

OPTIMASI WAKTU QUERY DAN FILTERING NAMA DOMAIN PADA DNS SERVER LOKAL MENGGUNAKAN BIND 9

Dian Novianto¹⁾

¹⁾Program studi Teknik Informatika STMIK Atma Luhur
Jl. Jendral Sudirman, Selindung Baru, Kec. Gabek Pangkalpinang Kode Pos 33117
Email : diannovianto@atmaluhur.ac.id¹⁾

ABSTRACT

DNS is made to facilitate users in accessing a website with a domain without having to continually update the files host.txt. DNS was developed in 1983, every user accessing a website using a domain name through a browser, will be routed by the router to a public DNS server to get a web address in the form of ip address. It takes time for DNS servers to reverse and lookup for translate domain names into ip addresses and vice versa. By creating a local DNS server as a cache, then it can be applied forwarding technique on DNS Server, so the time required to find the web server address of a destination website becomes faster. In addition to minimizing query time by implementing a local DNS server, can also be filtered against a particular domain name even though using a secure protocol like https by creating a zone for the web address you want to filter. So the use of the Internet becomes more useful. In this study the software used linux debian 8 as the operating system, and BIND9 as the software that runs the function of DNS Server.

Keywords : Forwarding DNS, BIND 9, Debian 8

1. Pendahuluan

Perkembangan teknologi informasi saat ini sudah sangat mendukung akan kebutuhan akan informasi, dimana seseorang yang membutuhkan sebuah informasi dapat langsung menggunakan perangkat yang mempunyai fasilitas untuk terhubung ke internet untuk mendapatkan informasi yang dibutuhkan. Dibidang komunikasi saat ini setidaknya ada 2 (dua) teknologi yang berkembang pesat, yaitu *smartphone* dan komputer berjaringan internet, yaitu komputer yang dapat menghubungkan seseorang dengan orang lain tanpa adanya batasan jarak dan waktu (Kasemin, 2015). Sistem yang baik merupakan sistem yang dapat bekerja secara efektif dan efisien, dimana saat seseorang sedang terhubung ke internet sistem jaringan yang dibangun harus mampu bekerja secara maksimal, cepat tetapi juga hemat dari sisi penggunaan *bandwidth*. Terlebih *bandwidth dedicated* yang harganya lebih mahal dibandingkan dengan harga internet *non dedicated* (*Up To*) sehingga harus dimanfaatkan sebaik mungkin. STMIK Atma Luhur Pangkalpinang merupakan salah satu perguruan tinggi yang bergerak di bidang pendidikan khususnya di bidang Teknologi Informasi, yang memiliki jumlah dosen tetap sebanyak 54 orang, dan jumlah mahasiswa sebanya 1.286 orang (ristekdikti, 2017). Sehingga perlu dirancang sebuah sistem jaringan yang mampu mengakomodasi kebutuhan informasi dari pengguna yang cukup besar tersebut. permasalahan yang timbul pada *router* selama ini adalah setiap pengguna meminta layanan untuk terhubung ke sebuah alamat *website*, maka *router* akan mencari DNS *server* keluar untuk mendapatkan alamat dari *website* yang ingin dituju atau *resolving* oleh pengguna, hal ini membutuhkan waktu lebih dan *bandwidth*, terlebih apabila *website* tersebut merupakan *website* yang sering di akses oleh banyak pengguna, oleh karena itu diperlukan sebuah sistem yang mampu mengatasi masalah ini, membangun

sebuah *cache site* yang besar, sehingga dapat menampung informasi alamat dari website yang pernah maupun sering diakses, agar semua permintaan *resolve dns* sebuah *website* yang di akses akan langsung diarahkan ke *cache dns* lokal untuk mencari informasi alamat *website* tersebut sehingga *router* dapat langsung meneruskan permintaan akses ke *web server* tujuan yang sudah diketahui informasi alamatnya, selain itu pentingnya untuk melakukan filtering terhadap akses internet karena menurut data trafik filtering lewat jaringan DNS Nawala, tiap hari tercatat satu juta akses ke halaman situs negatif yang diblokir di Indonesia. Itu artinya, kurang lebih ada satu juta orang yang meminta akses ke situs negatif (Chandraratuna dan Nur Ngazis, 2013). Dengan membuat zone palsu untuk nama domain dari website tertentu, maka secara otomatis website tersebut akan terfilter, sehingga penggunaan internet dapat menjadi lebih bermanfaat dan tidak melanggar kebijakan internet sehat yang telah ditetapkan.

A. Metodologi Penelitian

Metode yang digunakan dalam penelitian ini menggunakan metode kualitatif. Penelitian kualitatif disebut juga penelitian natural karena data pada penelitian ini bersifat alami atau natural, peneliti sebagai alat penelitian yang artinya peneliti sebagai alat utama pengumpulan data (Rahmat, 2009). Pada penelitian ini sumber data didapat dari hasil observasi terhadap sistem yang sedang berjalan. Pada proses ini lokasi penelitian dilakukan di bagian sistem informasi STMIK Atma Luhur divisi jaringan, karena bagian inilah yang bertanggung jawab terhadap akses internet di lingkungan kampus STMIK Atma Luhur. Metode pengembangan sistem yang digunakan adalah NDLC (*Network Development Life Cycle*) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan

aplikasi, dan analisis pendistribusian data. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan bisnis strategis (<https://sites.google.com/a/student.unsika.ac.id/metodepenelitian-owl>, diakses tanggal 4 desember 2017). Pada metode ini ada 6 tahapan yang harus dilalui, antara lain: Analisa, Desain, simulasi Prototipe, implementasi, monitoring dan manajemen (Stiawan, 2009). Tahapan analisa yang dilakukan adalah pengumpulan data dengan cara observasi sistem yang berjalan di bagian sistem informasi STMIK Atma Luhur divisi jaringan seperti perangkat lunak dan perangkat keras yang digunakan serta konfigurasi jaringan.

Tabel 1. Perangkat yang telah digunakan

Perangkat Lunak	Perangkat Keras
Debian 8 Squid 3. Iptables 1.414 Dhcp versi 2	Satu ML 30G9-069 paket SMB Server hp Proliant

Tabel 2. Perangkat tambahan

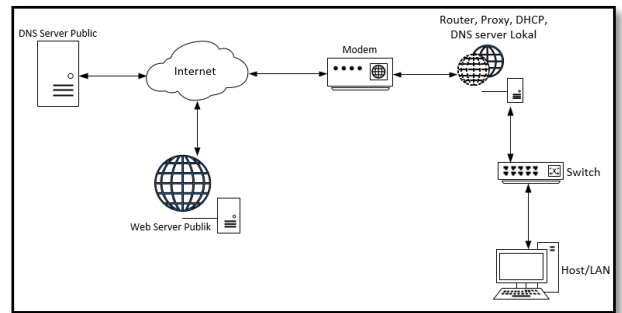
Perangkat Lunak
BIND 9.8.4

Pada tahapan analisa diketahui juga bahwa konfigurasi pada router terdapat *dhcp server* yang berfungsi membagi alamat ip untuk pengguna di jaringan LAN dengan media kabel yang *mac address* nya telah didaftarkan, karena *dhcp server* akan memberikan alamat ip statik sesuai dengan urutan pendaftaran *mac address* dimulai dari 192.168.0.2 dan alamat tersebut tidak dapat diubah, karena terdapat juga *filter* untuk *mac address* agar pengguna tidak bisa merubah ip address yang telah diberikan oleh *dhcp server*, sehingga apabila terdapat perubahan pada *mac address* pengguna harus mendaftarkan ulang perangkat, *filtering mac address* ini menggunakan perangkat lunak *iptables*.

Tabel 3. Data Alamat IP

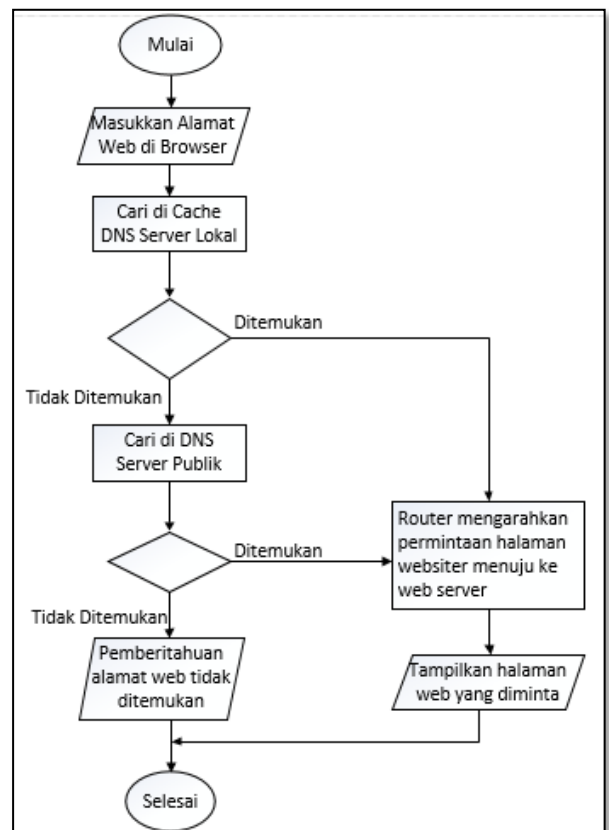
Nama konfigurasi	Keterangan
IP Address Public Router	103.94.xxx.98
Gateway Public Router	103.94.xxx.97
IP Address Private Router	192.168.0.1
IP Address LAN	192.168.0.2 – 192.168.xx.xx
Gateway LAN	192.168.0.1
DNS LAN	8.8.8.8 dan 8.8.4.4

Dari data alamat IP diatas dapat di lihat bahwa DNS LAN yang diberikan oleh DHCP server merupakan alamat DNS server publik yang dimiliki oleh perusahaan Google yang hanya bisa diakses melalui internet. Pada tahapan desain, yang dilakukan adalah membuat rancangan topologi, rancangan topologi ini nantinya yang akan digunakan dalam uji coba *forwarding* dan *filtering nama domain*, seperti gambar dibawah ini :

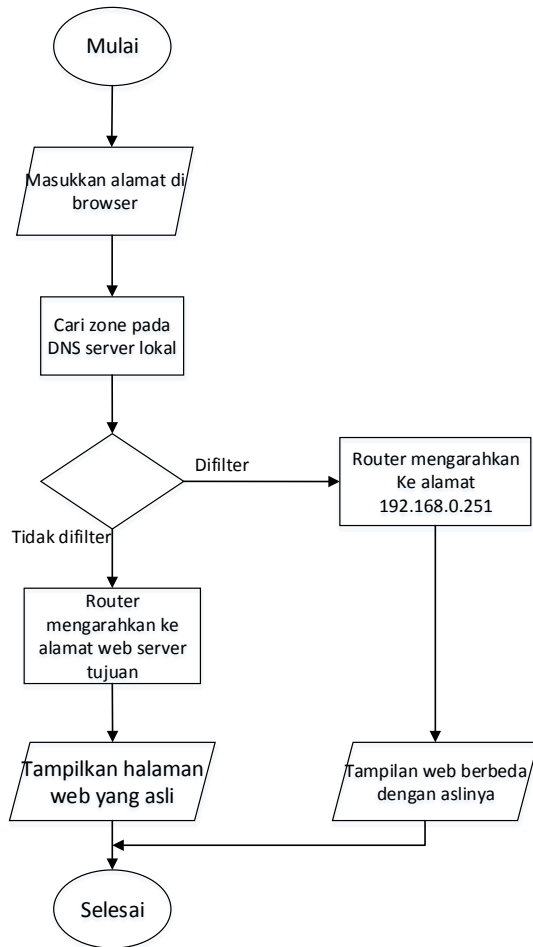


Gambar 1. Desain Topologi

Dimana DNS untuk pengguna LAN yang didapat dari DHCP akan berubah dari 8.8.8.8 dan 8.8.4.4 menjadi 192.168.0.1 sesuai DNS server lokal, yang menjadi satu dengan router yang juga sebagai *proxy* dan *DHCP server*. Sedangkan untuk DNS server publik pada router tetap diarahkan ke DNS server publik google, yaitu 8.8.8.8. dan 8.8.4.4. Pada tahapan yang ketiga, yaitu simulasi dan prototipe akan digambarkan menggunakan aplikasi visio 2013 berupa alur sistem atau *flowchart*, untuk menggambarkan bagaimana sistem akan bekerja nantinya.



Gambar 2. Flowchart forwarding DNS



Gambar 3. Flowchart filtering DNS

Pada tahapan simulasi ini diharapkan sistem nantinya akan bisa menangani semua permintaan DNS oleh pengguna dalam waktu yang relatif singkat, dengan cara melakukan *caching* alamat di DNS server lokal, sehingga pengguna lain yang mengakses alamat yang sama dapat langsung diarahkan ke *web server* tujuan. Akan tetapi jika alamat *website* tidak ditemukan di *cache* DNS, maka akan diarahkan ke DNS server publik sesuai dengan hirarkinya. Jika tetap tidak ditemukan, maka pengguna akan mendapatkan pemberitahuan bahwa server tujuan tidak ditemukan pada aplikasi *browser* nya.

2. Pembahasan

Berhasil atau tidaknya sebuah sistem tergantung dari bagaimana sistem itu di rancang, apakah berjalan sesuai dengan kebutuhan pengguna sehingga menghasilkan nilai efektif dan efisien. *Forwarder* adalah fungsi *Domain Name System (DNS) server* pada jaringan yang meneruskan permintaan DNS untuk nama DNS eksternal ke *server* DNS di luar jaringan itu (microsoft, 2017). Pada tahapan implementasi, yaitu tahapan ke 4 dalam NDLC, penulis menggunakan perangkat lunak *bind9* sebagai aplikasi DNS server karena *bind9* memungkinkan konfigurasi *forwarding* menggunakan pernyataan *forward* dan *forwarder* baik pada tingkat global atau basis per zona dari berkas *named.conf* (Aitchison, 2011).

Dalam ujicoba ini ada beberapa langkah yang dilakukan untuk mengetahui kinerja dari konfigurasi yang dilakukan, antara lain menggunakan perintah: *ping*, *dig*, *nslookup*, *tracert*, dan akses melalui *browser*, yang berfungsi menguji DNS server lokal. Sedangkan domain *website* tujuan yang digunakan untuk uji coba adalah *kopertis2.or.id* dan *www.bwin.com* di perangkat *router* dan di pc pengguna.

Parameter yang digunakan untuk mengukur kinerja *forwarding* pada uji coba pertama ini yaitu apabila *resolv.conf* menggunakan ip dns lokal 192.168.0.1, menggunakan perintah *dig* pada sisi *router* dan *query time* akses ke alamat web untuk kedua kalinya lebih cepat dari akses pertama lalu dibandingkan dengan apabila *resolv.conf* pada *router* menggunakan ip DNS publik 8.8.8.8, maka uji coba dianggap berhasil. Untuk mengetahui apakah penerapannya berhasil sesuai dengan analisa sebelumnya, dengan menggunakan teknik *forwarding* didapatkan hasil seperti gambar dibawah ini :

```

<<>> DiG 9.8.4-rpz2+r1005.12-P1 <<>> www.kopertis2.or.id
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 163
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.kopertis2.or.id.      IN      A

;; ANSWER SECTION:
www.kopertis2.or.id.    299     IN      A      45.64.1.156

Query time: 274 msec
SERVER: 192.168.0.1#53(192.168.0.1)
WHEN: Thu Dec 14 20:00:56 2017
MSG SIZE rcvd: 53
  
```

Gambar 4. Query time DNS lokal satu

Didapatkan hasil *query time* sebesar 274 ms, dan hasil ini akan dibandingkan dengan ujicoba selanjutnya. Pada pengujian kedua dilakukan untuk melihat perbedaan yang ada, dengan pengujian pertama dengan tetap menggunakan perintah *dig* pada *router* dengan alamat *www.kopertis2.or.id*, seperti gambar dibawah ini:

```

<<>> DiG 9.8.4-rpz2+r1005.12-P1 <<>> www.kopertis2.or.id
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 36212
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.kopertis2.or.id.      IN      A

;; ANSWER SECTION:
www.kopertis2.or.id.    270     IN      A      45.64.1.156

Query time: 0 msec
SERVER: 192.168.0.1#53(192.168.0.1)
WHEN: Thu Dec 14 20:01:25 2017
MSG SIZE rcvd: 53
  
```

Gambar 5. Query time DNS lokal dua

Hasil nya *query time* sebesar 0 ms, kemudian selanjutnya Penulis juga dua kali menguji sekenario jika tidak menggunakan konsep *forwarding* DNS, dimana permintaan alamat DNS langsung diarahkan ke DNS server publik 8.8.8.8 yang dimiliki oleh perusahaan google oleh *router*, seperti gambar dibawah ini:

```

;<<> DiG 9.8.4-rpz2+r1005.12-P1 <<> www.kopertis2.or.id
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 64296
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.kopertis2.or.id.      IN      A

;; ANSWER SECTION:
www.kopertis2.or.id.     299     IN      A      45.64.1.156

;; Query time: 53 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Dec 14 20:14:15 2017
;; MSG SIZE rcvd: 53
    
```

Gambar 6. Query time DNS publik satu

Hasil query time menggunakan DNS server publik 8.8.8.8 pada ujicoba pertama sebesar 53 ms, selanjutnya dilakukan ujicoba kedua seperti gambar dibawah ini:

```

;<<> DiG 9.8.4-rpz2+r1005.12-P1 <<> www.kopertis2.or.id
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 37270
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.kopertis2.or.id.      IN      A

;; ANSWER SECTION:
www.kopertis2.or.id.     299     IN      A      45.64.1.156

;; Query time: 64 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Dec 14 20:14:19 2017
;; MSG SIZE rcvd: 53
    
```

Gambar 7. Query time DNS publik dua

Dari gambar diatas terlihat saat pengguna mengakses alamat yang sama untuk kedua kalinya, tetap diarahkan ke DNS publik dengan query time sebesar 64 milisecond. Selanjutnya ujicoba yang dilakukan menggunakan perintah ping dari sisi klien untuk melihat koneksi antara klien dan web server yang dituju seperti gambar dibawah ini:

```

C:\Users\vian>ping kopertis2.or.id

Pinging kopertis2.or.id [45.64.1.156] with 32 bytes of data:
Reply from 45.64.1.156: bytes=32 time=23ms TTL=57
Reply from 45.64.1.156: bytes=32 time=23ms TTL=57
Reply from 45.64.1.156: bytes=32 time=23ms TTL=57
Reply from 45.64.1.156: bytes=32 time=23ms TTL=57

Ping statistics for 45.64.1.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 23ms, Average = 23ms
    
```

Gambar 8. Ping kopertis2.or.id

Hasil dari ping terlihat bahwa perangkat pengguna dapat mengakses website tujuan yaitu kopertis2.or.id dengan alamat 45.64.1.156. Pada uji coba selanjutnya yang dilakukan dengan perintah nslookup dari sisi pengguna untuk mengetahui server yang menjawab permintaan dari DNS, seperti gambar dibawah ini:

```

C:\Users\vian>nslookup kopertis2.or.id
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
Name:   kopertis2.or.id
Address: 45.64.1.156

C:\Users\vian>_
    
```

Gambar 9. nslookup kopertis2.or.id

Terlihat bahwa koneksi pertama diarahkan ke server DNS lokal dengan alamat 192.168.0.1, kemudian

diteruskan ke alamat 45.64.1.56 sesuai dengan alamat saat dilakukan ujicoba sebelumnya.

Untuk filtering akses internet, dilakukan penambahan zone pada berkas named.conf.local dengan membuat zone untuk domain dari website yang ingin di filter. Database DNS memuat objek-objek yang disebut resource record (RR), setiap resource record digunakan sebagai pengenal sumberdaya tertentu seperti name server, dns zone adalah bagian dari database DNS yang memuat resource record dari satu domain (DNS namespace) (Utama, 2008). Zone pada DNS server lokal inilah yang akan mengarahkan permintaan klien terhadap alamat tertentu menuju alamat yang sudah diatur, yaitu 192.168.0.251. Dan untuk menghindari perubahan alamat DNS Server oleh pengguna, digunakan perintah :

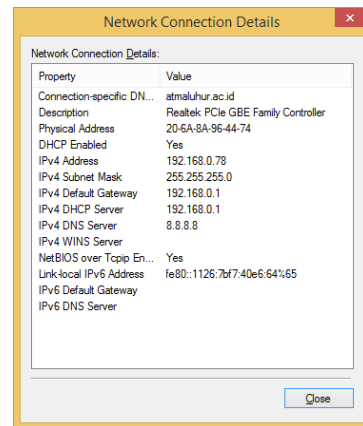
```

iptables -t nat -A PREROUTING -p tcp -m tcp --dport 53 -j DNAT --to-destination 192.168.0.1:53
    
```

```

iptables -t nat -A PREROUTING -p udp -m udp --dport 53 -j DNAT --to-destination 192.168.0.1:53
    
```

Perintah diatas berfungsi untuk mengalihkan setiap koneksi yang ingin mengakses port 53 yang menjalankan service DNS akan dialihkan ke alamat DNS server lokal secara otomatis, sehingga walaupun alamat DNS server pada perangkat pengguna menggunakan alamat DNS server publik seperti 8.8.8.8, filtering tetap dapat bekerja dengan baik. Konfigurasi pada pc pengguna seperti gambar dibawah ini:



Gambar 10. Informasi IP address Pengguna

Ada beberapa parameter yang digunakan dalam uji coba filtering ini untuk menyatakan bahwa filtering berjalan dengan baik.

Tabel 3. Parameter yang digunakan

DNS	Perintah Yang Digunakan			
	ping	nslookup	tracert	Akses browser
	Ya / Tidak	Ya / Tidak	Ya / Tidak	Ya / Tidak

Ya : apabila koneksi dialihkan ke 192.168.0.251 atau ter filter.

Tidak : apabila koneksi tetap diteruskan ke alamat asli atau gagal ter filter.

Pada uji coba pertama yang dilakukan adalah ping ke alamat uji coba untuk mengetahui komunikasi yang terjadi antara pengguna dengan server tujuan, seperti pada gambar dibawah ini:

```
C:\Users\vian>ping www.bwin.com

Pinging www.bwin.com [192.168.0.251] with 32 bytes of data:
Reply from 192.168.0.251: bytes=32 time=2ms TTL=64
Reply from 192.168.0.251: bytes=32 time=1ms TTL=64
Reply from 192.168.0.251: bytes=32 time=1ms TTL=64
Reply from 192.168.0.251: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\vian>
```

Gambar 11. Ping

Hasilnya zone mengarahkan komunikasi ke alamat 192.168.0.251, sesuai dengan konfigurasi. Uji coba yang kedua dilakukan menggunakan perintah nslookup seperti ditunjukkan oleh gambar hasil uji coba dibawah ini:

```
C:\Users\vian>nslookup www.bwin.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Name: www.bwin.com
Address: 192.168.0.251

C:\Users\vian>
```

Gambar 12. Nslookup

Hasilnya meskipun alamat DNS server pada sisi pengguna menggunakan alamat DNS publik 8.8.8.8, akan tetapi tetap saja domain name www.bwin.com diarahkan ke alamat 192.168.0.251. Selanjutnya pada uji coba ketiga yang dilakukan dengan perintah tracert, seperti gambar dibawah ini:

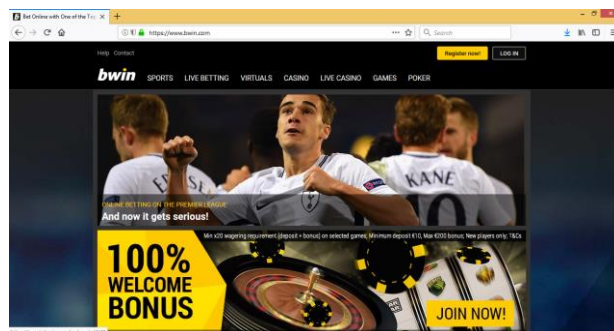
```
C:\Users\vian>tracert www.bwin.com

Tracing route to www.bwin.com [192.168.0.251]
over a maximum of 30 hops:

  0  1 ms  1 ms  1 ms  192.168.0.251
Trace complete.
```

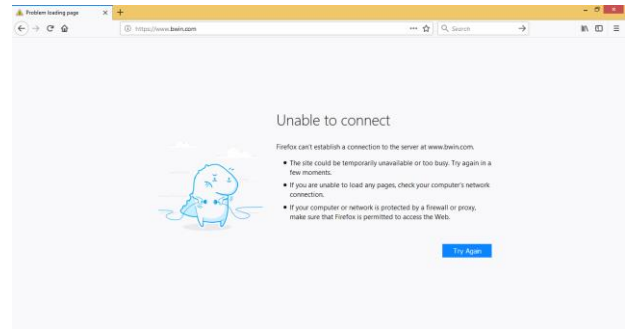
Gambar 13. Tracert

Hasilnya routing koneksi pengguna diarahkan ke alamat 192.168.0.251 oleh router. Sebelum dilakukan filtering, tampilan website dari www.bwin.com akan terlihat seperti gambar dibawah:



Gambar 14. Tampilan Sebelum Terfilter

Dalam uji coba yang ke empat dilakukan melalui browser, seperti gambar dibawah ini:



Gambar 15. Tampilan Sesudah Terfilter

Hasilnya browser tidak dapat menampilkan konten yang ingin diakses oleh pengguna, dengan notifikasi unable to connect. Hasil akhir dari keseluruhan uji coba terlihat dalam tabel dibawah ini:

Tabel 4. Hasil Uji Coba

DNS	Perintah Yang Digunakan			
	ping	nslookup	tracert	Akses browser
	Ya	Ya	Ya	Ya

Pada tahapan monitoring yang akan dilakukan adalah melihat logging dari sistem untuk mengetahui kinerja dari konfigurasi yang telah dijalankan, apakah ada pesan kesalahan dari sistem sehingga nantinya dapat menjadi bahan evaluasi.

```
root@InterLAN:~# systemctl status bind9.service
● bind9.service - LSB: Start and stop bind9
   Loaded: loaded (/etc/init.d/bind9)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Sat 2018-01-09 16:09:55 WIB; 2 days ago
   Process: 28693 ExecStop=/etc/init.d/bind9 stop (code=exited, status=0/SUCCESS)
   Process: 19956 ExecReload=/etc/init.d/bind9 reload (code=exited, status=0/SUCCESS)
   Process: 28704 ExecStart=/etc/init.d/bind9 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/bind9.service
            └─28712 /usr/sbin/named -u bind -f

Jan 12 15:05:30 InterLAN named[28712]: client 192.168.0.90#40552: RFC 1918 ...pa
Jan 12 15:05:56 InterLAN named[28712]: success resolving 'e13136.g.akamaied...ts
Jan 12 15:05:56 InterLAN named[28712]: success resolving 'negocco-ms-2025326...ts
Jan 12 15:05:56 InterLAN named[28712]: success resolving 'static.cookpad.co...ts
Jan 12 15:05:57 InterLAN named[28712]: success resolving 'api.c.avazunative...ts
Jan 12 15:09:44 InterLAN named[28712]: clients-per-query decreased to 13
Jan 12 15:10:36 InterLAN named[28712]: success resolving 'europe.pool.ntp.o...ts
Jan 12 15:10:47 InterLAN named[28712]: success resolving 'trkl.snt.inrworld...ts
Jan 12 15:12:19 InterLAN named[28712]: success resolving 'track.analytics-d...ts
Jan 12 15:12:46 InterLAN named[28712]: client 192.168.0.122#64581: RFC 1918...pa
```

Gambar 16. Log system

Dan pada tahapan manajemen yang akan dilakukan adalah mengatur domain lokal yang ada, baik untuk penambahan maupu penghapusan, serta pengaturan zone untuk filtering alamat domain website.

3. Kesimpulan

Berdasarkan hasil dari pengujian yang telah dilakukan bahwa DNS forwarding dapat diterapkan dengan baik pada router yang sekaligus sebagai DNS server lokal di jaringan STMIK Atma Luhur Pangkalpinang tanpa ada nya kendala, dan terbukti dapat menghemat proses pencarian alamat web server, dan menyimpan alamat tersebut kedalam cache DNS server lokal. Hasilnya dengan teknik forwarding di DNS server lokal 192.168.0.1, query time pertama sebesar 274 milisecond dan 0 milisecond untuk yang kedua, sedangkan tanpa

teknik *forwarding* didapat *query time* pertama sebesar 53 *milisecond* dan 64 *milisecond* untuk pengujian yang kedua. Selain itu juga *filtering* di DNS *server* lokal dapat memfilter akses ke *website* yang melanggar kebijakan penggunaan internet, meskipun *website* tersebut menggunakan protokol secure https, Hasilnya pengujian melalui perintah *ping*, *nslookup*, *tracert*, dan melalui browser menghasilkan parameter Ya yang artinya kesemua nya berhasil dan berjalan dengan baik.

Daftar Pustaka

- Aitchison Ron. 2011. Pro DNS and BIND 10. A Press: New York.
- Chandrataruna Muhammad dan Amal Nur Ngazis. <https://m.viva.co.id/digital/digilife/426514-1-juta-kali-hari-pengguna-internet-ri-akses-situs-negatif>, diakses tanggal 4 desember 2017.
- <https://sites.google.com/a/student.unsika.ac.id/metodepenelitian-owl>, diakses tanggal 4 desember 2017.
- Kasemin kasiyanto, 2015. Agresi Perkembangan Teknologi Informasi. Prenada Media Group: Jakarta.
- Microsoft. [https://technet.microsoft.com/en-us/library/cc730756\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730756(v=ws.11).aspx), diakses tanggal 4 Desember 2017.
- Rahmat Pupu Saeful. 2009. Penelitian Kualitatif. Equilibrium, 5(9). Pp:1-8.
- Ristekdikti. <http://forlap.ristekdikti.go.id>, diakses tanggal 4 desember 2017.
- Stiawan Deris. 2009. Fundamental Internetworking Development & Design Life Cycle. http://unsri.ac.id/upload/arsip/network_development_cycles.pdf. diakses 4 Desember 2017.
- Utama Irwin. 2008. Menguasai Active directory & Jaringan Windows server 2008. PT. Elex Media Komputindo: Jakarta.