OPTIMALISASI ROUTING MENGGUNAKAN SATU AUTONOMOUS SYSTEM NUMBER (ASN) BORDER GATEWAY PROTOCOL (BGP)

Muhammad Arif Zaky Zamany[1)], Hendra Supendar[2)], Sulistianto Sutrisno Wanda[3)]
[1,2,3]Prodi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri

Correspondence author: Sulistianto SW, sulistianto.sow@nusamandiri.ac.id, Jakarta, Indonesia

Abstract

Network routing that still uses two as numbers on the border gateway protocol, which allows the second as number to be a backup, which can be said to be ineffective. Moreover, the admin cannot know the backhoul network interference before monitoring a mass disturbance, so routing is switched manually. A Border Gateway Protocol is a path vector routing protocol that coordinates the routing of packets through multiple administrative domains by computing routes between every IP address the packet passes. Certain routers, called BGP speakers, are assigned to run the protocol. BGP speakers across different Autonomous Systems (AS) are interconnected in order to exchange routing information. BGP supports a feature called multihoming, which means connecting to multiple ISPs from different routers or points in the network. by using BGP one As Number, routing can choose the best or shortest path.

Keywords: network routing, BGP, autonomous, protocol

Abstrak

Pada *Network Routing* yang masih menggunakan dua *Autonomous System Number* pada *Border Gateway Protocol* yang memungkinkan *Autonomous System Number* kedua di jadikan *backup*, bisa dibilang tidak efektif. Terlebih lagi Admin tidak dapat mengetahui gangguan jaringan *backhoul* sebelum termonitor gangguan masal, sehingga *routing* dialihkan secara manual. *Border Gateway Protocol* adalah protokol jalur vektor yang mengkoordinasikan perutean paket melalui beberapa domain administratif dengan menghitung rute antara setiap alamat IP yang dilewati paket. *Router* tertentu, disebut *speaker BGP*, ditugaskan untuk menjalankan protokol. Dalam BGP, *Autonomous System* (AS) yang berbeda saling berhubungan untuk bertukar informasi *routing*. BGP mendukung fitur yang disebut *multihoming*, yang berarti menghubungkan ke beberapa ISP dari *router* atau titik yang berbeda dalam jaringan, dengan menggunakan BGP satu *Autonomous System Number*, routing bisa memilih jalur terbaik atau terpendek.

Kata Kunci: routing jaringan, BGP, autonomous, protokol

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

A. PENDAHULUAN

Dunia Perbankan saat ini membutuhkan informasi dan teknologi yang cepat dan tepat dalam menjalankan setiap transaksi nasabah yang sudah dapat dilakukan melalui *Internet Banking*, *Mobile Banking*, ATM, maupun langsung datang ke *Teller*/CS untuk menjalankan transaksi tersebut. Dalam menjalankan transaksi ini didukung oleh koneksi jaringan internet yang disediakan oleh masing-masing *Internet Service Provider* (ISP) yang bekerja sama dengan perbankan. Sehingga dengan adanya layanan internet dan perkembangan teknologi yang baik maka seluruh komponen transaksi akan berjalan dengan lancar.

Sebagaimana diketahui dengan perkembangan ilmu pengetahuan dan teknologi saat ini telah dikembangkan sistem yang dinamakan *Border Gateway Protocol* (BGP) yang berfungsi sebagai *switching* atau peralihan jaringan. Peralihan ini akan dilakukan jika pada jaringan utama mengalami gangguan.

BGP adalah protokol *routing* inti dari internet yg digunakan untuk melakukan pertukaran informasi *routing* antar jaringan. BGP bekerja dengan cara memetakan sebuah tabel IP *network* yang menunjuk ke jaringan yang dapat dicapai antar *Autonomous System (AS)* (Putra Yasa W, Rochim, & Christiyono, 2014). Menurut Paresmana (2009), *Border Gateway Protocol* (BGP) merupakan protokol *routing* standar yang bertujuan untuk memilih jalur *interdomain* yang berdasarkan pada *path vector* protokol. Fungsi utama BGP ini adalah mempertukarkan *network reachability* information antar *BGP router* dengan *router* BGP lain. *Autonomous System* merupakan suatu set *routing* dalam domain yang dikelola oleh satu otoritas sehingga pengaruhnya dapat langsung diketahui oleh *router* maupun *peer–router*. Dengan adanya informasi ini, dapat dibentuk grafik dari *AS path* yang saling terkoneksi sehingga dapat menghindari terjadinya *routing loop* (Nurhayati & Sulistianingsih, 2016).

Border Gateway Protocol (BGP) dapat diimplementasikan sebagai fungsi *switching routing* internet dari *main link* ke *backup link*. Dalam mengimplementasikan BGP ini, dibahas cara kerja BGP terhadap jaringan dalam mengatasi dan mengoptimalisasikan jaringan di dalam lingkungan perusahaan. Disamping itu juga dilakukan pembahasan peran utama BGP dalam jaringan internet, sehingga manfaat BGP berguna bagi kelancaran dan keamanan terhadap jaringan internet di perusahaan. Bagaimana merancang sistem dan mengimplementasikan BGP sebagai fungsi switching routing internet dari main link ke backup link. Ataupun load balance dari kedua ISP yang di gunakan dan jenis transmisinya.

Proses *routing* adalah suatu hal yang tidak bisa ditinggalkan oleh seorang admin jaringan. *Routing* merupakan teknik bagaimana menghubungkan komunikasi beberapa *router*. Sering ditemui seorang admin bingung dalam memilih jenis *routing* yang akan digunakan, karena masing masing *routing* memiliki kelebihan dan kekurangan. Parameter *packet loss* adalah salah satu kunci menentukan kinerja *routing* yang terbaik.

Kinerja sistem jaringan dengan menggunakan BGP lebih baik dibandingkan tanpa BGP. Perbandingan parameter rata-rata *latency* diperoleh nilai 0% (hampir tanpa *latency*) artinya kecepatan akses lebih cepat dibandingkan tanpa BGP, parameter *traceroute* (kontel lokal) 50% lebih baik dibandingkan tanpa BGP, namun untuk *traceroute* (kontel non lokal) memiliki nilai presentase yang sama hal ini dikarenakan seluruh *prefix* non lokal hanya didapatkan dari *port backbone* lama (Ernawati & Endrawan, 2018)

B. METODE PENELITIAN

Penelitian yang dilakukan dengan menggunakan metode penelitian eksperimental, berdasarkan pengalaman saat bekerja di PT. Bank Tabungan Pensiun Nasional dengan lokasi penelitian Jakarta. Pengumpulan data penelitian dilakukan dengan cara sebagai berikut:

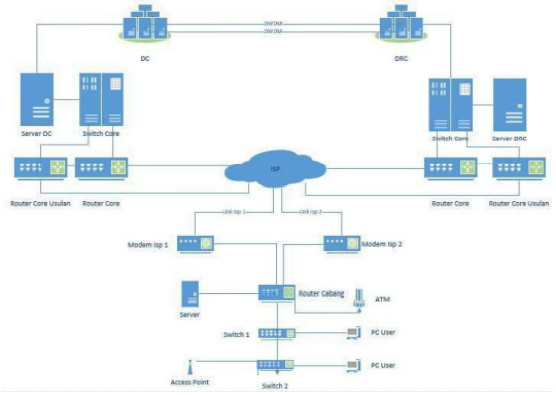
1. Metode Observasi dengan mengadakan observasi langsung di tempat penulis bekerja mulai 1 September hingga 30 Desember 2018, yang berkaitan langsung dengan monitoring lalu lintas data dari pusat ke cabang BTPN di seluruh Indonesia.
2. Metode Wawancara juga dilakukan untuk untuk menambah pengetahuan dan referensi dari pihak IT terkait untuk standart yang di gunakan.
3. Metode Studi Pustaka dilakukan dalam Pencarian langsung referensi terhadap landasan teori yang di gunakan selama eksperimen di Bank Tabungan Pensiun Nasional sebagai penunjang penelitian berkenaan dengan penelitian tentang *Border Gateway Protocol* (BGP) Menggunakan *Autonomous System* (AS).

C. HASIL DAN PEMBAHASAN

Topologi Jaringan

Topologi jaringan komputer adalah teknis, cara, dan aturan di dalam merangkai dan menghubungkan berbagai komputer dan perangkat terhubung lainnya ke dalam sebuah jaringan komputer, sehingga membentuk sebuah hubungan yang bersifat geometris (Pratama & Arief, 2015).

Pada penelitian ini, topologi jaringan menggunakan topologi yang sama, hanya mengusulkan untuk mengaktifkan 1 *router core* cadangan yang selama ini menjadi *backup* pada DC dan DRC untuk memisahkan 2 *provider* (Indosat dan Icon+) yang sering kali gangguan dan menyebabkan *flaping* sehingga mempengaruhi *link* lainnya, di hubungkan dengan IP *peer to peer* /30.



Gambar 1. Topologi Usulan

Router yang ada

```
JKT-MB-011DC-NR001-WM001#sh run int Gi0/1/1
Building configuration...

Current configuration : 231 bytes
!
interface GigabitEthernet0/1/1
 description LINK TO rO2-wm2-JKTMP
 ip address 10.1.127.245 255.255.255.252
```

Router Cadangan

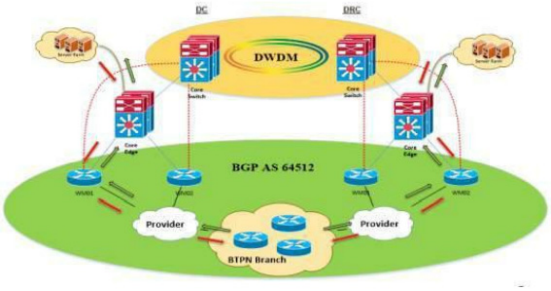
```
JKT-MB-011DC-NR002-WM002#sh run int Gi0/0/1
Building configuration...

Current configuration : 144 bytes
!
interface GigabitEthernet0/0/1
 description LINK to rO1-wm1-JKTMP
 ip address 10.1.127.246 255.255.255.252
```

Gambar 2. Konfigurasi *Peer to Peer Router Core*

Skema Jaringan

Pada skema jaringan, ada perubahan yang signifikan dan yang merupakan poin terpenting, yang sebelumnya menggunakan 2 *as number Border Gateway Protocol* yang di mana *as number* 64512 merupakan *main link* ke arah DC, mengusulkan untuk menghilangkan *as number backup* 64513 menjadi 64512 di DRC agar *load balance* ke ke dua *data center*.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

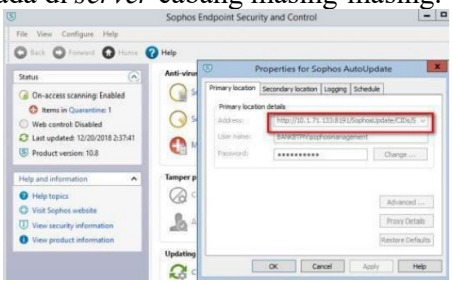


Gambar 3. Skema Usulan

Keamanan Jaringan

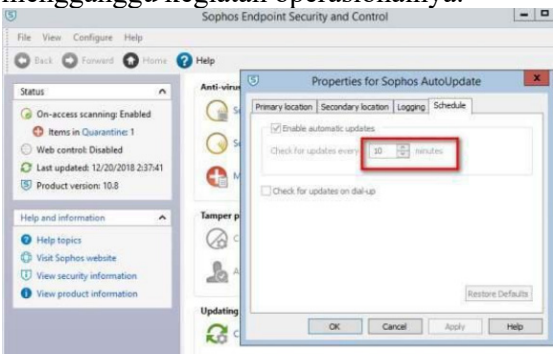
Menurut Internet Engineering Task Force (IETF), VPN merupakan suatu bentuk private internet yang melalui public network (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Prosedur enkripsi dilakukan terhadap data yang melalui VPN, sehingga keamanannya terjamin (Mulyadin, Sholeh, & Iswahyudi, 2016).

Di samping jaringan VPN sudah termasuk cukup aman untuk keamanan jaringan pada suatu jaringan yang cukup besar dan memiliki banyak *client*, di perlukan suatu mekanisme pengaturan jadwal *update* data manajemen *bandwidth*, di mana kendala *trafic full* sering terjadi saat jam-jam sibuk di karenakan suatu PC sedang update *windows* atau *antivirus*, disarankan untuk menggunakan *check point* pada satu PC di cabang yang kemudian PC *client* yang lain tinggal *update* di PC tersebut, sehingga tidak melakukan pemborosan *bandwidth* ke tiap-tiap PC. Dari gambar di bawah ini adalah *default check point* yang masih berada di *server*, *capture* ini disarankan hanya untuk *server* di cabang saja, untuk *client* lokasi *check point* nya berada di *server* cabang masing-masing.



Gambar 4. Check Point Anti Virus

Manajemen *bandwidth link* ke cabang ataupun *link* ke PC, untuk *update antivirus* nya di jadwalkan otomatis setiap hari pada jam setelah *office hour* agar tidak mengganggu kegiatan operasionalnya.



Gambar 5. Jadwal *Update* Anti Virus

Rancangan Aplikasi

Aplikasi yang digunakan untuk membandingkan konfigurasi usulan ini adalah dengan *secure* CRT untuk masuk ke CLI konfigurasi dari *router* yang nantinya dapat di lihat pada pengujian awal dan akhir, selain itu PRTG *traffic grapher* dan *ping ploter* juga digunakan untuk mengetahui *bandwidth* keluar masuk dan monitoring *availability link* serta *routing* per *hoop* bisa di ketahui.

Manajemen Jaringan

Menurut (Azza Roisatul, 2016) Manajemen Jaringan adalah suatu usaha untuk memelihara seluruh sumber jaringan dalam keadaan baik. Karena saat ini jaringan sangat kompleks, dinamika dan terdiri atas kompenen yang tidak dapat diandlkan, peralatan yang baik diperlukan untuk mengelola jaringan tersebut (Azzha, 2016).

Untuk manajemen jaringan merekomendasikan cabang yang memiliki lebih dari satu *link* untuk menggunakan *link* dengan berbeda jenis transmisi, seperti Metro – Mpls, Fiber Optik – tembaga – Radio, ataupun ditanyakan terlebih dahulu ke pada *provider* jalur mana yang di gunakan untuk meminimalisir gangguan

yang di sebabkan kerusakan di daerah tertentu secara bersamaan. Juga bisa menanyakan kepada *provider* apakah ada jalur *backup* ataupun kesepakatan lain bila *link* terlalu lama di perbaiki.

Pengujian Jaringan

Pada tahap pengujian jaringan, membandingkan proses pengujian pertama adalah sebelum di masukan rancangan usulan dengan sesudah rancangan usulan dengan *traceroute* guna mengetahui perbedaan *hoop* yang di lewati sebelum dan sesudahnya. Di uji langsung di jaringan BTPN yang aktif dengan mengambil beberapa contoh sample cabang yang berbeda dari sisi jenis transmisi, *bandwidth* dan perangkat yang di gunakan. Membedakan tampilan awal (*background* putih) dan tampilan usulan (*background* hitam).

Pengujian Awal

Awal Pengujian jaringan awal di mulai dengan konfigurasi *border gateway protocol* di sisi *router* cabang dan sisi *backhoul* dengan *as number* awal *backhou*l 64512 dan 64513, juga akan membahas *tunneling* untuk mengalokasikan *bandwidth* yang tersedian dengan membagi antara aplikasi *core banking* dan aplikasi *transaksional* lainnya.

Berikut beberapa *capture* pada tahap pengujian awal, membedakan tampilan awal (*background* putih) dan tampilan usulan (*background* hitam) :

a. Pengujian *border gateway protocol* dengan dua *as number*
   Capture di bawah ini menjelaskan *as number border gateway internal* di *router* 64534 dengan dua provider berbeda Indosat dan Telkom. Masih menggunakan dua *as number* yang berbeda 64512 dan 64513 untuk ke masing- masing *backhoul* nya.

```
r-0021-01#sh run | s router bgp
router bgp 64534
 bgp log-neighbor-changes
 network 10.66.134.0 mask 255.255.255.248
 network 10.66.134.127 mask 255.255.255.255
 network 10.66.134.128 mask 255.255.255.128
 network 10.66.201.0 mask 255.255.255.248
 network 10.66.201.8 mask 255.255.255.248
 network 10.66.201.64 mask 255.255.255.224
 network 10.66.201.127 mask 255.255.255.255
 network 10.66.201.128 mask 255.255.255.128
 neighbor 10.130.64.1 remote-as 64512
 neighbor 10.130.64.1 description "DC-ICON+-0021"
 neighbor 10.130.64.1 filter-list 2 out
 neighbor 10.130.64.2 remote-as 64513
 neighbor 10.130.64.2 description "DC-ICON+-0021"
 neighbor 10.130.64.2 filter-list 1 out
 neighbor 10.131.0.1 remote-as 64512
 neighbor 10.131.0.1 description "DC-INDOSAT-0021"
 neighbor 10.131.0.1 filter-list 2 out
 neighbor 10.131.0.2 remote-as 64513
 neighbor 10.131.0.2 description "DR-INDOSAT-0021"
 neighbor 10.131.0.2 filter-list 1 out
 maximum-paths 2
```

Gambar 6. *Capture* Konfiguasi BGP Cabang

Router BGP 64534 adalah *as number BGP* di cabang Madiun 0021, menggunakan dua *network* 10.66.134.0/24 dan 10.66.201.x/24 yang di *advertice* ke *as number BGP* DC (64512) dan *as number* DR (64513). Dalam configurasi BGP tersebut IP 60 *gateway* Indosat 10.131.0.1 dan 10.130.64.2 masih *remote* ke *as number BGP* DRC 64513.

```
neighbor 10.131.0.49 remote-as 64534
neighbor 10.131.0.49 peer-group INDOSAT
neighbor 10.131.0.49 description "DC-INDOSAT-0021"

neighbor 10.130.64.20 remote-as 64534
neighbor 10.130.64.20 peer-group ICON
neighbor 10.130.64.20 description "DR-ICON+-0021"
```

Gambar 7. *Capture* Konfigurasi BGP Backhoul

Konfigurasi BGP di sisi *backhoul* DC dan DRC, sama persis hanya beda deskripsinya saja. IP yang di gunakan di cabang 10.131.0.49 dan 10.130.64.20, *remote* langsung ke *as number BGP* yang ada di cabang 64534. kemudian melakukan *traceroute* untuk aplikasi yang berada di DRC aplikasi / *server* yang ada di DRC memiliki IP 10.2.x.x seperti yang sudah di jelaskan sebelumnya, masih melewati

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

backhoul DC terlebih dahulu kemudian ke DRC menggunakan *link* DWDM. 10.131.0.1 dan 10.130.64.1 merupakan *gateway* dari *provider* Indosat dan Icon+ yang berada di DC.

```
r-0021-01#traceroute 10.2.71.118
Type escape sequence to abort.
Tracing the route to 10.2.71.118
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 172.31.127.14 16 msec
    172.31.127.6 16 msec
    172.31.127.14 16 msec
  4 172.31.88.2 20 msec 20 msec 20 msec
  5 172.31.5.34 20 msec 20 msec 20 msec
  6 172.31.5.14 80 msec 20 msec 20 msec
```

Gambar 8. *Capture Traceroute Server* DRC

```
r-0021-01#traceroute 10.1.0.7
Type escape sequence to abort.
Tracing the route to 10.1.0.7
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 172.31.127.2 72 msec
    172.31.127.6 16 msec
    172.31.127.2 16 msec
  4 172.31.1.30 16 msec
    172.31.1.22 16 msec
    172.31.1.30 16 msec
  5 172.31.1.42 20 msec 20 msec 20 msec
  6 10.1.0.7 [AS 64512] 20 msec 20 msec 28 msec
```

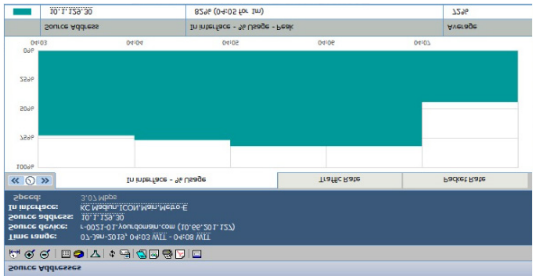
Gambar 9. *Capture Traceroute Server* DC

Bandingkan kedua *routing* di atas, saat akses Ke *server* yang berbeda *data center*, *gateway* nya tetap melewati DC.

```
r-0021-01#sh bgp sum
BGP router identifier 10.66.201.127, local AS number 64534
BGP table version is 62, main routing table version 62
17 network entries using 2516 bytes of memory
44 path entries using 2816 bytes of memory
7 multipath network entries and 14 multipath paths
15/5 BGP path/bestpath attribute entries using 2040 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
7 BGP filter-list cache entries using 112 bytes of memory
BGP using 7588 total bytes of memory
BGP activity 17/0 prefixes, 259/215 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.130.64.1     4        64512   45771   45766       62    0    0 4w0d            10
10.130.64.2     4        64513      10       6       60    0    0 00:00:20        8
10.131.0.1      4        64512    6009    6005       62    0    0 3d18h           10
10.131.0.2      4        64513       9       5       60    0    0 00:00:28        9
```

Gambar 10. *Capture* BGP Sum

b. Pengujian jaringan awal *tunneling*
Pengujian awal *tunneling* ini di khususkan untuk aplikasi *non core banking*, menggunakan *backup link* yang ada di cabang atau *persentase bandwidth* cabang yang di gunakan. Tidak ada konfigurasi sebelum di adakan *tuneling*, namun tetap mencoba *capture traceroute* dan *bandwidth* saat sebelum menggunakan *tunneling*.



Gambar 11. *Captrure Bandwidth* sebelum Penggunaan *Tunneling*

Sebelum menggunakan *tunnel*, aplikasi 10.1.129.30 (*server* DC) saat akses *traffic* hampir memenuhi *bandwidth* di cabang. Keuntungannya memang saat akses lebih cepat, namun saat akses aplikasi yang lebih *urgent* (aplikasi *core banking*) akan sangat terganggu bila di akses bersamaan.

```
r-0021-01#traceroute 10.1.129.30
Type escape sequence to abort.
Tracing the route to 10.1.129.30
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 10.1.134.1 [AS 64512] 16 msec 16 msec 20 msec
  4 10.1.128.2 [AS 64512] 20 msec 20 msec 16 msec
```

Gambar 12. *Capture Traceroute* sebelum Penggunaan *Tunnelling*

Dari *capture* di atas, sebelum penggunaan *tunneling*, *bandwidth* di dominasi beberapa menit oleh aplikasi *non core banking*. *Bandwidth* tersebut di peroleh saat mengirim dan menerima email, di sisi *routing* juga terlihat masih menggunakan *gateway* yang sama di DC 10.131.0.1 dan 10.130.64.1.

Pengujian Jaringan Akhir

Pada tahap pengujian jaringan akhir, akan memberikan beberapa konfigurasi

yang telah dicoba diterapkan untuk usulan pemecahan masalah tersebut. Konfigurasi pertama yang diubah adalah *as number border gateway protocol* yang berada di DRC dari 64513 ke 64512 (sama dengan *as number* di DC).

```
router bgp 64512
 bgp log-neighbor-changes
 network 10.1.0.0 mask 255.255.0.0
 network 10.2.0.0 mask 255.255.0.0
 network 10.5.0.0 mask 255.255.0.0
 network 10.64.0.0 mask 255.224.0.0
 network 10.66.197.104 mask 255.255.255.252
 network 10.107.0.176 mask 255.255.255.252
 network 172.67.0.16 mask 255.255.255.248
 network 172.68.0.16 mask 255.255.255.248
 network 192.168.32.0
 network 192.168.96.0
```

Gambar 13. *Captrure as number BGP* pada *Backhoul*

```
r-0021-01#sh run | s router bgp
router bgp 64534
 bgp log-neighbor-changes
 network 10.66.134.0 mask 255.255.255.248
 network 10.66.134.127 mask 255.255.255.255
 network 10.66.134.128 mask 255.255.255.128
 network 10.66.201.0 mask 255.255.255.248
 network 10.66.201.8 mask 255.255.255.248
 network 10.66.201.64 mask 255.255.255.224
 network 10.66.201.127 mask 255.255.255.255
 network 10.66.201.128 mask 255.255.255.128
 neighbor 10.130.64.1 remote-as 64512
 neighbor 10.130.64.1 description "DC-ICON+-0021"
 neighbor 10.130.64.1 filter-list 2 out
 neighbor 10.130.64.2 remote-as 64512
 neighbor 10.130.64.2 description "DC-ICON+-0021"
 neighbor 10.130.64.2 filter-list 1 out
 neighbor 10.131.0.1 remote-as 64512
 neighbor 10.131.0.1 description "DC-INDOSAT-0021"
 neighbor 10.131.0.1 filter-list 2 out
 neighbor 10.131.0.2 remote-as 64512
 neighbor 10.131.0.2 description "DR-INDOSAT-0021"
 neighbor 10.131.0.2 filter-list 1 out
 maximum-paths 2
```

Gambar 14. *Captrure as number BGP* pada Cabang

```
r-0021-01#sh bgp sum
BGP router identifier 10.66.201.127, local AS number 64534
BGP table version is 62, main routing table version 62
17 network entries using 2516 bytes of memory
44 path entries using 2816 bytes of memory
7 multipath network entries and 14 multipath paths
15/5 BGP path/bestpath attribute entries using 2040 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7476 total bytes of memory
BGP activity 17/0 prefixes, 259/215 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.130.64.1     4        64512   45807   45803       62    0    0 4w0d            10
10.130.64.2     4        64512     401     311       62    0    0 00:33:43         8
10.131.0.1      4        64512    6046    6042       62    0    0 3d19h           10
10.131.0.2      4        64512      45      42       62    0    0 00:33:51         9
r-0021-01#
```

Gambar 15, *Capture BGP* Sum sesudah

Berikut hasil *traceroute* aplikasinya :

```
r-0021-01#traceroute 10.2.71.118
Type escape sequence to abort.
Tracing the route to 10.2.71.118
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.2 16 msec 16 msec 20 msec
  2 10.2.194.2 [AS 64512] 20 msec 20 msec 20 msec
  3 172.31.127.109 20 msec 20 msec 20 msec
  4 172.31.5.34 20 msec 20 msec 20 msec
  5 172.31.5.14 20 msec 20 msec 20 msec
```

Gambar 16. *Traceroute* Aplikasi DRC Sesudah

Dapat terlihat dari *routing* di bandingkan sebelumnya, *hoop* yang di lewati lebih sedikit, karena tidak melewati DC terlebih dahulu. 10.131.0.2 adalah *gateway* dari Indosat yang berada di DRC.

Untuk pengujian *tunneling* mencoba mengkonfigurasi di *link* Icon+ karena dari hasil *traceroute* aplikasi *core banking* 10.1.0.7 mendahulukan *link* Indosat.

```
r-0021-01#sh ip ro 10.1.0.7
Routing entry for 10.1.0.0/16
  Known via "bgp 64534", distance 20, metric 96
  Tag 64512, type external
  Last update from 10.130.64.1 12:40:14 ago
  Routing Descriptor Blocks:
  * 10.131.0.1, from 10.131.0.1, 12:40:14 ago
      Route metric is 96, traffic share count is 1
      AS Hops 1
      Route tag 64512
      MPLS label: none
    10.130.64.1, from 10.130.64.1, 12:40:14 ago
      Route metric is 96, traffic share count is 1
      AS Hops 1
      Route tag 64512
      MPLS label: none
```

Gambar 17. Menampilkan *Link* yang Lebih Dominan

```
interface Tunnel0
 description ***Tunnel madiun 0021**
 bandwidth 1024
 ip address 10.107.2.38 255.255.255.252
 ip mtu 1500
 ip flow ingress
 ip flow egress
 ip nat outside
 ip virtual-reassembly in
 tunnel source 10.130.64.20
 tunnel destination 10.130.64.1
end
```

Gambar 18. Konfigurasi *Tunneling* di Cabang

Kemudian *static* kan IP aplikasi yang akan di alihkan ke *tunnel* 0, berikut konfigurasinya :

```
r-0021-01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r-0021-01(config)#ip route 10.1.129.30 255.255.255.255 Tunnel0 name EMAIL_Zimbra_DC
r-0021-01(config)#
```

Gambar 19. Konfigurasi IP *Static* ke *Tunneling* di Cabang

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Untuk *tunneling* sama dengan BGP, konfigurasi di dua sisi Cabang dan *backhoul*, kali ini hanya menggunakan *backhoul* sisi DC karena IP yang di coba adalah IP DC dan menggunakan *link* Icon+ karena *link* Indosat lebih dominan, bukan karena indosat *mainlink*. Karena di sini metro – metro adalah *loadbalance*.

```
interface Tunnel21
 description ***KC_Madiun Tunnel madiun 0021***
 bandwidth 1024
 ip address 10.107.2.37 255.255.255.252
 ip mtu 1500
 ip flow ingress
 ip flow egress
 keepalive 3 10
 tunnel source 10.130.64.1
 tunnel destination 10.130.64.20
end
```

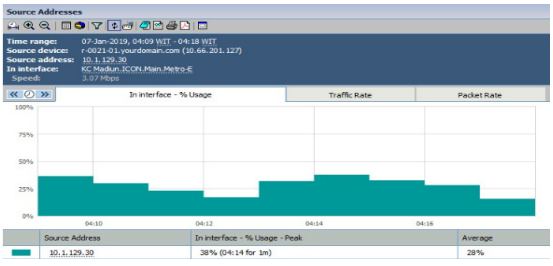
Gambar 20. Konfigurasi IP *Static* ke *Tunneling* di *Backhoul*

Berikut hasil dan bandingkan *traceroute* untuk IP aplikasi/*server* yang sudah di *static* kan ke *tunnel* :

```
r-0021-01#traceroute 10.1.129.30
Type escape sequence to abort.
Tracing the route to 10.1.129.30
VRF info: (vrf in name/id, vrf out name/id)
  1 10.107.2.37 20 msec
    10.107.15.5 20 msec
    10.107.2.37 20 msec
  2 10.1.2.6 [AS 64512] 20 msec
    10.1.2.10 [AS 64512] 20 msec
    10.1.2.6 [AS 64512] 20 msec
  3 10.1.134.1 [AS 64512] 20 msec 20 msec 20 msec
  4 10.1.128.2 [AS 64512] 20 msec 20 msec 20 msec
```

Gambar 21. Konfigurasi IP *Static* ke *Tunneling* di Cabang

Aplikasi *e-mail* 10.1.129.30 sudah melewati *tunnel*. Dan sementara *link* utama bebas dari *trafic* ip 10.1.129.30.



Gambar 22. *Netflow Trafic E-mail* sudah masuk ke Tunnel ke pusat (setelah pengujian)

D. PENUTUP

Hasil yang diperoleh setelah dilakukan analisa dan perancangan pembangunan jaringan komputer yang dibangun memberikan catatan penting dan kemungkinan perbaikan yang perlu dilakukan untuk pengembangan jaringan komputer selanjutnya.

Berdasarkan hasil riset pada PT. Bank Tabungan Pensiun Nasional (BTPN), menemukan beberapa permasalahan jaringan dan melakukan usulan jaringan dengan pengujian jaringan, yaitu :

1. Optimalisasi perangkat-perangkat jaringan di BTPN yang selama ini di jadikan cadangan, bisa di aktifkan sehingga routing menggunakan perangkat tersebut dan tidak membebani akses link DC – DRC.
2. Penggunaan BGP lebih disarankan karena saat BGP di nonkatifkan, pihak BTPN masih bisa memonitor link nya (saat intermitten).
3. Penggunakan BGP Load Balance DC – DRC dengan mengubah as number yang sama saat simulasi terbukti efektif mengurangi jalur routing.
4. Mengurangi traffic yang memenuhi bandwidth cabang dan link DC - DRC menggunakan tunneling berfungsi menjaga traffic tidak full untuk memberi bandwidth yang available untuk akses aplikasi core banking nya. Namun aplikasi yang di maksud menggunakan tunnel tidak dapat full akses bandwidth karena dibatasi bandwidth tunnel.
5. Gangguan yang di sebabkan provider, karena gangguan link ataupun flapping pada metro-E dengan cara provider masing-masing masih belum optimal, maka diusulkan untuk mengikuti dari Icon+ filtering mac address sebelum integrasi di perangkat jaringan BTPN.

E. DAFTAR PUSTAKA

Azzha, R. (2016). *Dasar Manajemen Jaringan dan Telekomunikasi*. Retrieved from Kompasiana: https://www.kompasiana.com/roisatulazza/5743de158c7e612207649eaa/dasar-manajemen-jaringan-dan-telekomunikasi

Ernawati, T., & Endrawan, J. (2018). Peningkatan Kinerja Jaringan Komputer dengan Border Gateway Protocol (BGP) dan Dynamic Routing (Studi Kasus PT Estiko Ramanda). *Khazanah Informatika, Vol.4 No.1*, 35-41.

Mulyadin, T., Sholeh, M., & Iswahyudi, C. (2016). Implementasi Routing Open Shortest Path First (OSPF) Melalui Tunnel Open VPN. *Jurnal JARKOM, vol. 4, no. 1*, 62-70.

Nurhayati, A., & Sulistianingsih, D. W. (2016). Simulasi Border Gateway Protocol (Bgp) Untuk Layanan Paket Data Menggunakan Simulator Gn3. *Jurnal ICT Penelitian Dan Penerapan Teknologi, 7(12)* , 12-23.

Pratama, A. P., & Arief, M. (2015). *Perancangan dan Analisis Desain Jaringan Wire dan Wireless dengan Pendekatan Green Network di Gedung Karang Fakultas Rekayasa Industri Universitas Telkom.* Bandung: Universitas Telkom.

Putra Yasa W, I. G., Rochim, A. F., & Christiyono, Y. (2014). Desain Dan Simulasi Internal Border Gateway Protocol (Ibgp) Menggunakan Graphical Network Simulator (Studi Kasus Pada Jaringan Universitas Diponegoro). *Transmisi, 16(1)*, 20-25.