Perancangan Jaringan Server dan Komputer Menggunakan Metode Scalable Multilayer Campus Design

TUGAS AKHIR

Oleh :

Derwanto 3310812023

Soni Broery 3310812036

Disusun untuk memenuhi syarat kelulusan Program Diploma III

PROGRAM STUDI TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

BATAM

2012

LEMBAR PENGESAHAN

Batam, 29 Juni 2012

Pembimbing I,	Pembimbing II,
Prasaja Wikanta, MT.	**Tandhy B. P. Simanjuntak, S.Kom.**
NIK. 103026	**NIK. 111085**

LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310812023

Nama : Derwanto

adalah mahasiswa Teknik Informatika Politeknik Batam yang menyatakan bahwa tugas akhir dengan judul:

PERANCANGAN JARINGAN SERVER DAN KOMPUTER MENGGUNAKAN METODE SCALABLE MULTILAYER CAMPUS DESIGN

disusun dengan:

1. Tidak melakukan plagiat terhadap naskah karya orang lain.
2. Tidak melakukan pemalsuan data.
3. Tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik.

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 29 Juni 2012

Derwanto
3310812023

LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : Soni Broery

Nama : 3310812036

adalah mahasiswa Teknik Informatika Politeknik Batam yang menyatakan bahwa tugas akhir dengan judul:

PERANCANGAN JARINGAN SERVER DAN KOMPUTER MENGGUNAKAN METODE SCALABLE MULTILAYER CAMPUS DESIGN

disusun dengan:

1. Tidak melakukan plagiat terhadap naskah karya orang lain.
2. Tidak melakukan pemalsuan data.
3. Tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik.

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 29 Juni 2012

Soni Broery
3310812036

KATA PENGANTAR

Puji dan Syukur kepada Tuhan Yang Maha Esa, karena atas segala rahmatNya-lah pada akhirnya Tugas Akhir dengan judul ”Perancangan Jaringan *Server* dan Komputer Menggunakan Metode Scalable Multilayer Campus Design” ini dapat diselesaikan dengan baik. Ucapan terima kasih dan penghargaan yang setinggi-tingginya kami sampaikan kepada orang tua kami masing-masing yang sudah memberikan dukungan doa, semangat dan materi. Buat rekan-rekan Politeknik Negeri Batam kelas karyawan, terima kasih atas segala dukungan yang diberikan. Juga kepada Bapak Prasaja Wikanta dan Bapak Tandhy, terima kasih atas segala saran dan arahan yang sangat membantu kami, sehingga Tugas Akhir ini dapat diselesaikan.

Selanjutnya kami menyadari bahwa *“tak ada gading yang tak retak”*. Bahwa penulisan dan isi Tugas Akhir ini tentu masih banyak kekurangannya. Maka dari itu, kami mengharapkan saran atau kritik yang konstruktif dari para pembaca, sehingga dapat memacu kami untuk bekerja lebih baik di kemudian hari.

Akhir kata, semoga karya kecil ini memberi manfaat bagi mereka yang menggunakannya, khususnya bagi yang hendak mengimplementasikan hasil perancangan ini.

Batam, 29 Juni 2012

Penulis

ABSTRAK

PERANCANGAN JARINGAN SERVER DAN KOMPUTER MENGGUNAKAN METODE SCALABLE MULTILAYER CAMPUS DESIGN

Perancangan jaringan *server* dan komputer ini bertujuan untuk mengatasi masalah yang terjadi dikarenakan tidak adanya segmentasi dan *single point of failure* pada jaringan. Metode yang digunakan dalam perancangan ini yaitu metode *Scalable MultiLayer Campus Design*. Hasil yang dicapai adalah rancangan sebuah jaringan yang memiliki standar *Scalable Multilayer Campus Design*, sehingga menghasilkan jaringan yang efisien, intelijen, dapat diukur dan mudah diatur. Kesimpulan yang didapat adalah dengan melakukan pengubahan sistem jaringan dengan melakukan segmentasi menggunakan VLAN pada jaringan dosen, laboratorium dan *server farm*. Implementasi protokol *routing* OSPF yang bekerja sangat efisien dalam pengiriman *update* informasi rute. Selain itu juga mengimplementasikan protokol *redundancy* VRRP untuk mengatasi terjadinya *failover* pada jaringan internal. Juga mengimplementasikan *access-list* yang difungsikan untuk penyaringan paket yang tidak diinginkan dalam kebijakan keamanan.

Kata Kunci: *Scalable Multilayer Campus Design, VLAN, OSPF, VRRP dan Access-list.*

ABSTRACT

INTERNETWORK DESIGN FOR SERVER AND COMPUTER USING THE METHOD OF SCALABLE MULTILAYER CAMPUS DESIGN

The objective of this internetwork design for server and computer is to address the issues raised due to no network segmentation and single point of failure in the network. The method used for this design is Scalable Multilayer Campus Design. The target of this design is a network which fulfill the criteria of Scalable Multilayer Campus Design, results an efficient, intelligent, scalable and manageable network. The major concept is to divide large networks such as lecture network, laboratory network and server farm in to smaller networks using VLAN. The implementation of OSPF routing protocol works efficiently in delivering routing update. Also, first hop redundancy which is VRRP is implemented to address the single point of failure in internal networks. There are access-lists which are intended to filter packets in term of security.

Key words: *Scalable Multilayer Campus Design, VLAN, OSPF, VRRP and Access-list.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Bab I Pendahuluan

I.1 Latar Belakang

Infrastruktur jaringan *server* dan komputer Politeknik Negeri Batam mengadopsi sebuah topologi jaringan yang sederhana. Data topologi jaringan *server* dan komputer Politeknik Negeri Batam ini menggunakan data valid pada tanggal 1 Mei 2010. Jaringan tersebut hanya memiliki tiga jaringan internal yaitu jaringan dosen, jaringan *student lab* dan jaringan *wifi*. Seluruh *host* pada jaringan dosen terhubung dalam satu segmen jaringan yang sama dan menggunakan *subnet* 192.168.2.0/24, sehingga semua *host* berada pada satu *broadcast domain*. Skenario ini juga diterapkan pada jaringan *student lab* dan jaringan *wifi* yang menggunakan *subnet* 172.16.0.0/16 dan 172.16.x.0/24. Jaringan Politeknik Negeri Batam hanya menggunakan PC *router* untuk menghubungkan jaringan internal dengan jaringan eksternal. Topologi seperti ini sangat sederhana dan kurang efektif dalam menangkal serangan dan gangguan dari jaringan eksternal.

Seiring dengan kebutuhan yang semakin meningkat, maka dilakukan penambahan *server-server* pada jaringan yang sudah ada. Dikarenakan rancangan topologi jaringan yang sederhana, maka *server-server* diletakkan berhadapan langsung dengan jaringan eksternal dan menggunakan alamat IP publik. Hal ini sangat mengancam sistem keamanan *server-server* tersebut.

Saat ini beberapa *server* berada dalam satu jaringan yang sama dengan salah satu jaringan internal tanpa adanya lapisan pengamanan maupun segmentasi. Dalam skenario jika salah satu komputer pada jaringan internal terinfeksi *virus*, maka tingkat kemungkinan penyebaran *virus* tersebut pada *server* sangat tinggi. Tidak ada implementasi segmentasi dalam jaringan-jaringan tersebut, sehingga membentuk sebuah jaringan yang besar dan hanya memiliki satu *broadcast domain*

pada setiap jaringan internal. Implementasi jaringan seperti ini tidak memenuhi kriteria sebuah rancangan jaringan yang baik, yaitu efisien, intelijen, dapat diukur dan mudah diatur [1].

I.2 Rumusan Masalah

1. *Server-server* berhadapan langsung dengan jaringan eksternal atau *internet*, menggunakan alamat IP publik tanpa adanya lapisan pengaman
2. Tidak ada implementasi segmentasi jaringan pada jaringan internal.
3. Beberapa *server* berada dalam satu jaringan yang sama dengan salah satu jaringan internal tanpa adanya lapisan pengamanan maupun segmentasi.
4. *Single point of failure*.

I.3 Batasan Masalah

1. Perancangan ini tidak menangani *bandwitdh management*.
2. Perancangan ini tidak menangani *network monitoring*.

I.4 Tujuan

Perancangan ini dibuat agar infrastruktur jaringan *server* dan komputer Politeknik Negeri Batam memenuhi standar *Scalable Multilayer Campus Design*, sehingga menghasilkan jaringan yang efisien, intelijen, dapat diukur dan mudah diatur.

I.5 Sistematika Penulisan

Bab I **Pendahuluan**

Bagian ini membahas tentang gambaran umum jaringan komputer saat ini, latar belakang, rumusan masalah, batasan masalah, tujuan dan sistematika penulisan.

Bab II **Tinjauan Pustaka**

Bagian ini membahas mengenai landasan teori dan konsep dasar yang berhubungaan dengan perancangan jaringan *server* dan

komputer menggunakan metode *Scalable Multilayer Campus Design*.

Bab III Bab-Bab Perancangan

Bagian ini memuat uraian tentang langkah-langkah penyelesaian masalah, yaitu meliputi rancangan topologi, deskripsi perancangan topologi, pengalamatan IP, penomoran VLAN, teknologi-teknologi yang diterapkan dalam rancangan dan kebutuhan perangkat keras pada perancangan.

Bab IV Bab-Bab Implementasi dan Pengujian

Bagian ini memuat uraian langkah implementasi perancangan berupa simulasi jaringan menggunakan GNS3, analisis dan pengujian dari perancangan yang dibangun.

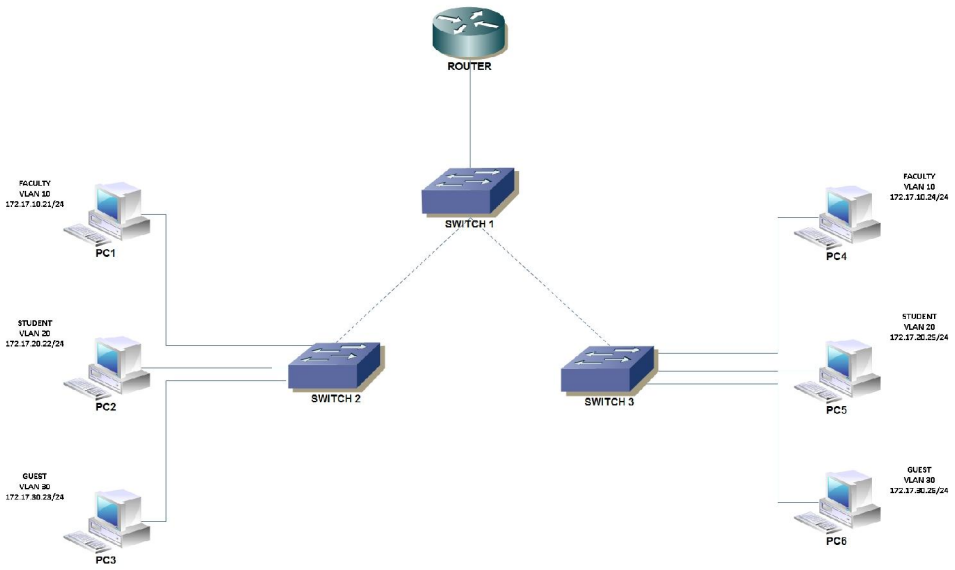
Bab V Kesimpulan dan Saran

Bagian ini memuat tentang kesimpulan perancangan dan juga saran-saran pengembangan dari perancangan yang telah dibangun.

Bab II Landasan Teori

II.1 VLAN(*Virtual Local Area Network*)

Kinerja sebuah jaringan yang baik sangat dibutuhkan oleh organisasi terutama dalam hal kecepatan dalam pengiriman data. Salah satu teknologi untuk meningkatkan kinerja jaringan adalah dengan kemampuan untuk membagi sebuah jaringan yang besar menjadi beberapa jaringan yang lebih kecil dengan menggunakan VLAN. Jaringan yang lebih kecil akan membatasi *host* yang terlibat dalam aktivitas penyebaran (*broadcast*) dan membagi *host* ke dalam beberapa kelompok berdasarkan fungsinya, seperti layanan basis data untuk departemen akuntansi dan transfer data yang cepat untuk departemen teknik.



Gambar 1 VLAN

Teknologi VLAN (Virtual Local Area Network) bekerja dengan cara melakukan segmentasi jaringan secara logika ke dalam beberapa *subnet*. VLAN adalah kelompok *host* dalam sebuah LAN yang dikonfigurasi (menggunakan manajemen perangkat lunak) sehingga *host-host* dapat saling berkomunikasi apabila dihubungkan dengan jaringan yang sama walaupun secara fisik *host-host* berada

pada segmen LAN yang berbeda [2]. VLAN diciptakan bukan berdasarkan koneksi fisik namun koneksi logikal yang tentunya lebih fleksibel. Secara logika, VLAN membagi jaringan ke dalam beberapa *subnet*. VLAN mengijinkan banyak *subnet* dalam jaringan dengan menggunakan *manageable switch*.

Dalam LAN tradisional, masing-masing *host* terhubung dengan *host* yang lain dalam sebuah *hub*. Perangkat ini akan menyebarkan semua lalu lintas data di seluruh jaringan. Jika ada dua *host* yang mencoba mengirimkan informasi pada waktu yang sama, sebuah tabrakan (*collision*) akan terjadi dan semua pengiriman data akan hilang. Jika tabrakan telah terjadi, pengiriman data akan dilanjutkan disebar ke seluruh jaringan oleh *hub*. Informasi data asal akan terus mengirim sampai dengan *collision* hilang. Dengan demikian akan banyak membuang waktu dan sumber daya (*resource*). Untuk mengatasi *collision* di sebuah jaringan, maka digunakanlah sebuah *bridge* atau *switch*. Perangkat ini menggunakan jalur yang berbeda-beda dalam mengirimkan informasi ke masing-masing *host* sehingga *collision* dapat tereliminasi.

Keanggotaan dalam sebuah VLAN dapat diklasifikasikan berdasarkan *port* yang digunakan, alamat MAC, tipe protokol dan sebagainya. Semua informasi yang mengandung penandaan atau pengalamatan suatu VLAN atau yang biasanya dinamakan *tagging* disimpan dalam sebuah basis data atau tabel. Jika proses penandaan berdasarkan *port* yang digunakan maka basis data harus menyimpan informasi mengenai *port-port* yang digunakan oleh VLAN. Proses penandaan pada umumnya dilakukan oleh *switch* yang bisa diatur atau yang biasanya dinamakan *manageable switch*. *Switch* inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi VLAN serta menjamin semua *switch* yang ada pada sebuah jaringan memiliki informasi yang sama. Berdasarkan informasi dari basis data atau tabel, maka *switch* dapat menentukan kemana data-data akan diteruskan dan sebagainya.

Berikut ini adalah beberapa keuntungan penggunaan VLAN:

1. Keamanan – keamanan data dari setiap departemen lebih terjamin karena lalu lintas data dapat dibatasi melalui masing-masing segmen yang telah dipisah secara logika.
2. Pengurangan biaya – penghematan dari penggunaan *bandwidth* yang ada dan dari *upgrade* perluasan jaringan yang memerlukan biaya yang besar.
3. Kinerja yang lebih baik – pembagian jaringan *layer* kedua ke dalam beberapa kelompok *broadcast domain* yang lebih kecil akan mengurangi lalu lintas paket yang tidak dibutuhkan dalam jaringan.
4. *Broadcast storm mitigation* – pembagian jaringan ke dalam VLAN-VLAN akan mengurangi jumlah *host* yang berpartisipasi dalam pembuatan *broadcast storm.* Hal ini terjadi karena adanya pembatasan *broadcast domain*.

II.1.1 *Local* VLAN dan *end to end* VLAN

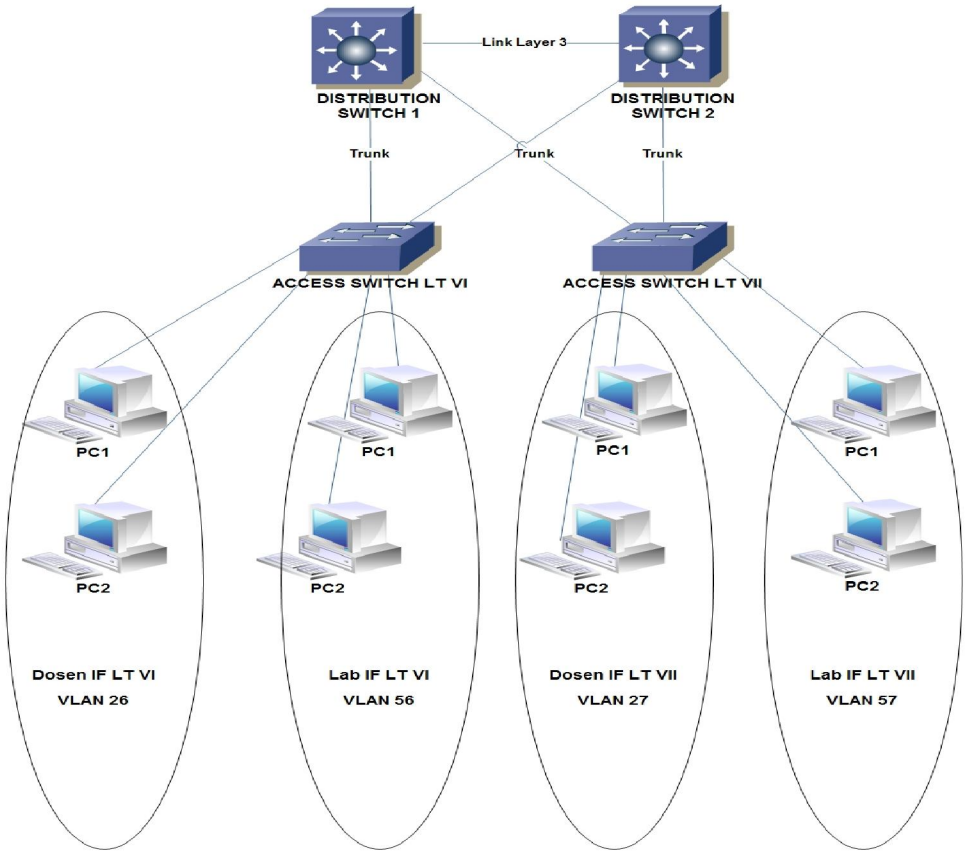
Local VLAN dikonfigurasi berdasarkan lokasi fisik dan bukan oleh fungsi, proyek, departemen dan sebagainya. Sedangkan *end-to-end* VLAN dikonfigurasi untuk mengizinkan keanggotaan VLAN berdasarkan fungsi, proyek, departemen, dan sebagainya [3]. Fitur terbaik dari *end-to-end* VLAN adalah bahwa pengguna dapat ditempatkan dalam VLAN terlepas dari lokasi fisik mereka.

Berikut adalah beberapa panduan dalam merancang *local* VLAN:

1. Harus melakukan segmentasi jaringan menjadi VLAN-VLAN berdasarkan lokasi fisik *host-host* daripada berdasarkan kategori *host-host*.

2. Implementasi *local* VLAN hanya berada diantara *layer access* dan *distribution* saja.

3. Trafik dari *local* VLAN akan di-*route* pada *layer distribution* dan *core* agar mencapai ke jaringan tujuan.



Gambar 2 Contoh Implementasi *Local* VLAN Jaringan Politeknik Negeri Batam pada Lantai VI dan Lantai VII

Pada masa lalu, perancang jaringan berusaha mengimplementasi aturan 80/20 ketika merancang sebuah jaringan. Aturan tersebut didasari oleh pengamatan dimana pada umumnya 80% trafik dari sebuah segmen jaringan hanya melewati diantara perangkat-perangkat *local*, dan hanya 20% yang ditujukan ke luar segmen jaringan. Oleh karena itu, arsitektur jaringan lebih suka menggunakan model *end-to-end* VLAN. Untuk menghindari komplikasi *end-to-end* VLAN, *server-server* digabungkan pada sebuah lokasi yang terpusat dalam jaringan dan menyediakan akses ke sumber daya eksternal seperti *internet*. Oleh karena itu, paradigma sekarang lebih dekat dengan aturan 20/80 dimana lebih banyak trafik yang meninggalkan segmen *local* dan menuju ke segmen eksternal, sehingga *local* VLAN menjadi lebih efisien.

II.1.2 *Trunk*

Trunk adalah saluran yang menghubungkan dua buah *node*, dimana jumlah saluran di *trunk* lebih kecil dari saluran di tiap *node*. *Trunk link* dibuat untuk menghubungkan dua buah *switch* atau lebih, dimana *link* tersebut akan digunakan untuk melewatkan data-data dari vlan yang berbeda. Untuk membedakan data dari satu vlan dengan vlan yang lainnya, maka setiap data yang melewati *trunk link* harus diberi vlan *taging*. Secara otomatis vlan *taging* akan dibuang ketika data akan dikirim ke komputer. *Identifier* vlan adalah *tag* yang dienkapsulasi dengan data. ISL dan 802.1Q adalah dua jenis enkapsulasi yang digunakan untuk membawa data dari beberapa vlan melalui *trunk link*. Ada 2 jenis vlan *taging* (*encapsulation*) yang dapat diimplementasikan pada teknologi *fastethernet*, yaitu ISL (*Inter Switch Link*) dan dot1q.

1. ISL (*Inter Switch Link*)

   ISL (*Inter Switch Link*) merupakan protokol *proprietary* cisco untuk hubungan antar *switch*, artinya tidak akan mungkin *switch* merk perangkat lain untuk menggunakan ISL. ISL *header* panjangnya 26 *byte* ditambah dengan 4 *byte* CR, sehingga panjang total *frame*-nya melebihi panjang *frame ethernet*. NIC biasa tidak dapat membaca *frame* format ini karena dianggap sebagai *frame giant*. ISL hanya mendukung 1000 vlan. Dalam ISL, *original frame* akan di enkapsulasi dan ditambahkan sebuah *header* sebelum *frame* dibawa melalui *line trunk*. Setelah *fram*e tersebut sampai di penerima akhir *trunk*, maka *header* yg ditambahkan kemudian dibuang dan kemudian *frame* diteruskan ke vlan yg dituju.

2. Dot1Q

   Encapsulation dot1q merupakan standar yang dikeluarkan IEEE 802.1Q. Berbeda dengan ISL, maka penambahan *tag* dot1q sangat efisien karena hanya menyisipkan 4 *byte tag* ke dalam *header ethernet*, ehingga NIC biasapun masih bisa membaca *frame* ini.

II.2 Scalable Multilayer Campus Design

Scalable Multilayer Campus Design merupakan model *internetwork* hirarkis yang dikembangkan oleh Cisco. Sebagai kiblat dalam dunia jaringan, Cisco membangun sebuah *internetworking* yang mengedepankan keamanan, kecepatan dan performa. Model ini menyederhanakan tugas dalam membangun *internetworking* yang handal, dapat diukur, dan lebih fleksibel. Sebuah *Scalable Multilayer Campus Design* memiliki tiga lapisan [1], yaitu sebagai berikut:

1. *Core layer*: Lapisan ini merupakan inti dari sebuah jaringan yang mencakup *switch high-end* dan kabel berkecepatan tinggi seperti kabel serat. Lapisan ini menjamin pengiriman paket dengan cepat dan aman.
2. *Distribution layer*: Lapisan ini mencakup LAN berbasis *router* dan *switch.* Lapisan ini memastikan bahwa paket dikirimkan ke *subnet* atau VLAN yang benar. Lapisan ini juga dinamakan lapisan *workgroup.*
3. *Access layer*: Lapisan ini mencakup *hub* dan *switch*. Lapisan ini juga dinamakan lapisan *desktop* karena berfokus pada titik-titik *host* yang terhubung, seperti komputer, *server* atau perangkat keras lainnya. Lapisan ini memastikan bagaimana paket dikirim dan sampai ke *host.*

II.3 Protokol *Routing*

Protokol *routing* merupakan aturan dalam komunikasi antar *router-router*. Protokol *routing* mengijinkan *router-router* untuk membagi informasi tentang jaringan dan koneksi antar *router* [6]. *Router* menggunakan informasi ini untuk membangun dan memperbaiki tabel *routing*. *Routing* adalah aksi pengiriman-pengiriman paket data ke jaringan tujuan dengan menggunakan rute berdasarkan tabel *routing*.

Tujuan utama dari protokol *routing* adalah untuk membangun dan memperbaiki tabel *routing*. Dimana tabel ini berisi informasi mengenai jaringan-jaringan dan *interface* yang berhubungan dengan jaringan tersebut. Protokol *routing* mempelajari semua *router* yang ada dan juga menghapus rute ketika rute tersebut

tidak berlaku lagi. *Router* menggunakan informasi dalam tabel *routing* untuk melewatkan paket-paket *routed* protokol.

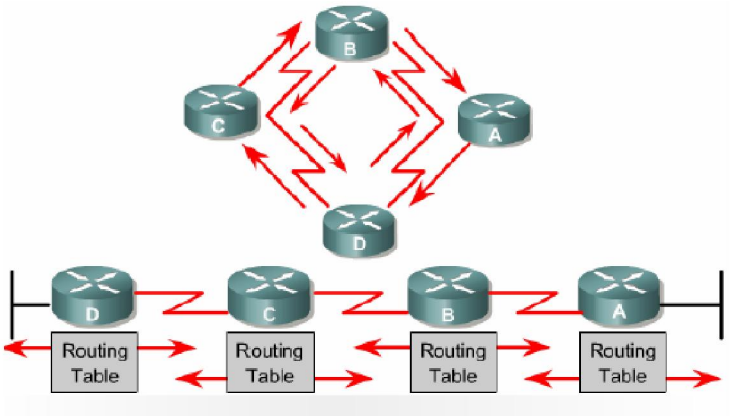
Algoritma *routing* adalah elemen dasar dari sebuah protokol *routing*. Ketika sebuah topologi jaringan mengalami perubahan karena perkembangan jaringan, konfigurasi ulang atau terjadi masalah pada jaringan, maka *router* dapat mengetahui perubahan tersebut. Dasar pengetahuan dari algoritma *routing* ini dibutuhkan secara akurat untuk melihat topologi yang baru.

Pada saat semua *router* dalam jaringan pengetahuannya sudah sama semua berarti dapat dikatakan *internetwork* dalam keadaan konvergen. Keadaan konvergen yang cepat sangat diharapkan karena dapat menekan waktu pada saat *router* meneruskan untuk mengambil keputusan *routing* yang tidak benar.

Sebagian besar algoritma *routing* dapat diklasifikasikan menjadi dua kategori berikut:

1. *Distance vector*

   Routing distance vector bertujuan untuk menentukan arah atau *vector* dan jarak ke *link-link* lain dalam sebuah *internetwork*. Algoritma *routing distance vector* secara periodik menyalin tabel *routing* dari *router* ke *router*. Perubahan tabel *routing* ini diperbaharui antar *router* yang saling berhubungan pada saat terjadi perubahan topologi.

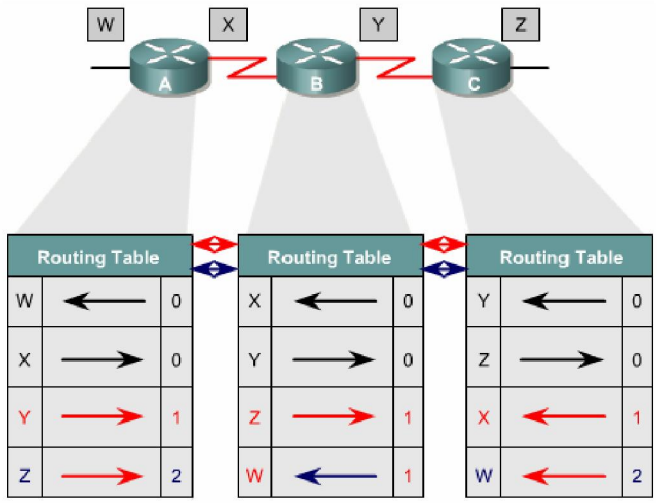


Gambar 3 Konsep *Distance Vector*

Setiap *router* menerima tabel *routing* dari *router* tetangga yang terhubung langsung. Gambar 3 mendeskripsikan konsep kerja *distance vector*.

Router B menerima informasi dari *router* A. *Router* B menambahkan nomor *distance vector*, seperti jumlah *hop*. Jumlah ini menambahkan nilai *distance vector*. *Router* B menyampaikan tabel *routing* baru ini ke *router-router* tetangganya yang lain, yaitu *router* C. Proses ini akan berlangsung untuk semua *router*.

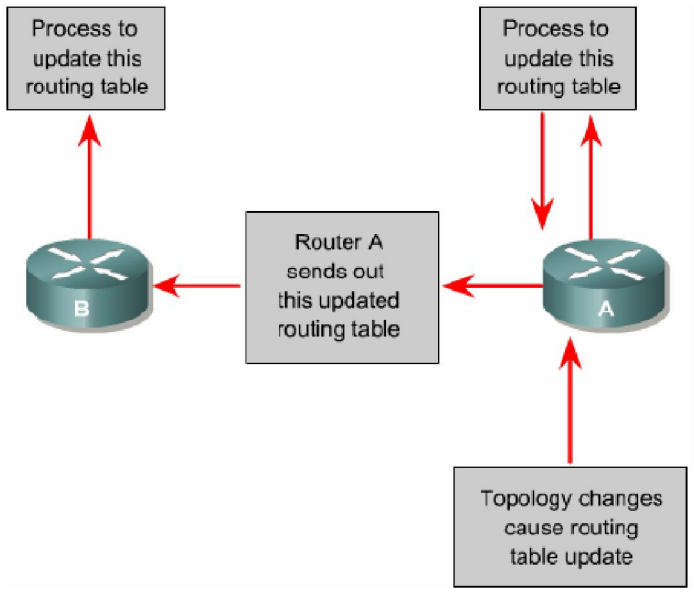
Algoritma ini mengakumulasi jarak jaringan sehingga dapat digunakan untuk memperbaiki basis data informasi mengenai topologi jaringan. Akan tetapi algoritma *distance vector* tidak mengijinkan *router* untuk mengetahui secara pasti topologi *internetwork* karena hanya melihat *router-router* tetangganya.



Gambar 4 Jaringan *Distance Vector Discovery*

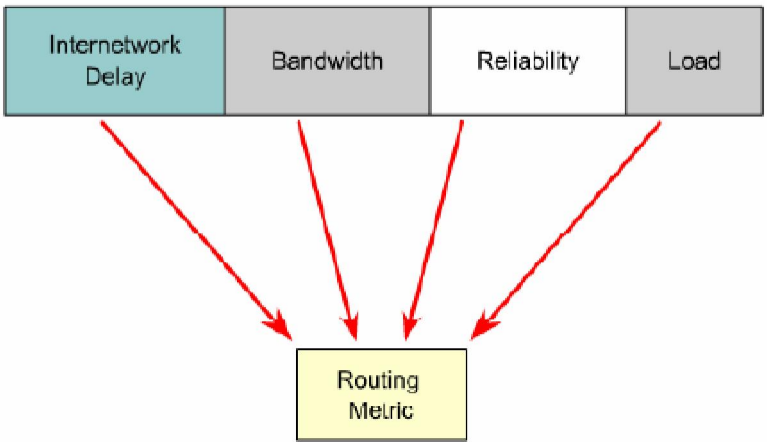
Interface yang terhubung langsung ke *router* tetangganya mempunyai nilai *distance* 0. *Router* yang menerapkan *distance vector* dapat menentukan jalur terbaik untuk menuju ke jaringan tujuan berdasarkan informasi yang diterima dari tetangganya. *Router* A mempelajari jaringan lain berdasarkan informasi yang diterima dari *router* B. Masing-masing *router* lain

menambahkan nilai *distance* dalam tabel *routing*-nya untuk melihat sejauh mana jaringan yang akan dituju, seperti yang diilustrasikan pada gambar 4.



Gambar 5 Perubahan Topologi *Distance Vector*

Pembaharuan tabel *routing* terjadi ketika ada terjadi perubahan pada topologi jaringan. Sama dengan proses *discovery*, proses pembaharuan topologi selangkah demi selangkah dari *router* ke *router*. Gambar 5 menunjukkan algoritma *distance vector* memanggil ke semua *router* untuk mengirim pembaharuan ke tabel *routing*-nya.



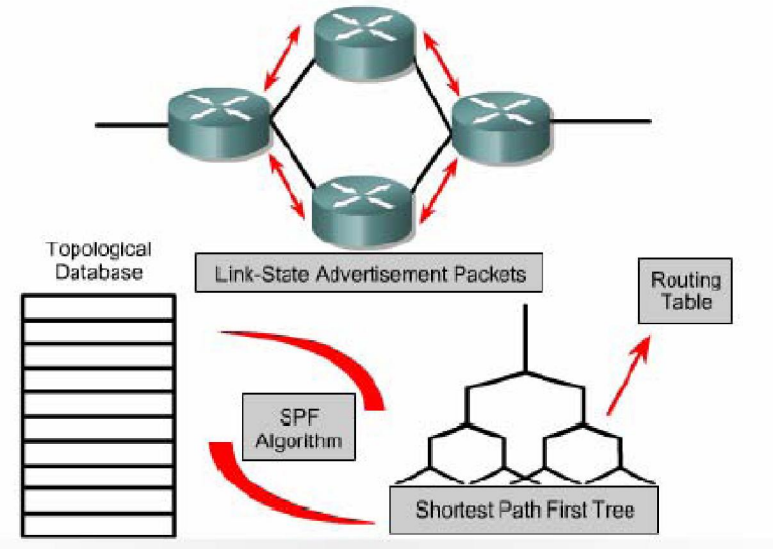
Gambar 6 Komponen-Komponen *Routing Metric*

Tabel *routing* berisi informasi tentang *total path cost* yang ditentukan oleh metrik dan alamat logika dari *router* pertama dalam jaringan yang ada didalam tabel *routing*, seperti yang diilustrasikan pada gambar 6.

Analogi *distance vector* dapat digambarkan seperti jalan tol. Tanda yang menunjukkan titik menuju ke tujuan dan menunjukkan jarak ke tujuan. Dengan adanya tanda-tanda seperti itu pengendara dengan mudah mengetahui perkiraan jarak yang akan ditempuh untuk mencapai tujuan, dalam hal ini jarak terpendek adalah rute yang terbaik.

2. *Link-state*

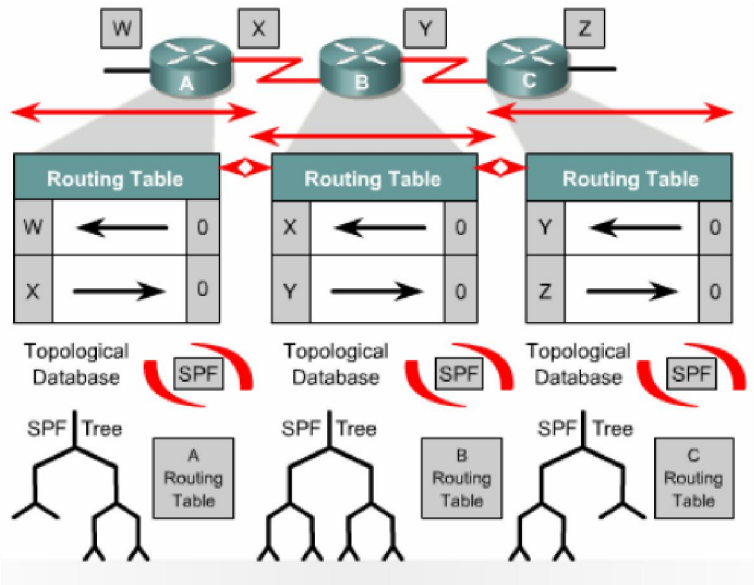
   Algoritma *link-state* juga dikenal dengan algoritma *shortest path first* (SPF). Algoritma ini memperbaiki informasi basis data dari informasi topologi. Algoritma *distance vector* memiliki informasi yang tidak spesifik tentang jarak jaringan dan tidak mengetahui jarak *router*. Sedangkan algoritma *link-state* memperbaiki kekurangan tersebut dan mempelajari bagaimana *router-router* saling terhubung.



Gambar 7 Elemen-elemen *Routing Link-state*

Gambar 7 mendeskripsikan elemen-elemen yang dimiliki oleh *routing link-state*, diantaranya:

a. *Link-state advertisement* (LSA), adalah paket kecil dari informasi *routing* yang dikirim antar *router*.
b. *Topological database*, adalah kumpulan informasi dari LSA-LSA.
c. SPF *Algorithm*, adalah hasil perhitungan pada basis data sebagai hasil dari pohon SPF.
d. Tabel *Routing*, adalah daftar rute dan *interface*.

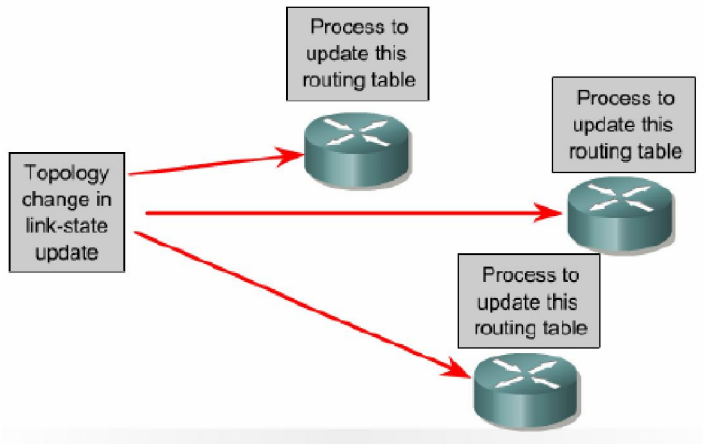


Gambar 8 Jaringan *Link-state Discovery*

Gambar 8 mengilustrasikan proses *discovery* dari *routing link-state*. Ketika *router* melakukan pertukaran LSA, dimulai dengan jaringan yang terhubung langsung tentang informasi yang mereka miliki. Masing-masing *router* membangun basis data topologi yang berisi pertukaran informasi LSA.

Algoritma SPF menghitung jaringan yang dapat dicapai. *Router* membangun topologi logika berbentuk pohon (*tree*), dengan *router* sebagai *root*. Topologi ini berisi semua rute-rute yang mungkin untuk mencapai jaringan dalam protokol *link-state internetwork*. *Router* kemudian

menggunakan SPF untuk memperpendek rute, mendaftarkan rute-rute terbaik dan *interface* ke jaringan yang dituju ke dalam tabel *routing*. *Link-state* juga memperbaiki basis data topologi yang lain dari elemen-elemen topologi dan status secara detail. *Router* pertama yang mempelajari perubahan topologi *link-state* mengirimkan informasi sehingga semua *router* dapat menggunakannya untuk proses pembaharuan.



Gambar 9 Perubahan Topologi *Link-state*

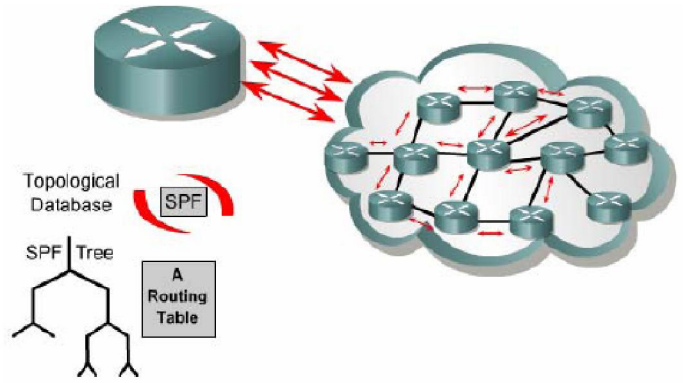
Gambar 9 adalah informasi *routing* dikirim ke semua *router* dalam *internetwork*. Untuk mencapai keadaan konvergen, setiap *router* mempelajari *router-router* tetangganya. Termasuk nama dari *router-router* tetangganya, status *interface* dan *cost* dari *link* ke tetangganya. *Router* membentuk paket LSA yang mendaftar informasi ini dari tetangga-tetangga baru, perubahan *cost link* dan *link-link* yang tidak lagi berlaku. Paket LSA ini kemudian dikirim keluar sehingga *router-router* lainnya menerima informasi tersebut.

Pada saat *router* menerima LSA, kemudian memperbaharui tabel *routing* dengan sebagian besar informasi yang terbaru. Data hasil perhitungan digunakan untuk membuat peta *internetwork* dan algoritma SPF digunakan untuk menghitung jalur terpendek ke jaringan lain. Jika paket LSA

menyebabkan perubahan pada basis data *link-state*, maka SPF melakukan perhitungan ulang untuk jalur terbaik dan memperbaharui tabel *routing*.

Ada beberapa kelemahan yang berhubungan dengan protokol *link-state*, diantaranya:

a. *Processor overhead*
b. Kebutuhan memori
c. Konsumsi *bandwidth*



Gambar 10 *Link-state Concern*

Router-router yang menggunakan protokol *link-state* membutuhkan memori lebih dan proses data yang lebih daripada *router-router* yang menggunakan protokol *distance vector*. *Router link-state* membutuhkan memori yang cukup besar untuk menangani semua informasi dari basis data, pohon topologi dan tabel *routing*. Gambar 10 menunjukkan inisialisasi paket *flooding link-state* yang mengkonsumsi *bandwidth*. Pada proses inisialisasi *discovery*, semua *router* yang menggunakan protokol *routing link-state* mengirimkan paket LSA ke semua *router* tetangganya. Peristiwa ini menyebabkan pengurangan *bandwidth* yang tersedia untuk me-*routing* trafik yang membawa data pengguna. Setelah inisialisasi *flooding* ini, protokol *routing link-state* pada umumnya membutuhkan *bandwidth* untuk mengirim paket-paket LSA yang menyebabkan perubahan topologi.

Pada *layer internet* TCP/IP, *router* dapat menggunakan protokol *routing* untuk membentuk *routing*, diantaranya:

1. RIP *(Routing Information Protocol)*

   Routing Information Protocol (RIP) adalah sebuah *routing protocol* yang menggunakan protokol *routing interior* dengan algoritma *distance vector*, dimana RIP mengirimkan *routing table* yang lengkap ke semua *interface* yang aktif setiap 30 detik. RIP hanya menggunakan jumlah *hop* untuk menentukan cara terbaik ke sebuah *network remote*, tetapi RIP secara *default* memiliki sejumah nilai jumlah *hop* maksimum yang diizinkan, yaitu 15 yang berarti 16 dianggap tidak terjangkau *(unreachable)*.

2. IGRP *(Interior Gateway Routing Protocol)*

   Interior Gateway Routing Protocol atau yang biasa dikenal dengan sebutan IGRP merupakan suatu protokol jaringan kepemilikan yang mengembangkan sistem Cisco. IGRP dirancang pada sistem otonomi untuk menyediakan suatu alternatif RIP *(Routing Information Protocol)*. IGRP merupakan suatu penjaluran jarak antara vektor protokol, yaitu bahwa masing-masing penjaluran bertugas untuk mengirimkan semua atau sebagian dari isi tabel penjaluran dalam penjaluran pesan untuk memperbaharui pada waktu tertentu untuk masing-masing penjaluran. Penjaluran memilih alur yang terbaik antara sumber dan tujuan. Untuk menyediakan fleksibilitas tambahan, IGRP mengijinkan untuk melakukan penjaluran multipath. Bentuk garis *equal bandwidth* dapat menjalankan arus lalu lintas dalam *round robin*, dengan melakukan peralihan secara otomatis kepada garis kedua jika sampai garis kesatu turun.

3. OSPF *(Open Shortest Path First)*

   Open Shortest Path First adalah *routing protocol* yang secara umum dapat digunakan seluruh *router* yang ada di dunia ini. *Router* cisco, seperti juniper, huawei dan lainnya dapat mengadopsi *routing protocol* OSPF. Teknologi yang digunakan oleh *routing protokol* ini adalah teknologi *link-state* yang memang didisain untuk bekerja dengan sangat

efisien dalam proses pengiriman *update* informasi rute. Cara *update*nya itu secara *triggered update*, maksudnya tidak semua informasi yg ada di *router* akan dikirim seluruhnya ke *router-router* lainnya, tetapi hanya informasi yang berubah/bertambah/berkurang saja yang akan dikirim ke semua *router* dalam satu area, sehingga mengefektifkan dan mengefisienkan *bandwidth* yg ada.

4. EIGRP (*Enhanced Interior Gateway Routing Protocol)*

   Enhanced Interior Gateway Routing Protocol (EIGRP) adalah sebuah protokol *proprietary* (milik) Cisco. Protokol EIGRP ini bekerja pada *router* Cisco dan pada prosesor-prosesor *route* internal. Protokol ini diterapkan pada *switch core layer* dan *switch distribution layer*. EIGRP menggunakan protokol *routing interior* dengan algoritma *advanced* Cisco *distance vector*

   EIGRP kadang-kadang disebut sebagai protokol *routing hybrid* karena protokol ini memiliki karakteistik-karakteristik baik dari protokol *distance-vector* maupun dari protokol *link-state*. EIGRP tidak mengirimkan paket-paket *link-state* seperti yang dilakukan OSPF, melainkan mengirimkan informasi pembaharuan *distance vector* yang tradisional yang berisi informasi tentang jaringan-jaringan, ditambah dengan *cost* untuk mencapai tujuan. EIGRP juga memiliki karakteristik-karakteristik *link-state*, yaitu menyinkronisasi tabel *routing* antara *router-router* tetangga pada saat mulai dijalankan. Setelah itu EIGRP mengirimkan informasi pembaharuan yang spesifik hanya jika topologi jaringan berubah. Karakteristik-karakteristik tersebut membuat EIGRP cocok untuk jaringan-jaringan berskala besar.menggunakan protokol *routing interior* dengan algoritma *advanced* Cisco *distance vector.*

Ada sejumlah fitur yang membuat EIGRP jauh lebih baik dibandingkan protokol-protokol lainnya, diantaranya sebagai berikut :

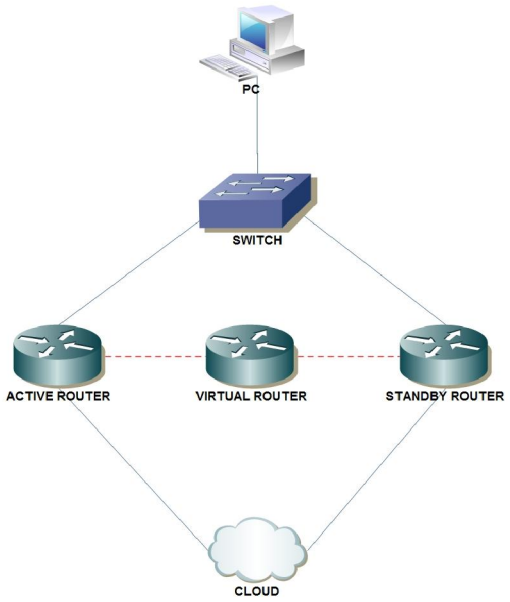
a. Mendukung IP, IPX dan AppleTalk melalui modul-modul yang bersifat protokol *dependent*.
b. Pencarian jaringan tetangga *(network discovery)* yang dilakukan dengan efisien.
c. Komunikasi melalui *Reliable Transport Protocol* (RTP).
d. Pemilihan jalur terbaik melalui *Diffusing Upadsate Algorithm* (DUAL).

5. BGP *(Border Gateway Protocol)*

   Border Gateway Protocol disingkat BGP adalah inti dari protokol *routing* internet. Protokol ini yang menjadi *backbone* dari jaringan internet dunia. BGP adalah protokol *routing* inti dari internet yg digunakan untuk melakukan pertukaran informasi *routing* antar jaringan. BGP menggunakan protokol *routing exterior* dengan algoritma *distance vector.*

II.4 Default Gateway Redundancy

Dalam model hirarkis yang dianjurkan, *switch-switch multilayer* pada *distribution layer* bertindak sebagai *default gateway* untuk semua *switch-switch access layer*. *Default gateway redundancy* sangat dibutuhkan untuk mengantisipasi dampak yang terjadi jika perangkat yang bertindak sebagai *default gateway* bermasalah/ gagal.



Gambar 11 Contoh Topologi *Default Gateway Redundancy*

II.4.1 HSRP - *Hot Standby Router Protocol*

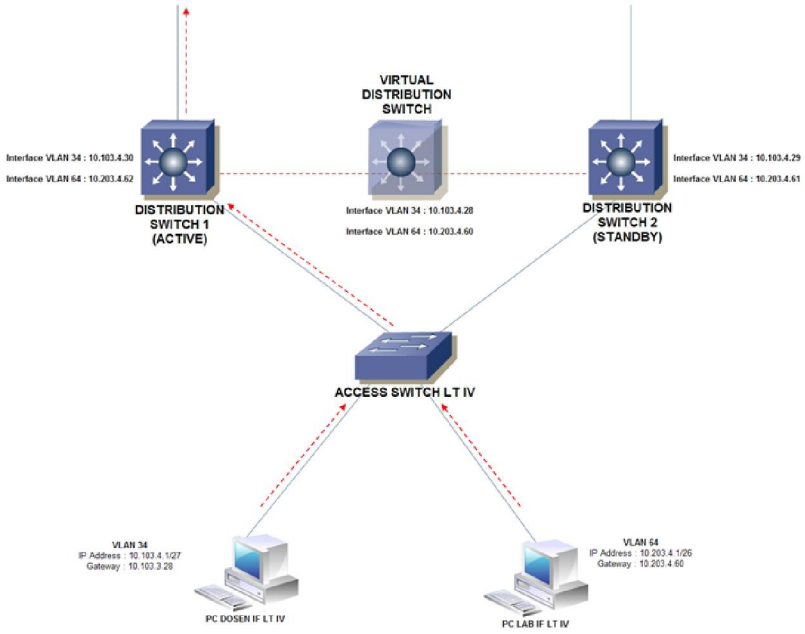
HSRP adalah sebuah protokol *redudancy* standar Cisco yang menetapkan sebuah *router* yang secara otomatis mengambil alih jika *router* utama gagal me-*routing*. HSRP mendefinisikan dua status *router* yaitu *router* aktif dan *router standby*. *Router standby* digunakan sebagai *redundancy* dari *router* aktif jika *router* aktif gagal me-*routing* [7]. HSRP adalah salah satu fitur perangkat lunak yang dapat dikonfigurasi untuk menyediakan *layer* 3 *redundancy* untuk *host-host* pada jaringan.

Dua *interface router* bekerja sama untuk menyediakan satu *virtual router* atau *default gateway* untuk *host* dalam sebuah jaringan. *Virtual router* tersebut digunakan agar jika salah satu *router* yang dikonfigurasi gagal, HSRP pada jaringan tersebut akan tetap berjalan dikarenakan alamat IP *gateway* yang dipakai *host* adalah alamat IP *virtual router*.

Sebuah HSRP *group* terdiri atas :

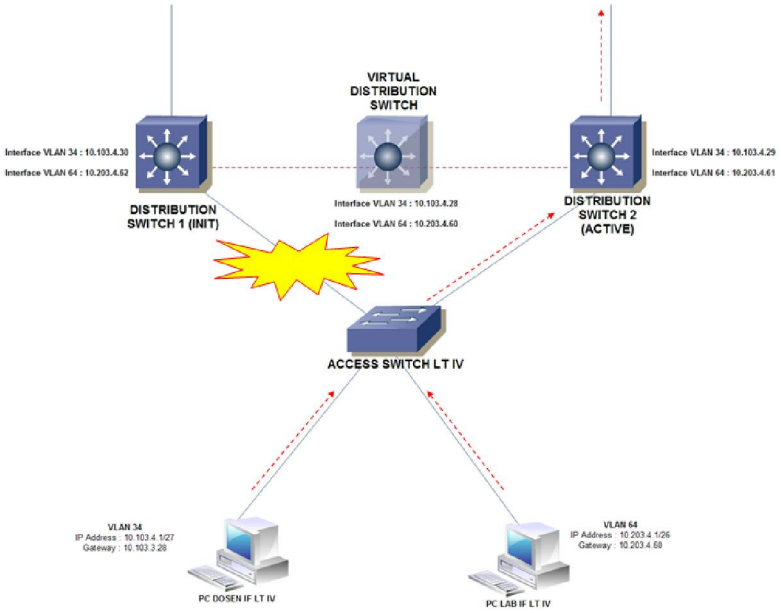
1. *Active Router* - *Router* yang meneruskan paket ke *virtual router*.
2. *Standby Router* - *router* yang berpatisipasi dalam HSRP yang mengemulasi *Virtual Router*.
3. *Virtual Router*.

HSRP *Active* dan *Standby Router* mengirimkan *hello message* ke alamat *multicast* 224.0.0.2 User Datagram Protocol (UDP) *port* 1985. Berikut adalah contoh implementasi *default gateway redundancy* menggunakan HSRP.



Gambar 12 Contoh Implementasi HSRP – Sebelum *Failover*

Gambar 12 mengilustrasikan bagaimana kondisi jaringan sebelum koneksi atau *active distribution switch* gagal. Hanya *active distribution switch* yang menerima paket yang sebenarnya ditujukan ke alamat MAC dan IP *virtual distribution switch*. *Standby distribution switch* tidak memiliki peranan apa-apa sampai jika koneksi atau *active distribution switch* gagal.



Gambar 13 Contoh Implementasi HSRP – *Setelah Failover*

Gambar 13 mengilustrasikan bagaimana kondisi jaringan jika koneksi atau *active distribution switch* gagal. Semua *frame* dan paket yang ditujukan ke alamat MAC dan IP *virtual distribution switch* akan secara otomatis berpindah jalur dan melalui *distribution* 2. Dalam kondisi ini, *distribution switch* 1 akan berubah status menjadi *standby distribution switch* dan *distribution switch* 2 akan berubah status menjadi *active distribution switch*.

II.4.2 VRRP – *Virtual Router Redundancy Protocol*

Pada dasarnya VRRP memiliki fungsi dan cara kerja yang serupa dengan HSRP, namun dengan beberapa fitur tambahan dan kesesuaian terhadap standar IEEE. Seperti HSRP, VRRP memperbolehkan sekelompok *router* membentuk satu *virtual router*. Dalam satu HSRP *group* atau VRRP *group*, sebuah *router* ditunjuk untuk mengelola semua permintaan yang ditujukan ke alamat *virtual* IP. Pada HSRP, *router* ini dinamakan *active router*, namun pada VRRP, *router* tersebut dinamakan *master router*.

Berikut adalah beberapa elemen-elemen yang membedakan VRRP dengan HSRP:

1. VRRP adalah protocol berstandar IEEE (RFC 2338 pada tahun 1998, dan kemudian RFC 3768 pada tahun 2005) untuk *redundancy router*. HSRP adalah protokol *proprietary* (milik) Cisco, diciptakan pada tahun 1994 dan disempurnakan berdasarkan RFC 2281 pada bulan Maret 1998.
2. Pada VRRP, *virtual router* mewakili sekelompok *router* yang biasanya dinamakan VRRP *group*.
3. Pada VRRP, *active router* dinamakan master *virtual router*.
4. Pada VRRP, *master virtual router* boleh memiliki alamat IP yang sama dengan *virtual router*.
5. Pada VRRP, beberapa *router* dapat bertindak sebagai *backup router*.
6. Komunikasi didalam sebuah *group* menggunakan alamat IP *multicast* 224.0.0.2. untuk HSRP dan 224.0.0.18 untuk VRRP.
7. HSRP dapat melacak *interface* dan objek namun VRRP hanya bisa melacak objek.
8. *Timer* VRRP lebih pendek dibandingkan HSRP. Hal ini membuat banyak *network administrator* menggangap VRRP lebih cepat daripada HSRP. Namun pada kenyataannya, kecepatan konvergensi pada saat terjadinya *failover* tergantung pada konfigurasi *timer* secara aktual.

Selain dari beberapa perbedaan diatas, HSRP dan VRRP memiliki cara kerja dan fitur yang sama. Perbedaan utama adalah HSRP merupakan protokol *proprietary* (milik) cisco dan VRRP adalah sebuah protokol *open standard*. Hal ini berakibat HSRP hanya ditemukan pada jaringan yang menggunakan produk cisco dan VRRP digunakan pada implementasi *multivendor*.

II.4.3 GLBP – *Gateway Load Balancing Protocol*

Gateway Load Balancing Protocol (GLBP) adalah protokol standar Cisco yang membagi kinerja *router* yang besarnya sama atau seimbang. *Gateway Load Balancing Protocol* (GLBP) sendiri lahir dari konsep *load balancing*, yang merupakan konsep yang gunanya untuk menyeimbangkan beban atau muatan pada

beberapa koneksi yang menuju jaringan tujuan yang sama. Dengan begitu koneksi jaringan tidak akan terganggu apabila terjadi kerusakan yang ditimbulkan oleh salah satu *router* tersebut.

Pada dasarnya GLBP adalah HSRP dan VRRP dengan penambahan kemampuan *load sharing* menggunakan cukup satu IP *gateway*. Pada *primary router* disebut sebagai *Active Virtual Gateway* (AVG), sedangkan *router* lainnya akan berperan sebagai *Active Virtual Forwarder* (AVF). Setiap *router* dalam GLBP *group* mengirimkan *hello message* setiap 3 detik menggunakan *multicast* 224.0.0.102 *port* UDP 3222. Pada GLBP, paket-paket yang dilewatkan akan dibagi oleh *router* yang terdapat dalam GLBP *group*, sehingga semua *router* dan koneksi akan berfungsi dalam pengiriman paket, sedangkan pada HSRP dan VRRP hanya koneksi utama saja yg aktif dan koneksi lainnya dalam status siaga.

Berikut ini adalah beberapa mekanisme kerja GLBP:

1. GLBP *Active Virtual Gateway*

   Anggota dari GLBP *group* memilih satu *gateway* yang akan menjadi *active virtual gateway* (AVG) untuk *group* tersebut. Anggota *group* lain menjadi pengganti AVG untuk menghindari jika AVG tersebut sewaktu-waktu tidak aktif lagi. *Gateway* lainnya menganggap hubungan perjalanan paket mengirim ke *virtual* MAC *address* ditentukan oleh AVG. G*ateway* yang mengetahui *active virtual* MAC *address,* selanjutnya AVG bertanggung jawab untuk menjawab *request* dari *address resolution protocol* (ARP) untuk meminta *virtual* IP *address*. *Load sharing* terjadi ketika AVG membalas ARP *request* dengan *virtual* MAC *address* yang berbeda.
2. GLBP *Virtual Gateway Redundancy*

   Menjalankan *Virtual Gateway Redundancy* pada GLBP sama dengan HSRP. *Gateway* yang berwenang untuk memutuskan adalah AVG, sedangkan *gateway* lainnnya sebagai *standby virtual gateway*. *Sedangkan gateway* yang tersisa ditempatkan di tempat yang sudah diperhatikan. Jika

terjadi kerusakan pada AVG, maka *standby virtual gateway* akan menerima tanggung jawab sebagai Virtual IP address. *Standby Virtual Gateway* yang baru akan ditempatkan di tempat yang mudah diperhatikan.

3. GLBP *Virtual Forwarder Redundancy*

   Virtual Forwarder Redundancy sama seperti *Virtual Gateway Redundancy* dengan suatu AVF. Apabila AVF mengalami gangguan, maka *Secondary Virtual Forwarder* (SVF) akan menerima status dan bertanggungjawab pada *virtual* MAC *address*. AVF yang baru akan menjadi *primary virtual forwarder* untuk sebuah nomor *forwarder* yang berbeda.

II.5 Access-list

Access Control Lists adalah daftar kondisi yang digunakan untuk menguji trafik jaringan yang mencoba melewati *interface* router. ACLs ini diimplementasikan pada router yang dijadikan gateway yang menghubungkan jaringan LAN dan WAN. Daftar ini memberitahu router, paket-paket mana yang akan diterima atau ditolak, yaitu penerimaan dan penolakan berdasarkan kondisi tertentu. Untuk mem-filter trafik jaringan, ACLs menentukan jika paket itu dilewatkan atau diblok pada *interface* router. Router ACLs membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port. Tanpa *Access-list*, semua paket bisa terpancarkan ke semua bagian pada jaringan. ACLs harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada *interface*, ACLs harus didefinisikan setiap protokol pada *interface*nya. ACLs mengontrol trafik pada satu arah dalam *interface*, sehingga dua ACLs terpisah harus dibuat untuk mengontrol trafik *inbound* (ke-dalam) dan *outbound* (ke-luar). Setiap *interface* boleh memiliki banyak protokol dan arah yang sudah didefinisikan.

II.5.1 Jenis-jenis *Access-list*

Acces-list memiliki dua jenis daftar akses, yaitu sebagai berikut:

1. *Standard access-list*

   Jenis *Access-list* ini hanya menggunakan alamat IP sumber dalam paket IP sebagai kondisi tes. Semua keputusan dibuat berdasarkan alamat IP sumber. Hal ini berarti bahwa daftar akses standar pada dasarnya mengizinkan atau menolak seluruh paket protokol, yaitu tidak adanya pembedaan antara berbagai jenis lalu lintas IP seperti WWW, Telnet, UDP dan lain-lain.

2. *Extended access-list*

   Extended access-list dapat mengevaluasi banyak bidang lain dalam lapisan 3 dan lapisan 4 *header* pada paket IP. Mereka dapat mengevaluasi sumber dan tujuan alamat IP, protokol lapangan di *header* lapisan *Network*, dan nomor *port* pada *header* lapisan *Transport*. Hal ini memberikan *Extended access-list* kemampuan untuk membuat keputusan yang jauh lebih rinci saat pengendalian lalu lintas.

II.5.2 Lalu lintas pada *interface*

Untuk menggunakan daftar akses sebagai paket *filter,* maka perlu diterapkan pada *interface* di sebuah router, yaitu dimana lalu lintas yang ingin disaring dan harus ditentukan lalu lintas yang ingin diterapkan *access list*. Ada dua jenis lalu lintas untuk antarmuka tunggal:

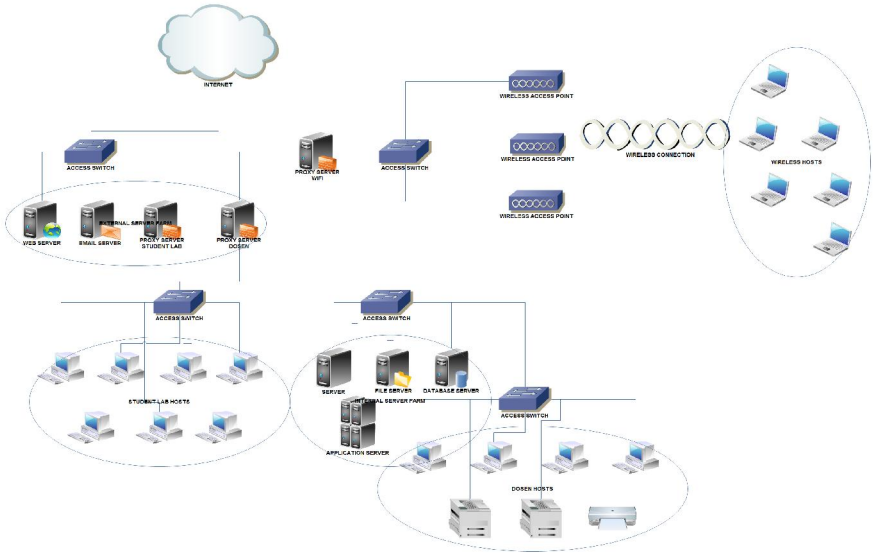
1. *Inbound access-list*

   Ketika *access-list* diterapkan di paket *inbound* pada *interface*, paket itu diproses melalui *access-list* sebelum di*routing* ke paket *outbound*. Beberapa paket yang ditolak tidak akan di*routing* karena mereka dihapus sebelum proses *routing* dipanggil.

2. *Outbound access-list*

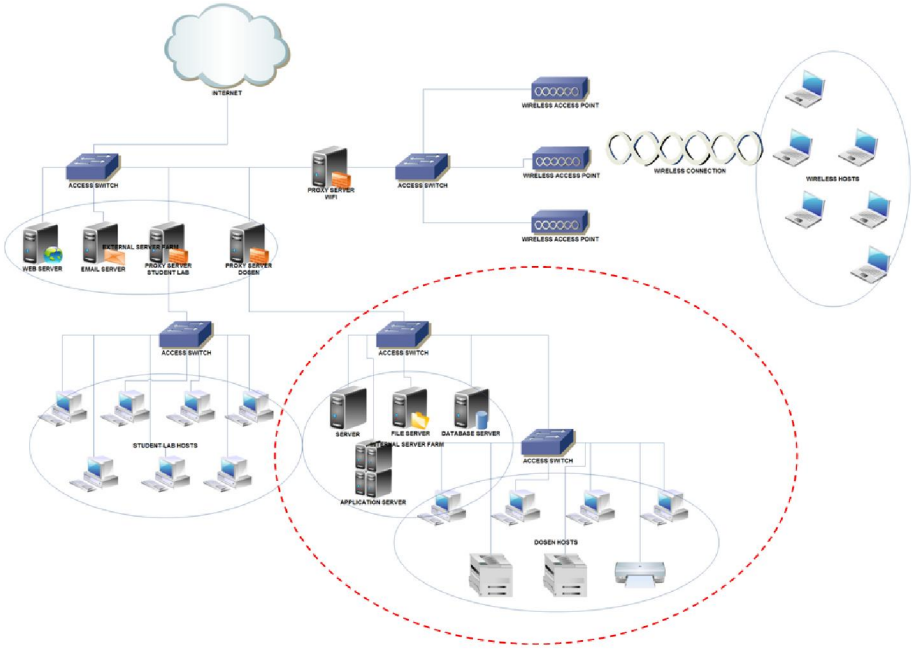
   Ketika daftar akses yang diterapkan pada paket *outbound* pada sebuah *interface*, paket tersebut diteruskan ke *outbound interface* dan kemudian diproses melalui daftar akses.

II.6 Infrastruktur Jaringan Saat Ini



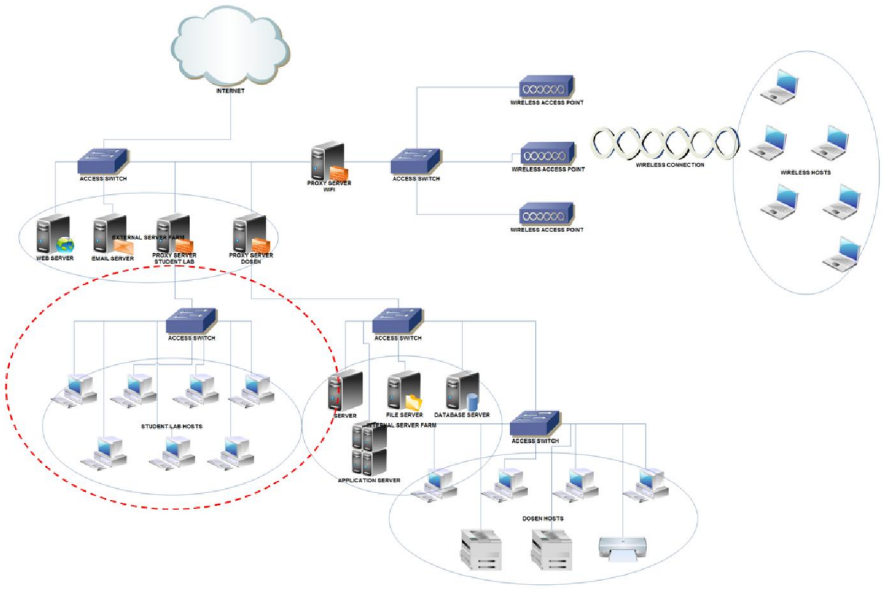
Gambar 14. Infrastruktur Jaringan Saat Ini

Gambar 14 mendeskripsikan infrastruktur jaringan Politeknik Negeri Batam saat ini. Jaringan internal Politeknik Negeri Batam terdiri dari tiga jaringan yang besar, yaitu jaringan dosen, jaringan *student lab* dan jaringan *wifi*. Jaringan-jaringan internal belum disegmentasi menjadi *subnet-subnet* yang lebih kecil, sehingga membentuk *broadcast domain* yang besar.



Gambar 15. *Broadcast Domain* Jaringan Dosen

Gambar 15 mendeskripsikan *broadcast domain* yang terjadi pada jaringan dosen. Jaringan ini memiliki beberapa internal *server* yang diletakkan dalam satu *subnet* dengan komputer-komputer dosen. Jaringan dosen menggunakan alamat 192.168.2.0/24, sehingga jumlah maksimum *host* yang dapat digunakan pada jaringan ini adalah 254 *host*.

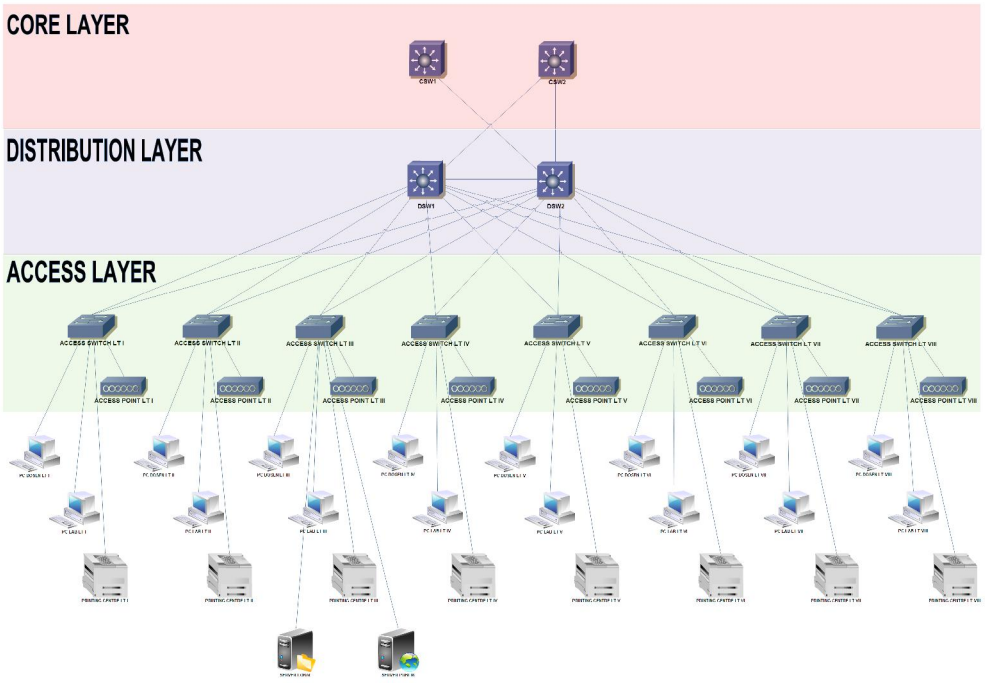


Gambar 16. *Broadcast Domain* Jaringan *Student Lab*

Gambar 16 mendeskripsikan *broadcast domain* yang terjadi pada jaringan *student lab*. Jaringan *student lab* menggunakan alamat 172.16.0.0/16 sehingga jumlah maksimum *host* yang dapat digunakan pada jaringan ini adalah 65534 *host*.

Bab III Analisis dan Perancangan

III.1 Perancangan Topologi



Gambar 18 Rancangan Topologi

Gambar 18 adalah rancangan jaringan Politeknik Negeri Batam sesuai dengan metode *Scalable Multilayer Campus Design.* Dalam rancangan ini terdapat tiga *layer* yaitu *access layer, distribution layer* dan *core layer*. Ketiga *layer* tersebut memiliki tugas dan peranannya masing-masing dalam jaringan Politeknik Negeri Batam.

III.1.1 *Access Layer*

Rancangan *access layer* digunakan untuk menyediakan fasilitas akses ke dalam jaringan bagi *host-host*. Fungsi utama *access layer* adalah menjadi sarana bagi suatu *host* yang ingin berhubungan dengan jaringan luar. *Switch-switch* yang terdapat pada *access layer* terhubung ke dua *distribution switch* yang berbeda,

yang digunakan untuk *redundancy*. Teknologi-teknologi yang diimplementasikan pada *access layer* antara lain sebagai berikut:

1. VLAN - VLAN berfungsi untuk segmentasi jaringan menjadi *broadcast domain* yang lebih kecil.
2. STP *Port-fast* - Seluruh *switchport* yang terhubung ke *end devices* (komputer, printer) akan diaktifkan STP *Port-fast*. *Port-fast* digunakan untuk mempercepat transisi *port host* untuk antisipasi jika transisi lambat dari berbagai kondisi STP. Tanpa mengaktifkan *port-fast*, kebanyakan koneksi akan mengalami *time-out* saat melakukan koneksi pertama kali.
3. Beberapa *security service* tambahan untuk meningkatkan sistem keamanan jaringan. *Security service* yang akan digunakan antara lain :
    a. *Port Security*, berfungsi untuk menghindari serangan pada tabel CAM (*Content Addressable Memory*). Apabila *switch* dihujani dengan alamat *mac* yang melebihi kemampuannya maka kinerja *switch* menurun secara drastis.
    b. DHCP *Snooping*, berfungsi untuk melindungi jaringan dari DHCP *server* palsu sehingga *user* tidak mendapatkan alamat IP yang keliru.
    c. *Dynamic* ARP *Inspection*, melindungi jaringan dari ARP *Spoofing*.

III.1.2 *Distribution Layer*

Fungsi utama *distribution layer* adalah menyediakan *routing, filtering* dan menentukan cara terbaik untuk menangani permintaan layanan dalam jaringan. Setelah *distribution layer* menentukan lintasan terbaik, selanjutnya permintaan diteruskan ke *core layer*. Koneksi antar *distribution switch* menggunakan *link layer* 3 agar terhindar dari *layer* 2 *loops*.

Teknologi-teknologi yang diimplementasikan pada *distribution layer* yaitu:

1. VRRP – VRRP merupakan *default gateway redudancy* yang berfungsi agar *host-host* pada *access layer* dapat terhubung ke jaringan luar walaupun salah satu *distribution switch* gagal.
2. OSPF – Protokol *Routing*.
3. *Access List* - *Access list* berfungsi untuk memfilter atau membatasi akses-akses yang tidak diijinkan.

III.1.3 *Core Layer*

Core Layer atau lapisan inti merupakan tulang punggung *(backbone)* sebuah *internetwork*. Dalam lapisan ini, data-data diteruskan secepatnya dengan menggunakan perangkat jaringan tercepat *(high speed)* seperti *Gigabit Ethernet*. Didalam lapisan ini tidak diijinkan melakukan penyaringan/*filter* paket data karena akan memperlambat transmisi data. *Layer* ini menggunakan koneksi *redundancy layer* 3, menghindari *layer* 2 *loops* dan rumitnya *redundancy layer* 2.

III.2 Pengalamatan IP

Pengalamatan IP digunakan sebagai alamat identifikasi untuk tiap *host* dalam jaringan yang menunjukkan alamat dari komputer tersebut pada jaringan. Dalam perancangan jaringan ini, pengalamatan IP menggunakan *Base Network* 10.0.0.0/8 yang memiliki *Address Range* 10.0.0.1 – 10.255.255.254. Pada pengalamatan IP ini, oktet kedua digunakan sebagai identitas kategori jaringan, sedangkan untuk oktet ketiga digunakan sebagai identitas pada lantai berapa *host* tersebut berada. Implementasi pengalamatan IP untuk oktet kedua dan oktet ketiga terdapat pada tabel 1 dan tabel 2.

Tabel 1 Pengalamatan IP pada oktet kedua

Nomor Oktet	Keterangan
101	Dosen Manajemen Bisnis
102	Dosen Informatika
103	Dosen Elektro
104	Dosen Teknik Mesin
201	Lab Manajemen Bisnis
202	Lab Informatika
203	Lab Elektronika
204	Lab Teknik Mesin
10	Server Lokal
20	Server Publik
30	Direksi
40	Pegawai
50	Wifi
60	Printing Center

Tabel 2 Pengalamatan IP pada oktet ketiga

Nomor Oktet	Keterangan
1	Lantai I
2	Lantai II
3	Lantai III
4	Lantai IV
5	Lantai V
6	Lantai VI
7	Lantai VII
8	Lantai VIII

Pengalamatan IP pada perancangan ini menerapkan *subnetting* pada setiap jaringan. Pada jaringan lab, pengalamatan IP akan menggunakan *subnet* /26.

Pengalamatan IP untuk jaringan *wifi* juga menggunakan subnet /26. *Subnet* /26 ini memiliki jumlah *host* maksimum 62 *host*. Sedangkan pada jaringan dosen akan menggunakan *subnet* /27. *Subnet* /27 ini memiliki jumlah *host* maksimum 30 *host*.

III.3 Penomoran VLAN

Pada implementasi teknologi VLAN, perancangan ini menggunakan dua angka untuk setiap nomor VLAN. Angka pertama digunakan sebagai identitas kategori jaringan, seperti Dosen Manajemen Bisnis, Lab Informatika dan lain-lain. Sedangkan untuk angka kedua digunakan sebagai identitas pada lantai berapa *host* tersebut berada. Implementasi penomoran VLAN terdapat pada tabel 3 dan tabel 4.

Tabel 3 Penomoran VLAN pada angka pertama

Angka Pertama VLAN	Keterangan
1	Dosen Manajemen Bisnis
2	Dosen Informatika
3	Dosen Elektro
4	Lab Manajemen Bisnis
5	Lab Informatika
6	Lab Elektro
7	Dosen Teknik Mesin
8	Lab Teknik Mesin
9	Server Lokal
10	Server Publik
11	Direksi
12	Pegawai
13	Wifi
14	Printing Center

Tabel 4 Penomoran VLAN pada angka kedua

Angka Kedua VLAN	Keterangan
1	Lantai I
2	Lantai II
3	Lantai III
4	Lantai IV
5	Lantai V
6	Lantai VI
7	Lantai VII
8	Lantai VIII

III.4 Teknologi-Teknologi Yang Diterapkan Pada Rancangan

Pada perancangan ini menerapkan beberapa teknologi yang disesuaikan dengan kebutuhan dan metode yang digunakan. Beberapa teknologi tersebut antara lain *local* VLAN, OSPF dan VRRP.

III.4.1 *Local* VLAN

Jaringan Politeknik Negeri Batam mengadopsi model *local* VLAN. VLAN yang terdapat pada salah satu *switch access* tidak akan ditemukan pada *switch access* yang lain, misalnya nomor VLAN jaringan dosen informatika yang berada di lantai VI berbeda dengan nomor VLAN jaringan dosen informatika yang berada di lantai VII. Koneksi antara *switch access* ke *switch distribution* menggunakan *trunk*. Jika *host* berpindah dari satu lokasi ke lokasi yang lain di dalam *campus network*, maka keanggotaan VLAN mereka akan berubah sesuai lokasi barunya. Dalam sebuah *local* VLAN, *layer* 2 *switching* diimplementasikan pada *layer access*, sedangkan *routing* diimplementasikan pada *layer distribution*.

III.4.2 *OSPF*

Perancangan jaringan *server* dan komputer ini menggunakan protokol *routing* OSPF. Berikut adalah beberapa alasan penggunaan protokol *routing* OSPF pada perancangan ini :

1. OSPF mendukung VLSM, dimana hampir semua alamat jaringan dari perancangan ini menggunakan IP *classless*.
2. OSPF dapat diimplementasikan pada multivendor atau produk-produk *non*-Cisco. Langkah ini merupakan tindakan preventif jika Politeknik Negeri Batam akan menggunakan produk *non*-Cisco seperti Juniper dan Huawei di kemudian hari.

III.4.3 *VRRP*

Jaringan Politeknik Negeri Batam menggunakan VRRP sebagai *default gateway redundancy* untuk mengantisipasi putusnya akses *host* ke jaringan luar jika perangkat yang bertindak sebagai *default gateway* bermasalah atau gagal.

Alasan penggunaan VRRP dikarenakan protokol ini dapat diimplementasikan pada multivendor atau produk-produk *non*-Cisco. Langkah ini merupakan tindakan preventif jika Politeknik Negeri Batam akan menggunakan produk *non*-cisco seperti juniper dan huawei di kemudian hari. Selain masalah kompatibilitas, VRRP juga memiliki waktu konvergensi yang lebih pendek dibandingkan HSRP tanpa melalui konfigurasi yang lebih jauh.

III.4.4 *Access-list*

Access-list pada jaringan Politeknik Negeri Batam bertujuan untuk menyaring paket yang tidak diinginkan ketika menerapkan kebijakan-kebijakan keamanan. *Access-list* bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. *Access-list* menjadi *tool* pilihan untuk pengambilan keputusan pada situasi ini.

Ilustrasi rancangan *access-list* yang akan diimplementasikan pada jaringan Politeknik Negeri Batam, secara garis besar yaitu sebagai berikut:

1. Jaringan dosen, pegawai dan direksi dapat mengakses internet, *server farm* lokal, *server farm* public dan *printer centre*.
2. Jaringan laboratorium mahasiswa hanya bisa mengakses ke *server farm* publik melalui *port* 80 saja.
3. Wifi hanya bisa mengakses internet *port* 80 dan *port* 443 saja (akses ke *server farm* publik melalui IP publik).

III.5 Kebutuhan Perangkat keras

Implementasi jaringan *server* dan komputer Politeknik Negeri Batam dengan metode Scalable Multilayer Campus Design membutuhkan perangkat keras yang dipilih dengan pertimbangan berdasarkan fitur-fitur yang dibutuhkan dan biaya untuk pengadaan perangkat tersebut. Berikut tabel kebutuhan perangkat keras pada *layer core, distribution* dan *access*:

Tabel 5 Kebutuhan perangkat keras pada *core layer*

Vendor	Cisco
Tipe	WS-C3750G-12S-E *with Enhanced Multilayer Image.*
Jumlah	2
Spesifikasi	*12 SFP-based Gigabit Ethernet ports, 32-Gbps, high-speed stacking bus, Innovative stacking technology, 1 RU stackable multilayer switch, Enterprise-class intelligent services delivered to the network edge dan IP Services software feature set (IPS).*
Keterangan	Router-switch cisco tipe ini memiliki fitur teknologi Cisco *StackWise* yang merupakan interkoneksi tumpukan 32 Gbps yang memungkinkan pelanggan untuk membangun sistem *switching* terpadu.

Tabel 6 Kebutuhan perangkat keras pada *distribution layer*

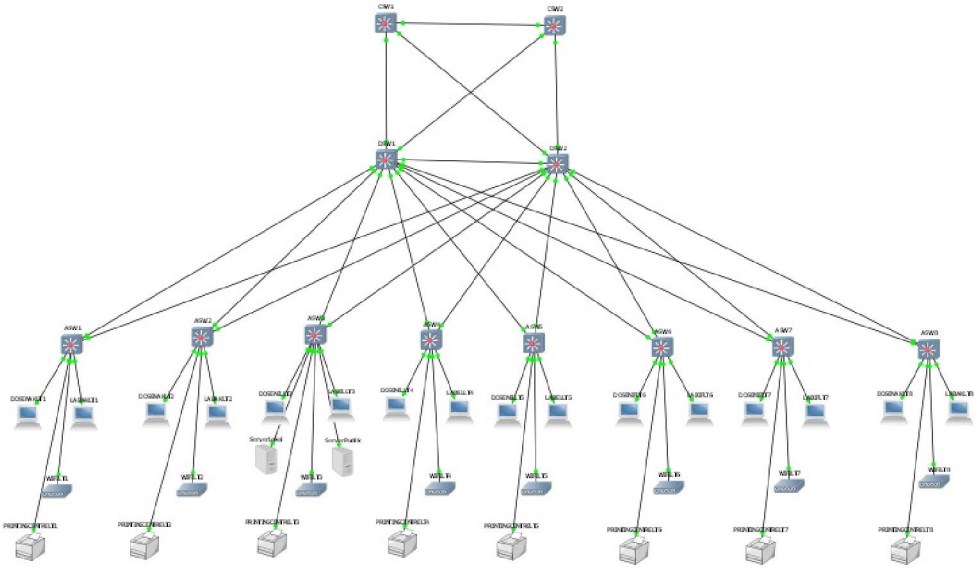
Vendor	Cisco
Tipe	WS-C3560G-48TS-E *with Enhanced Multilayer Image.*
Jumlah	2
Spesifikasi	*48 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports, 1RU fixed-configuration, multilayer switch, Enterprise-class intelligent services delivered to the network edge, IP Services software feature set (IPS) dan Provides full IPv6 dynamic routing.*
Keterangan	Router-switch cisco tipe ini memiliki fitur switch kelas enterprise yang mencakup IEEE 802.3af. Router-switch cisco ini juga memiliki fungsi Power Cisco prestandard over Ethernet (PoE) dalam konfigurasi Fast Ethernet dan Gigabit Ethernet. Cisco catalyst 3560 memiliki beberapa fitur lainnya seperti *default gateway redundancy* HSRP/VRRP, protokol *routing* OSPF/EIGRP, Access List dan Filtering.

Tabel 7 Kebutuhan perangkat keras pada *access layer*

Vendor	Cisco
Tipe	Cisco Catalyst WS-C2960G 48TC-L *with* LAN *Image*
Jumlah	16
Spesifikasi	*48-48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports.*
Keterangan	Switch cisco tipe ini memiliki beberapa fitur seperti VLAN, STP PortFast, *port security*, DHCP *snooping*, *Dynamic* ARP *Inspection*.

Bab IV Implementasi dan Pengujian

IV.1 Implementasi Menggunakan Simulator GNS3



Gambar 19 Rancangan topologi pada simulator GNS3

IV.1.1 Konfigurasi pada *Access Switch*

Masing-masing *access switch* memiliki dua *link,* yaitu fa1/14 dan fa1/15 menuju *distribution switch*. *Link-link* tersebut dikonfigurasi menjadi *mode trunk* agar bisa dilewati oleh *frame-frame* dari banyak VLAN. Selain dari dua *link* tersebut, *link-link* lainnya yang terhubung langsung ke *end devices*, dikonfigurasi menjadi *mode access* dan STP *portfast* diaktifkan.

Tabel 8 Contoh konfigurasi *switchmode trunk* pada ASW1

Perintah	Tujuan
ASW1>en	Masuk ke *privilege mode.*
ASW1#conf t	Masuk ke *global config.*
ASW1(config)#int range fa1/14 - 15	Masuk ke *interface level* yang akan dikonfigurasi ke *trunk.*

ASW1(config-if-range)#switchport	Konfigurasi *interface* menjadi *interface layer 2.*
ASW1(config-if-range)#switchport mode trunk	Konfigurasi *interface* menjadi *trunk.*
ASW1(config-if-range)#switchport trunk encapsulation dot1q	Konfigurasi enkapsulasi *trunk* ke dot1q.
ASW1(config-if-range)#switchport trunk allowed vlan 1,11,41,131,141,1002-1005	Konfigurasi agar hanya VLAN 1, 11, 41, 131, 141, 1002 sampai 1005 yang bisa melewati *trunk* ini.
ASW1(config-if-range)#no shut	Konfigurasi agar *interface* tidak *administrative down.*

Tabel 9 Contoh konfigurasi *switchmode access* pada ASW1

Perintah	Tujuan
ASW1>en	Masuk ke *privilege mode.*
ASW1#conf t	Masuk ke *global config.*
ASW1(config)#int range fa1/1 - 13	Masuk ke *interface level* yang akan dikonfigurasi ke *access.*
ASW1(config-if-range)#switchport	Konfigurasi *interface* menjadi *interface layer* 2.
ASW1(config-if-range)#switchport mode access	Konfigurasi *interface* menjadi *access.*
ASW1(config-if-range)#spanning-tree portfast	Konfigurasi *interface* menjadi *portfast.*
ASW1(config-if-range)#no shut	Konfigurasi agar *interface* tidak *administrative down.*

IV.1.2 Konfigurasi pada *Distribution Switch*

Distribution switch mempunyai peranan yang sangat vital pada jaringan ini, dimana *first hop redundancy*, protokol *routing* dan *access-list* dikonfigurasi pada *layer* ini.

Tabel 10 Konfigurasi VRRP VLAN 11 pada DSW1

Perintah	Tujuan
DSW1>en	Masuk ke *privilege mode.*
DSW1#conf t	Masuk ke *global config.*
DSW1(config)#int vlan 11	Masuk ke *interface level* yang akan dikonfigurasi VRRP.
DSW1(config-if)#vrrp 11 ip 10.101.1.28	Aktifkan VRRP untuk VLAN 11 dengan alamat *virtual router* 10.101.1.28.
DSW1(config-if)#vrrp 11 priority 110	Konfigurasi DSW1 menjadi *master router* untuk VLAN 11.
DSW1(config-if)#vrrp 11 timers advertise msec 500	Dikarenakan DSW1 merupakan *master router* untuk VLAN 11, maka status aktifnya akan dikirim setiap 500 milidetik.
DSW1(config-if)#vrrp 11 track 99 decrement 20	Melakukan *tracking* ke 99 (*link* ke *core layer*), jika *link* putus maka *priority* akan berkurang 20.

Tabel 11 Konfigurasi VRRP VLAN 11 pada DSW2

Perintah	Tujuan
DSW2>en	Masuk ke *privilege mode.*
DSW2#conf t	Masuk ke *global config.*
DSW2(config)#int vlan 11	Masuk ke *interface level* yang akan dikonfigurasi VRRP.
DSW2(config-if)#vrrp 11 ip	Aktifkan VRRP untuk VLAN 11

10.101.1.28	dengan alamat *virtual router* 10.101.1.28.
DSW2(config-if)#vrrp 11 timers learn	Mempelajari status aktifnya DSW1.

Tabel 12 Konfigurasi protokol *routing* pada DSW1

Perintah	Tujuan
DSW1>en	Masuk ke *privilege mode.*
DSW1#conf t	Masuk ke *global config.*
DSW1(config)#router ospf 1	Aktifkan protokol *routing* OSPF dengan ID 1.
DSW1(config-router)#network 10.0.0.0 0.255.255.255 area 0	Konfigurasi alamat jaringan untuk OSPF dengan nomor area 0.

Tabel 13 Konfigurasi protokol *routing* pada DSW2

Perintah	Tujuan
DSW2>	Masuk ke *privilege mode.*
DSW2#conf t	Masuk ke *global config.*
DSW2(config)#router ospf 1	Aktifkan protokol *routing* OSPF dengan ID 1.
DSW2(config-router)#network 10.0.0.0 0.255.255.255 area 0	Konfigurasi alamat jaringan untuk OSPF dengan nomor area 0.

Tabel 14 Konfigurasi *loopback interface* untuk dijadikan *router* ID pada DSW1

Perintah	Tujuan
DSW1>en	Masuk ke *privilege mode.*
DSW1#conf t	Masuk ke *global config.*
DSW1(config)#interface loopback 0	Aktifkan *interface loopback* 0
DSW1(config-if)#ip address 3.3.3.3 255.255.255.255	Konfigurasi alamat IP *interface loopback* 0 untuk dijadikan *router* ID

Tabel 15 Konfigurasi *loopback interface* untuk dijadikan *router* ID pada DSW2

Perintah	Tujuan
DSW2>en	Masuk ke *privilege mode.*
DSW2#conf t	Masuk ke *global config.*
DSW2(config)#interface loopback 0	Aktifkan *interface loopback* 0
DSW2(config-if)#ip address 4.4.4.4 255.255.255.255	Konfigurasi alamat IP *interface loopback* 0 untuk dijadikan *router* ID

Tabel 16 Konfigurasi DSW1 menjadi DR Other untuk OSPF

Perintah	Tujuan
DSW1>en	Masuk ke *privilege mode.*
DSW1#conf t	Masuk ke *global config.*
DSW1(config)#interface range fa1/13 - 14	Masuk ke *interface level fast ethernet* 1/13 dan 1/14
DSW1(config-if-range)#ip ospf priority 0	Konfigurasi *interface* ospf *priority* menjadi 0 (*Designated Router Other*)
DSW1(config-if-range)#interface fa2/0	Masuk ke *interface level fast ethernet* 2/0
DSW1(config-if)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 0 (*Designated Router Other*)

Tabel 17 Konfigurasi DSW2 menjadi DR Other untuk OSPF

Perintah	Tujuan
DSW2>en	Masuk ke *privilege mode.*
DSW2#conf t	Masuk ke *global config.*
DSW2(config)#interface range fa1/13 - 14	Masuk ke *interface level fast ethernet* 1/13 dan 1/14
DSW2(config-if-range)#ip ospf priority 0	Konfigurasi *interface* ospf *priority* menjadi 0 (*Designated Router Other*)
DSW2(config-if-range)#interface fa2/0	Masuk ke *interface level fast ethernet*

	2/0
DSW2(config-if)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 0 (*Designated Router Other*)

Tabel 18 Konfigurasi *access-list* pada jaringan lab lantai 1 di DSW1

Perintah	Tujuan
DSW1>en	Masuk ke *privilege mode.*
DSW1#conf t	Masuk ke *global config.*
DSW1(config)#access-list 100 remark LAB-TO-SERVERPUBLIK-ONLY-HTTP-ONLY	Menulis *access-list* 100 dengan penandaan LAB-TO-SERVERPUBLIK-ONLY-HTTP-ONLY.
DSW1(config)#access-list 100 permit ospf any any	Mengizinkan paket-paket OSPF melewati *access-list* 100.
DSW1(config)#access-list 100 permit ip host 224.0.0.18 any	Mengizinkan paket-paket VRRP melewati *access-list* 100.
DSW1(config)#access-list 100 permit ip any host 224.0.0.18	Mengizinkan paket-paket VRRP melewati *access-list* 100.
DSW1(config)#access-list 100 permit tcp 10.200.0.0 0.7.255.255 10.20.3.0 0.0.0.15 eq www	Mengizinkan jaringan lab mengakses jaringan *server* publik hanya melewati port 80.
DSW1(config)#exit	Kembali ke *privilege mode.*
DSW1(config)#int vlan 41	Masuk ke *interface* jaringan lab lantai 1.
DSW1(config)# ip access-group 100 in	Memasang *access-list* 100 pada *interface* jaringan lab lantai 1.

Tabel 19 Konfigurasi access-list pada jaringan lab lantai 1 di DSW2

Perintah	Tujuan
DSW2>en	Masuk ke *privilege mode.*
DSW2#conf t	Masuk ke *global config.*
DSW2(config)#access-list 100 remark LAB-TO-SERVERPUBLIK-ONLY-HTTP-ONLY	Menulis *access-list* 100 dengan penandaan LAB-TO-SERVERPUBLIK-ONLY-HTTP-ONLY.
DSW2(config)#access-list 100 permit ospf any any	Mengizinkan paket-paket OSPF melewati *access-list* 100.
DSW2(config)#access-list 100 permit ip host 224.0.0.18 any	Mengizinkan paket-paket VRRP melewati *access-list* 100.
DSW2(config)#access-list 100 permit ip any host 224.0.0.18	Mengizinkan paket-paket VRRP melewati *access-list* 100.
DSW2(config)#access-list 100 permit tcp 10.200.0.0 0.7.255.255 10.20.3.0 0.0.0.15 eq www	Mengizinkan jaringan lab mengakses jaringan *server* publik hanya melewati port 80.
DSW2(config)#exit	Kembali ke *privilege mode.*
DSW2(config)#int vlan 41	Masuk ke *interface* jaringan lab lantai 1.
DSW2(config)# ip access-group 100 in	Memasang *access-list* 100 pada *interface* jaringan lab lantai 1.

IV.1.3 Konfigurasi pada *Core Switch*

Pada *Core Switch* hanya diimplementasikan protokol *routing* OSPF yang bertujuan untuk mengurangi waktu *latency* dalam penyampaian paket. Selain itu juga mengimplementasikan *loopback interface* yang difungsikan sebagai *router* ID.

Tabel 20 Konfigurasi protokol *routing* pada CSW1

Perintah	Tujuan
CSW1>en	Masuk ke *privilege mode.*
CSW1#conf t	Masuk ke *global config.*
CSW1(config)#router ospf 1	Aktifkan protokol *routing* OSPF dengan ID 1.
CSW1(config-router)#network 10.0.0.0 0.255.255.255 area 0	Konfigurasi alamat jaringan untuk OSPF dengan nomor area 0.

Tabel 21 Konfigurasi protokol *routing* pada CSW2

Perintah	Tujuan
CSW2>en	Masuk ke *privilege mode.*
CSW2#conf t	Masuk ke *global config.*
CSW2(config)#router ospf 1	Aktifkan protokol *routing* OSPF dengan ID 1.
CSW2(config-router)#network 10.0.0.0 0.255.255.255 area 0	Konfigurasi alamat jaringan untuk OSPF dengan nomor area 0.

Tabel 22 Konfigurasi *loopback interface* untuk dijadikan *router* ID pada CSW1

Perintah	Tujuan
CSW1>en	Masuk ke *privilege mode.*
CSW1#conf t	Masuk ke *global config.*
CSW1(config)#interface loopback 0	Aktifkan *interface loopback* 0
CSW1(config-if)#ip address 1.1.1.1 255.255.255.255	Konfigurasi alamat IP *interface loopback* 0 untuk dijadikan *router* ID

Tabel 23 Konfigurasi *loopback interface* untuk dijadikan *router* ID pada CSW2

Perintah	Tujuan
CSW2>en	Masuk ke *privilege mode.*
CSW2#conf t	Masuk ke *global config.*

CSW2(config)#interface loopback 0	Aktifkan *interface loopback* 0
CSW2(config-if)#ip address 2.2.2.2 255.255.255.255	Konfigurasi alamat IP *interface loopback* 0 untuk dijadikan *router* ID

Tabel 24 Konfigurasi CSW1 menjadi Designated Router untuk OSPF

Perintah	Tujuan
CSW1>en	Masuk ke *privilege mode.*
CSW1#conf t	Masuk ke *global config.*
CSW1(config)#interface range fa0/0 - 1	Masuk ke *interface level fast ethernet* 0/0 dan 0/1
CSW1(config-if-range)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 1 (*Designated Router*)
CSW1(config-if-range)#interface fa1/0	Masuk ke *interface level fast ethernet* 1/0
CSW1(config-if)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 1 (*Designated Router*)

Tabel 25 Konfigurasi CSW2 menjadi Designated Router untuk OSPF

Perintah	Tujuan
CSW2>en	Masuk ke *privilege mode.*
CSW2#conf t	Masuk ke *global config.*
CSW2(config)#interface range fa0/0 - 1	Masuk ke *interface level fast ethernet* 0/0 dan 0/1
CSW2(config-if-range)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 1 (*Designated Router*)
CSW2(config-if-range)#interface fa1/0	Masuk ke *interface level fast ethernet* 1/0
CSW2(config-if)#ip ospf priority 1	Konfigurasi *interface* ospf *priority* menjadi 1 (*Designated Router*)

IV.2 Analisis dan Pengujian

Implementasi rancangan ini menggunakan *simulator* GNS3 dengan IOS cisco, sehingga hasil yang diperoleh mendekati kualitas dari perangkat cisco aslinya. Perancangan jaringan *server* dan komputer ini hanya memakai protokol-protokol *open standard*. Hal ini dilakukan agar Politeknik Negeri Batam dapat menggunakan produk-produk *non*-cisco yang harganya jauh lebih murah. Pengujian pada perancangan ini dilakukan terhadap beberapa teknologi utama seperti protokol *routing* OSPF, protokol *redundancy* VRRP dan *access-list*. Dari pengujian pada *simulator* GNS3, diperoleh hasil yang sesuai dengan perancangan yang telah dibangun. Berikut adalah pengujian terhadap protokol *routing* OSPF, protokol *redundancy* VRRP dan *access-list*.

1. Pengujian Protokol *Routing* OSPF

   Pengujian pada protokol *routing* OSPF ini melakukan pengecekan *router-router* mana saja yang menjadi *router* tetangga dalam satu *area* OSPF *network*. Selain itu juga dilakukan pengecekan tabel *routing*.

```
CSW1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:31    10.100.5.2      FastEthernet1/
0
4.4.4.4           0   FULL/DROTHER    00:00:36    10.100.3.2      FastEthernet0/
1
3.3.3.3           0   FULL/DROTHER    00:00:36    10.100.1.2      FastEthernet0/
0
CSW1#
```

Gambar 20 Pengecekan *router* tetangga dari CSW1

Gambar 20 mendeskripsikan bahwa *router-router* tetangga dari CSW1 yaitu CSW2 dengan *neighbor id* 2.2.2.2, DSW1 dengan *neighbor id* 3.3.3.3 dan DSW2 dengan *neighbor id* 4.4.4.4.

```
CSW2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:36    10.100.5.1      FastEthernet1/
0
3.3.3.3           0   FULL/DROTHER    00:00:31    10.100.4.2      FastEthernet0/
1
4.4.4.4           0   FULL/DROTHER    00:00:31    10.100.2.2      FastEthernet0/
0
CSW2#
```

Gambar 21 Pengecekan *router* tetangga dari CSW2

Gambar 21 mendeskripsikan bahwa *router-router* tetangga dari CSW2 yaitu CSW1 dengan *neighbor id* 1.1.1.1, DSW1 dengan *neighbor id* 3.3.3.3 dan DSW2 dengan *neighbor id* 4.4.4.4.

```
DSW1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           0   2WAY/DROTHER    00:00:35    10.100.0.2      FastEthernet2/
0
1.1.1.1           1   FULL/DR         00:00:30    10.100.1.1      FastEthernet1/
14
2.2.2.2           1   FULL/DR         00:00:30    10.100.4.1      FastEthernet1/
13
DSW1#
```

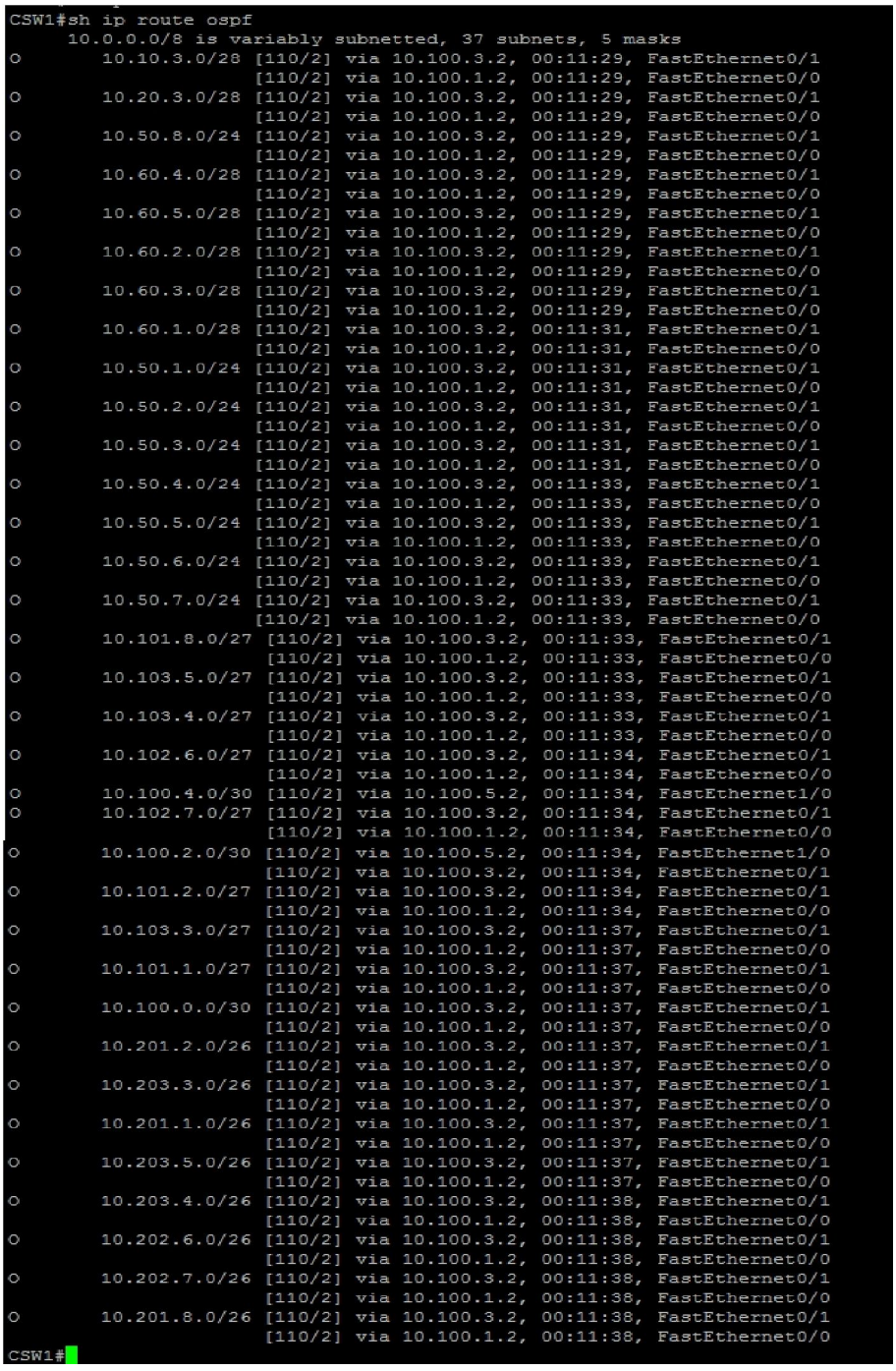
Gambar 22 Pengecekan *router* tetangga dari DSW1

Gambar 22 mendeskripsikan bahwa *router-router* tetangga dari DSW1 yaitu CSW1 dengan *neighbor id* 1.1.1.1, CSW2 dengan *neighbor id* 2.2.2.2 dan DSW2 dengan *neighbor id* 4.4.4.4.

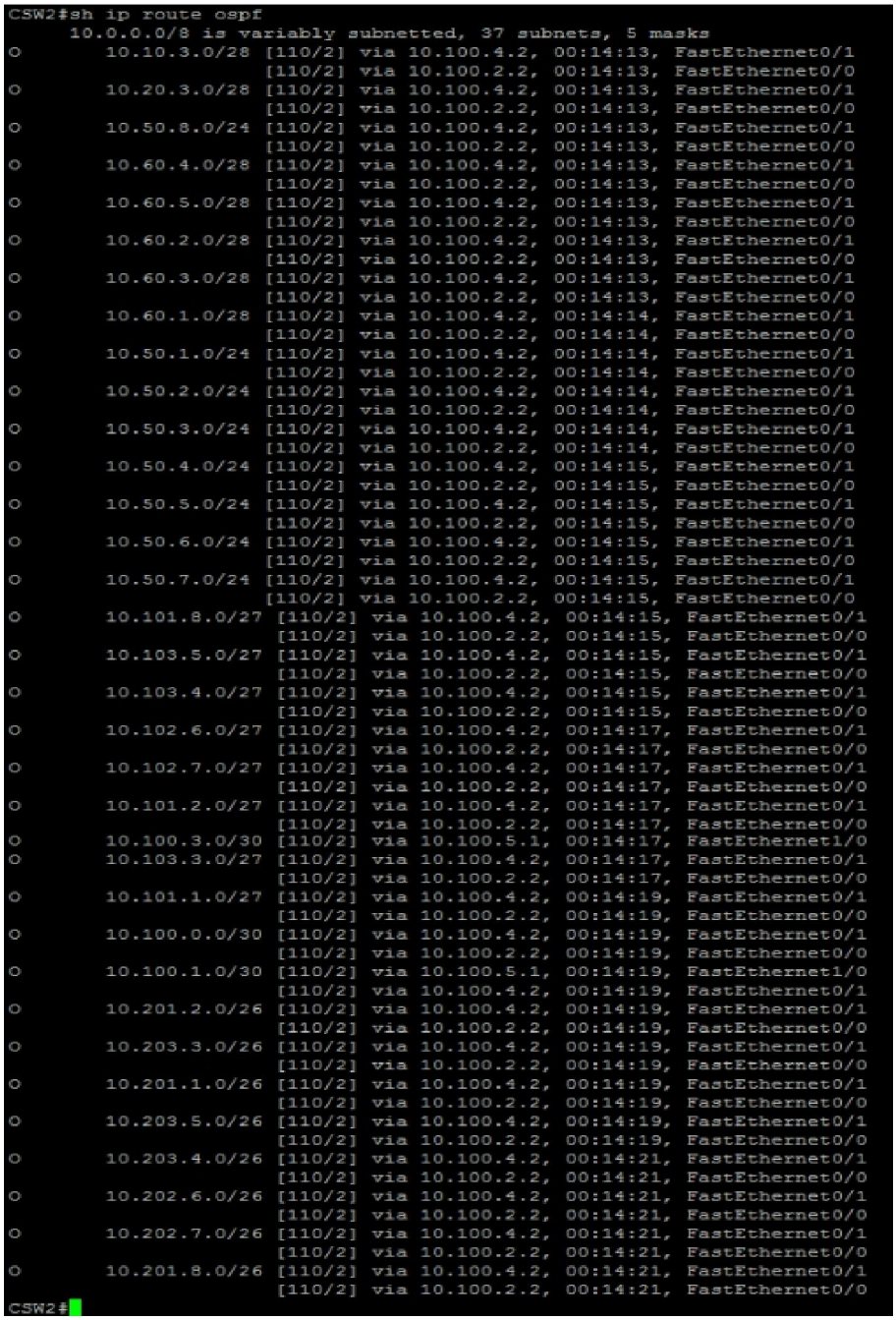
```
DSW2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   2WAY/DROTHER    00:00:38    10.100.0.1      FastEthernet2/
0
2.2.2.2           1   FULL/DR         00:00:33    10.100.2.1      FastEthernet1/
14
1.1.1.1           1   FULL/DR         00:00:33    10.100.3.1      FastEthernet1/
13
DSW2#
```

Gambar 23 Pengecekan *router* tetangga dari DSW2

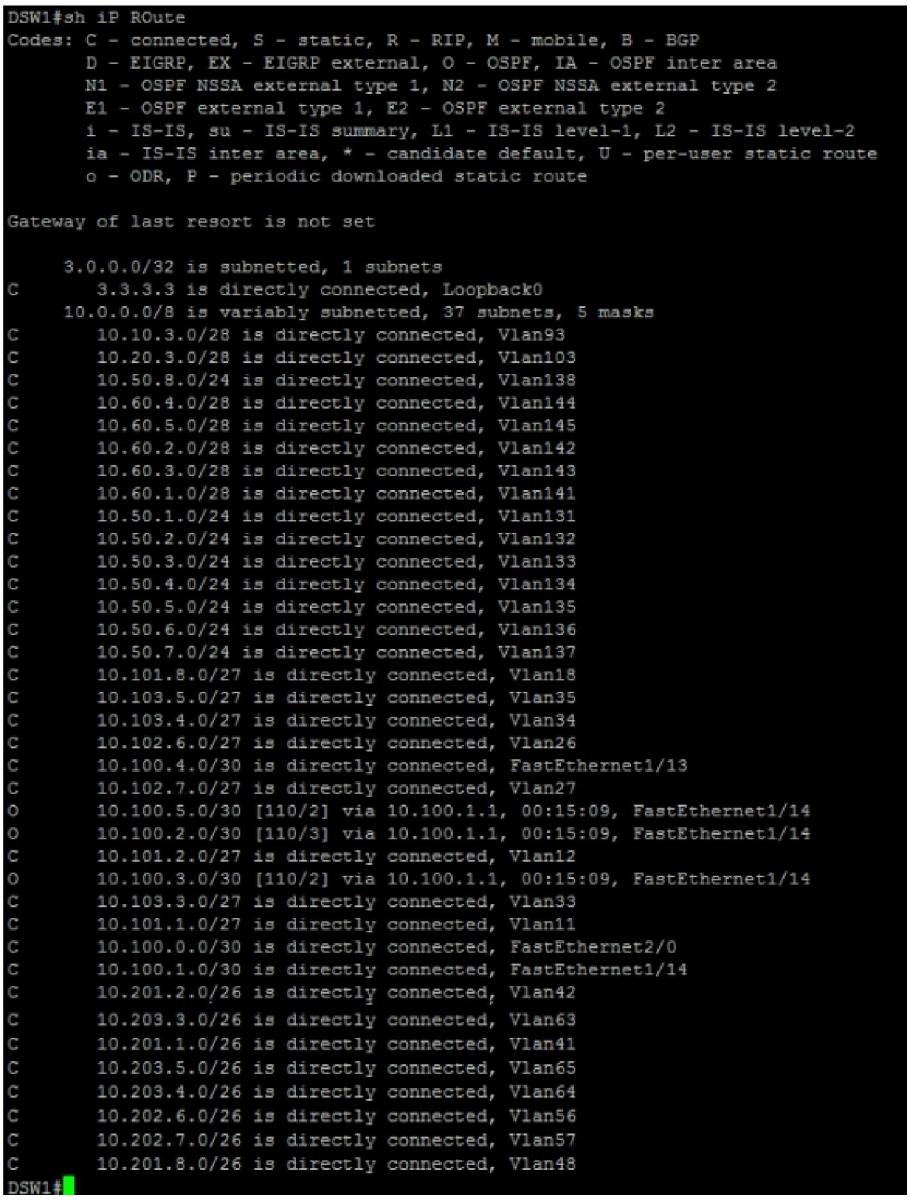
Gambar 23 mendeskripsikan bahwa *router-router* tetangga dari DSW2 yaitu CSW1 dengan *neighbor id* 1.1.1.1, CSW2 dengan *neighbor id* 2.2.2.2 dan DSW1 dengan *neighbor id* 3.3.3.3.



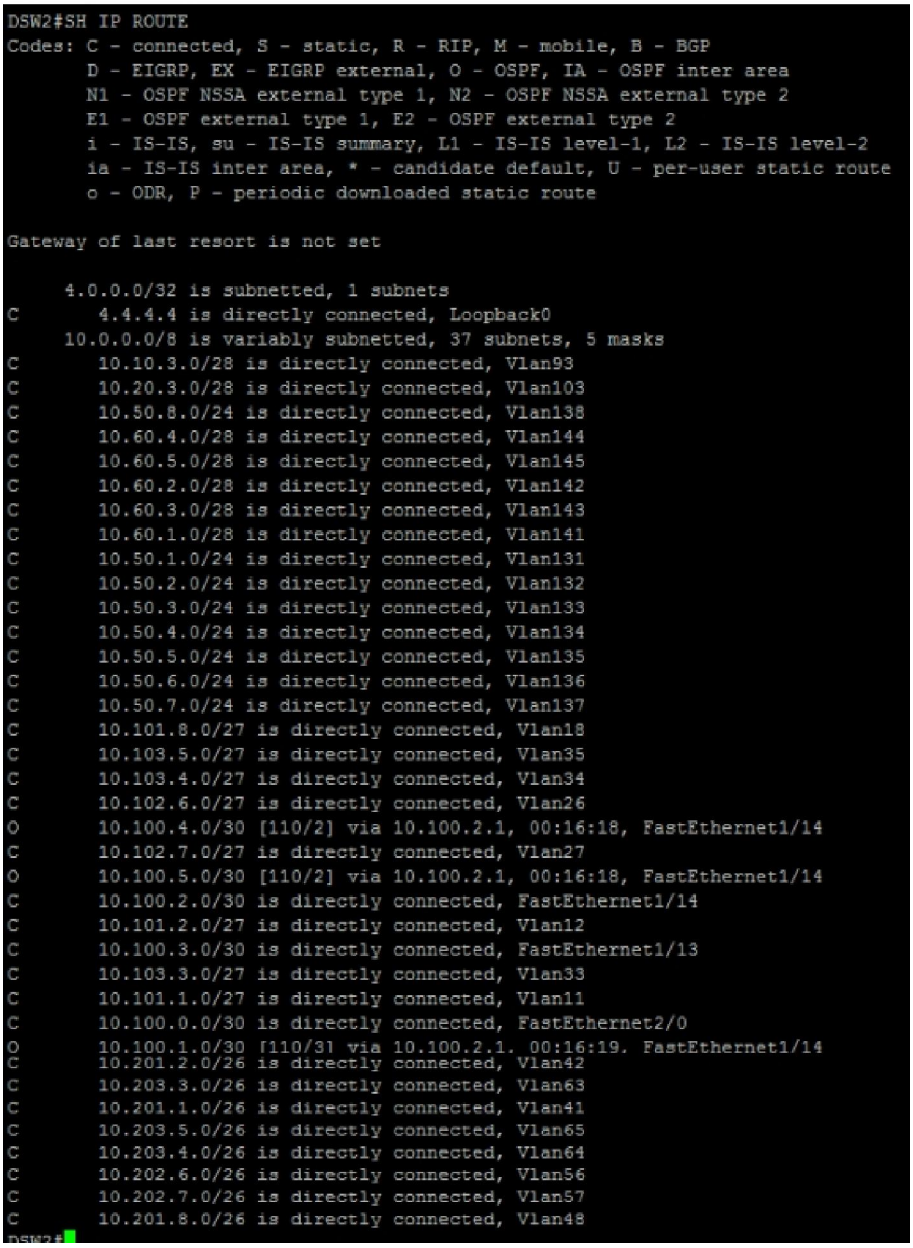
Gambar 24 IP route pada CSW1



Gambar 25 IP route pada CSW2



Gambar 26 IP route pada DSW1



Gambar 27 IP route pada DSW2

Gambar 24, 25, 26 dan 27 mendeskripsikan tabel *routing*, masing-masing pada CSW1, CSW2, DSW1 dan DSW2.

2. Pengujian Protokol *Redundancy* VRRP

   Pengujian VRRP ini dilakukan pada jaringan dosen informatika di lantai VII. Jaringan dosen di lantai VII menggunakan DSW2 sebagai *master router* dan DSW1 sebagai *backup router*.

```
DOSENIFLT7#ping 10.102.7.28

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.102.7.28, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/44 ms
DOSENIFLT7#ping 10.100.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/39/100 ms
DOSENIFLT7#traceroute 10.100.2.1

Type escape sequence to abort.
Tracing the route to 10.100.2.1

  1 10.102.7.30 68 msec 16 msec 4 msec
  2 10.100.2.1 48 msec *  60 msec
```

Gambar 28 Skenario ideal pada jaringan dosen informatika lantai 7

Gambar 28 mendeskripsikan bagaimana *host* pada dosen informatika lantai VII melakukan *ping* ke *virtual router* jaringan dosen informatika dan ke CSW2. *Trace route* menunjukkan bahwa koneksi ke CSW2, *host* pada jaringan dosen informatika lantai VII melewati DSW2.

```
DOSENIFLT7#ping 10.100.2.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.100.2.1, timeout is 2 seconds:
!!!!!!!!!!!!....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 96 percent (96/100), round-trip min/avg/max = 8/112/448 ms
DOSENIFLT7#
```

Gambar 29 *Test ping* ke CSW2 dengan pengulangan 100 kali

Gambar 29 mendeskripsikan bagaimana *host* pada jaringan dosen lantai VII melakukan *ping* ke CSW2 dengan pengulangan sebanyak seratus kali. Beberapa saat kemudian koneksi yang menghubungkan ASW7 ke DSW2 diputuskan, hal ini dimaksudkan untuk mengetahui berapa lama waktu yang dibutuhkan untuk melakukan perpindahan *master router* dari DSW2 ke DSW1. Cara untuk memutuskan koneksi yang menghubungkan ASW7 ke DSW2 terlihat seperti pada gambar 30.

```
Enter configuration commands, one per line.  End with CNTL/Z.
DSW2(config)#int fa1/6
DSW2(config-if)#shut
DSW2(config-if)#
*Mar  1 00:06:02.139: %DTP-5-NONTRUNKPORTON: Port Fa1/6 has become non-trunk
*Mar  1 00:06:02.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan27,
anged state to down
*Mar  1 00:06:02.639: %VRRP-6-STATECHANGE: Vl27 Grp 27 state Master -> Init
*Mar  1 00:06:02.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan57,
anged state to down
*Mar  1 00:06:02.655: %VRRP-6-STATECHANGE: Vl57 Grp 57 state Master -> Init
*Mar  1 00:06:02.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan137
hanged state to down
*Mar  1 00:06:02.671: %VRRP-6-STATECHANGE: Vl137 Grp 137 state Master -> Init
DSW2(config-if)#
*Mar  1 00:06:02.719: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Vlan27 from F
 to DOWN, Neighbor Down: Interface down or detached
*Mar  1 00:06:02.775: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Vlan57 from F
 to DOWN, Neighbor Down: Interface down or detached
*Mar  1 00:06:02.787: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Vlan137 from
L to DOWN, Neighbor Down: Interface down or detached
*Mar  1 00:06:03.587: %LINK-5-CHANGED: Interface FastEthernet1/6, changed sta
to administratively down
DSW2(config-if)#
*Mar  1 00:06:04.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEth
et1/6, changed state to down
DSW2(config-if)#
```

Gambar 30 Memutuskan koneksi yang menghubungkan ASW7 ke DSW2

```
DOSENIFLT7#traceroute 10.100.2.1

Type escape sequence to abort.
Tracing the route to 10.100.2.1

  1 10.102.7.29 44 msec 72 msec 96 msec
  2 10.100.0.2 144 msec 264 msec 72 msec
  3 10.100.2.1 212 msec *  56 msec
DOSENIFLT7#
```

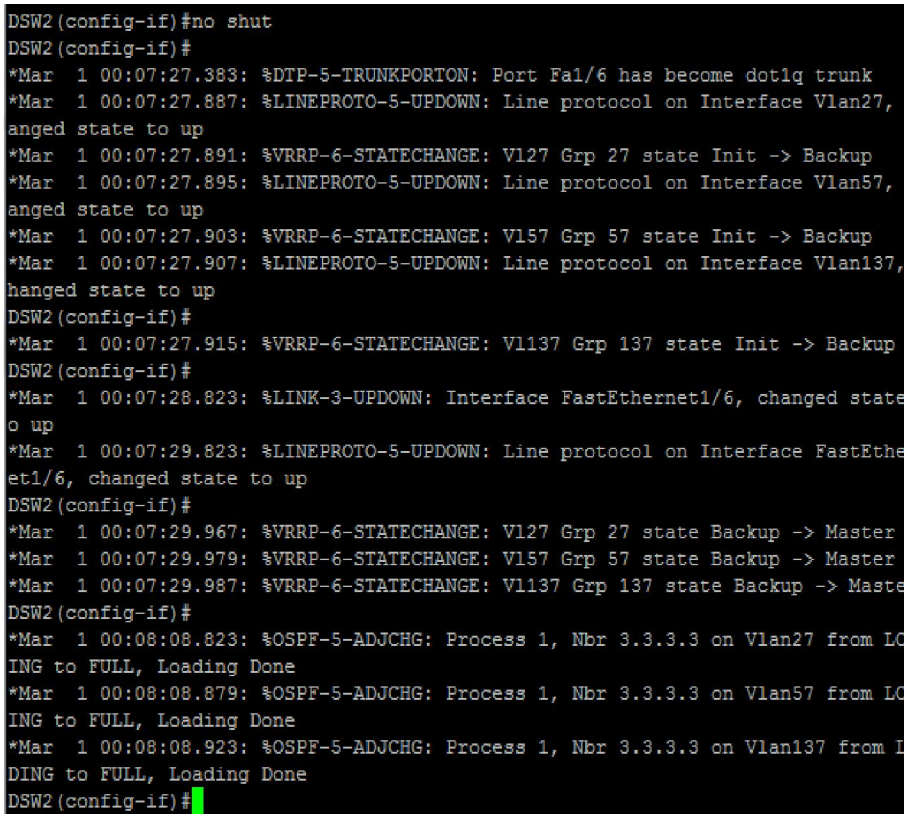
Gambar 31 *Trace route* ke CSW2

Gambar 31 mendeskripsikan jalur yang dilewati dari jaringan dosen informatika lantai VII menuju CSW2. *Trace route* menunjukkan bahwa *master router* jaringan dosen informatika lantai VII berubah dari DSW2 ke DSW1.

```
DOSENIFLT7#ping 10.100.2.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.100.2.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
.....................!!!!!!!!!
Success rate is 76 percent (76/100), round-trip min/avg/max = 20/117/544 ms
DOSENIFLT7#
```

Gambar 32 *Ping* ke CSW2 dengan pengulangan 100 kali

Gambar 32 mendeskripsikan bagaimana *host* pada jaringan dosen lantai VII melakukan *ping* ke CSW2 dengan pengulangan sebanyak seratus kali. Beberapa saat kemudian koneksi yang menghubungkan ASW7 ke DSW2 dikembalikan. Hal ini dimaksudkan untuk mengetahui berapa lama waktu yang dibutuhkan untuk melakukan perpindahan *master router* dari DSW1 ke DSW2. Dari gambar 32 terlihat bahwa waktu yang dibutuhkan untuk melakukan perpindahan *master router* kembali ke DSW2 lebih lama. Hal tersebut dikarenakan DSW2 memerlukan waktu untuk mempelajari jaringan baru yang aktif. Cara untuk mengembalikan koneksi yang menghubungkan ASW7 ke DSW2 terlihat seperti pada gambar 33.



Gambar 33 Mengembalikan koneksi yang menghubungkan ASW7 ke DSW2

```
DOSENIFLT7#traceroute 10.100.2.1

Type escape sequence to abort.
Tracing the route to 10.100.2.1

  1 10.102.7.30 68 msec 16 msec 4 msec
  2 10.100.2.1 48 msec *  60 msec
```

Gambar 34 *Trace route* ke CSW2

Gambar 34 mendeskripsikan jalur yang dilewati dari jaringan dosen informatika lantai VII menuju CSW2. Dari hasil *trace route* terlihat bahwa *master router* telah kembali ke DSW2.

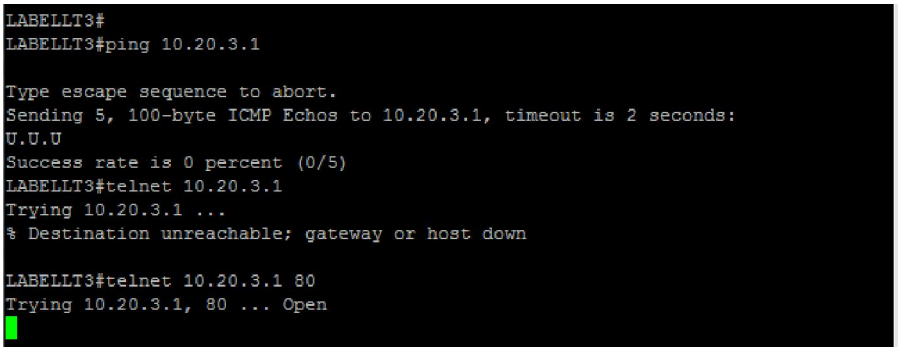
3. Pengujian *access-list* pada jaringan dosen

```
DOSENELLT3#ping 10.10.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/40 ms
DOSENELLT3#ping 10.20.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/84/136 ms
DOSENELLT3#ping 10.203.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.203.3.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
DOSENELLT3#
```

Gambar 35 Pengujian access-list pada jaringan dosen Elektro lantai III

Gambar 35 mendeskripsikan bagaimana pengujian fungsi *access-list* pada jaringan dosen elektro lantai III. *Host* jaringan dosen elektro lantai III dapat melakukan koneksi ke *server farm* lokal dan *server farm* publik, tetapi tidak dapat melakukan koneksi ke jaringan laboratorium mahasiswa.

4. Pengujian *access-list* pada jaringan laboratorium mahasiswa



Gambar 36 Pengujian Jaringan Lab mengakses *server* publik melalui port 80

Gambar 36 menunjukkan jaringan laboratorium tidak bisa melakukan ICMP dan *telnet* ke jaringan *server* publik dikarenakan *server* publik hanya bisa diakses melalui port 80.

Bab V Kesimpulan dan Saran

V.1 Kesimpulan

1. Perancangan ini dapat mengatasi adanya *broadcast domain* yang besar pada jaringan dosen, laboratorium mahasiswa dan *server farm* dengan melakukan segmentasi menggunakan VLAN pada jaringan-jaringan tersebut.

2. Perancangan ini dapat mengatasi *single point of failure* pada jaringan *server* dan komputer dengan mengimplementasikan protokol *redundancy* VRRP.

3. Perancangan ini disesuaikan dengan metode *Scalable Multilayer Campus Design*, sehingga jaringan *server* dan komputer Politeknik Negeri Batam memiliki jaringan yang efisien, intelijen, dapat diukur dan mudah diatur.

V.2 Saran

1. Perancangan ini dapat dikembangkan sehingga juga menyajikan solusi jaringan *voice* untuk keperluan VOIP.
2. Perancangan ini dapat disertakan analisis migrasi sesuai infrastruktur jaringan dari hasil perancangan.

DAFTAR PUSTAKA

[1] Hucaby, David. *CCNP SWITCH 642 – 813 Official Certification Guide*, Cisco Press, January 2010.

[2] Davis, David, 2009. What is a VLAN? How to Setup a VLAN on a Cisco Switch. http://www.petri.co.il/csc_setup_a_vlan_on_a_cisco_switch.htm. Diakses pada tanggal 10 Mei 2011.

[3] Botha, Deon, 2008. Local vlan vs end to end vlan. http://networkninja.co.za/cisco-systems/end-to-end-vlans/. Diakses pada tanggal 13 Mei 2011.

[4] Sivasubramanian, Balaji, Erum Frahim, Richard Froom, 2010. Analyzing the Cisco Enterprise Campus Architecture. http://www.ciscopress.com/articles/article.asp?p=160813. Diakses pada tanggal 10 Mei 2011.

[5] BRKCRS-2031, Cisco, 2011. Multilayer Campus Architectures & Design Principles. http://home.komsys.org/~jocke/ciscolivemelbourne2011/BRKCRS-2031_Multilayer_Campus_Architectures_&_Design_Principles.pdf. Diakses pada tanggal 11 Mei 2011.

[6] Indrawan, Wahyoe, S. Routing Protocol. http://wawans84.wordpress.com/2010/12/13/routing-protokol-ospf-dan-rip/ . Diakses pada tanggal 10 Mei 2011.

[7] Cisco Validated Design, 2008. Campus Network for High Availability Design Guide. http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html . Diakses pada tanggal 13 Mei 2011.

[8] Empson, Scott & Hans Roth. CCNP SWITCH Portable Command Guide. Cisco Press, March 2010.