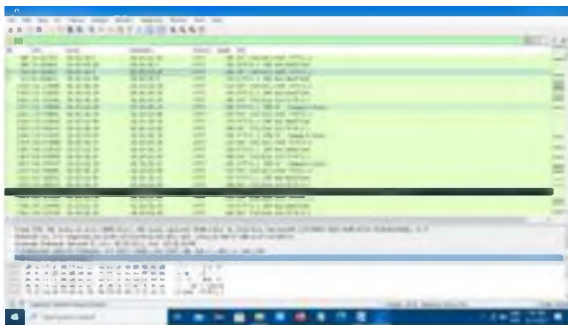


Gambar 5. Jaringan komputer yang digunakan untuk akses internet

3.3 Pembahasan

Data hasil pengujian untuk skema gambar 4 dan 5 didapatkan dengan meletakkan komputer yang didalamnya dipasang perangkat lunak untuk mendapatkan data hasil pengujian yaitu *wire shark*. Agar data dapat direkam dan diamati menggunakan *wire shark*, perlu dilakukan *port mirroring* dari port yang terhubung ke router ke arah port yang terhubung dengan komputer yang ada *wire shark*-nya. Untuk pembuatan atau konfigurasi *port mirroring* dapat lihat dibawah ini :

1. Router#configure terminal
2. Router(config)#monitor session 1 source interface FastEthernet0/0
3. Router(config)#monitor session 1 destination interface FastEthernet0/1



Gambar 6. Data hasil perekaman menggunakan *Wire shark*

Hasil perekaman data menggunakan *wire shark* seperti terlihat pada gambar 6, dilakukan proses filtering untuk mendapatkan data yang lebih valid dengan memasukkan kata http pada *display filter*. Hasil perekaman tersebut kemudian dijadikan tabel agar mudah dilihat dan dibaca selengkapnya ada pada tabel 1.

Tabel 1 Hasil *Capture* Jaringan LAN di Switch-0

No	Source	Destination Web Server- 1	Web Server- 2	Protocol
1	30.30.30.5	✓	✓	HTTP
2	30.30.30.10	✓	✓	HTTP
3	30.30.30.15	✓	✓	HTTP

4	30.30.30.20	✓	✓	HTTP
5	30.30.30.25	✓	✓	HTTP
6	30.30.30.30	✓	✓	HTTP
7	30.30.30.35	✓	✓	HTTP
8	30.30.30.40	✓	✓	HTTP
9	30.30.30.45	✓	✓	HTTP
10	30.30.30.50	✓	✓	HTTP
11	30.30.30.55	✓	✓	HTTP
12	30.30.30.60	✓	✓	HTTP
13	30.30.30.65	✓	✓	HTTP
14	30.30.30.70	✓	✓	HTTP
15	30.30.30.75	✓	✓	HTTP
16	30.30.30.80	✓	✓	HTTP
17	30.30.30.85	✓	✓	HTTP
18	30.30.30.90	✓	✓	HTTP
19	30.30.30.95	✓	✓	HTTP
20	30.30.30.100	✓	✓	HTTP
21	30.30.30.105	✓	✓	HTTP
22	30.30.30.110	✓	✓	HTTP
23	30.30.30.115	✓	✓	HTTP
24	30.30.30.120	✓	✓	HTTP
25	30.30.30.125	✓	✓	HTTP
26	30.30.30.130	✓	✓	HTTP
27	30.30.30.135	✓	✓	HTTP
28	30.30.30.140	✓	✓	HTTP
29	30.30.30.145	✓	✓	HTTP
30	30.30.30.150	✓	✓	HTTP

30 komputer yang ada pada laboratorium komputer dengan NA 30.30.30.0 dapat mengakses web server sebanyak 2 buah yang diletakkan dibelakang router 1 seperti pada gambar 4 melalui perangkat lunak browser masing-masing komputer tersebut. Ketika browser mampu menampilkan halaman index.html dari web server maka akan diberi tanda centang (✓). Kemudian hasil ini dibandingkan dengan data yang didapat melalui *wire shark* seperti pada gambar 7. Setiap komputer dari 30 komputer memiliki alamat IP yang dibaca sebagai source, sedangkan alamat IP web server 1 dan 2 dibaca sebagai destination.



Gambar 7. Hasil show packet in new window pada *wire shark* dari alamat IP 30.30.30.5

Pada gambar 7 terlihat bahwa komputer yang mengakses *web server 1* menggunakan alamat IP 30.30.30.5 disalin alamatnya oleh NAT statis menjadi alamat 10.10.10.30 yang merupakan alamat dari interface milik router 0. Komputer lainnya jika mengakses *web server 2* akan disalin alamatnya menggunakan alamat IP 10.10.10.40 milik router 1 oleh NAT statis. Sehingga 30 komputer yang mengakses *web server 1* dan 2 melalui NAT statis yang dipasang pada router 0 akan menggunakan alamat IP dari 10.10.10.1 hingga 10.10.10.254 melalui perangkat lunak yang dihasilkan dari penelitian ini satu per satu dimasukkan dan diaktifkan melalui submit pada menu create.

Pada pengujian yang menggunakan jaringan komputer terhubung ke internet, dengan menggunakan dua buah *web server* seperti pada pengujian di jaringan LAN, didapatkan data bahwa kedua *server* tersebut dapat diakses oleh semua komputer yang terhubung ke jaringan internet. *Web server* yang diletakkan dibelakang router *web server* dapat diakses melalui browser komputer datanya dapat dilihat pada tabel 2.

Tabel 2. Hasil *Capture* jaringan internet menggunakan *Wire shark*

No	Alamat Komputer	Provider	Destination Web Server-1	Destination Web Server-2	Protocol
1	10.169.57.71	Telkomsel	✓	✓	HTTP
2	10.115.3.225	XI	✓	✓	HTTP
3	10.28.140.103	Tri	✓	✓	HTTP
4	10.120.78.53	Indosat	✓	✓	HTTP

Akses komputer dari jaringan internet menggunakan browser untuk membuka alamat *index.html* yang ada pada *web server 1* dan 2 yang terletak dibelakang router *web sever* dapat dilakukan oleh semua komputer dengan menggunakan provider apapun dengan syarat memiliki alamat IP public yang akan disalin menggunakan alamat IP milik router internet seperti terlihat pada gambar 5. Hal ini terjadi karena pada router internet diberi NAT statis dan *routing* statis dari alamat 0.0.0.0 dengan

subnet 0.0.0.0 ke NA 10.10.10.0. Pembuatan NAT statis dan *routing* statis dilakukan dengan menggunakan perangkat lunak hasil dari penelitian ini. Hanya perlu tambahan yang tidak begitu banyak agar akses menggunakan browser dengan memasukkan nama komputer *web server 1* dan 2, bukan alamat ip dari komputer tersebut melalui Domain Name *Server*.

Proses konfigurasi menggunakan perangkat lunak yang dihasilkan dari penelitian ini kemudian dibandingkan dengan CLI untuk pembuatan NAT Statis yang dapat dilihat pada tabel 3.

Tabel 3. Perbandingan Perangkat Lunak hasil penelitian dengan CLI

No	Jenis Aktivitas	CLI	Perangkat Lunak hasil Penelitian
1	Buat NAT	<ol style="list-style-type: none"> Router1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.30 Router1(config)#ip nat inside source static 30.30.30.5 10.10.10.10 Router1(config)#int fa0/0 Router1(config-if)#ip nat inside Router1(config-if)#exit Router1(config)#int fa0/1 Router1(config-if)#ip nat outside 	
2	Hapus NAT	<ol style="list-style-type: none"> Router1(config)#no ip route 0.0.0.0 0.0.0.0 10.10.10.30 Router1(config)#no ip nat inside source static 30.30.30.5 10.10.10.10 Router1(config)#int fa0/0 Router1(config-if)#no ip nat inside Router1(config-if)#exit Router1(config)#int fa0/1 Router1(config-if)#no ip nat outside 	

Pada tabel 3 terlihat bahwa untuk membuat NAT statis menggunakan perangkat lunak hasil penelitian hanya dibutuhkan memasukkan *ip address* pada kolom *ip local* dan *ip public* serta menekan tombol *submit* pada

menu. Sedangkan untuk menghapus NAT, masukan *ip address* pada kolom *ip local* dan *ip public* serta menekan tombol *submit*. Pada pembuatan NAT static menggunakan perintah melalui CLI, harus menggunakan perangkat lunak bantu untuk proses *console*, dapat menggunakan *teraterm* atau *winscp*. Proses pembuatan dan penghapusan harus mengetikkan 7 baris perintah untuk setiap komputer yang akan dihubungkan ke NAT, sehingga kalau ada 30 komputer maka waktu yang digunakan untuk pembuatan NAT menggunakan CLI semakin lama.

4. Kesimpulan

Konfigurasi NAT statik yang biasanya menggunakan perintah yang diketikkan menggunakan *keyboard* komputer pada *command line interface* dapat diubah dan digantikan menggunakan perangkat lunak berbasis web yang memanfaatkan *keyboard* dan klik *mouse*. Perangkat lunak yang dibuat pada penelitian ini terbukti dapat bekerja untuk pembuatan NAT baik statik atau dinamik melalui perangkat lunak *wire shark* yang memperlihatkan proses penyalinan alamat IP source menjadi alamat IP yang ada pada NA antar router yang saling terhubung. Sehingga dari 30 komputer dalam jaringan LAN dan semua komputer yang mengakses melalui jaringan internet 100% dapat mengakses web *server* yang ada dibelakang router NAT.

Referensi

- Adriant, M. F., & Mardianto, I. (2015). Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan. *Seminar Nasional Cendekiawan*, 224–228.
- Afrida, F. A., & Rahmatia, S. (2018). Analisis Internet Group Management Protocol (Icmp) Menggunakan Software Wireshark Dalam Layanan Live Streaming Iptv Pada Multi Service Access Network (Msan) Di Area Darmo, Surabaya. *Jurnal Al-Azhar Indonesia Seri Sains Dan Teknologi*, 4(4), 176–181.
- Ardianto, F., Alfaresi, B., & Darmadi, A. (2018). Rancang Bangun Load Balancing Dua Internet Service Provider (Isp) Berbasis Mikrotik. *Jurnal Surya Energy*, 3(1), 198–202.
- Ayuningtyas, A., Sudaryanto, S., & Cessara, D. D. (2020). Sistem Manajemen Virtual Local Area Network (Vlan) Pada Cisco Catalyst 3750 Berbasis Web. *Jurnal Simetris*, 11(1), 297–306.
- Diansyah, T. M. (2015). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark. *Jurnal Times*, 1v(2), 20–23.
- Fauzi, M. F., Nugroho, K., & Wahyudi, E. (2018). Analisis Performansi Routing Protocol Ospf Dengan Metode Translasi Nat-Pt Ipv4 / Ipv6. *Proceedings On Conference On Electrical Engineering, Telematics, Industrial Technology, And Creative Media*, 351–353.
- Ginting, E. S., Suroso, & Hadi, I. (2020). Pengujian Konfigurasi Otomatis Penambahan Gateway Pada Virtual Router Menggunakan Aplikasi Otomatisasi Jaringan Berbasis Web. *Jurnal Media Informatika Budidarma*, 4(4), 1126–1131. <https://doi.org/10.30865/Mib.V4i4.2485>
- Natali, J., Fajrillah, F., & Diansyah, T. M. (2016). Implementasi Static Nat Terhadap Jaringan Vlan Menggunakan Ip Dynamic Host Configuration Protocol (Dhcp). *Jurnal Ilmiah Informatika*, 1(1), 51–58.
- Octafian, D. T. (2016). Sistem Pencegah Flooding Data Pada Jaringan Komputer. *It Journal*, 4(2), 163–169.
- Pambudi, R., & Muslim, M. A. (2017). Implementasi Policy Base Routing Dan Failover Menggunakan Router Mikrotik Untuk Membagi Jalur Akses Internet Di Fmipa Unnes. *Jurnal Teknologi Dan Sistem Komputer*, 5(April), 57–61. <https://doi.org/10.14710/Jtsiskom.5.2.2017.57-61>
- Rachmawan, D., Irwan, D., & Argyawati, H. (2016). Penerapan Teknik Load Balancing Pada Web Server Lokal Dengan Metode Nth Menggunakan Mikrotik. *Jurnal Penelitian Ilmu Komputer, System Embedded & Logic*, 4(2), 98–108.
- Rahman, T., Sumarna, & Nurdin, H. (2020). Analisis Performa Routers Mikrotik Pada Jaringan Internet. *Inovtek Polbeng - Seri Informatika*, 5(1), 178–192.
- Tedyyana, A., & Kurniati, R. (2016). Membuat Web Server Menggunakan Dinamic Domain. *Jurnal Teknologi Informasi & Komunikasi Digital Zone*, 7(1), 1–10.
- Tujini, B., & S, P. A. (2019). Implementasi Dynamic Nat Dan Ip Dhcp Pada Jaringan Vlan Menggunakan Simulasi Packet Tracer. *Seminar Hasil Penelitian Vokasi (Semhavok)*, 1(1), 109–116.
- Tutang, Tutuko, A., & Rosyidin, K. (2015). Implementasi Network Address Translation (Nat) Menggunakan Kerio Control Versi 7.4.1 Di Pusat Penelitian Bioteknologi – Lipi. *Baca: Jurnal Dokumentasi Dan Informasi*, 36(1), 97–108.
- Wiryawan, R. A., & Rosyid, N. R. (2019). Pengembangan Aplikasi Otomatisasi Administrasi Jaringan Berbasis Website Menggunakan Bahasa Pemrograman Python. *Jurnal Simetris*, 10(2), 741–752.

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU PEER REVIEW
KARYA ILMIAH : JURNAL ILMIAH

Judul Karya Ilmiah (Artikel) : Analisis Pengaruh Konfigurasi Network Address Translator (NAT) Statik Berbasis Web Menggunakan Wire Shark

Penulis Jurnal Ilmiah : Hero Wintolo, Salam Aryanto, Muhamad Hafish

Identitas Jurnal Ilmiah : a. Nama Jurnal : Jurnal Informatika
b. Nomor/Volume : 1/8
c. Edisi (bulan/tahun) : April 2021
d. Penerbit : UBSI
e. url dokumen : <https://ejournal.bsi.ac.id/ejurnal/index.php/ii/article/view/10166/pdf>

Hasil Penilaian Peer Review :

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah										Nilai Akhir Yang Diperoleh	
	Internasi onal Bereput asi	Internasional	Nasio nal Terakredita si	Nasiona l Tidak Terakre ditasi	Nasio nal Terin deks DOAJ	Jurnal Nasional Terakreditasi Kemristekdikti Peringkat						
						1	2	3	4	5	6	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
a. Kelengkapan unsur isi buku (10%)									2			1,6
b. Ruang lingkup dan kedalaman pembahasan (30%)									6			4,8
c. Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)									6			4,8
d. Kelengkapan unsur dan kualitas penerbit (30%)									6			4,8
Total = (100%)									20			
Kontribusi Pengusul (Penulis Kedua dari Tiga Penulis)												(60% x 16 = 9,6)
Komentar Peer Review	1. Tentang kelengkapan unsur isi buku <u>Editorial & isi buku lengkap sesuai standar jurnal</u> 2. Tentang ruang lingkup dan kedalaman pembahasan <u>penulisan ditulis cukup mendalam</u> 3. Tentang kecukupan dan kemutakhiran data/informasi dan metodologi <u>data & informasi cukup lengkap - metodologi juga cukup mutakhir</u> 4. Tentang Kelengkapan unsur dan kualitas penerbit <u>Kualitas penerbit buku, unsur lengkap dan dapat diakses online</u>											

Yogyakarta, 08 - 11 - 2021

Reviewer 1

(Signature)
 Suhirman, Ph.D
 Unit Kerja: ST-UTY

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU PEER REVIEW
KARYA ILMIAH : JURNAL ILMIAH

Judul Karya Ilmiah (Artikel) : Analisis Pengaruh Konfigurasi Network Address Translator (NAT) Statik Berbasis Wi Menggunakan Wire Shark

Penulis Jurnal Ilmiah : Hero Wintolo, Salam Aryanto, Muhamad Hafish

Identitas Jurnal Ilmiah : a. Nama Jurnal : Jurnal Informatika
b. Nomor/Volume : 1/8
c. Edisi (bulan/tahun) : April 2021
d. Penerbit : UBSI
e. url dokumen : <https://ejournal.bsi.ac.id/ejournal/index.php/ii/article/view/10166/pdf>

Hasil Penilaian Peer Review :

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah										Nilai Akhir Yang Diperoleh	
	Internasi onal Bereput asi <div><input type="checkbox"/></div>	Internasional <div><input type="checkbox"/></div>	Nasio nal Terakredita si <div><input type="checkbox"/></div>	Nasiona l Tidak Terakre ditasi <div><input type="checkbox"/></div>	Nasio nal Terin deks DOAJ <div><input type="checkbox"/></div>	Jurnal Nasional Terakreditasi Kemristekdikti Peringkat						
						1	2	3	4	5	6	
						<div><input type="checkbox"/></div>	<div><input type="checkbox"/></div>	<div><input type="checkbox"/></div>	<div>v</div>	<div><input type="checkbox"/></div>	<div><input type="checkbox"/></div>	
a. Kelengkapan unsur isi buku (10%)									2			1,5
b. Ruang lingkup dan kedalaman pembahasan (30%)									6			4,6
c. Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)									6			4,6
d. Kelengkapan unsur dan kualitas penerbit (30%)									6			4,6
Total = (100%)									20			15,4
Kontribusi Pengusul (Penulis Kedua dari Tiga Penulis)												(60% x 15,4 9,24
Komentar Peer Review	<div>1. Tentang kelengkapan unsur isi bukuterdapat benang merah antara topik, latar belakang, metode, hasil pembahasan serta kesimpulan</div> <div>2. Tentang ruang lingkup dan kedalaman pembahasankontribusi hasil penelitian terdapat dengan baik</div> <div>3. Tentang kecukupan dan kemutakhiran data/informasi dan metodologi.....Metadologi sesuai dan valid dalam proses pembahasan dan kesimpulan</div> <div>4. Tentang Kelengkapan unsur dan kualitas penerbit.....kelengkapan isi jurnal dan terbitan</div>											

Yogyakarta. 09 - 11 - 2021

Reviewer 2

(Dr. Enny Ite Sda, Ssi, M. Kom.)
Unit Kerja : Informatika - Ufy