

Implementasi Dan Analisa Kinerja Jaringan Cisco RPVST+ Load Balancing

Firmansyah¹, Eka Kusuma Pratama², Sari Dewi³

Abstrack-- The RPVST + computer network is a network concept used to make access selections based on a VLAN priority that has been embedded in a switch. By using RPVST + feature we can minimize the occurrence of a collision data or the occurrence of a data queue that causes the delay when transferring data. By utilizing the features of RPVST + Load Balancing, we can redundancy or automatic access removal if there are problems with the device being used. RPVST + Load Balancing is implemented and measured from the running network can be seen that a switch that gives priority to the VLAN will be passed by VLANs that get the top priority, but will receive secondary priority VLAN access if a device fails. RPVST + Load Balancing can be used to maintain network performance and perform minimalist collision data.

Intisari— Jaringan komputer RPVST+ merupakan sebuah konsep jaringan yang digunakan untuk melakukan pemilihan akses berdasarkan sebuah prioritas VLAN yang telah ditanamkan pada sebuah switch. Dengan menggunakan fitur RPVST+ kita dapat meminimalis terjadinya sebuah collision data ataupun terjadinya sebuah antrian data yang menyebabkan terjadinya delaynya pada saat melakukan transfer sebuah data. Dengan memanfaatkan fitur dari RPVST+ Load Balancing, kita dapat melakukan redundancy ataupun pemindahan akses secara otomatis jika terdapat permasalahan terhadap device yang sedang digunakan. RPVST+ Load Balancing diterapkan dan dilakukan pengukuran dari jaringan berjalan dapat dilihat bahwa sebuah switch yang memberikan prioritas terhadap VLAN akan dilalui oleh VLAN yang mendapatkan prioritas utama, namun akan menerima akses VLAN prioritas secondary jika terdapat device yang mengalami kegagalan. RPVST+ Load Balancing dapat digunakan untuk menjaga kinerja jaringan dan melakukan minimalis terjadinya collision data.

Kata Kunci: RPVST+, RPVST+ Load Balancing, VLAN, Collision

I. PENDAHULUAN

Jaringan komputer merupakan aspek yang begitu penting dalam kehidupan kita saat ini. Tanpa adanya jaringan komputer kita tidak dapat berkomunikasi antara satu dengan yang lainnya jika dipisahkan oleh jarak dan waktu. Maka dari itu ketersediaan jaringan komputer saat ini sangatlah

penting untuk menunjang komunikasi bahkan untuk menunjang pekerjaan kita selama 24 jam setiap harinya. Setiap kegagalan dalam sistem jaringan komputer harus diminimalisir sedemikian mungkin. Kegagalan pada jaringan komputer terdiri dari kegagalan perangkat (device) yang digunakan, serta manajemen jaringan yang digunakan. Kegagalan pada sebuah perangkat jaringan akan mengakibatkan terjadinya kendala pada Quality of Services (QoS). Ada beberapa parameter yang sangat mempengaruhi QoS antara lain packet loss, delay dan jitter pada jaringan. Untuk mengurangi dan meminimalis kegagalan terhadap QoS pada suatu jaringan, kita dapat memanfaatkan sebuah fitur yang terdapat pada perangkat cisco dengan menggunakan protokol RPVST+ Load Balancing. Sebuah teknik yang digunakan untuk memberikan prioritas terhadap lalu lintas dari sebuah pengiriman dan penerimaan dari sebuah paket data.

Dalam hal pelaksanaannya, masih sering menemukan kendala seperti proses monitoring dan remote management lambat bahkan bukan hanya itu monitoring dan remote management pun bisa terputus karena koneksi internetnya down, karena setiap akan melakukan monitoring dan remote management ke setiap pelanggannya harus menggunakan koneksi yang cepat dan stabil serta tidak terputus. Ketersediaan sistem cluster memiliki pengertian bahwa sebuah sistem yang dibangun akan terus menjaga kontinuitas sistemnya dengan cara melakukan backup sistem jaringan server komputer (redundancy), failover apabila ada salah satu perangkat jaringan server yang bermasalah atau mati total maka load balancing akan membagi jalur akses dari client untuk mengakses ke server sehingga pemrosesan data maupun aplikasi dapat dilakukan lebih cepat. Untuk menanggulangi hal tersebut maka dibutuhkanlah sebuah pengembangan sistem management di sebuah jaringan sehingga diharapkan dapat mengurangi kesulitan yang ada sehingga sistem bekerja secara optimal dalam melakukan pelayanan.

II. KAJIAN LITERATUR

A. Collision Data

Sebuah permasalahan didalam jaringan pastilah akan terjadi, salah satunya seperti collision data. Menurut (Rafudin, Rahmat: 2015), collision adalah kondisi dimana dua bit paket data menyebar secara bersamaan ke sebuah poin network [6]. Hal ini dapat terjadi jika didalam jaringan yang sangat kompleks terjadi kurangnya pemetaan ataupun managed dari jaringan yang digunakan. Collision data sering terjadi dikarenakan faktor sistem CSMA/CD yang menggunakan satu media saja namun digunakan untuk device yang banyak. Collision data biasanya terjadi pada

^{1,2} Program Pasca Sarjana Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, Jl. Damai No. 8, Warung Jati Barat, Margasatwa, Ragunan, Ps. Minggu, Jakarta Selatan (email : Firmansyah.fmy@bsi.ac.id, Eka.eem@bsi.ac.id)

³ Manajemen Informatika AMIK BSI Pontianak, Jl. Abdurahman Saleh No 18, Pontianak, (email : sari.sre@bsi.ac.id)

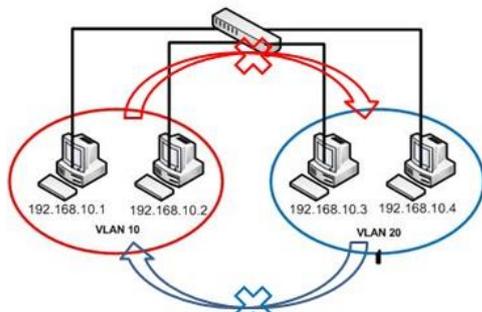
repeater dan hub, tidak terjadi pada perangkat switch, sebab switch membuat aliran data menggunakan ARP.

B. VLAN

Menurut (Odom, Wendell: 2013). Sebuah jaringan komputer tanpa menggunakan VLAN switch tidak akan mempertimbangkan untuk berada dalam domain broadcast yang sama. Artinya, untuk sebuah switch akan memiliki satu buah broadcast saja dan dapat memicu terjadinya collision data [3].

Sedangkan menurut (Sofana, Iwan: 2012), VLAN dapat mengatasi beberapa kesulitan yang tidak dapat diselesaikan oleh LAN Tradisional [5].

Dengan menggunakan jaringan VLAN, jaringan komputer akan lebih stabil dan akan lebih meminimalis terjadinya sebuah benturan data.

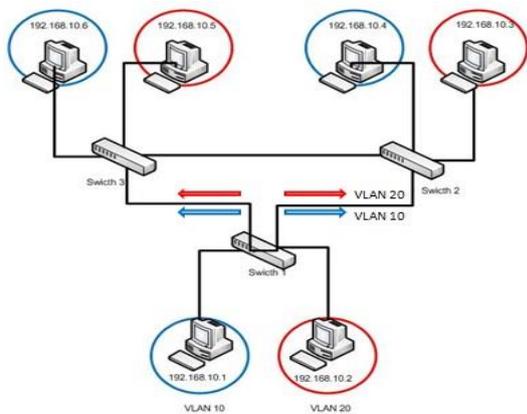


Gbr 1. VLAN

Jika dilihat pada Gbr 1, jaringan komputer menggunakan VLAN akan melakukan pembedaan akses terhadap VLAN-VLAN yang telah ditentukan, VLAN 10 tidak dapat melakukan transfer data dengan VLAN 20 maupun sebaliknya walaupun dalam 1 network yang sama. Yang artinya VLAN dapat membagi sebuah broadcast domain menjadi dua buah broadcast domain.

III. SPANNING TREE

Menurut (Donohue, Denise., Stewart, Brent: 2010). Spanning Tree merupakan protokol yang mencegah pembentukan loop dengan mendeteksi redundant link dan mampu menonaktifkan sebuah port yang tidak diizinkan[1].



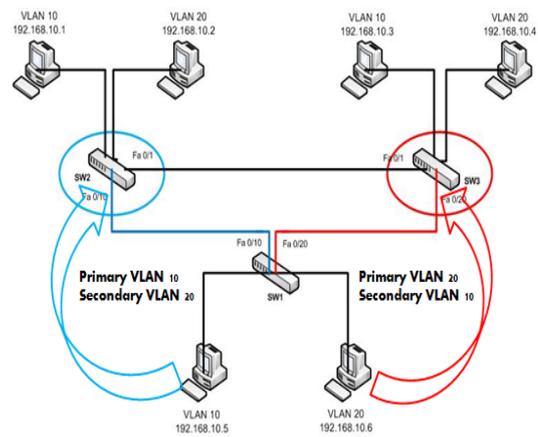
Gbr 2. Spanning Tree

Jaringan Spanning Tree akan melakukan transfer data menggunakan switch terdekat dari pengirim paket ke alamat tujuan paket. Sebagai contoh pada Gambar 2, PC dengan alamat IP 192.168.10.1 akan melakukan pengiriman paket data ke PC dengan IP 192.168.10.4. Maka, transfer data akan memilih melalui Switch 1 lalu menuju ke Switch 2. Begitu pula, jika PC yang sama akan melakukan transfer data ke PC dengan IP 192.168.10.6 maka akan memilih akses melalui Switch 1 menuju ke Switch 3 dikarenakan memiliki jarak yang relatif lebih singkat.

IV. RPVST+ (RAPID PER-VLAN SPANNING TREE PLUS)

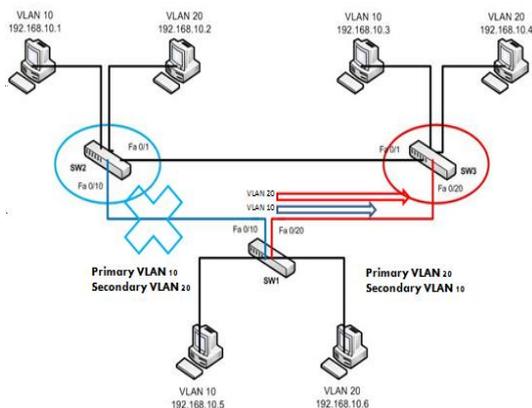
Menurut (Kocharians, Nabik., Vinson, Terry: 2015) RPVST+ merupakan sebuah kombinasi dari PVST+ dengan Rapid Spanning Tree. RPVST+ menyediakan waktu konvergensi subsecond dan kompatibel dengan PVST+ serta MSPT [2].

Sedangkan menurut (Wellace, Kevin: 2015) Rapid-PVST+ memungkinkan terjadinya banyak konvergensi yang lebih cepat (umumnya kurang dari satu detik) dibandingkan dengan STP yang memiliki waktu paling cepat 50 detik [4].

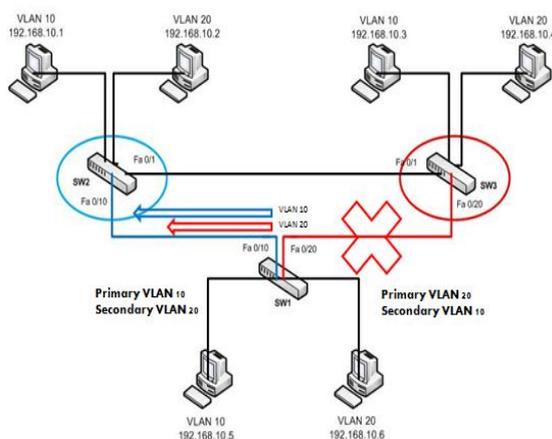


Gbr 3. RPVST+

Dengan menggunakan jaringan RPVST+, pengiriman paket akan dilakukan berdasarkan prioritas akses. Jika kita melihat pada gambar 3, switch 2 memprioritaskan akses terhadap VLAN 10. Sedangkan pada Switch 3 lebih memprioritaskan akses dari VLAN 20. Dengan menggunakan metode RPVST+ ini, setiap switch memiliki prioritas VLAN masing-masing yang bertujuan untuk meminimalisir terjadinya collision data yang mungkin terjadi.



Gbr 4. Load Balancing VLAN 10



Gbr 5. Load Balancing VLAN 20

Sedangkan, pada jaringan RPVST+ Load Balancing jika terjadi sebuah permasalahan pada Switch 2 maupun Switch 3, salah satu switch akan melakukan pembacupan akses secara otomatis seperti terlihat pada gambar 4 dan Gambar 5. Perpindahan akses secara otomatis akan bekerja dibawah prioritas VLAN yang telah ditentukan.

IV. METODE PENELITIAN

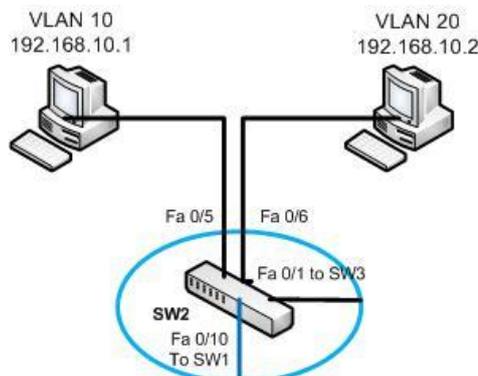
Dalam penelitian jaringan RPVST+ Load Balancing, penulis menggunakan bantuan Software Cisco Packet Tracer untuk membuat simulasi jaringan yang dijalankan secara virtualisasi namun tidak merubah dan mengurangi fitur device seperti aslinya.

Pada jaringan RPVST+ Load Balancing ini, penulis menggunakan 3 buah switch Series 2960 yang akan digunakan sebagai tolak ukur dari jaringan RPVST+ Load Balancing. Pada switch 2 digunakan untuk memberikan prioritas terhadap VLAN 10 dengan VLAN 20 sebagai secondary. Sedangkan pada switch 3 memberikan prioritas terhadap VLAN 20 dan VLAN 10 sebagai secondary. Serta melakukan pengujian terhadap kinerja jaringan Load Balancing pada masing-masing switch.

V. HASIL DAN PEMBAHASAN.

A. Konfigurasi RPVST+ Load Balancing Switch 2

Untuk melakukan konfigurasi jaringan RPVST+ Load Balancing, kita akan mengacu terhadap Gambar 3. Dari skema jaringan yang digunakan terdapat 3 buah Switch yang akan dikonfigurasi.



Gbr 6. Konfigurasi SW2

Untuk melakukan konfigurasi RPVST+ Load Balancing pada Switch 2 kita harus memasukan perintah:

```
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

```
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

Konfigurasi ini digunakan untuk melakukan pembuatan VLAN pada interface Fa0/5 dan interface Fa0/6. Dikarenakan jaringan RPVST+ merupakan langkah lanjutan dari sebuah VLAN. Maka langkah selanjutnya mengaktifkan portfast dan bpduguard pada interface Fa0/5 dan Fa0/6. Langkah selanjutnya ialah memberikan hak akses terhadap interface Fa0/1 maupun Fa0/10 sebagai trunking.

```
interface FastEthernet0/1
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20
switchport mode trunk
```

```
interface FastEthernet0/10
switchport trunk native vlan 99
```

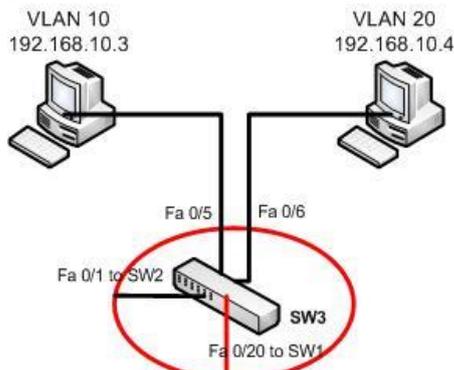
```
switchport trunk allowed vlan 10,20
switchport mode trunk
```

Dengan menggunakan fitur allowed vlan, diharapkan interface fa0/1 dan fa0/10 dapat melihat vlan10 dan vlan20.

spanning-tree mode pvst
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672

Sedangkan, konfigurasi “spanning-tree mode pvst” digunakan untuk memberikan akses RPVST+ Load Balancing dengan memberikan prioritas utama terhadap VLAN 10 dan prioritas secondary terhadap VLAN 20. VLAN 10 dengan prioritas 4096 sedangkan VLAN 20 dengan prioritas 28672.

B. Konfigurasi RPVST+ Load Balancing Switch 3



Gbr 7. Konfigurasi SW3

Konfigurasi pada Switch3 secara keseluruhan hampir sama dengan konfigurasi yang digunakan pada Switch2 baik konfigurasi VLAN serta konfigurasi Trunking yang digunakan untuk menghubungkan antara Switch. Namun, terjadi perbedaan pada konfigurasi prioritas yang akan digunakan.

spanning-tree mode pvst
spanning-tree vlan 10 priority 28672
spanning-tree vlan 20 priority 4096

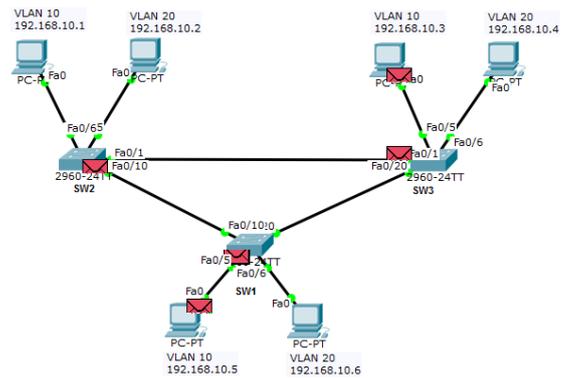
Konfigurasi yang diterapkan terhadap Switch3, yaitu memberikan prioritas utama terhadap akses VLAN 20 sedangkan VLAN 10 menjadi prioritas secondary. VLAN 10 dengan prioritas 28672 sedangkan VLAN 20 dengan prioritas 4096.

C. Uji Konektifitas

Setelah melakukan konfigurasi terhadap Switch2 dan Switch3. Tentunya kita harus melakukan uji konektifitas dari sebuah jaringan yang telah dibuat. Adapun cara pengujian jaringan RPVST+ Load Balancing adalah dengan melakukan perbandingan akses dari masing-masing switch yang digunakan, baik pengukuran dari VLAN10 maupun VLAN20 serta melakukan pengujian terhadap kinerja Load Balancing.

1. VLAN 10

Pengujian konektifitas yang pertama kali ialah melakukan uji konektifitas terhadap sebuah jaringan VLAN yang telah dibuat.



Gbr 8. Tracer VLAN 10

```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

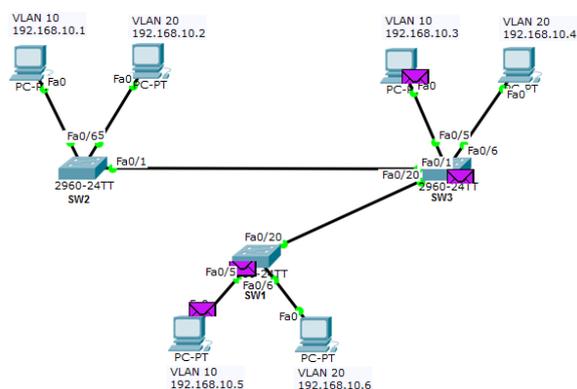
Reply from 192.168.10.3: bytes=32 time=12ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 6ms
```

Gbr 9. Ping Client VLAN 10

Pada gambar 8, dijelaskan VLAN 10 melakukan transfer data dari PC dengan alamat IP: 192.168.10.5 ke PC beralamatkan IP: 192.168.10.3 melalui Switch1 menuju ke Switch2. Hal ini terjadi dikarenakan Switch2 memberikan prioritas utama terhadap lalu lintas data dari VLAN 10 sedangkan VLAN 20 sebagai prioritas secondary. Jika kita tidak menggunakan fitur RPVST+ dan hanya menggunakan fitur dari STP, maka pemilihan akses akan memilih Switch1 menuju langsung ke Switch3 dengan jarak yang relatif lebih dekat.

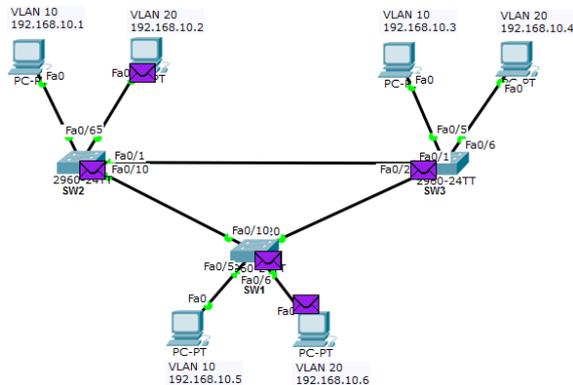
Namun, jika terjadi sebuah permasalahan pada Switch2. Akses VLAN 10 akan dialihkan secara otomatis melalui Switch3 dengan prioritas dibawah VLAN 20 seperti pada gambar 10.



Gbr 10. Load Balancing VLAN 10

2. VLAN 20

Langkah selanjutnya setelah melakukan uji konektivitas terhadap VLAN 10. Maka langkah selanjutnya kita akan melakukan uji konektivitas terhadap VLAN 20 yang merupakan prioritas dari Switch3.

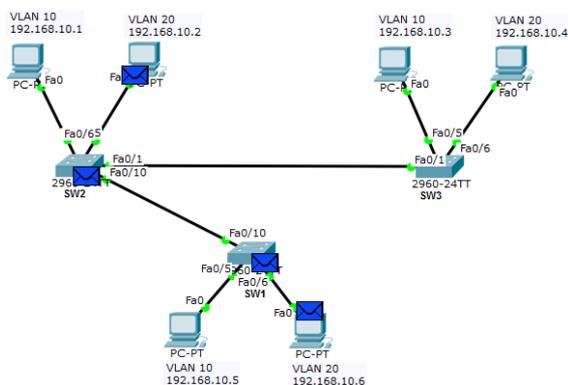


Gbr 11. Traceret VLAN 20

Pada gambar 11 dijelaskan, PC dengan alamat IP: 192.168.10.6 melakukan transfer data menuju PC dengan alamat IP: 192.168.10.2 melalui Switch1 menuju ke Switch3 terlebih dahulu dan menuju ke Switch2. Hal ini terjadi dikarenakan Switch3 memberikan prioritas utama terhadap VLAN 20 sedangkan VLAN 10 sebagai prioritas secondary dari Switch3.

Jika pada jaringan yang telah kita buat tidak menggunakan protokol RIPv2 Load Balancing, maka semua pengiriman paket data memilih jalur terpendek. Yang artinya jika mengacu terhadap gambar 11, seharusnya PC dengan alamat IP: 192.168.10.6 yang akan melakukan transfer data terhadap PC beralamat IP: 192.168.10.2 akan memilih akses melalui Switch1 dan langsung terhubung terhadap Switch2.

Pemindahan lalu lintas secara langsung dapat terjadi jika terdapat sebuah permasalahan terhadap Switch3 yang merupakan prioritas utama dari VLAN 20 dan akses data akan dipindahkan ke Switch2 seperti terlihat pada gambar 12. Hal yang sama akan terjadi pula terhadap Switch2 jika mengalami kendala, maka akses data akan dipindahkan secara otomatis ke Switch3.



Gbr 12. Load Balancing VLAN 20

VI. KESIMPULAN

Berdasarkan hasil analisa dan pembahasan yang telah diuraikan, dapat diambil kesimpulan sebagai berikut ini:

1. Dengan menggunakan RIPv2 dapat dilakukan pemetaan terhadap prioritas akses sebuah VLAN.
2. Dengan menggunakan RIPv2 Load Balancing, jika terjadi sebuah permasalahan kinerja terhadap salah satu switch maka akses prioritas akan dipindahkan secara otomatis.
3. RIPv2 Load Balancing dapat digunakan untuk menjaga kinerja jaringan dan melakukan minimalis terjadinya collision data.

REFERENSI

- [1] Donohue, Denise., Stewart, Brent (2010). CCNP Routing and Switching Quick Reference. USA: Cisco Press.
- [2] Kocharians, Nabrik., Vinson, Terry (2015). CCIE Routing and Switching v5.0 Volume 2 Fifth Edition. USA: Cisco Press.
- [3] Kocharians, Nabik., Vinson, Terry (2015). CCNP Routing and Switching ROUTE 300-101. USA: Cisco Press.
- [4] Odom, Wendell (2013). Cisco CCNA Routing and Switching 200-120 Official Cert Guide Library. USA: Cisco Press.
- [5] Sofana, Iwan (2012). Cisco CCNA & Jaringan Komputer Edisi Revisi. Bandung: Informatika.
- [6] Wellace, Kevin (2015). CCIE Collaboration Lab Lessons, USA: Cisco Press
- [7] Rafiudin, Rahmat (2015). Panduan Membangun Jaringan Komputer Untuk Pemula. Jakarta: Elex Media Komputindo



Firmansyah, S.Kom, dilahirkan di Ibu Kota Jakarta, Lulus pendidikan S1 (Teknik Informatika) di STMIK Nusa Mandiri Jakarta tahun 2014, dan saat ini sedang melanjutkan program studi Pasca Sarjana di STMIK Nusa Mandiri Jakarta. Saat ini aktif sebagai tenaga pendidik di AMIK BSI Jakarta. Selain aktif sebagai tenaga pendidik sampai saat ini aktif sebagai assessor kompetensi BNSP dan Instruktur Cisco Networking Academy



Eka Kusuma Pratama, S.Kom, lahir pada tahun 1993 di Kota Tulungagung, Lulus pendidikan S1 (Teknik Informatika) di STMIK Nusa Mandiri Jakarta tahun 2016, dan saat ini sedang melanjutkan program studi Pasca Sarjana di STMIK Nusa Mandiri Jakarta dan aktif sebagai tenaga pendidik di AMIK BSI Jakarta. Selain sebagai pengajar, saat ini aktif sebagai Instruktur Cisco Networking Academy



Sari Dewi, M.Kom, Lahir di Cirebon 6 Juli 1989. Lulus S1 dari STMIK Nusa Mandiri Jakarta Program Studi Teknik Informatika 2013 dan S2 STMIK Nusa Mandiri Program Studi Ilmu Komputer 2015. Menjadi pengajar di AMIK BSI dan Pernah menulis pada jurnal paradigma dan jurnal Techno.