Analisa Sistem Keamanan Jaringan dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan InformatikaJakarta Barat

SKRIPSI

Diajukan untuk memenuhi salah satu syarat kelulusan Program Sarjana

SYAIFUL JAMAL

12140391

Program Studi Teknik Informatika

STMIK Nusa Mandiri

Jakarta

2018

PERSEMBAHAN

Dengan mengucapkan puji syukur kepada Allah S.W.T, skripsi ini kupersembahkan untuk:

1. Ayah dan Ibu tercinta, motivasi terbesar dalam hidupku yang tak pernah jemu mendo'akan dan menyayangiku, tak pernah cukup kumembalas cinta Ayah dan Ibuku.
2. Kakakku (Zamaril, Zainal, Ermiza, Emzita, Isnaniah, Ahsanulhusnaini, Siti Rasidah) yang selalu memberi semangat, aku selalu sayang kalian.
3. Ramos Chaniago dan Isnaniah selaku kakak ipar dan kakak kandungku, yang telah berperan banyak dalam proses Pendidikanku, terimakasih telah selalu memberikan semangat dan arahannya.

Tanpa mereka,

aku dan karya ini tak akan pernah ada

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini

Nama	Syaiful Jamal
NIM	12140191
Perguruan Tinggi	*STMIK Nusa Mandiri Jakarta*

Dengan ini menyatakan bahwa skripsi yang telah saya buat dengan judul **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat"**, *adalah asli (orisinil) atau tidak plagiat (menjiplak) dan belum pernah diterbitkan/dipublikasikan dimanapun dan dalam bentuk apapun*

Demikianlah surat pernyataan ini saya buat dengan sebenar-benarnya tanpa ada paksaan dan pihak manapun juga. Apabila dikemudian hari ternyata saya memberikan keterangan palsu dan atau ada pihak lain yang mengklaim bahwa skripsi yang telah saya buat adalah hasil karya milik seseorang atau badan tertentu, saya bersedia diproses baik secara pidana maupun perdata dan kelulusan saya dari **STMIK Nusa Mandiri Jakarta** *dicabut/dibatalkan*

Dibuat di Tangerang
Pada tanggal : 18 Juli 2018
Yang menyatakan,

Syaiful Jamal

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini, saya

Nama	Syaiful Jamal
NIM	12140391
Program Studi	Teknik Informatika
Perguruan Tinggi	STMIK Nusa Mandiri Jakarta

Dengan ini menyetujui untuk memberikan ijin kepada pihak **STMIK Nusa Mandiri Jakarta**, Hak Bebas Royalti Non-Eksklusif *(Non-exclusive Royalti-Free Right)* atas karya ilmiah kami yang berjudul **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat"**, beserta perangkat yang diperlukan (apabila ada).

Dengan **Hak Bebas Royalti Non-Eksklusif** ini pihak **STMIK Nusa Mandiri Jakarta** berhak menyimpan, mengalih-media atau *formatkan*, mengelolanya dalam pangkalan data *(database)*, mendistribusikannya dan menampilkan atau mempublikasikannya di *internet* atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari kami selama tetap mencantumkan nama kami sebagai penulis/pencipta karya ilmiah tersebut.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak STMIK Nusa Mandiri Jakarta, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Tangerang
Pada tanggal : 18 Juli 2018
Yang menyatakan,

Syaiful Jamal

PERSETUJUAN DAN PENGESAHAN SKRIPSI

Skripsi ini diajukan oleh

Nama	SYAIFUL JAMAL
NIM	12140391
Program Studi	TEKNIK INFORMATIKA
Jenjang	STRATA-1
Judul Skripsi	Analisa Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security Pada Suku Dinas Komunikasi Dan Informatika Jakarta Barat

Telah dipertahankan pada periode 2018-1 dihadapan penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh SARJANA KOMPUTER (S.Kom) pada Program STRATA-1 Program Studi Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri

Jakarta, 14 Agustus 2018

PEMBIMBING SKRIPSI

Dosen Pembimbing	Irwan Agus Sobari, M.Kom
Asisten Pembimbing	Bambang Wijonarko, M.Kom

D E W A N P E N G U J I

Penguji I	Cahyani Budihartanti, M.Kom
Penguji II	Anggi Puspita Sari, ST, M.Kom

PANDUAN PENGGUNAAN HAK CIPTA

Skripsi sarjana yang berjudul **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat"** adalah hasil karya tulis asli SYAIFUL JAMAL dan bukan hasil terbitan sehingga peredaran karya tulis hanya berlaku dilingkungan akademik saja, serta memiliki hak cipta. Oleh karena itu, dilarang keras untuk menggandakan baik sebagian maupun seluruhnya karya tulis ini, tanpa seizin penulis.

Referensi kepustakaan diperkenankan untuk dicatat tetapi pengutipan atau peringkasan isi tulisan hanya dapat dilakukan dengan seizin penulis dan disertai ketentuan pengutipan secara ilmiah dengan menyebutkan sumbernya.

Untuk keperluan perizinan pada pemilik dapat menghubungi informasi yang tertera di bawah ini:

Nama : SYAIFUL JAMAL

Alamat : Elista Village Blok Kuskovo no 27, Tangerang

No. Telp : 085375061513

E-mail : guwejamal@gmail.com

KATA PENGANTAR

Alhamdulillah, dengan mengucapkan puji syukur kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga pada akhirnya penulis dapat menyelesaikan tugas ini dengan baik. Dimana Skripsi ini penulis sajikan dalam bentuk buku yang sederhana. Adapun judul Skripsi, yang penulis ambil sebagai berikut, **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat".**

Tujuan penulisan Skripsi ini dibuat sebagai salah satu syarat kelulusan Program Sarjana STMIK Nusa Mandiri Jakarta. Sebagai bahan penulisan diambil berdasarkan hasil penelitian (eksperimen), observasi dan beberapa sumber literatur yang mendukung penulisan ini. Penulis menyadari bahwa tanpa bimbingan dan dorongan dari semua pihak, maka penulisan Skripsi ini tidak akan lancar. Oleh karena itu pada kesempatan ini, izinkanlah penulis menyampaikan ucapan terima kasih kepada:

1. Ketua STMIK Nusa Mandiri Jakarta
2. Wakil Ketua I STMIK Nusa Mandiri Jakarta
3. Ketua Program Studi Teknik Informatika STMIK Nusa Mandiri Jakarta.
4. Bapak Irwan Agus Sobari, M.kom selaku Dosen Pembimbing I Skripsi.
5. Bapak Bambang Wijonarko, M.kom selaku Dosen Pembimbing II Skripsi.
6. Bapak/ibu dosen Teknik Informatika STMIK Nusa Mandiri Jakarta yang telah memberikan penulis dengan semua bahan yang diperlukan.

7. Orang tua tercinta yang telah memberikan dukungan moral maupun spritual.
8. Ramos Chaniago dan Isnaniah, kakak ipar dan kakak kandung saya yang telah berpran banyak dari awal kuliah samai pada penyusunan skripsi ini.
9. Rekan-rekan mahasiswa kelas TI-8A

Serta semua pihak yang terlalu banyak untuk disebut satu persatu sehingga terwujudnya penulisan ini. Penulis menyadari bahwa penulisan skripsi ini masih jauh sekali dari sempurna, untuk itu penulis mohon kritik dan saran yang bersifat membangun demi kesempurnaan penulisan dimasa yang akan datang.

Akhir kata semoga skripsi ini dapat berguna bagi penulis khususnya dan bagi para pembaca yang berminat pada umumnya.

Tangerang, 19 Juli 2018

Penulis

Syaiful Jamal

ABSTRAK

Syaiful Jamal (12140391), Analisa Kemanan Jaringan dengan Menggunakan Switch Port Security Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

Keamanan jaringan sangat penting bagi sebuah perusahaan atau institusi dalam menjaga kelancaran proses pekerjaan, seluruh komputer yang terhubung ke switch tentunya diharapkan memberikan kemanan terhadap komputer tersebut dari orang atau pihak yang tidak bertanggung jawab. Penerapan kemanan terhadap switch menjadi sangat penting untuk mengontrol siapa saja yang bisa mengakses jaringan. Untuk itu perlunya diterapkan keamanan pada switch seperti pemberian *username* dan *password*, mengengkripsi *password*, *remot* jaringan dan penerapan VLAN. Supaya lebih memudahkan administrator dalam mengontrol jaringan dan mempersempit terjadi nya tidak kejahatan dalam jaringan seperti pencurian data, merubah konfigurasi yang telah diterapkan pada switch dan menetakan port yang terhubung atau yang bisa di aksess oleh komputer atau client.

Kata kunci: Switch, security,port

ABSTRACT

Syaiful Jamal (12140391), Analysis of Network Security by Using Switch Port Security at the West Jakarta Communication and Information Office.

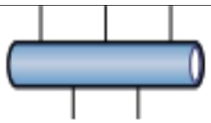
Network security is very important for a company or institution to maintain the smooth process of work, all commuters connected to the switch are certainly expected to provide security to the commuter from irresponsible people or parties. The application of security to switches is very important to control who can access the network. For this reason, it is necessary to apply security to switches such as giving us a username and password, password encryption, network remote and the application of VLANs. In order to make it easier for administrators to control the network and check the occurrence of it is not a crime in the network such as data theft, changing the configuration that has been applied to the switch and mapping the connected port or that can be accessed by the computer or client.

Keywords: Switch, security, port

DAFTAR ISI

DAFTAR SIMBOL

	Server
	Mainframe
	Router
	Hub
	Switch
	Bridge
	Modem
	Communication Link
	Wireless Access Point
	Firewall

	Printer
	Ethernet
	Telephone
	Personal Computer
	Laptop
	Scanner
	User

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Walikota Jakarta Barat adalah salah satu instansi pemerintah, dipimpin oleh Walikota yang bertanggung jawab kepada Gubernur Provinsi DKI Jakarta melalui sekretaris daerah. Walikota dalam melaksanakan tugas dan fungsinya dan dibantu Wakil Walikota dalam melaksanakan tugas – tugas nya.

Suku Dinas Komunikasi dan Informatika Jakarta Barat (SUDIN KOMINFO) yang ada di dalam instansi Pemerintahan Kota Administrasi Jakarta Barat sangat berpengaruh dalam membangun citra Walikota dan Wakil Walikota Jakarta Barat. Suku Dinas Komunikasi dan Informatika Jakarta Barat dipimpin oleh seorang kepala sudin dan terbagi dalam 3 divisi, tiap – tiap divisi dibantu oleh beberapa orang staf. Salah satu tugas Suku Dinas Komunikasi dan Informatika Jakarta Barat adalah dalam mengelola jaringan komputer yang ada di Kantor Administrasi Walikota Jakarta Barat.

Kebutuhan jaringan komuter semakin bertambah penting seiring kemajuan teknologi dan tuntutan dalam kehidupan baik dalam bidang Pendidikan maupun dalam bidang pekerjaan, salah satu yang paling penting dalam mengelolah jaringan adalah masalah keamanan, banyak tindakan kejahatan didalam jaringan, misalkan contoh nya seperti penyebaran virus, pencurian data dan lain sebagai nya. Salah satu cara untuk mempersempit peluang untuk melakukan kejahatan di dalam jaringan salah satunya adalah mebuat sebuah keamanan di switch, di sini lah nanti

akan di batasi siapa saja yang bisa mengakses atau bisa masuk dalam sebuah jaringan.

Menurut (Dewanto & Andiani, 2015) Penerapan VLAN adalah Memudahkan administrator dalam megontrol jaringan mebuat sekmentasi tiap divisi nya, contohnya divisi aplikasi hanya bisa terhubung ke divisi aplikasi sehingga menghindari tabrakan data. Yang mana penyebab melambatnya suatu perfoma jaringan adalah *broadcast domain*.

Menurut (T.Putra Ning, 2016) Virtual LAN merupakan salah satu bentuk pengembangan arsitektur jaringan dasar komputer yaitu Local Area Network (LAN) yang bertujuan untuk mencapai efisiensi dan keamanan infrastruktur jaringan komputer Menurut (Sakti, Aziz, & Doewes, 2013) SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Terutama banyak digunakan pada sistem berbasis linux (UNIX like) dan Unix untuk mengakses akun shell. SSH dirancang sebagai pengganti Telnet dan shell remote tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk plain text yang membuatnya mudah untuk disadap.

1.2 Maksud dan Tujuan

Maksud dari penulisan skripsi yang berjudul **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* pada Suku Dinas Komunikasi dan Informatika Jakarta Barat"** ini adalah sebagai berikut:

1. Untuk mengetahui keamanan switch yang terdapat pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

2. Meningkatkan keamanan jaringan pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

3. Untuk mengetahui manajeman jaringan, khususnya port yang bermaslah dan solusi pemecahan maslah nya.

Tujuan penulisan skripsi ini adalah untuk melengkapi salah satu syarat yang telah di tentukan dalam mencapai kelulusan program strata 1 (S1) .Program Studi Teknik Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri (STMIK Nusa Mandiri) Jakarta.

1.3 Metode Penelitian

Metode penelitian ini sangat penting dalam penyusunan skripsi, metode yang penulis gunakan untuk mengumpulkan data dalam penyusunan skripsi yang berjudul **"Analisa Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat"** ini adalah:

1.3.1 Metode Pengumpulan Data

Metode yang penulis gunakan dalam mengumpulkan data dalam penyusunan skripsi ini adalah:

1. Wawancara(*interview*)

Untuk mendapatkan informasi yang dibutuhkan maka penulis melakukan wawancara kepada bapak Yasri Rahman Malano, S.Kom selaku *staff IT* yang terdapat pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

2. Pengamatan(*observasi*)

Metode ini dilakukan untuk mendapatkan data atau informasi dengan cara mengamati secara lansung sistem jaringan berjalan yang ada pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

3. Studi pustaka

Penulis juga memperoleh informasi dan data dari membaca dan mempelajari karya ilmiah, jurnal ilmiah, buku-buku di perpustakaan dan artikel-artikel di *internet* yang berhubungan dengan penyusunan skripsi ini.

1.3.2 Analisa Penelitian

Analisa penelitian yang di perlukan dalam penyusunan skripsi ini adalah sebagai berikut:

1. Analisa Kebutuhan

dalam memeksimalkan hasil penelitian untuk penyusunan skripsi ini, dibutuhkan beberapa *hardware* dan *software*. *hardware* yang dibutuhkan 1 buah laptop dan 1 buah *switch*. Sedangakan *software* yang di butuhkan adalah *Cisco Packet Traicer*.

2. Desain

Desain jaringan yang digunakan pada skripsi ini adalah desain jaringan yang menghubungkan jaringan komputer pada Suku Dinas Komunikasi dan Informatika Jakarta Barat dangan jaringan komputer yang berada pada seluruh jaringan di Kantor Walikota Jakarta Barat. Akan tetapi menjadi fokus pada pembahasan skripsi ini adalah keamanan jaringan pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

3. Testing

Pengujian keamanan jaringan pada Suku Dinas Komunikasi dan Informatika Jakarta Barat akan menganalisa *Virtual Local Area Network* (VLAN) yang di konfigurasi dalam switch manageable. Jika seluruh pc yang ada di Suku Dinas Komunikasi dan Informatika Jakarta Barat saling terhubung, maka system keamanan VLAN belum berhasil. Jika seluruh pc yang ada di Suku Dinas Komunikasi dan Informatika Jakarta Barat tidak saling terhubung (segmentasi) maka di anggap sistem keamanan jaringan menggunakan VLAN telah berhasil.

4. Implementasi

Sistem keamanan jaringan menggunakan *switch port security* sudah di implementasi kan di Suku Dinas komunikasi dan Informatika Jakarta Barat, dan akan di simulasikan lagi menggunakan *cisco packet traicer.*

1.4 Ruang Lingkup

Supaya dalam penulisan skripsi ini lebih terarah dan mendalam, penulis hanya membahas tentang keamanan jaringan, tentang setting dan cara kerja switch pada pemberian username, password dan cara mengengkripsi password pada *switch* supaya tidak sembarangan orang bisa masuk dan merubah komfigurasi yang telah ada pada *switch*, penerapan VLAN supaya memudahkan manajeman jaringan pembagian tiapa departemen, remot jaringan menggunakan telnet/SSH dan *Acccess List Control* (ACL) yang meliputi: *software: cisco packet tracer*. *Hardware*: PC

BAB II
LANDASAN TEORI

2.1. Tinjauan Jurnal

Menurut (Sulaiman, 2016) Sebuah kemampuan *switch manageable* untuk meningkatkan keamanan dengan menggunakan *port-port* yang tersedia pada *switch*. Pertama: *default / static port security* , port security ini difungsikan maka mac address port security akan diaktifkan pada port switch. Kedua: *port security dynamic learning,* MAC address dipelajari secara dinamis ketika perangkat terhubung ke switch mac address tersebut di simpan mac address table. Ketiga: *sticky port security,* kemampuan switch dalam mengenal mac address tiap tiap perangkat yang terhubung dan akan memblok setiap mac yang tealah terdaftar.

Menurut (Sobari, 2015)Implementasi jaringan nirkabel (wirelless) yang tidak memiliki perencanaan keamanan informasi yang matang akan membuka banyak celah keamanan yang dapat ditembus dan dimanfaatkan oleh penyusup atau orang yang tidak bertanggung jawab. Seorang penyusup yang berhasil masuk melalui jaringan nirkabel (*wireless*) dan melakukan kerusakan informasi atau sistem informasi sebuah organisasi atau perusahaan memiliki kemungkinan lolos yang cukup besar dari usaha identifikasi.

Menurut (Zuhri & Sobari, 2017) Jenis jaringan komputer dapat dibedakan berdasarkan jenis *transmisi* dan *geografis*. Trdapat dua jenis jaringan berdasarkan teknologi *transmini*. pertama:jaringan *broadcast,* memiliki saluran komunikasi tunggal yang dipakai bersama - sama oleh semua *device* yang trkoneksi ke jaringan.

Kedua: jaringan *poin-to-point*, terdiri dari beberapa koneksi pasangan individu, dari satu *device* ke satu *device* lain.

Menurut (Primartha, 2013) Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah **enkripsi** (*encryption*).

Menurut (Prasetyo & Hikmawan, 2013) Proses penyandian pesan dari plaintext ke ciphertext dinamakan enkripsi/enchipering. Sedangkan proses mengembalikan pesan dari chipertext ke plaintext dinamakan deskripsi/dechipering. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan. Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dandekripsi.

Menurut (Nurmanina, 2013) Kriptografi mempunyai sejarah yang sangat panjang. Kriptografi sudah digunakan 4000 tahun yang lalu dan diperkenalkan oleh orang-orang mesir lewat hieroglyph.

Menurut (Hidayatulloh, 2014) *Firewall* adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas firewall adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan.

Firewall bertanggung jawab untuk memastikan bahwa *acces control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut.

2.2. Konsep Dasar Jaringan

2.2.1. Pengertian Jaringan Komputer

Menurut (Natali, Fajrillah, & Diansyah, 2016) Jaringan komputer merupakan kumpulan dari beberapa perangkat yang terkoneksi oleh sebuah media pengiriman data, mekanisme yang memungkinkan perangkat yang terdistribusi dan penggunanya untuk saling berkomunikasi dan berbagi sumber daya.

Dua buah komputer dikatakan "interkoneksi" apabila keduanya bisa berbagi *resources* yang dimiliki, seperti saling bertukar data/informasi, berbagi printer, berbagi media penyimpanan (*hard disk*, *floppy disk*, CD ROM, *flash disk*, *dan sebagainya).*

Data berupa teks, audio maupun video, mengalir melalui media jaringan (baik kaber atau nirkabel) sehingga memungkinkan pengguna jaringan komputer bertukar *file*/data, menggunakan rinter yang sama, menggunakan *hardware/software* yang yang terhubung dalam jaringan.

Beberapa ahli mendefinisikan komputer sebagai berikut:

Menurut Hamacher:

komputer adalah mesin penghitung elektronik yang cepat dan dapat menerima informasi input digital, kemudian memprosesnya sesuai dengan program yang tersimpan di memorinya dan menghasilkan output berupa informasi.

Menurut Blissmer:

Komputer adalah suatu alah elektronik yang mampu melakukan beberapa tugas sebagai berikut:

a) Menerima input
b) Memproses input tadi sesuai dengan programnya
c) Menyimpan perintah-perintah dan hasil dari pengolahan
d) Menyediakan output dalam bentuk informasi

Sedangkan Fuori berpendapat bahwa:

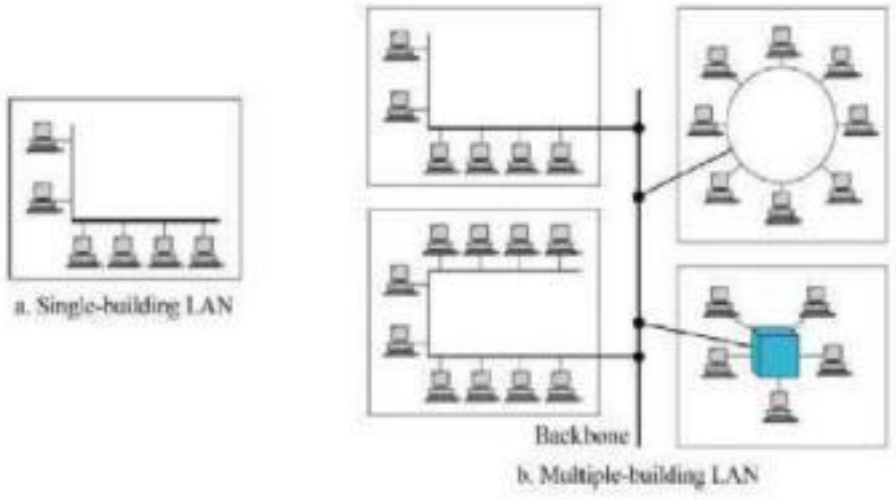
Komputer adalah suatu pemroses data yang dapat melakukan perhitungan besar secara cepat, termasuk perhitungan aritmatika dan operasi logika, tanpa campurtangan manusia.

2.2.2. Jenis-Jenis Jaringan Komputer

Jaringan komputer secara umum dibagi atas empat jenis, yaitu:

1) Local Area Network

Local Area Network (LAN) dapat di definisikan sebagai kumpulan komputer yang saling di hubungkan bersama didalan satu area tertentu yang tidak begitu luas, seperti didalam satu kantor atau gedung. LAN dapat juga didefinisikan berdasarkan pada penggunaan alamat IP komputer pada jaringan. Satu kmputer atau host dapat dikatakan satu LAN bila memiliki alamat IP yang masih dalam satu alamat jaringan, sehingga tidak memerlukan router untuk berkomunikasi. Contoh jaringan LAN seperti di perlihatka pada gambar 1.



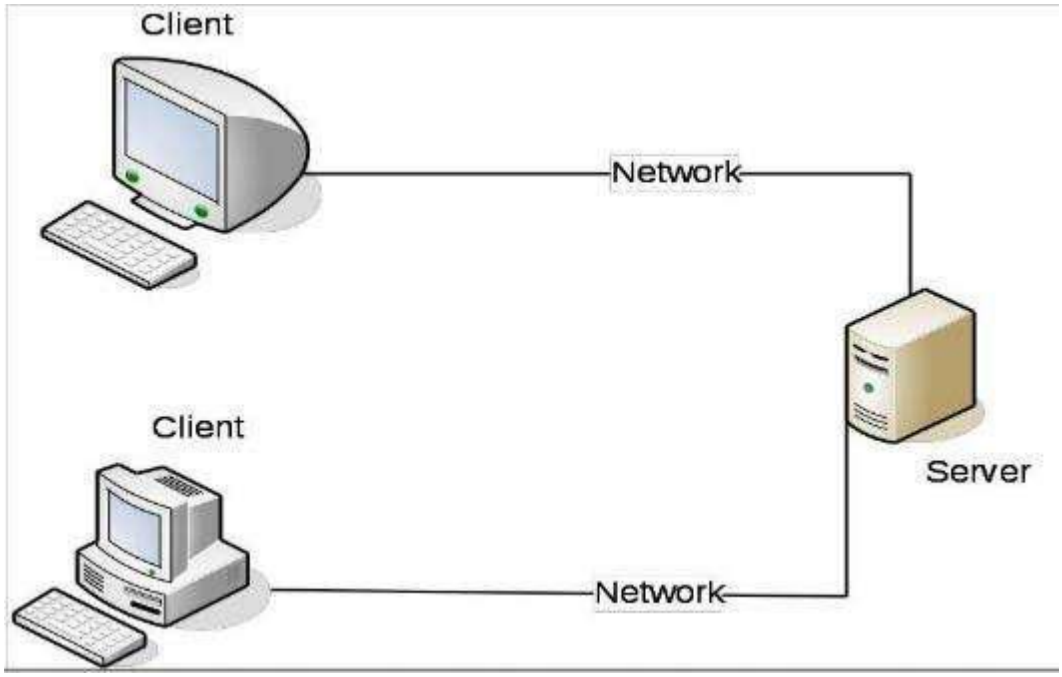
Sumber: Ebook

Gambar 1 Jaringan Local Area Network

Jaringan LAN juga dapat dibagi menjadi dua tipe, yaitu jaringan peer to peer dan jaringan client-server. Pada jaringan peer to peer, setiap komputer yang terhubung dapat bertindak baik sebagi workstation maupun server. Sedangkan pada jaringan client-server, hanya satu komputer yang bertindak sebagai server dan komputer lain sebagi workstation. Contoh jaringan LAN peer to peer dan client-server seperti diperlihatkan pada gambar 2 dan 3.

Sumber: Ebook

Gambar 2 Jaringan Peer to Peer

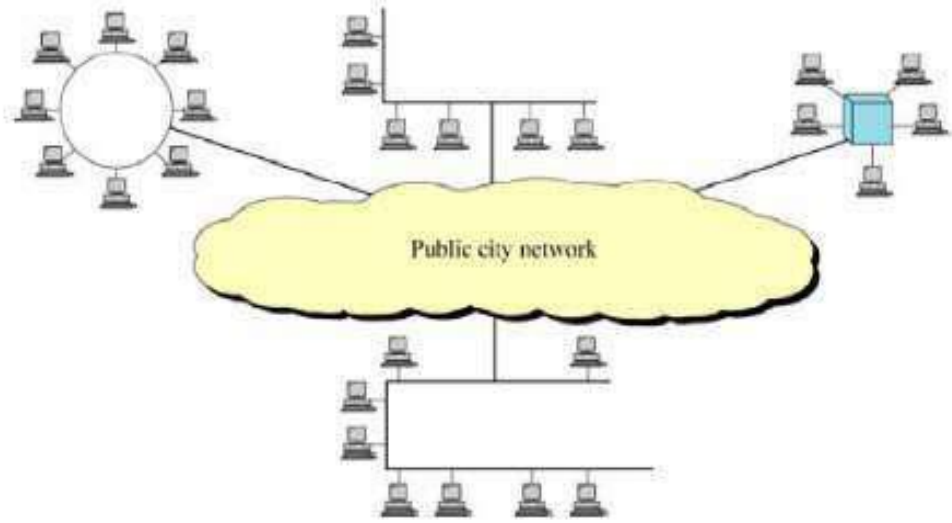


Sumber: Ebook

Gambar 3 Jaringan Client-Server

2) Metropolitan Area Network

Metropolitan Area Network (MAN) merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat di manfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel. Contoh jaringan MAN seperti di perlihatakan pada gambar 4.



Sumber: Ebook

Gambar 4 Jaringan Metropolitan Area Network

3) Wide Area Network

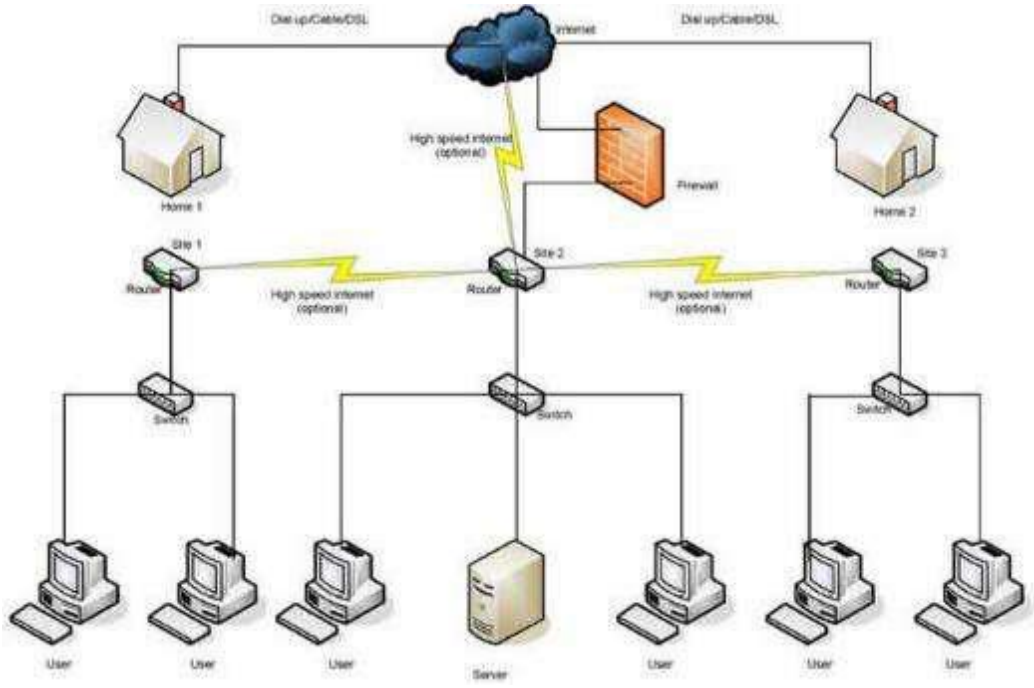
Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media wireless, sarana satelit ataupun kabel serat optik, karena jangkauan yang lebih luas, bukan hanya meliputi satu kota atau antara kota suatu wilayah, tetapi mulai menjangakau area/wilayah otoritas Negara lain. WAN biasanya lebih rumit dan sangat kompleks bila dibandingkan LAN maupun MAN. WAN menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN kedalam komunikasi global seperti internet, meski deminkian antara LAN, MAN dan WAN tidak banyak berbeda satu di antara yang lainnya. Contoh jaringan WAN seperti di perlihatkan pada gambar 5.

Sumber: Ebook

Gambar 5 Jaringan Wide Area

Network 4) Internet dan Intranet

Internet yang merupakan gabungan dari LAN, MAN dan WAN, adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia. Setiap komputer dan jaringan terhubung secara lansung maupun tidak lansung ke beberapa jalur utama yang disebut internet backbone dan di bedakan satu dengan yang lainnya menggunakan alamat unik yang biasa di sebut dengan alamat Internet Protocol (IP). Contoh jaringan internet dan intranet seperti di perlihatkan pada gambar 6.



Sumber: Internet

Gambar 6 Jaringan Internet dan Intranet

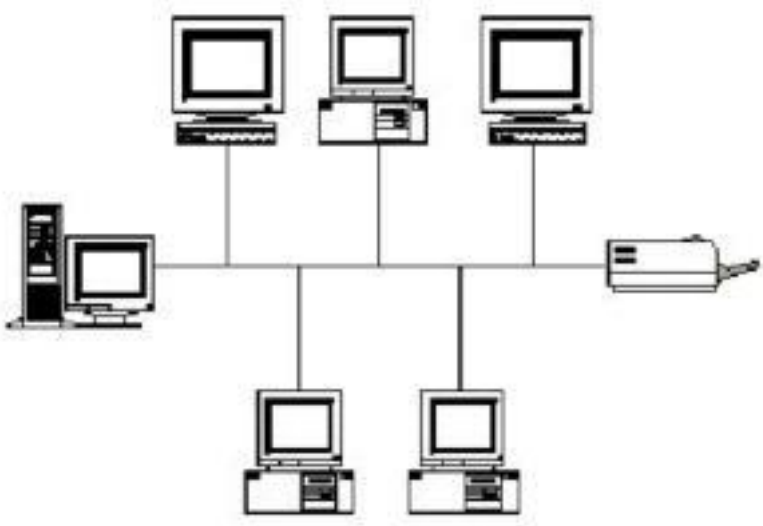
Aplikasi pada jaringan internet dapat juga di terpkan pada sebuah LAN yang memiliki server. Sebagai contoh di perusahaan yang memiliki jaringa client-server. Bila aplikasi yang ada pada internet, seperti mail server, di terapkan pada perusahaan tersebut, maka jaringan ini dapat di sebut sebagai jaringan internet. Client dapat mengakses server tersebut seperti mengakses internet pada umumnya. Client juga dapat mengakses aplikasi lain diluar server perusahaan (internet).

2.2.3. Topologi Jaringan Komputer

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang umum di gunakan saat ini adalah bus, token-ring, star dan mesh.

1) Topologi Bus

Pada topologi bus digunakan sebuah kabel tunggal atau kabel pusat dimana saluran workstation dan server dihubungkan. Keunggulan topologi bus adalah pengembangan jaringan atau penambahan workstation baru dapat di lakukan dengan mudah tanpa mengganggu workstation lain. Kelemahan dari topologi ini adalah bila terdapat gangguan di sepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan. Contoh topologi bus seperti diperlihatkan pada gambar 7.



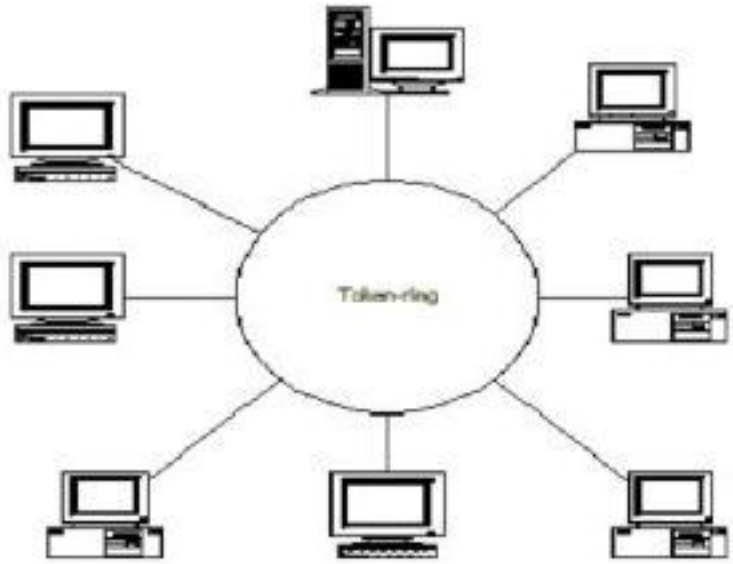
Sumber: Ebook

Gambar 7 Topologi Bus

1) Topologi Ring

Pada topologi ring, semua workstation dan server di hubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap workstation ataupun server akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat-alamat yang di maksud sesuai maka informasi diterima bila tidak informasi akan dilewatkan.

Kelemahan dari topologi ini adalah setiap node dalam jaringan akan selalu ikut serta mengelola informasi yang di lewatkan dalam jaringan. Sehingga bila terdapat gangguan di suatu node maka seluruh jaringan akan terganggu. Keunggulan topologi ring adalah tidak terjadinya collision atau tabrakan pengiriman data seperti pada topologi bus, karena hanya satu node dapat mengirimkan data pada suatu saat. Contoh topologi token ring seperti diperlihatkan pada Gambar 8.



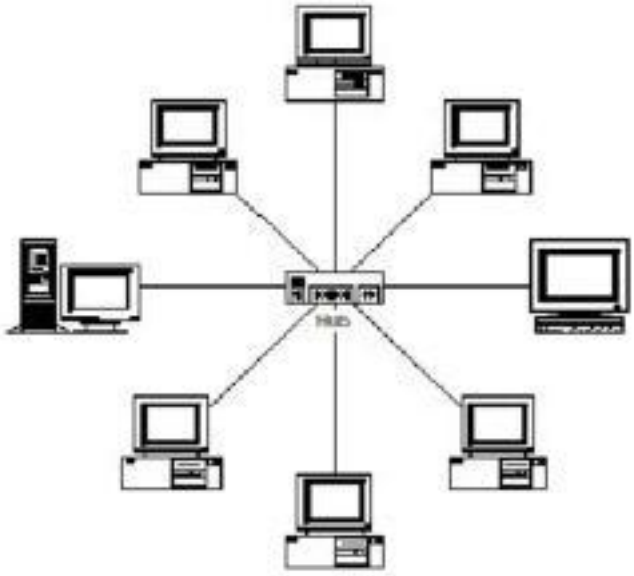
Sumber: Ebook

Gambar 8 Topologi Token Ring

1) Topologi Star

Pada topologi star, masing-masing workstation dihubungkan secara lansung ke server atau hub. Keunggulan dari topologi star adalah dengan adanya kabel tersendiri untuk setiap workstation ke server, maka bandwidth atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan untuk kerja jaringan secara keseluruhan. Bila terdapat gangguan di suatu jalur kabel maka

gangguan hanya akan terjadi dalam komunikasi antara worksatation yang bersangkutan dengan server, jaringan secara keseluruhan tidak mengalami gangguan. Kelemahan dari topologi star adalah kebutuhan kabel yang lebih besar disbanding topologi lainnya. Contoh topologi star seperti yang diperlihatkan pada Gambar 9.

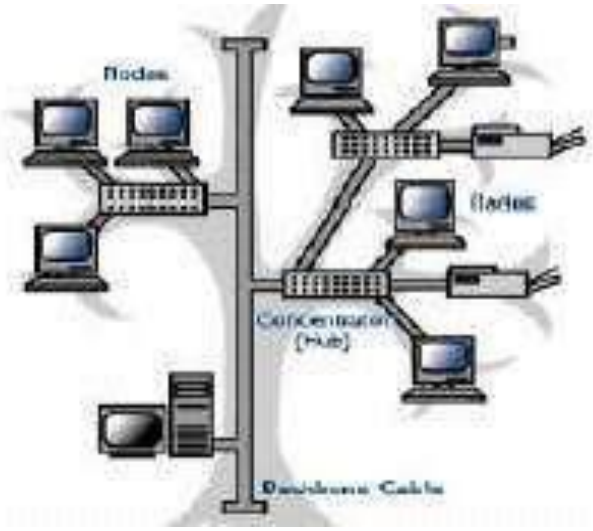


Sumber: Ebook

Gambar 9 Topologi Star

1) Topologi Tree

Topologi tree dapat berupa gabungan dari topologi star dan topologi bus. Contoh topologi tree seperti yang diperlihatakan pada Gambar 10.

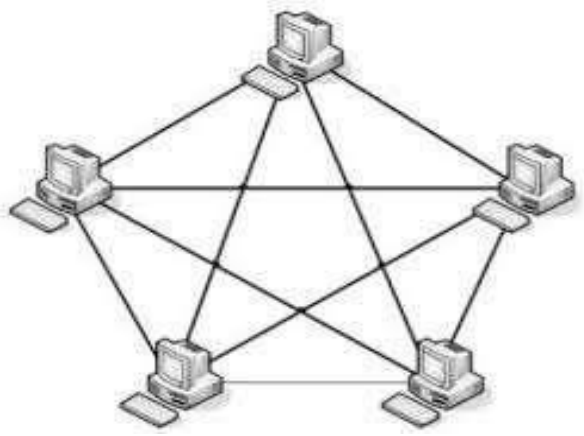


Sumber: Ebook

Gambar 10 Topologi Tree

1) Topologi Mesh

Topologi mesh digunakan pada kondisi dimana tidak ada hubungan komunikasi terputus secara absolut antar node komputer. Topologi ini merefleksikan desain internet yang memiliki multi path ke berbagai lokasi. Contoh topologi mesh seperti yang diperlihatkan pada Gambar 11.



Sumber: Ebook

Gambar 11 Topologi Mesh

2.2.4. Perangkat Jaringan

Perangkat jaringan adalah semua komputer, peripheral, interface card, dan perangkat tambahan yang terhubung ke dalam suatu sistem jaringan komputer untuk melakukan komunikasi data. Perangkat jaringan komputer terdiri dari:

1) *Server*

Server merupakan pusat control dari jaringan komputer. Server berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. Server akan melayani seluruh clien atau workstation yang terhubung ke jaringan. Sistem operasi yang digunakan pada server adalah sistem operasi yang khusus yang dapat memberikan layanan bagi workstation.

2) *Workstation*

Workstation adalah komputer yang terhubung dengan sebuah LAN. Semua komputer yang terhubung dengan jaringan dapat dikatakan sebagai workstation. Komputer ini yang melakukan akses ke server guna mendapat layangan yang telah disediakan oleh server.

3) *Network Interface Card*

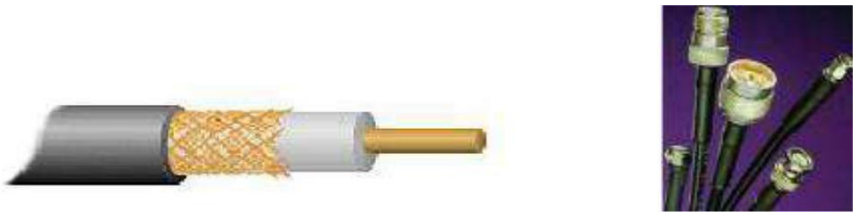
Network Interface Card (NIC) adalah expansion board yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protocol, dan media tertentu. NIC bisa disebut LAN card. Contoh sebuah LAN card seperti di perlihatkan pada Gambar 12.

Sumber:Ebook

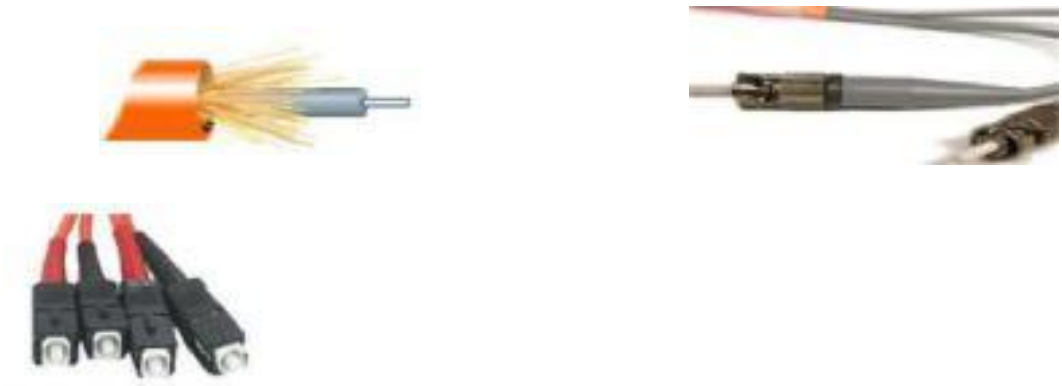
Gambar 12 Network Interface Card

4) Kabel

Kabel adalah saluran yang menghubungkan dua workstation atau lebih. Jenis-jenis kabel yang digunakan dalam jaringan antara lain kabel coaxial, fiber optic, dan twised pair. Jenis-jenis kabel tersebut seperti diperlihatkan pada Gambar 13.



Kabel Coaxial



Fiber Optic

Twised Pair

Sumber: Ebook

Gambar 13 Kabel

Kabel coaxial hanya memiliki satu konduktor yang berada di pusat kabel. Kabel ini memiliki lapisan plastic yang berfungsi untuk pembatas konduktor dengan anyaman kabel yang ada pada lapisan berikutnya. Kabel coaxial memiliki kecepatan transfer sampai 10 Mbps. Kabel coaxial seing digunakan untuk kabel TV, ARCnet, thick Ethernet dan thin Ethernet. Thick coaxial/ 10 base5/ RG-8 sering digunakan untuk backbone, untuk instalasi jaringan antar gedung. Kabel ini secara fisik berat dan tidak fleksibel, namun ia mampu menjangkau jarak 500 m bahkan lebih. Thin coaxial/ 10Base2/ RG-58/ cheapernet sering digunakan antar workstation. Kabel ini secara fisik lebih mudah di tangani dari pada RG-8 karena lebih fleksibel dan ringan. Thick coax mempunyai diameter rata-rata 12 mm

sedangan thin coaxial mempunyai diameter rata-rata berkisar 5mm. setiap perangkat dihubungkan dengan BNC T-connector.

Kabel fiber optik memiliki inti kaca yang dilindungi oleh beberapa pelindung. Pengiriman data pada kabel ini menggunakan sinsar. Kabel fiber optik memiliki jarak yang lebih jauah dari pada twisted pair dan coaxial. Kabel ini juga memiliki kecepatan transfer data yang lebih baik dalam pengiriman data, yaitu mencapai 155 Mbps. Kabel fiber optik memiliki dua tipe, yaitu single mode dan multi mode. Tipe single mode memiliki diameter core 9 micron, sedangkan kabel multi mode memiliki diameter core sebesar 62,5 micron.

Kabel twisted pair, secara umum dibagi menjadi dua tipe, Shielded Twisted Pair (STP) dan Unshielded Twisted Pair (UTP). Sepasang kabel yang di-twist (pilih), yang jumlah pasangannya dapat terdiri dari dua, empat atau lebih. Fungsi twist bertujuan untuk megurangi interfensi elektromagnetik terhadap kabel lain atau terhadap sumber eksternal. Kecepatan transfer data yang dapat dilayani sampai 10 Mbps. Konektor yang bisa di gunakan adalah RJ-11 atau RJ-45. Dari kedua tipe ini, tipe UTP adalah tipe yang sering digunakan pada jaringan LAN. UTP memiliki 4 pasang kabel terpilih (8 buah kabel) dan hanya 4 buah kabel yang digunakan dalam jaringan. Perangkat yang berkenaan dengan penggunaan jenis kabel ini adalah konektor RJ45 dan Hub/Switch.

5) Modem

Modem adalah sebuah device yang digunakan sebagai penghubung dari sebuah PC atau jaringan ke penyedia layanan internet (Internet Service Provider /

ISP). Salah satu modem yang dipakai untuk koneksi ke internet ialah model ADSL. Modem ini biasanya digunakan oleh ISP Telkom Speedy.

2.3. Switch

2.3.1 Seluk Beluk

Tidak semua jaringan komuter bekrja pada *layer network* dan tidak semua perangkat jaringan komputer dapat mengenali paket data yang dihasilkan oleh perangkat yang bekerja pada *layer network*. Cukup banyak jaringan komputer atau perangkat yang bekerja pada *layer data link*. Dan hanya mengenali frame. Kondisi semacam ini menyebabkan teknologi routing tidak dapat digunakan.

Sebagai gantinya dapat digunakan teknologi *switching*. Dari sisi teknologi, *switching* sebenarnya jauh lebih sederhana dibandingkan *routing*. Persoalannya adalah, *switching* berhubungan lansung dengan sejumlah besar *device*, termasuk komputer, *switch* lain, dan perangkat lainnya. Sehingga teknologi *switching* menjadi sangat kompleks.

Kita akan sering berhadapan denga *switch* dan jarang menjumpai *router*. Pada sebuah LAN bisa saja digunakan puluhab buah *switch* yang menghubungkan ratusan buah komputer. Namun mungkin hanya ada sebuah *router*, yang *gateway router* yang digunakan untuk mengakses internet atau *network* eksternal.

2.3.2. Fitur *Switch*

Sebuah *Switch* memiliki kemampuan:

a) Mengendalikan aliran data (*flow control*)

b) Menangani frame yang *error*

c) Menyediakan akses kemedia fisik

d) Dapat membagi sebuah *network* menjadi beberapa *network* yang lebih kecil (segmen-segmen *network*).

Frame yang melalui *switch* akan "diseleksi" sedemikian rupa. Jika frame diangga *error* maka *switch* akan membuang frame tersebut (drop), sehingga *network* tidak "dibajiri" oleh frame yang tidak bermanfaat. Jika frame tidak *error* maka *switch* akan meneruskannya (mem-*forward*) ke komputer target, sesuai dengan alamat *hardware* yang tercantum ada *header* setiap frame.

Tugas utama sebuah *switch* dapat dijelaskan sebagai berikut:

a) *MAC address learning*

Ketika sebuah komputer hendak mengirim data maka komputer lain akan "ditanyai" MAC address-nya. Pada *network* radisional (yang tidak menggunakan switch), kondisi semacam ini akan terjadi berulang-ulang.

Sebuah *switch* mampu mempelajari MAC *address* dan menentukan rute menuju komputer tertentu. *Switch* dapat mencatat daftar MAC *address* dan secara dinamis dapat mempelajari perubahan yang terjadi pada *network*.

b) *Forwarding dan filtering*

Tidak semua data yang mengalir pada *network* "bermanfaat" dan tidak "memiliki tujuan yang jelas". *Switch* mampu menentukan "nasib" frame yang melaluinya. Apakah frame harus "dibuang" karena *error* atau "tidak bertujuan", ataukan frame akan diteruskan ke komputer atau segmen lain. Sebuah *switch* dapat mengetahui secara pasti rute menuju tujuan.

Pada *network* tanpa *switch*, hal semacam ini tidak dapat dilakukan. Frame yang *error* atau tidak bertujuan akan mengganggu *network*.

c) *Segmenting end stations*

Sebuah *network* umumnya menyediakan berbagai service. Masing-masing service berpotensi menimbulkan *congestion*. Hal ini, sering terjadi ada *network* tradisional.

Switch yang baik mampu melakukan segmentasi, menentukan jalur virtual, dan mengelompokan berdasarkan service-service tertentu.

2.3.3. Cara Kerja *Switch*

Dilihat dari cara kerjanya maka *switch* dapat dikelompokan menjadi beberapa jenis, yaitu:

a) *Cut through* atau *fash forward*

Switch jenis ini hanya mengecek alamat tujuan (yang ada ada *header* frame). Selanjutnya frame akan di teruskan ke *node* tujuan. Kondisi ini dapat mengurangi ”waktu tunggu” atau *latency*. Inilah jenis *switch* “tercepat” diantara jenis lainya.

Kelemahan *switch* jenis ini yaitutidak dapat mengecek frame-frame yang *error*. Frame yang *error* akan tetap diteruskan ke *node* tujuan.

b) *Store and forward*

Switch akan menyimpan semua frame untuk sementara waktu sebelum diteruskan ke *node* tujuan . seluruh frame akan dicek melalui mekanisme CRC (*Cyclie Redundancy Check)*. Jika ditemukan *error* maka frame akan

"dibuang" dan tidak diteruskan ke *host* tujuan. *Switch* jenis ini paling "terpercaya" diantara jenis lainya.

Kelemahan *switch* jenis ini adalah meningkatnya *latency* karena adanya proses pengecekan seluruh frame yang melalui *switch*.

c) *Fragment free* atau *modifield cut through*

Switch akan membaca 64 byte dari frame sebelum meneruskanya ke *node* tujuan. Nilai 64 byte ini meruakan jumlah minimum byte yang dianggap penting untuk menentukan apakah frame *error* atau tidak. Sehingga *switch* jenis ini memiliki tujuan kerja yang cukup baik dan teta dapat diandalkan.

Cintoh hub dan switch seperti yang diperlihatkan pada Gambar 14.

Sumber: Ebook

Gambar 14 HUB dan Switch

2.4. Port

2.4.1. Tentang Port

Dalam protokol jaringan TCP/IP, sebuah *port* adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP.

Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-Bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.

Dilihat dari penomorannya, port UDP dan TCP dibagi menjadi tiga jenis, yakni sebagai berikut:

1) *Well-known Port*: yang pada awalnya berkisar antara 0 hingga 255 tapi kemudian diperlebar untuk mendukung antara 0 hingga 1023. Port number yang termasuk ke dalam well-known port, selalu merepresentasikan layanan jaringan yang sama, dan ditetapkan oleh Internet Assigned Number Authority (IANA). Beberapa di antara port-port yang berada di dalam range Well-known port masih belum ditetapkan dan direservasikan untuk digunakan oleh layanan yang bakal ada di masa depan. *Well-known port* didefinisikan dalam RFC 1060.
2) *Registered Port*: Merupakan Port-port yang digunakan oleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi yang mereka buat. Registered port juga diketahui dan didaftarkan oleh IANA tapi tidak dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama. Range registered port berkisar dari 1024 hingga 49151 dan beberapa port di antaranya adalah *Dynamically Assigned Port*.

3) *Dynamically Assigned Port*: merupakan port-port yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani request dari pengguna sesuai dengan kebutuhan. Dynamically Assigned Port berkisar dari 1024 hingga 65536 dan dapat digunakan atau dilepaskan sesuai kebutuhan.

Berikut Ini Adalah Beberapa Contoh Dari Welknown Yang Sering kali KitaGunakan Port Beserta Dengan Fungsi Port-Port tersebut

Table 1 Port

Port	Jenis Port	Keyword	Digunakan oleh
20	TCP, UDP	ftp-data	File Transfer protocol (default data)
21	TCP, UDP	ftp	File Transfer protocol (control),connection dialog
23	TCP, UDP	telnet	telnet
25	TCP, UDP	Smtp	Simple Mail Transfer Protocol alias = mail
53	TCP, UDP	Domain	Domain Name System Server

67	TCP, UDP	Bootpc	DHCP/BOOTP Protocol Server
68	TCP, UDP	Bootpc	DHCP/BOOTP Protocol Server
69	TCP, UDP	Tftp	Trivial File Transfer Protocol
80	TCP, UDP	www	World Wide Web HTTP
110	TCP, UDP	pop3	PostOfficerotocolversion3(POP3);alias=postoffice
123	TCP, UDP	Ntp	Network Time Protocol; alias = ntpd ntp
220	TCP, UDP	imap3	Interactive Mail Access Protocol versi 3

Sumber: Jurnal

Berikut Ini pengertian nama-nama kegunaan port tersebut

1) FTP (singkatan dari *File Transfer Protocol*) adalah sebuah protokol Internetyang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) computer antar mesin-mesin dalam sebuah *internetwork*

2) SMTP (*Simple Mail Transfer Protocol*) merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di Internet. Protokol ini dipergunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima.
3) HTTP (*Hypertext Transfer Protocol*, lebih sering terlihat sebagai *http*) adalah protocol yang dipergunakan untuk mentransfer dokumen dalam *World Wide Web* (WWW). Protokol ini adalah protokol ringan, tidak berstatus dan generik yang dapat dipergunakan berbagai macam tipe dokumen.
4) POP3 (*Post Office Protocol version 3*) adalah protokol yang digunakan untuk mengambil surat elektronik (email) dari server email.
5) IMAP (*Internet Message Access Protocol*) adalah protokol standar untuk mengakses/mengambil e-mail dari server. IMAP memungkinkan pengguna memilih pesan e-mail yang akan ia ambil, membuat folder di server, mencari pesan e-mail tertentu, bahkan menghapus pesan e-mail yang ada.

2.4.2. Pengertian port dan fungsi port

Port adalah soket atau jack koneksi yang terletak di luar unit sistem sebagai tempat kabel-kabel yang berbeda ditancapkan. Setiap port pasti berbeda fungsi dan bentuk fisiknya. Port-port tersebut adalah port serial, port paralel, port SCSI (dibaca "scuzzy"), port USB. Selama ini kita biasanya memanfaatkan port-port tersebut untuk mentransmisikan data.

1) Port serial digunakan untuk mentransmisikan data dari jarak jauh secara lambat, seperti keyboard, mouse, monitor, dan modem dial-up.

2) Port paralel untuk mentransmisikan data pada jarak yang pendek secara cepat. Port ini sering dipakai untuk menghubungkan printer, disk eksternal, atau tape magnetik untuk bacup.
3) Port SCSI (*small computer system interface*), untuk mentransmisikan data secara cepat bahkan dapat dipakai untuk 7 alat sekaligus atau "*daisy chain*".

   Contoh daisy chain : dari SCSI kontroller kemudian disambungkan ke perangkat hardisk drive eksternal, dari HDD eksternal disambungkan secara seri ke perangkat yang lain seperti tape drive, kemudian dari tape drive tsb bisa juga disambungkan ke CD/DVD drive dan seterusnya.
4) Port USB (*universal serial bus*), untuk mentransmisikan data hingga 127 periferal dalam rangkaian daisy chain.
5) Port tambahan khusus seperti : FireWire, MIDI, IrDa, Bluetooth, dan ethernet. Fire Wire berfungsi untuk camcorder, pemutar DVD, dan TV. Sedangkan port MIDI (*musical instrument digital interface*) untuk menghubungkan instrumen musik. Kemudian port IrDA (*Infrared Data Association*) untuk koneksi nirkabel sejauh beberapa kaki. Port Bluetooth adalah gelombang radio jarak pendek yang bisa menstransmisikan sejauh 9 m. Port ethernet adalah untuk LAN.

Pada terminologi jaringan komputer, port merupakan titik komunikasi spesifik yang digunakan oleh sebuah aplikasi yang memanfaatkan lapisan *transport* pada teknologi TCP / IP. Artikel ini menceritakan tentang beberapa port yang digunakan oleh aplikasi ataupun protokol standar.

Pada terminologi komputer ada dua jenis Port yaitu :

1) Port Fisik,adalah soket/ slot / colokan yang ada di belakang CPU sebagai penghubung peralatan input-output komputer, misalnya PS2 Port yang digunakan oleh Mouse dan Keyboard, USB Port atau Paralel Port.
2) Port Logika (non fisik),adalah port yang di gunakan oleh aplikasi sebagai jalur untuk melakukan koneksi dengan komputer lain mealalui teknologi TCP/IP, tentunya termasuk koneksi internet.

Yang akan dibahas pada artikel ini adalah port logika, mungkin akan berguna bagi anda yang mengelola server linux untuk berbagai keperluan.

2.4.3. Port Standar dan Kegunaan

1-19, berbagai protokol, Sebagian banyak port ini tidak begitu di perlukan namun tidak dapat diganggu. Contohnya layanan echo (port 7) yang tidak boleh dikacaukan dengan program ping umum.

20 – FTP-DATA. "Active" koneksi FTP menggunakan dua port: 21 adalah port kontrol, dan 20 adalah tempat data yang masuk. FTP pasif tidak menggunakan port 20 sama sekali.

21 – Port server FTP yang digunakan oleh *File Transfer Protocol*. Ketika seseorang mengakses FTP server, maka ftp client secara default akan melakukan koneksi melalui port 21.

22 – SSH (Secure Shell), Port ini ini adalah port standar untuk SSH, biasanya diubah oleh pengelola server untuk alasan keamanan.

23 – Telnet server. Jika anda menjalankan server telnet maka port ini digunakan client telnet untuk hubungan dengan server telnet.

25 – SMTP, *Simple Mail Transfer Protocol*, atau port server mail, merupakan port standar yang digunakan dalam komunikasi pengiriman email antara sesama SMTP Server.

37 – Layanan Waktu, port built-in untuk layanan waktu.

53 – DNS, atau *Domain Name Server* port. Name Server menggunakan port ini, dan menjawab pertanyaan yang terkait dengan penerjamahan nama domain ke IP Address.

67 (UDP) – BOOTP, atau DHCP port (server). Kebutuhan akan *Dynamic Addressing* dilakukan melalui port ini.

68 (UDP) – BOOTP, atau DHCP port yang digunakan oleh client.

69 – tftp, atau *Trivial File Transfer Protocol*.

79 – Port Finger, digunakan untuk memberikan informasi tentang sistem, dan login pengguna.

80 – WWW atau HTTP port server web. Port yang paling umum digunakan di Internet.

81 – Port Web Server Alternatif, ketika port 80 diblok maka port 81 dapat digunakan sebagai port altenatif untuk melayani HTTP.

98 – Port Administrasi akses web Linuxconf port.

110 – POP3 Port, alias *Post Office Protocol*, port server pop mail. Apabila anda mengambil email yang tersimpan di server dapat menggunakan teknologi POP3 yang berjalan di port ini.

111 – sunrpc (*Sun Remote Procedure Call*) atau portmapper port. Digunakan oleh NFS (Network File System), NIS (Network Information Service), dan berbagai layanan terkait.

113 – identd atau auth port server. Kadang-kadang diperlukan, oleh beberapa layanan bentuk lama (seperti SMTP dan IRC) untuk melakukan validasi koneksi.

119 – NNTP atau Port yang digunakan oleh *News Server*, sudah sangat jarang digunakan.

123 – *Network Time Protocol* (NTP), port yang digunakan untuk sinkronisasi dengan server waktu di mana tingkat akurasi yang tinggi diperlukan.

137-139 – NetBIOS (SMB).

143 – IMAP, *Interim Mail Access Protocol*. Merupakan aplikasi yang memungkinkan kita membaca e-mail yang berada di server dari komputer di rumah / kantor kita, protokol ini sedikit berbeda dengan POP.

161 – SNMP, *Simple Network Management Protocol*. Lebih umum digunakan di router dan switch untuk memantau statistik dan tanda-tanda vital (keperluan monitoring).

177 – XDMCP, *X Display Management Control Protocol* untuk sambungan *remote* ke sebuah X server.

443 – HTTPS, HTTP yang aman (WWW) protokol di gunakan cukup lebar.

465 – SMTP atas SSL, protokol server email

512 (TCP) – exec adalah bagaimana menunjukkan di netstat. Sebenarnya nama yang tepat adalah rexec, untuk Remote Execution.

512 (UDP) – biff, protokol untuk mail pemberitahuan.

513 – Login, sebenarnya rlogin, alias Remote Login. Tidak ada hubungannya dengan standar / bin / login yang kita gunakan setiap kali kita log in.

514 (TCP) – Shell adalah nama panggilan, dan bagaimana netstat menunjukkan hal itu. Sebenarnya, rsh adalah aplikasi untuk "Remote Shell". Seperti semua "r" perintah ini melemparkan kembali ke kindler, sangat halus.

514 (UDP) – Daemon syslog port, hanya digunakan untuk tujuan logging *remote*.
515 – lp atau mencetak port server.

587 – MSA, *Mail Submission Agent*. Sebuah protokol penanganan surat baru didukung oleh sebagian besar MTA's (*Mail Transfer Agent*).
631 – CUPS (Daemon untuk keperluan printing), port yang melayani pengelolaan layanan berbasis web.

635 – Mountd, bagian dari NFS.

901 – SWAT, Samba Web Administration Tool port. Port yang digunakan oleh aplikasi pengelolaan SAMBA berbasis web.

993 – IMAP melalui SSL.

995 – POP melalui SSL.

1024 – Ini adalah port pertama yang merupakan *Unprivileged* port, yang ditugaskan secara dinamis oleh kernel untuk aplikasi apa pun yang memintanya. Aplikasi lain umumnya menggunakan port *unprivileged* di atas port 1024.
1080 – Socks Proxy Server.

1433 – MS SQL Port server.

2049 – NFSd, *Network File Service Daemon* port.

2082 – Port cPanel, port ini digunakan untuk aplikasi pengelolaan berbasis web yang disediakan oleh cpanel.

2095 – Port ini di gunakan untuk aplikasi webmail cpanel.

2086 – Port ini di gunakan untuk WHM, atau Web Host Manager cpanel.

3128 – Port server Proxy Squid.

3306 – Port server MySQL.

5432 – Port server PostgreSQL.

6000 – X11 TCP port untuk *remote*. Mencakup port 6000-6009 karena X dapat mendukung berbagai menampilkan dan setiap tampilan akan memiliki port sendiri. SSH X11Forwarding akan mulai menggunakan port pada 6.010.

6346 – Gnutella.

6667 – ircd, *Internet Relay Chat Daemon*.

6699 – Napster.

7100-7101 – Beberapa Font server menggunakan port tersebut.

8000 dan 8080 – Common Web Cache dan port server Proxy Web.

10000 – Webmin, port yang digunakan oleh webmin dalam layanan pengelolaan berbasis web.

2.5 Manajemen Jaringan

Pada awal 1980-an, jaringan komputer mulai dikembangkan dan saling terkoneksi. Kebutuhan akan sebuah manajeman jaringan semakin meningkat karena jaringan yang terus berkembang membesar semakin sulit untuk dikelola dengan baik. Salah satu bentuk manajemen jaringan yang paling kuno adalah *remote login*, yang digunakan untuk memonitor atau melakukan konfigurasi sebuah perangkat jaringan. Saat ini, banyak metode manajemen jaringan yang dapat ditemui. Manajemen jaringan merupakan sebuah persyaratan bagi semua orang yang ingin mengontrol dan memonitor jaringan.

2.5.1. Fungsi Manajemen Jaringan

Manajemen jaringan merupakan kemempuan untuk mengontrol dan memonitor sebua jaringan komputer dari sebuah lokasi. *The International Organization for Standardization* (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi manajemen jaringan.

1) Manajemen Kesalahan (Fault Manajemen)

Menyediakan fasilitas yang memungkinkan administrator jaringan untukmengetahui kesalahan (fault) pada perangkat yang dikelola, jaringan, dan operasi jarigan, agar dapat segera menentukan apa penyebab dan dapat segera mengambil tindakan (perbaikan). Untuk itu, manajemen kesalahan memiliki mekanisme untuk:

a) Meleporkan terjadinya kesalahan
b) Mencatat laporan kesalahan (logging)

c) Melakukan diagnosis

d) Mengoreksi kesalahan (dimungkinkan secara otomatis)

1. Manajemen Konfigurasi (Configuration Manajemen)

Memonifor informasi konfigurasi jaringan sehingga dampak dari perangkat keras ataupun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan untuk instalisasi, konfigurasi ulang, pengoperasian, dan mematiakan perangkat yang dikelola.

2) Pelaporan (Accounting)

Mengukur utilitas jaringan dari pengguna atau group tertentu untuk:

a) Menghasilkan informasi tagihan (billing)

b) Mengatur pengguna atau group

c) Membantu dan menjaga performa jaringan pada level tertentu yang dapat diterima

3) Manajemen Performa (Performance Manajement)

Mengukur sebagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistic sistem sehingga dapat dikelola dan dipertahankan pada level tertentu yang dapat diterima. Untuk itu, manajemen performa memiliki kemampuan untuk:

a) Memperoleh utilitas dan dan tingkat kesalahan dari perangkat jaringan

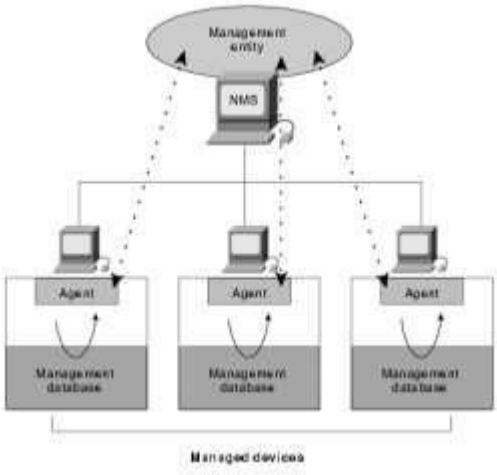
b) Mempertahankan performa pada level tertentu dengan memastiakan perangkat memiliki kapasitas yang dicukupi

4) Manajemen Keamanan (Security Manajement)

Mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin. Hal tersebut dilakukan dengan cara:

a) Membatasi akses ke sumber daya jaringan
b) Memberi emberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan

2.5.2 Arsitektur Manajemen Jaringan



Sumber: Jurnal

Gambar 15 Arsitektur Manajeman Jaringan

Arsitektur terdiri dari elemen-elemen sebagai berikut:

Network Manajemen Station (NMS)

Menjalankan aplikasi manajemen jaringan yang mampu mengumpulkan informasi mengenai perangkat yang dikelola dari agen manajemen yang terletak dalam perangkat. Aplikasi manajemen jaringan harus memproses data dalam jumlah yang besar, bereaksi terhadap peristiwa tertentu (*event*), dan mempersiapkan informasi yang relevan untuk ditampilkan. NMS biasanya memiliki *console* kendali dengan

sebuah antarmuka GUI yang memungkinkan pengguna untuk melihat reprensentasi grafis dari jaringan, mengontrol perangkat dalam jaringan yang dikelola, dan memprogram aplikasi manajemen jaringan. Beberapa aplikasi manajemen jaringan dapat deprogram untuk bereaksi terhadap informasi yang dapat dari agen manajemen dan / atau mengeset nilai ambang (*threshold*) dengan cara:

a) Melakukan tes kan koreksi otomatis (konfigurasi ulang, memetikan perangkat yang dikelola)
b) Mencatat yang terjadi pada jaringan (*logging*)
c) Memberikan informasi status dan peringatan pada pengguna

1) Perangkat yang dikelola, berupa semua jenis perangkat yang berada dalam jaringan seperti komputer, printer, ataupun router. Dalam perangakat, terhadap agen manajemen.
2) Agen manajemen, memberikan informasi mengenai perangakat yang dikelola kepada NMS dan dapat juga menerima informasi kendali / control.
3) Protokol manajemen jaringan, digunakan oleh NMS dan agen manajemen untuk bertukar informasi.
4) Informasi manajemen, merupakan informasi yang dipertukarkan antara NMS dan agen manajemen yang memungkinkan proses monitor dan control dari perangkat.

Perangkat linak manajaemen jaringan (aplikasi manajemen jaringan dan agen) biasanya berdasarkan protocol manajemen jaringan tertentu dan kemempuan manajemen jaringan yang diberikan oleh perangkat lunak biasanya berdasarkan pada fungsi yang didukung oleh protocol manajemen jaringan. Pemilihan perangkat lunak manajemen jaringan ditentukan oleh:

a) Lingkungan jaringan (jangkauan dan sifat jaringan)

b) Persyaratan manajemen jaringan

c) Biaya

d) Sistem operasi

Protokol manajemen jaringan yang paling umum digunakan adalah:

a) *Simple Network Manajement Protocol* (SNMP)

b) *Common Manajement Information Protocol* (CMIP)

SNMP merupakan protokol yang paling banyak digunakan pada lingkungan jaringan lokal (LAN). Sedangkan, CMIP digunakan pada lingkungan telrkomunikasi, dimana jaringan lebih besar dan kompleks.

BAB III

ANALISA JARINGAN BERJALAN

3.1. Tinjauan Perusahaan

Kota Administrasi adalah pembagian wilayah Administrasi di Indonesia Provinsi DKI Jakarta terdapat 5 kota Administrasi yaitu Jakarta Barat, Jakarta timur, Jakarta Utara, Jakarta Selatan dan Jakarta Pusat yang hanya berada di Provinsi DKI Jakarta serta 1 Kabupaten Administrasi yaitu Kabupaten Kepulauan Seribu yang dipimpin oleh seorang Bupati. Berbeda dengan kota-kota lain di Indonesia, kota administrasi bukanlah daerah otonom. Kota Administrasi dipimpin oleh seorang Walikota dan dibantu oleh Wakil Walikota yang diangkat oleh Gubernur dari kalangan Pegawai Negeri Sipil (PNS). Perangkat daerah Kota Administrasi terdiri atas Sekretariat Kota Administrasi, Suku Dinas, lembaga teknis lain, kecamatan dan kelurahan.

3.1.1. Sejarah Perusahaan

Kota Administrasi Jakarta Barat mempunyai luas wilayah : 12.615,14 Ha dan terletak antara 106 - 48 BT, 60 - 12 LU dan dibatasi oleh wilayah sebagai berikut: Sebelah Selatan: Kota Administrasi Jakarta Selatan dan Kabupaten/Kodya Tangerang, Sebelah Barat: Kabupaten dan Kotamadya Tangerang, Sebelah Timur: Kota Administrasi Jakarta Utara dan Kota Administrasi Jakarta Pusat, sedangkan Sebelah Utara: Kabupaten/Kota Madya Tangerang dan Kota Administrasi Jakarta Utara. Jakarta Barat mempunyai 8 Kecamatan, 56 Kelurahan, 578 Rukun Warga, 6.348 Rukun Tetangga. Dari segi personilnya, Walikota Jakarta Barat mempunyai

10.589 orang Pegawai yang terdiri dari: 1. Pegawai Pemerintahan : 3.364 orang 2. Guru SD, SLTP, SLTA 6.537 orang 3. Medis dan Paramedis 688 orang.

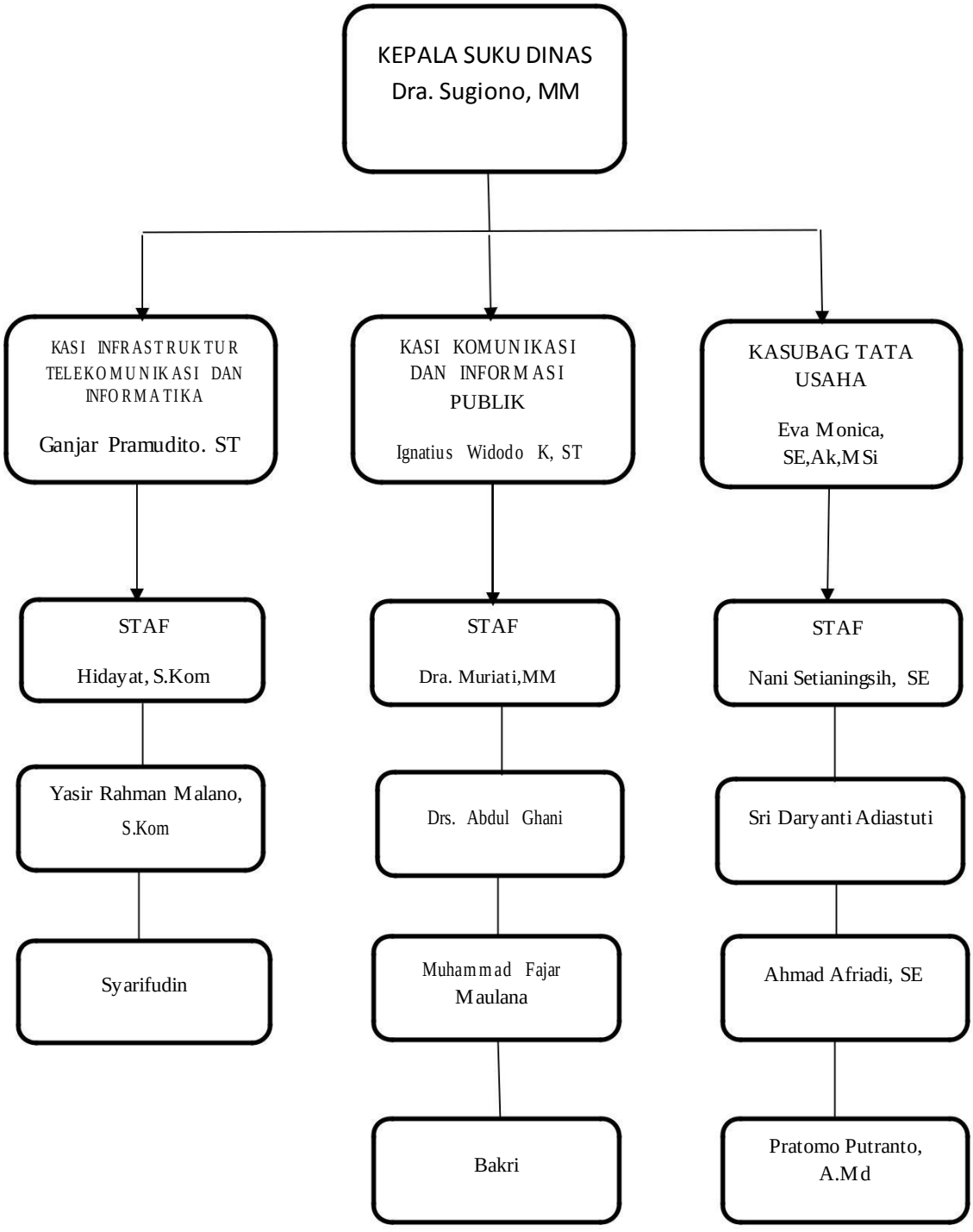
Jakarta Barat mempunyai visi agar terwujudnya Kota Administrasi Jakarta Barat sebagai Kota jasa yang nyaman dan sejahtera. Dan misi untuk membangun tata pemerintahan yang baik guna terwujudnya kota jasa dan wisata budaya dan sejarah. Meningkatkan kualitas lingkungan perkotaan yang berkelanjutan dan memberdayakan masyarakat dengan mengembangkan nilai, norma serta pranata sosial, guna meningkatkan kualitas pelayanan masyarakat. Motto Jakarta Barat adalah "Kampung Kite Kalo Bukan Kite Nyang Ngurusin Siape Lagi" Motto ini mempunyai makna dan harapan akan besarnya rasa tanggung jawab dan rasa cinta warga masyarakat pada Kota Administrasi Jakarta Barat yang diwujudkan dengan peran serta dan kerjasama yang erat dan terpadu antara pemerintah, pihak swasta dan masyarakat dalam memajukan pembangunan kota disegala bidang demi kesejahteraan semua masyarakat termasuk bersama-sama untuk menjaga dan menciptakan lingkungan yang aman, tertib dan bersih. Dengan ini juga sarat makna yang sangat disadari bahwa kitalah yang menentukan keberhasilan itu semua dengan segala daya dan upaya kita sendiri. Pemerintah Kota Administrasi Jakarta Barat mempunyai 59 Unit Kerja Perangkat Daerah (UKPD) yang membantu dalam penyelenggaraan pemerintah di wilayah Jakarta Barat. Salah satunya adalah Suku Dinas Komunikasi , Informatika dan Statistik yang beralamat di Kantor Walikota Jakarta Barat Jalan Kembangan Raya No. 2 Kelurahan Kembangan Utara, Kecamatan Kembangan, Jakarta Barat, 11610.

Peraturan Pemerintah Nomor : 25 Tahun 1978, wilayah DKI Jakarta di bagi menjadi 5 (lima) wilayah kota administrasif. Wilayah kotamadya Jakarta Barat merupakan

salah satu bagian yang memiliki kedudukan setingkat dengan Kotamadya Tingkat II. Walikotamadya yang bertanggungjawab langsung kepada Gubernur KDKI Jakarta Berdasarkan Penetapan Presiden RI No.2 Tahun 1961 tentang Pemerintahan DKI Jakarta dan Penjelasan Undang-undang No. 5 Tahun 1974 tentang pokok-pokok pemerintah di daerah, bahwa tugas, wewenang dan kewajiban Walikotamadya adalah menjalankan Pemerintahan pembangunan dan pembinaan kemasyarakatan dalam wilayah. Tugas-tugas tersebut meliputi bidang pemerintahan, ketentraman dan ketertiban, kesejahteraan masyarakat, sosial politik, agama, tenaga kerja, pendidikan, pemudan dan olah raga. Kependudukan perekonomian dan pembangunan fisik prasarana lingkungan serta bidang-bidang lain yang ditetapkan oleh Gubernur Kepala daerah Khusus Ibukota Jakarta. Pemukiman di daerah sangat padat penduduk seperti Kelurahan Kali Anyar sudah tidak layak huni dan tidak memenuhi persyaratan kesehatan. Mata pencaharian penduduk Kodya Jakarta Barat:

a) Pertanian : 1.02%
b) Pertambangan : 0.30%
c) Industri : 23.24%
d) Listruk/gas/air minum : 1.17%
e) Perdagangan : 33.28%
f) Angkutan dan komunikasi : 6.22%
g) Keuangan/asuransi : 3.47%
h) Bangunan : 5.66%
i) Jasa dan lainnya : 25.64%

3.1.2 Struktur Organisasi dan Fungsi



Sumber: SUDIN Kominfo Jakarta Barat

Gambar 16 Struktur Organisasi Walikota

1) Tugas Kepala Suku Dinas

a) Memimpin dan mengkoordinasikan pelaksanaan tugas dan fungsi suku dinas.

b) Mengkoordinasikan pelaksanaan tugas dan fungsi subbagian, seksi, dan subkelompok jabatan fungsional.

c) Melaksanakan koordinasi dan kerjasama dengan satuan perangkat daerah (SKPD), unit kerja perangkat daerah (UKPD), dan atau instansi pemerintah atau swasta dalam rangka pelaksanaan tugas dan fungsi suku dinas.

d) Melaporkan dan mempertanggung jawabkan pelaksanaan tugas dan fungsi suku dinas.

2) Tugas Kasi Infrastruktur Telekomunikasi dan Informatika

Dinas komunikasi dan informatika merupakan unsur pelaksanaan Pemerintah Daerah, yang dipimpin oleh Kepala Dinas dan mempunyai tugas melaksanakan urusan pemerintah daerah dibidang komunikasi dan informatika berdasarkan asas desentralisasi dan tugas pembantuan.

Tugas pokok

Dinas kominfo Kota Jakarta Barat mempunyai tugas membantu kepala daerah dalam menyelenggarakan usuran rumah tangga daerah dalam bidang komunikasi dan informatika serta melaksanakan tugas pembantuan sesuai dengan bidang tugasnya.

3) Tugas Kasi Komunilasi dan Informasi Publik

Memimpin, merencanakan operasional, mengendalikan dan mengevaluasi kegiatan bidang layanan informasi publik melalui kegiatan seksi pengelolaan dan pelayanan informasi publik, serta kegiatan bimtek, supervise, pemantauan, pelaporan, evaluasi dan pendokumentasian kegiatan berdasarkan ketentuan dan prosedur yang berlaku agar tewujudnya pelayan seksi yang maksimal dan handal.

4) Tugas Kasubag Tata Usaha

Sub bagian tata usaha dipimpin oleh Kepala sub Bagian, dengan tugas pokok pemberian pelayanan teknis dan administrasi kepada semua satuan unit dibidang tata usaha meliputi perncanaan, pelaporan, kepegawaian, keuangan rumah tangga, keprotokoleran, perlengkapan serta peralatan kantor.

3.2. Skema Jaringan Berjalan

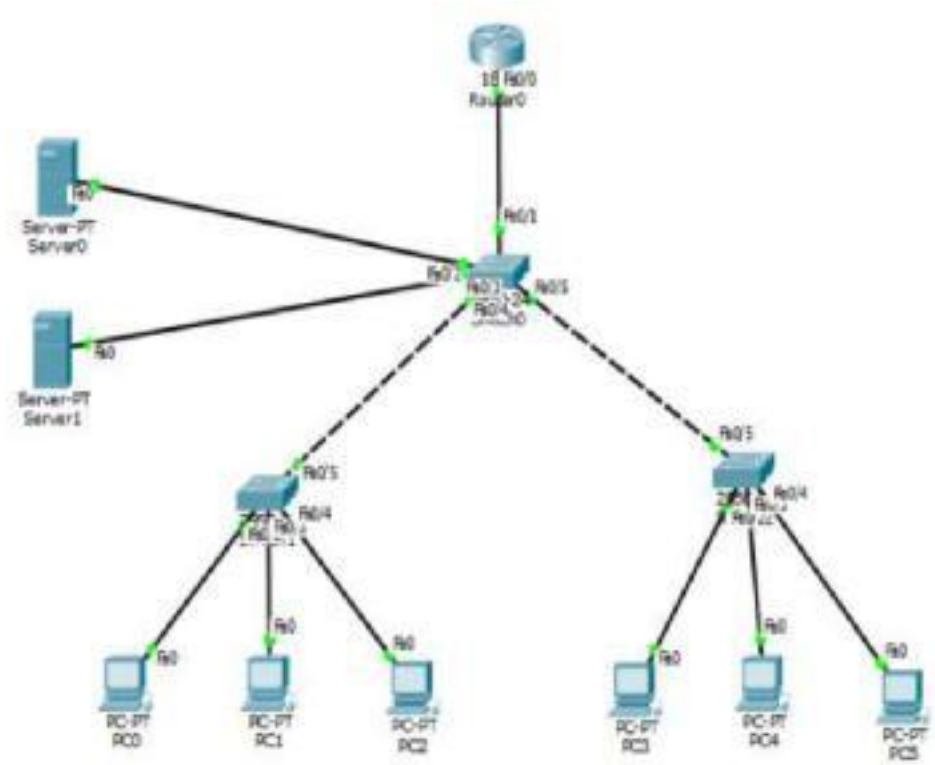
Dalam membangun sebuah keamanan jaringan atau *Virtual Local Area Network* (VLAN) tidak hanya terpusat pada transfer atau akses data nya saja tapi infrastruktur sebuah jaringan harus lebih dierhatikan, karena infrastruktur ini akan membuktikan apakah sebuah jaringan akan bertahan lama atau sebaliknya.

3.2.1. Topologi Jaringan

Toologi jaringan meruakan hal yang paling mendasar dalam membentuk sebuah jaringan . topologi yang digunakan pada Suku Dinas Komunikasi dan Informatiaka Kantor Walikota Jakarta Barat adalah Star. Semua perangkat jaringan *client* dan *server* terhubung ke jaringan melalui perangkat *switch*.

3.2.2. Skema Jaringan

Skema jaringan pada Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat yaitu:



Sumber: SUDIN Kominfo Jakarta Barat

Gambar 17 Skema Jaringan SUDIN Kominfo Jakbar

Gambar jaringan pada Suku Dinas Komunikasi dan Informatika Kantor Jakarta Barat terdiri dari *router, switch, proxy, web server.*

System jaringan di Suku Dinas Komunikasi dan Informatika Kantor Walikota Jakarta Barat pertama di hubungkan dari *router* ke *switch* yang berfungsi sebagi *gateway* yang terhubung ke *server1* dan *server2* salanjutnya terhubung ke

dua buah *switch* yang selanjutnya menghubungkan ke beberapa PC yang terhubung Ke *switch*.

3.2.3. Keamanan Jaringan

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelanggaran dan perusakan oleh penyusup. Beberapa pakar jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk mewujudkan sistem jaringan komputer yang aman yaitu dengan menggunkan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain hanya komputer yang tidak terhubung jaringanlah yang mempunyai keamanan yang sempurna. Sistem keamanan yang diterapkan pada jaringan yang sedang berjalan, hanya berkisar pada komputer *server* dan komputer *client* yang dipasang *software* antivirus trend micro dari sistem operasi yang digunakan.

a) Sebuah aturan yang bisa diterapkan pada komponen *hardware,software* maupun sistem itu sendiri yang bertujuan untuk melindungi dengan teknik *filterisasi*, membatasi, juga dengan menolak sebuah permintaan koneksi. Fungsi dari *firewall* yaitu mengontrol dan mengatur lalu lintas jaringan, melakukan proses pengecekan dan pemberian ijin terhadap suatu akses, melindungi setiap sumber daya yang terdapat di dalam jaringan *private*, mencatat setiap aktivitas dan melaporkannya kepada *administrator* jaringan melalui catatan *log*.
b) Port berfungsi untuk mencegah ada nya penyusup yang mencoba masuk ke dalam jaringan, melindungi jaringan dari pehak yang tidak bertanggung

jawab. Dan melindungi jaringan dari IP yang tidak dikenal atau yang tidak di daftarkan oleh admin jaringan.

3.2.4. Spesifikasi *Hardware* dan *Software* Jaringan

Jaringan *Metropolitan Area Network* (MAN) digunakan untuk menghubungkan komputer pusat dan komputer cabang yang menggunakan peralatan untuk saling bertukar informasi. Di dalam pemakaian jaringan *Metropolitan Area Network* (MAN) disebuah perusahaan atau perkantoran dibutuhkan beberapa perangkat keras (*hardware*). Berikut adalah beberapa perangkat keras yang digunakan oleh Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat guna mendukung instalasi jaringannya.

1) Perangkat Keras (*Hardware*)

a) PC *Server*

Server adalah sebuah komputer yang digunakan sebagai pusat data dari client. Dimana dari *server* inilah data-data bisa di *backup* dan dikendalikan, ada begitu banyak jenis *server* yang biasa di pakai untuk jaringan, tergantung dari pemilihan instansi atau perusahaan tersebut. Suku Dinas Komunikasi dan Informatiak Kantor Walikota Jakarta Barat menggunakan.

Table 2 Spesifikasi PC Server

No	**Nama PC Server**		**Spesifikasi**
1.	DELL PowerEdge T110II	Processor Harddisk RAM NIC OS	Intel Xeon (8M Cache, 3.20 GHz) 1 TB Serial ATA-II/30. 7200 RPM 4 GB Embedded Gigabit Ethernet Controller Windows Server 2003 Enterprice

Sumber: WEB DELL

b) PC *client*

Client adalah sebagai tempat untuk memproses source di komputer *server*. Berikut adalah spesifikasi dari komputer *client* pada Suku Dinas Komunikasi dan Informatika Kantor Walikota Jakarta Barat:

Table 3 Spesifikasi PC Client

No	Hardware	Spesifikasi
1.	Processor	Core 2 Duo 1,8 GHz
2.	Motherboard	ECS G41T-M16
3	Memory	DDR2-2 GB
4.	Harddisk	Seagate 500 GB
5.	NIC	Atheros AR8151 PCI-E Gigabit Ethernet Controller
6.	OS	Windows 7 Profesional
7.	Keyboard, Mouse	USB Logitech

Sumber: WEB DELL

c) *Modem*

Modem yang digunakan oleh Suku Dinas Komunikasi dan Informatika Kantor Walikota Jakarta Barat yaitu Modem *Type* TP-Link TD-W8951ND.

Table 4 Spesifikasi Modem

No	Hardware Features	
1.	Interface	4 10/100Mbps RJ45 Ports 1 RJ11 Ports
2.	Button	1 Power On/Off Switch 1 WPS Button 1 Wi-Fi On/Off Button
3.	External Power Supply	9VDC/0.6A
4.	IEEE Standards	IEEE 802,3, 802,3u
5.	ADSL Standards	Full-rate ANSI T1.413 Issue 2,ITU-T G.992.1(G.DMT), ITU-T G.992.2(G.Lite), ITU-T G.994.1(G.hs), ITU-T G.995.1, ITU-T G.996.1, ITU-T G.997.1, ITU-T K.2.1
6.	ADSL2 Standards	ITU-T G.992.3 (G.dmt.bis), ITU-T G.992.4 (G.Lite.bis)
7.	ADSL2+ Standards	ITU-T G.992.5
8.	Dimensions (w*D*H)	7.1*4.9*1.4 in.(181*125*36mm)
9.	Antenna Type	Omni Directional, Detachable, Reverse SMA
10.	Antenna Gain	1*5dbi

Sumber: WEB TP-Link

d) *Router*

Router yang digunakan oleh Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat adalah *type* RB951UI-2nD. Berikut adalah spesifikasi Mikrotik RB951UI-2nD Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat :.

Table 5 Spesifikasi Router

No	**Spesifikasi**	
1.	Produck code	RB951Ui-2nD
2.	Architecture	MIPSBE
3.	CPU	QCA9531
4.	CPU Core Count	1
5.	CPU Nominal frequency	650 MHz
6.	Dimensions	113*89*28mm
7.	License level	4
8.	Operating System	RouterOS
9.	Size of RAM	64 MB
10	Storage Size	16 MB
11	Storage type	Flash
12.	Tested ambient temperature	-30+70 C
13.	Suggested price	$45.00

Sumber: WEB Cisco

e) *Switch*

Switch yang digunakan oleh Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat yaitu merk CISCO SRW224G4-K9-EU

24-Ports 10/100 Managed Switch sebanyak 2 (Dua) buah dan merk CISCO SG220-26-K9-EU Switch Managed sebanyak 2 (dua) buah.

Table 6 Spesifikasi Switch

No	**Spesifikasi**	
1.	Releas Date	01-AUG-2010
2.	Rack-Mount 23 in.(58.4 cm) EIA:	Included
3.	Jumbo Frame Support	10 KB
4.	RAM	128 MB
5.	Power Device	Power Adater-external
6.	Flash Memory	16 MB
7.	Performance	Switching capacity: 12.8 Gbps; Forwarding Performance(64-byte packet size): 95.2 Mbps
8.	Port	24*10/100+2*Combo Gigabit SFP +2*10/100/1000
9.	MAC Address Table Size	16k entries

Sumber: WEB Cisco

2) Perangkat Lunak(*Software*)

Perangkat Lunak (*Software)* yang digunakan Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat menggunakan beberapa perangkat lunak yang menjadi infrastruktur dasar dan saran untuk kebutuhan pekerjaan dan juga untuk mengakses ke internet

Adapun jenis – jenis perangkat lunak yang digunakan yaitu :

a) Microsoft Office 2010
b) Adobe Reader
c) WinZip/WinRar
d) Mozilla Firefox
e) Anti Virus

3.3. Permasalahan

Permasalahan system jaringan komputer pada Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat, yaitu:

1. Belum maksimalnya penerapan VLAN pada SUDIN Komunikasi dan Informatika Jakarta barat
2. Belum menerapkan remot jaringan untuk memermudah mengontrol jaringan.
3. Konfigurasi yang telah di lakukan di *switch* telah menerapkan username dan password namaun belum di *encryption* jadi masih rentan akan tindakan kejahatan.

3.4. Alternatif Pemecahan Masalah

Alternatif pemecahan masalah sistem jaringan komputer pada Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat, yaitu:

1. Memaksimalkan VLAN di seluruh manajemen di Kantor Walikota Jakarta Barat, khusus nya SUDIN Kominfo. Sehingga memermudah kerja karyawan dalam proses pekerjaan dan memperhemat bandwith di Suku Dinas Komunikasi dan Informatika Kantor Walikota Jakrta Barat.

2. Menerapkan remot jaringan Telnet atau SSH suaya lebih mempermudah staf IT dalam mengontrol jaringan
3. Melakukan *encryption password* pada *switch* supaya tidak sembarangan *user* bisa masuk dan mengubah konfigurasi yang telah di buat pada *switch*.

BAB IV

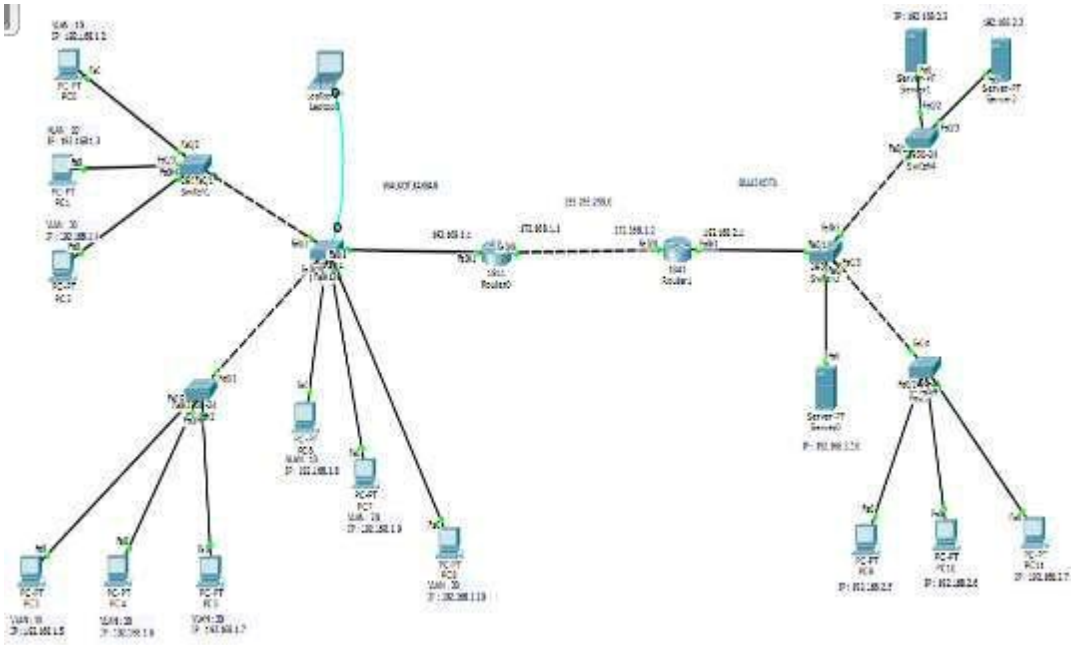
RANCANGAN JARINGAN USULAN

4.1 Analisa Jaringan

Berdasarkan penelitian dan Analisa jaringan yang sedang berjalan, khususnya keamanan jaringan pada Suku Dinas Komunikasi dan Informatika Walikota Jakarta Barat, maka usulan atau solusi dari keamanan jaringan yang sudah ada, dengan menggunakan keamanan ada *switch*. penulis menggunakan aplikasi *Cisco Packet Tracer* 6.1 sebagai alat untuk melakukan simulasi. Alasan penggunaan alat simulasi ini adalah untuk memudahkan dalam penggunaan aplikasi karena dilengkapi dengan berbagai macam perangkat yang dibutuhkan dalam melakukan simulasi nantiknya.

4.1.1 Toologi Jaringan Baru

Gambar IV.1 menunjukana topologi yang baru pada Suku Dinas Komunikasi dan Informatika Jakarta Barat. Dari topologi tersebut terlihat dua buah *switch* terhubung ke sebuah *switch*/backbone dan ini memebrikan beberpa keuntungan bagi staf IT untuk menerakan kemanan jaringan, seperti VLAN yang membuat segmen yang ada tiap *switch*, penerapan remot jaringan dan tentunya memudah dalam manjemen jaringan.



Sumber: Data Pribadi

Gambar 18 Topologi Jaringan

4.1.2 Pembagian IP Address

Setelah topologi jaringan baru yang telah dibuat, selanjut nya adalah melakukan pemberian IP address kepada semua PC, *switch*, *router*, seuai dengan kebutuahan yang ada dan menetap kan port-port masing masing device untuk memudah kan melakukan konfigurasi dalam menerapkan keamanan jaringan.

Pada table IV.1 dapat diliahat setiap divisi akan diberi IP address sesuai dengan kebutuahan yang ada pada Suku Dinas Komunikasi dan Informatika Jakarta Barat.

Table 7 IP Address Walikota

PERANGKAT	IP ADDRESS	NETMASK	GATEWAY
PC0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	192.168.1.3	255.255.255.0	192.168.1.1
PC2	192.168.1.4	255.255.255.0	192.168.1.1
PC3	192.168.1.5	255.255.255.0	192.168.1.1
PC4	192.168.1.6	255.255.255.0	192.168.1.1
PC5	192.168.1.7	255.255.255.0	192.168.1.1
PC6	192.168.1.8	255.255.255.0	192.168.1.1
PC7	192.168.1.9	255.255.255.0	192.168.1.1
PC8	192.168.1.10	255.255.255.0	192.168.1.1
Switch0	192.168.1.1	255.255.255.0	192.168.1.1
Switch1	192.168.1.1	255.255.255.0	192.168.1.1
Switch2	192.168.1.1	255.255.255.0	192.168.1.1
Router0	192.168.1.1	255.255.255.0	192.168.1.1

Sumber: SUDIN Kominfo Jakarta Barat

Table 8 IP Address Balaikota

PERANGKAT	IP ADDRESS	NETMASK	GATEWAY
PC9	192.168.2.5	255.255.255.0	192.168.2.1
PC10	192.168.2.6	255.255.255.0	192.168.2.1
PC11	192.168.2.7	255.255.255.0	192.168.2.1
Server0	192.168.2.10	255.255.255.0	192.168.2.1
Server1	192.168.2.2	255.255.255.0	192.168.2.1
Server2	192.168.2.3	255.255.255.0	192.168.2.1
Switch3	192.168.2.1	255.255.255.0	192.168.2.1
Switch4	192.168.2.1	255.255.255.0	192.168.2.1
Switch5	192.168.2.1	255.255.255.0	192.168.2.1
Router1	192.168.2.1	255.255.255.0	192.168.2.1

Sumber: SUDIN Kominfo Jakarta Barat

4.1.3 Menghubungkan 2 Router Walikota dan Balaikota

Setelah topologi dirancang selanjut nya melakukan konfigurasi kepada kedua router, router Walikota dan router Balaikota supaya kedua router ini terhubung dan bisa saling bertukar data.

Router(config)#router rip

Router(config-router)#network IP yang berlawanan

Router(config)ip route network,mask,next hop(yangberlawana)

Lakukan juga konfigurasi yang sama pada *router* lawan

4.1.4 Konfigurasi *Username* dan *Password* pada *Switch*

Selanjutnya cara melakukan konfigurasi *password* pada *switch* supaya tidak sembarangan *user* atau orang yang tidak diingikan bisa masuk.

Switch(config)#username … password …

Switch(config)#line console 0

Switch(config-line)#login local

4.1.5 Konfigurasi Enkrisi *Password*

Setelah *username* dan *password* diterakan pada *switch* tentu *switch* sudah aman, namaun supaya lebih aman lagi *usename* dan *password* yang telah dibuat harus di enkripsi untuk lebih aman.

Switch(config)#service password-encryption

4.1.6 Konfigurasi VLAN

Selanjutnya bagai mana cara melakukan konfigurasi VLAN pada *switch* sehingga penerapannya sesuai dengan yang direncanakan.

Switch(config)#interface Faseternet port

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan id

4.1.7 Konfigurasi Telnet

Setelah melakukan berbagai macam konfigurasi pada *switch* dan berbagai macam kemanan yang dibutuhkan yang telah di terapkan tentu tak kalah pentingnya adalah penerapan konfigurasi telnet, yang mana fungsi nya untuk remot jaringan.

Switch(config)#line vty 0 1

Switch(config-line)#transort input telnet

Switch(config-line)#password …

Switch(config-line)#login

Switch(config)#enable secret …

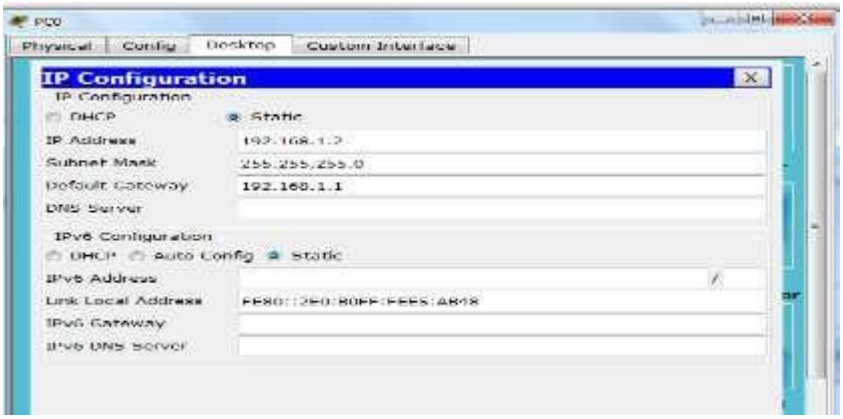
4.2 Pengujian Jaringan

Selanjutnya dilakukan pengujian keamanan jaringan yang akan diterapkan di Suku Dinas Komunikasi dan Informatika Jakarta Barat adalah, penerapan *username, password,* enkripsi *password,* penerapan VLAN, remot jaringa menggunakan telnet.

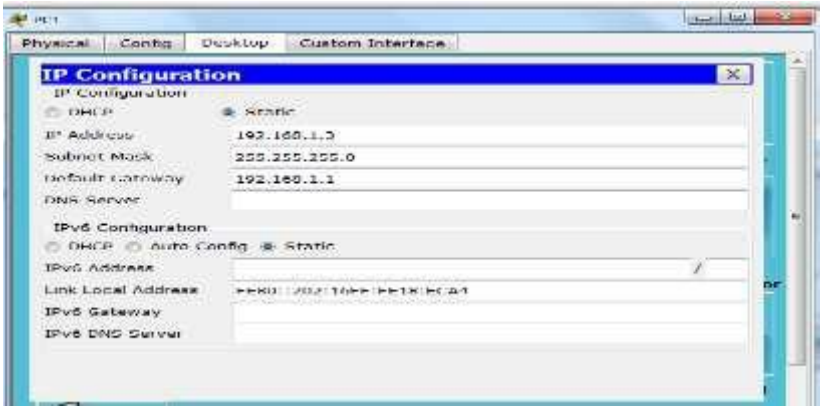
4.2.1 Menghubungkan dua Buah *Router*

a. Setting IP

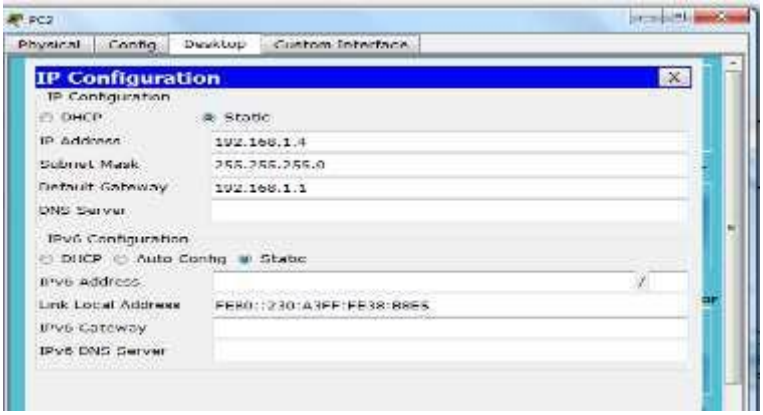
PC0


PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:80FF:FEE5:A818
IPv6 Gateway
IPv6 DNS Server

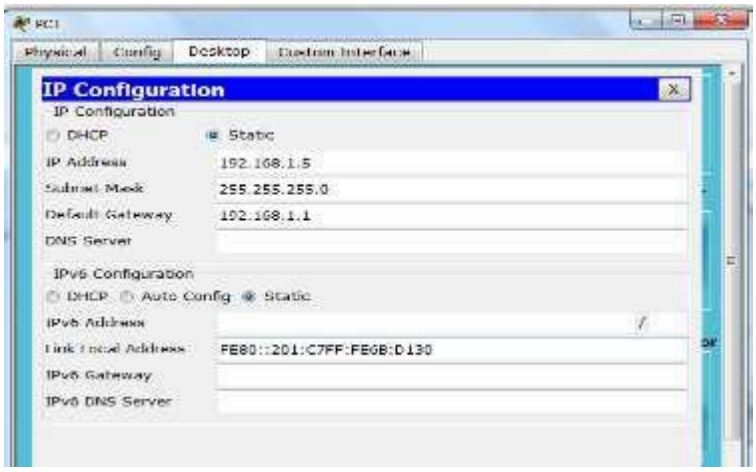
PC1


Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
IPv6 Gateway
IPv6 DNS Server

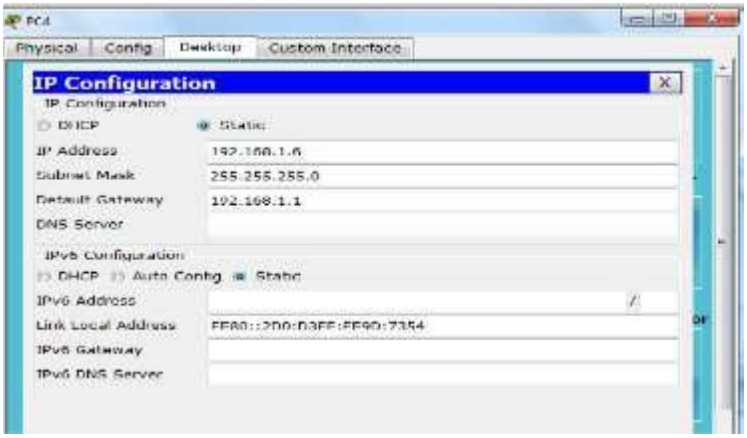
PC2


Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::230:A3FF:FE38:8865
IPv6 Gateway
IPv6 DNS Server

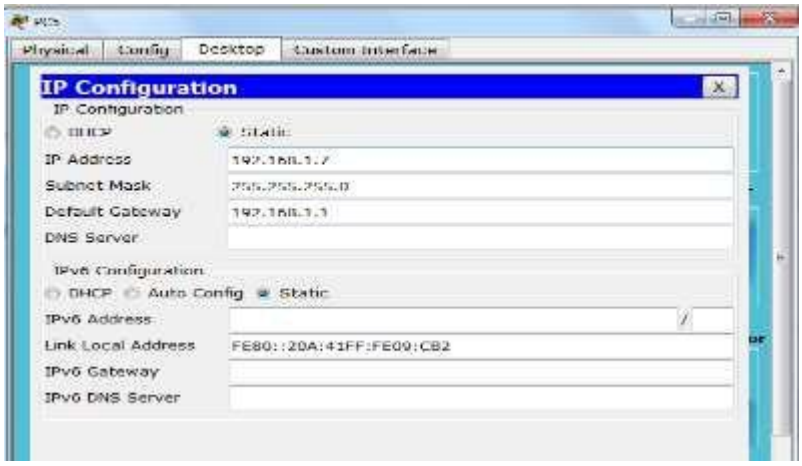
PC3


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.5
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:C7FF:FE6B:D130
IPv6 Gateway
IPv6 DNS Server

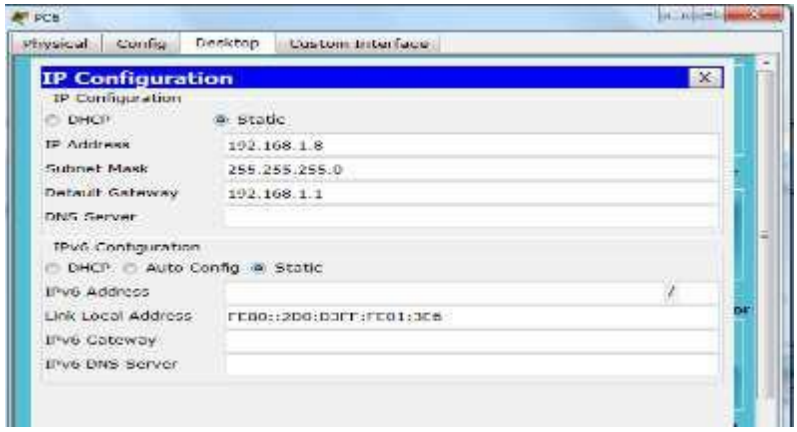
PC4


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.6
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::200:D3FF:FE9D:7354
IPv6 Gateway
IPv6 DNS Server

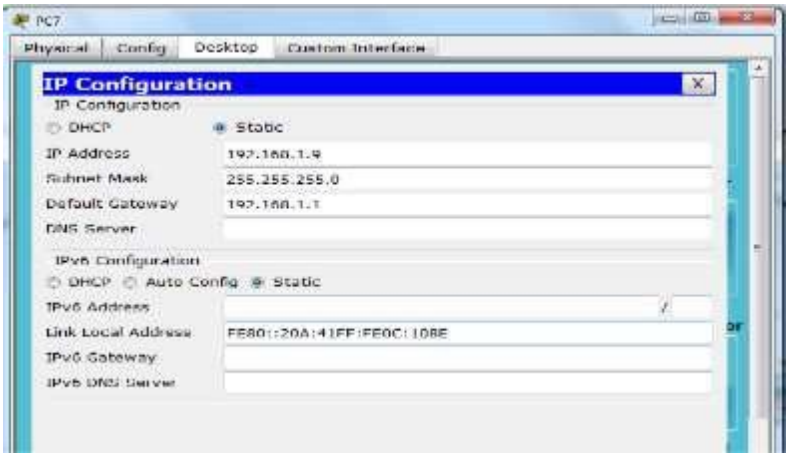
PC5


Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FE09:CB2
IPv6 Gateway
IPv6 DNS Server

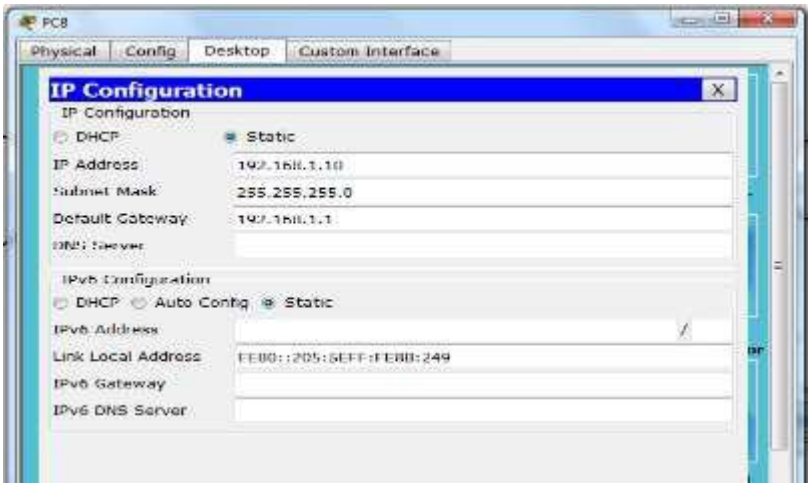
PC6


PC6
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.8
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
IPv6 Gateway
IPv6 DNS Server

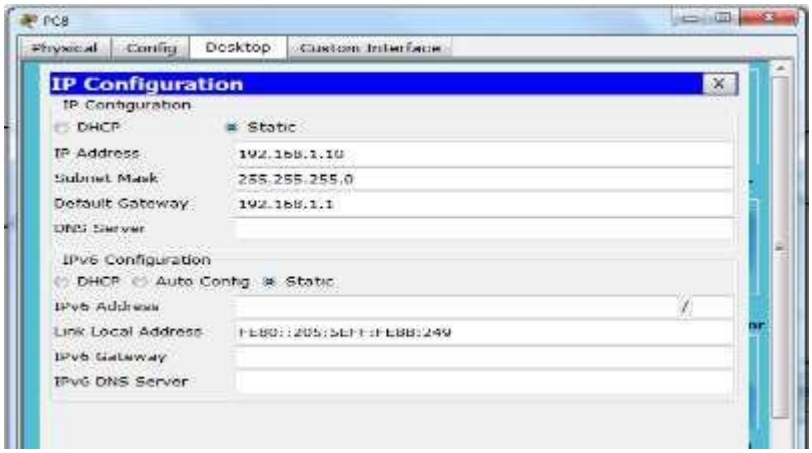
PC7


PC7
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.9
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FE0C:108E
IPv6 Gateway
IPv6 DNS Server

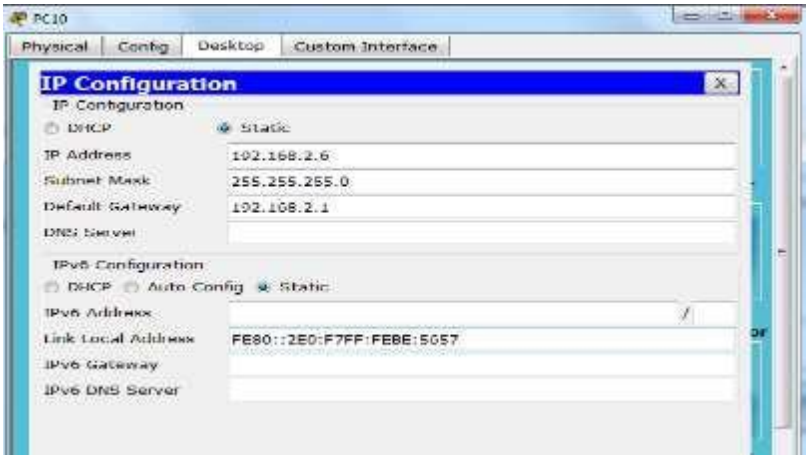
PC8


PC8
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::205:5EFF:FE80:249
IPv6 Gateway
IPv6 DNS Server

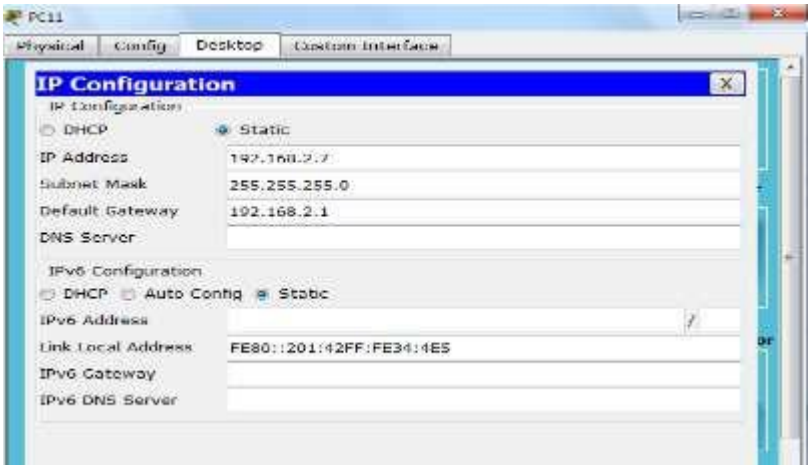
PC9



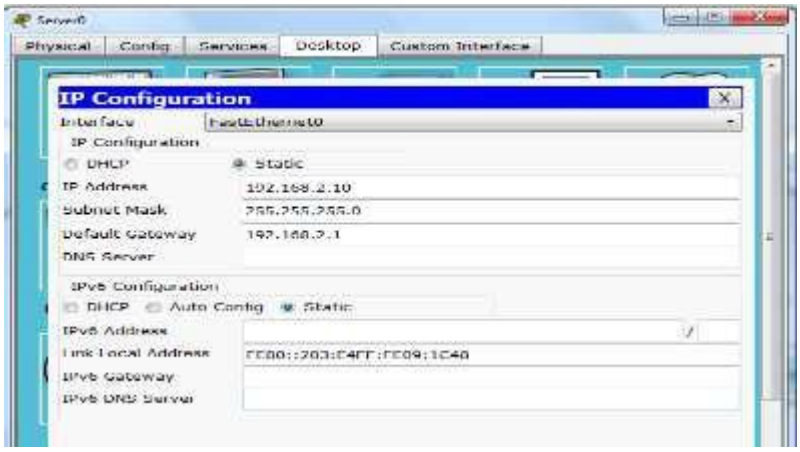
PC10



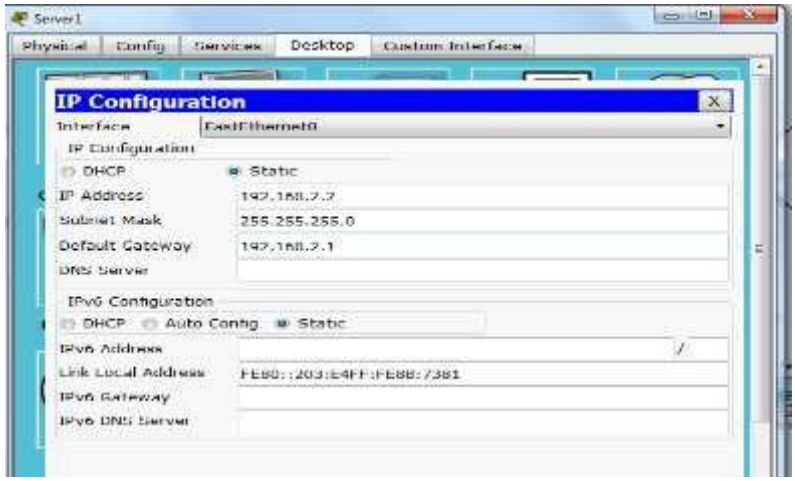
PC11



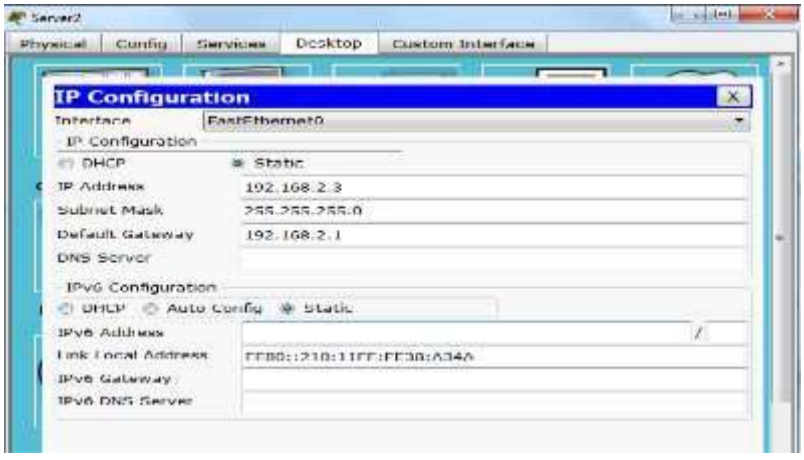
Server0



Server1



Server2



b. Konfigurasi *Router* Tambahkan IP *Router*.

Router0

Router0>Enable

Router0#Configure terminal

Router0(config)#Interface fasteternet0/0

Router0(config-if)#Ip address 172.168.1.1 255.255.255.0

Router0(config-if)#No shutdown

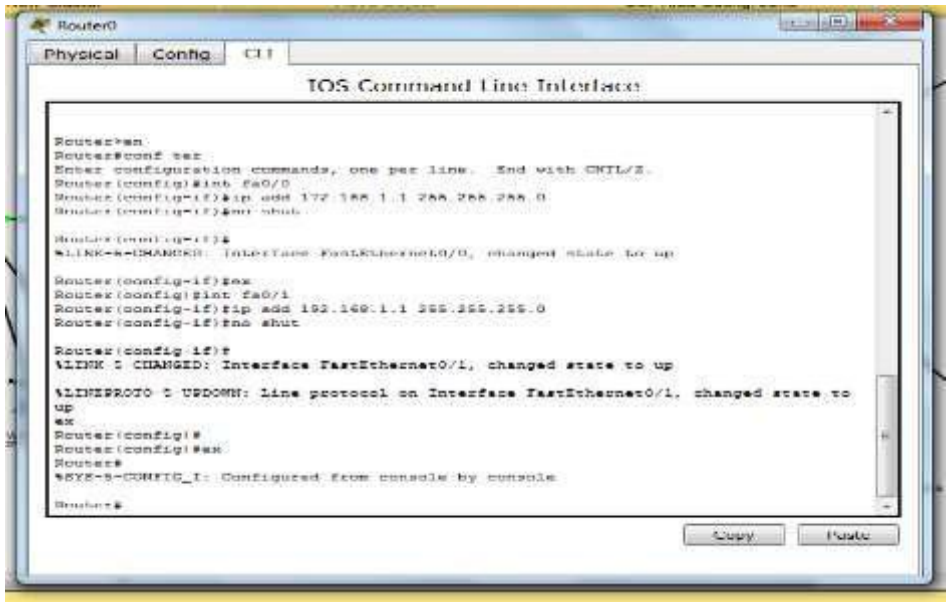
Router0(config-if)#Exit

Router0(config)#Interface fasteternet0/1

Router0(config-if)#Ip address 192.168.1.1 255.255.255.0

Router0(config-if)#No shutdown

Router0(config-if)#Exit



Router1

Router1>Enable

Router1#Conf ter

Router1(config)#Interface fasteternet0/0

Router1(config-if)#Ip address 172.168.1.2 255.255.255.0

Router1(config-if)#No shutdown

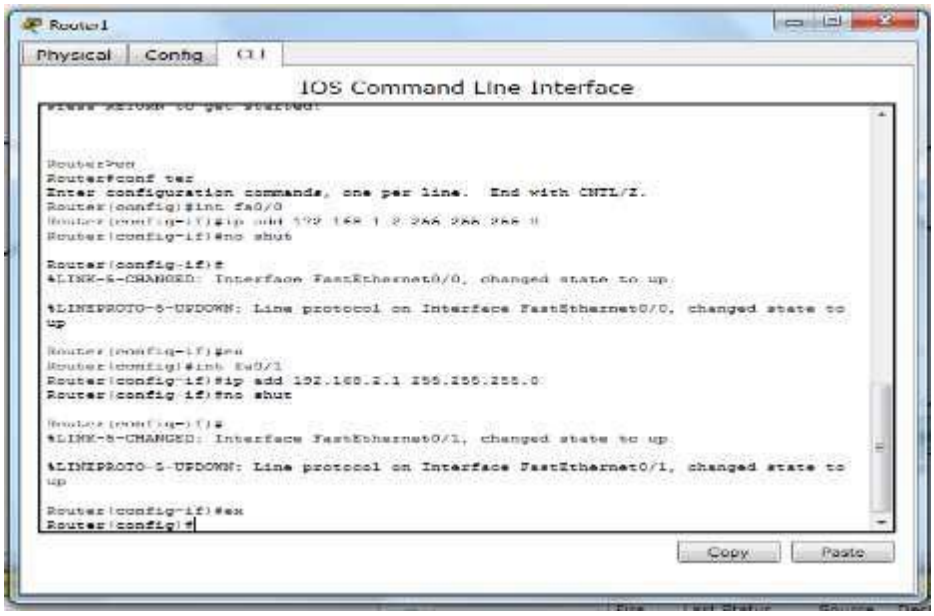
Router1(config-if)#Exit

Router1(config)#Interface fasteternet0/1

Router1(config-if)#Ip address 192.168.2.1 255.255.255.0

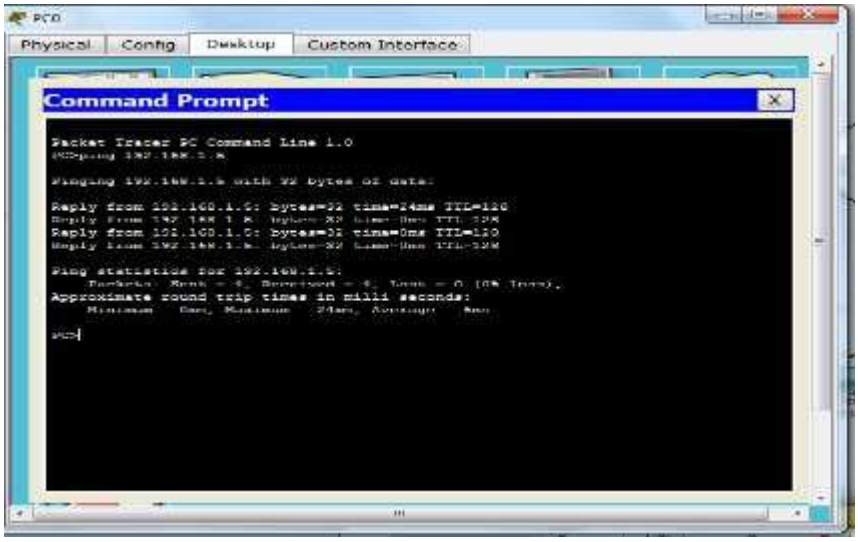
Router1(config-if)#No shutdown

Router1(config-if)#Exit

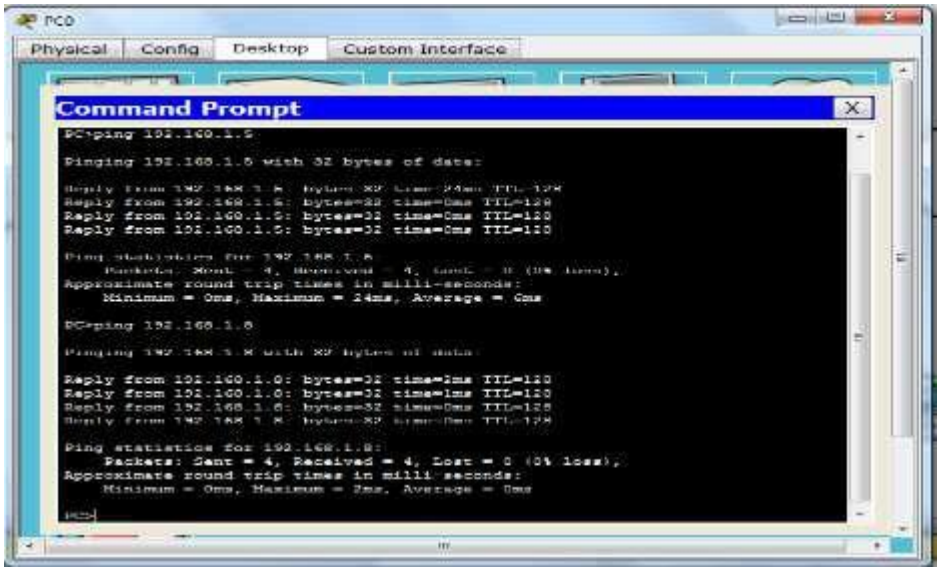


c. Cek Koneksi

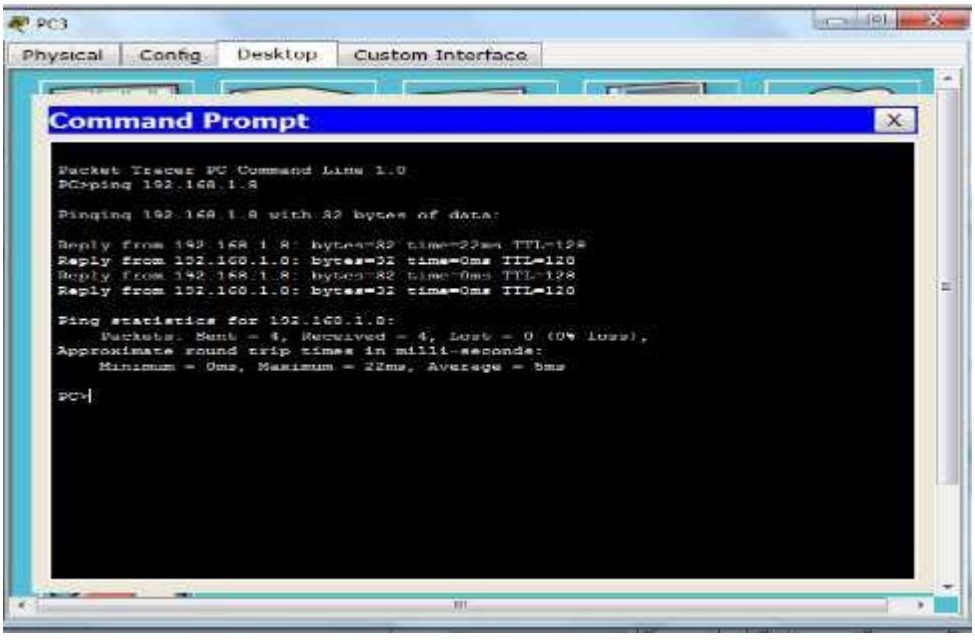
Ping PC0 ke PC3



Ping PC0 ke PC6

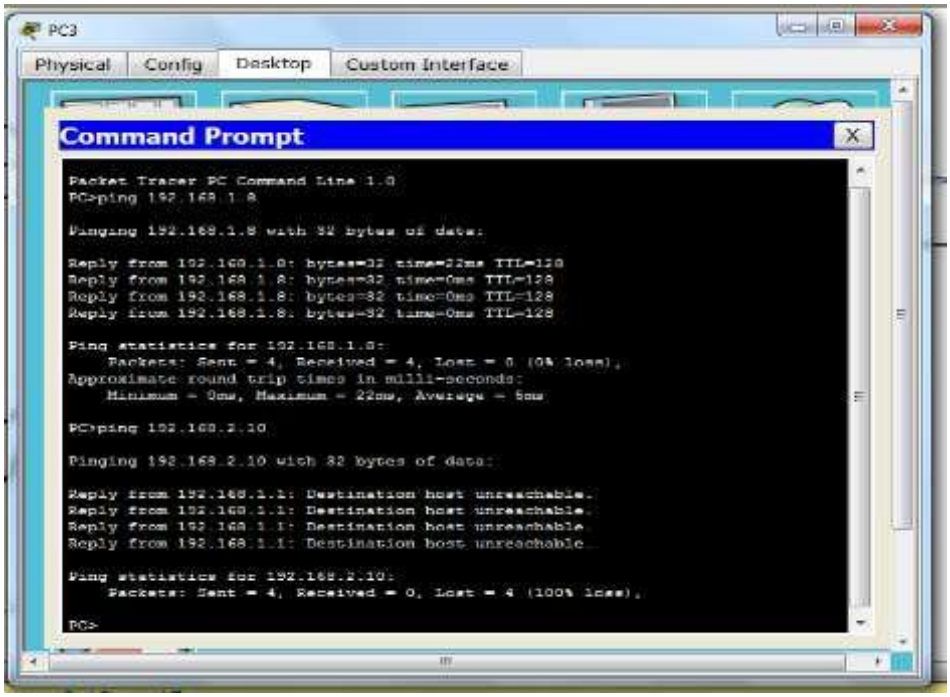


Ping PC3 ke PC6



Sekarang coba konek kan dari Walikota ke Balaikota, dari PC3 ke Server0

Ping PC3 ke Server0

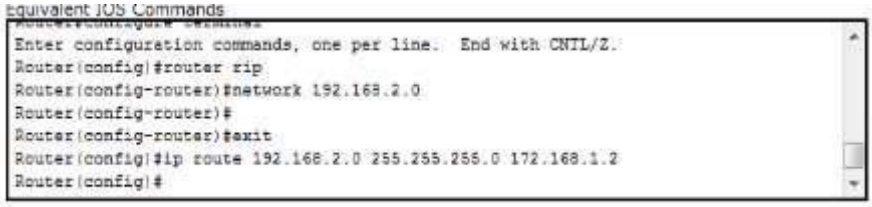


Ternyata tidak bisa, harus mengkonfigurasi kedua *router* dulu supaya saling terhubung.

d. Konfigurasi kedua router supaya saling terhubung

Router0

```
Router0>Enable
Router0#Conf ter
Router0(config)#Router rip
Router0(config-router)#Network 192.168.2.0
Router0(config-router)#Exit
Router0(config)#Ip route 192.168.2.0.255.255.255.0  172.168.1.2
```



Router1

Router1>Enable

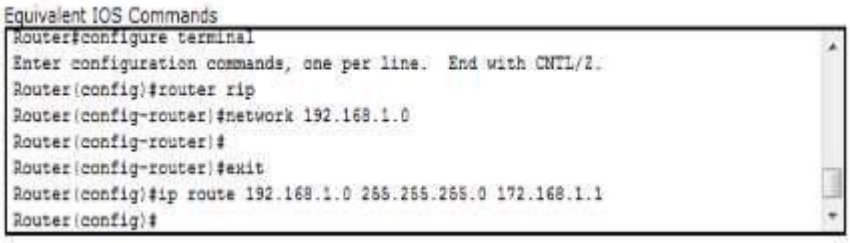
Router1#Conf ter

Router(config)#Router rip

Router(config-router)#Network 192.168.1.0

Router(config-router)#Exit

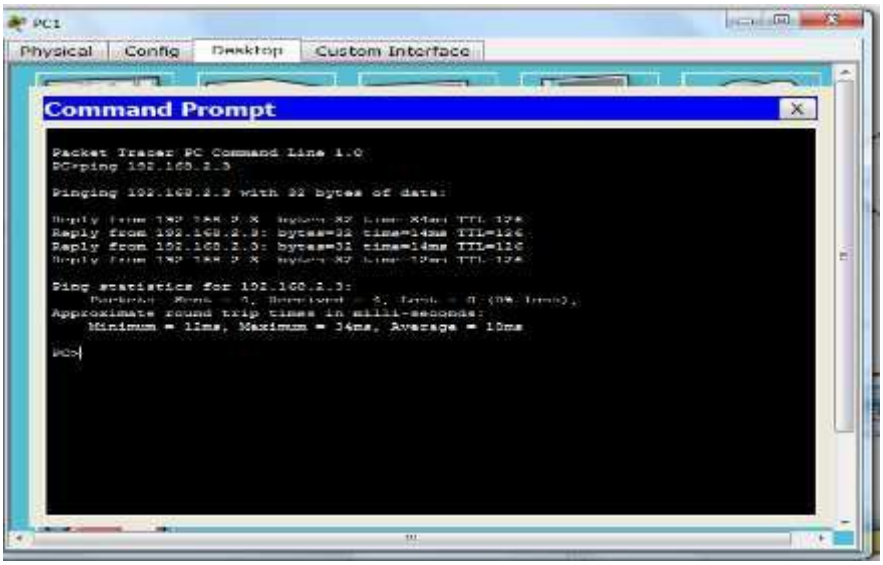
Router(config)#Ip route 192.168.1.0 255.255.255.0 172.168.1.1



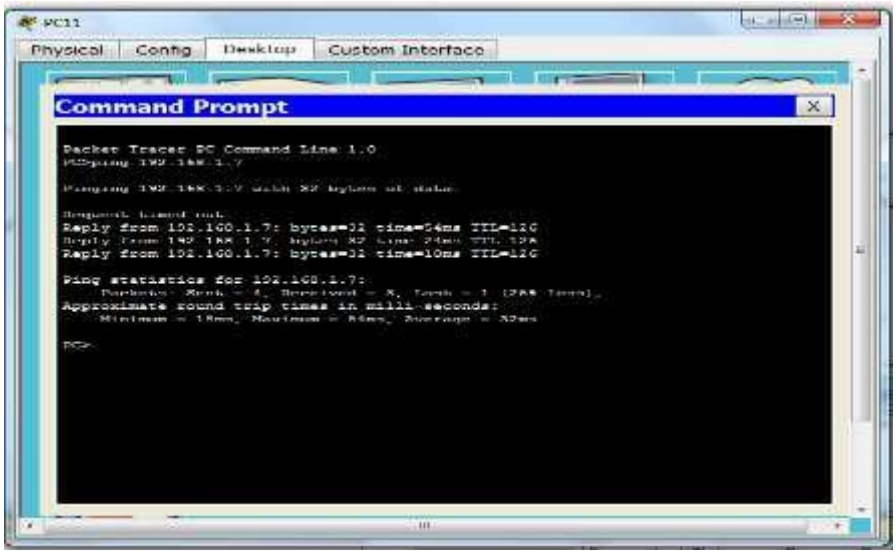
Setelah kedua router dikonfigurasi, coba tes koneksi kedua *router* melalui PC

e. Koneksikan kedua *router* atau LAN Walikota dengan LAN Balaikota

Ping PC1 ke Server2



Ping PC11 ke PC5



Jadi menghubungkan kedua *router* atau LAN sudah berhasil.

4.2.2 Konfigurasi *username* dan *password* pada *switch*

Tujuannya adalah tidak sembarangan *user* bisa merubah konfigurasi yang telah dibuat.

Switch0>Enable

Switch0#Conf ter

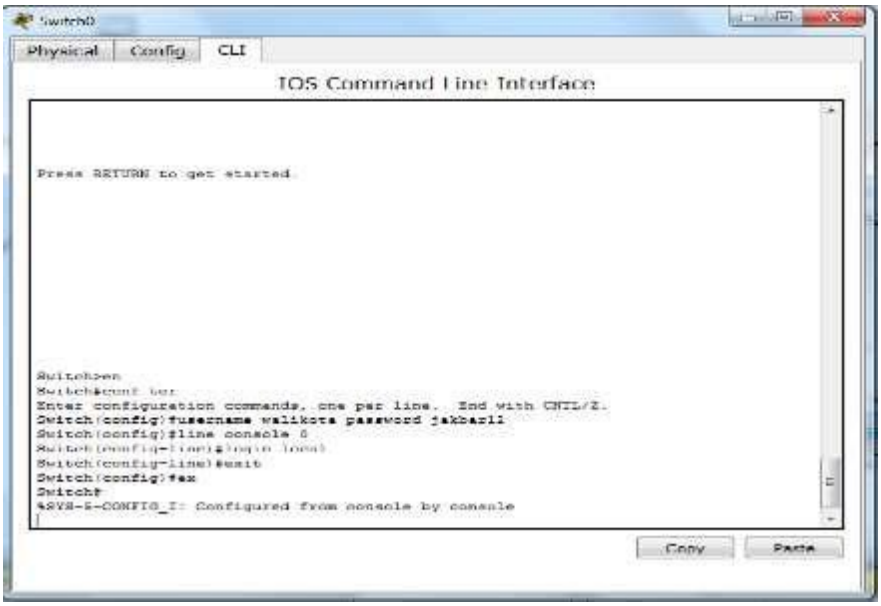
Switch0(config)#username walikota password jakbar12

Switch0(config)#line console 0

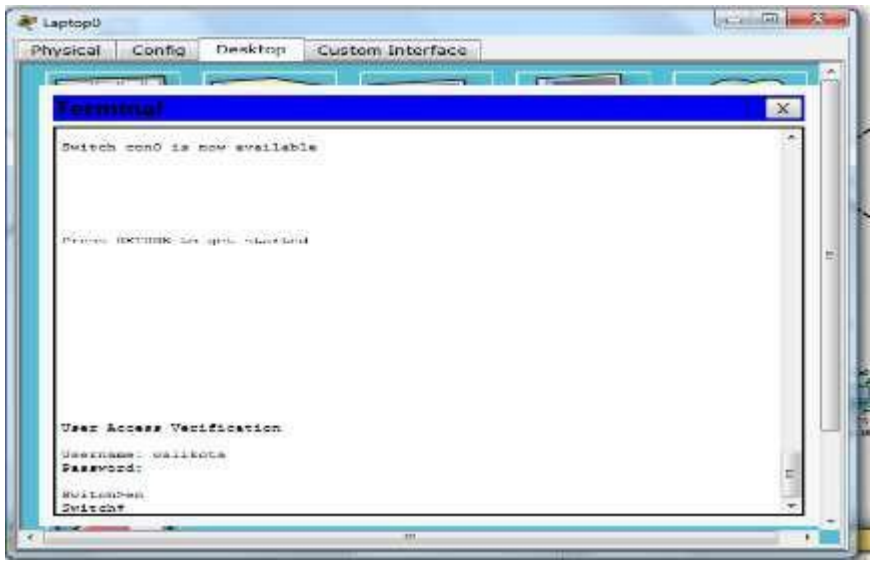
Switch0(config-line)#Login local

Switch0(config-line)#Exit

Switch0(config)#Exit



Kemudian cek pada laptop0



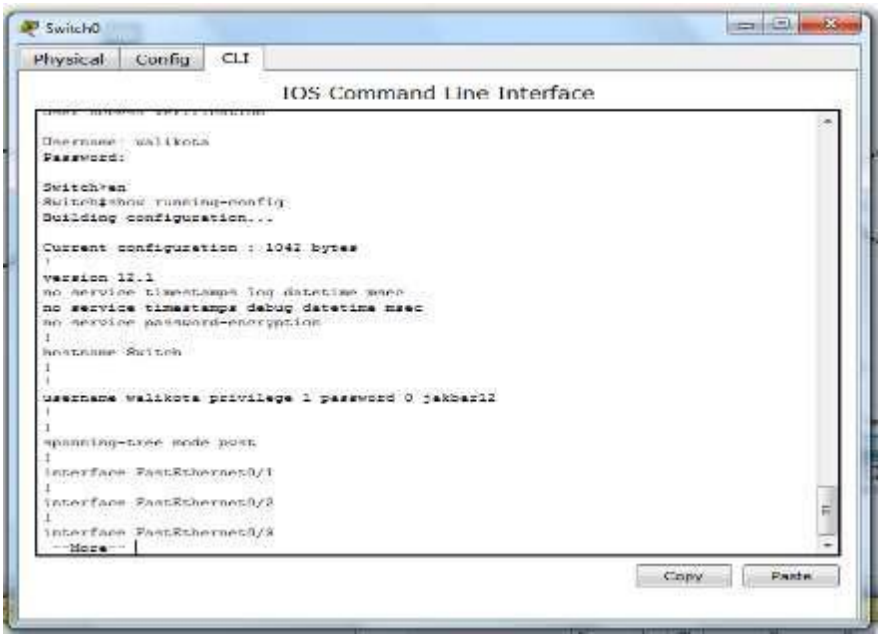
Telah berhasil membuat *username* dan *password*

4.2.3 Enkripsi *Password*

Tujuannya adalah supaya *password* yang telah dibuat tidah terlihat dan tentunya ini lebih memberikan keamanan ada *switch*.

Switch0>enable

Switch0#show running-config

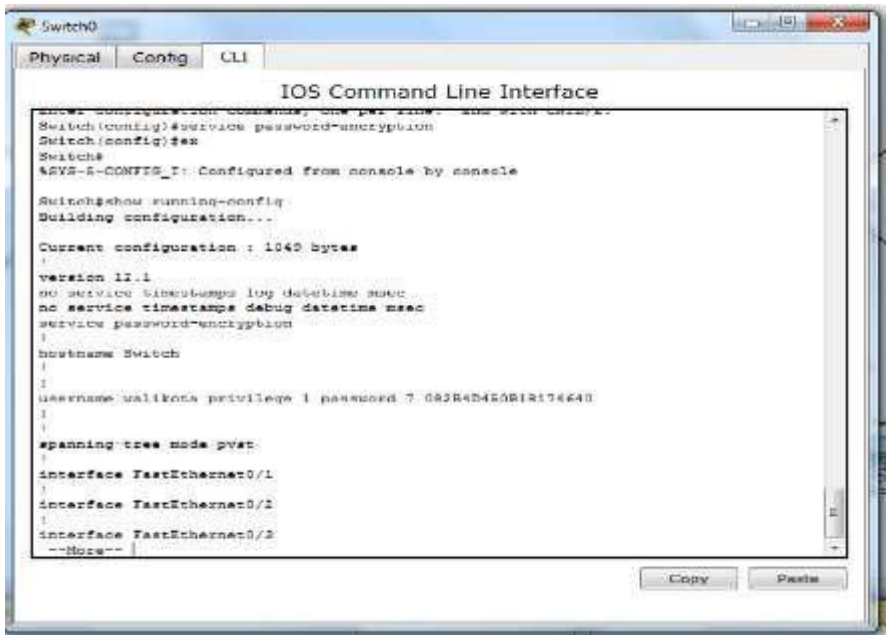


Password masih kelihatan, sekarang lakukan enkripsi

Switch0>enable

Switch0#conf ter

Switch0(config)#service password-encryption



Password berhasil di enkripsi, sekarang *password* tidak kelihatan.

4.2.4 Remot Jaringan dengan Telnet

Tujuan nya untuk memermudah staf dalam mengontrol jaringan.

Switch0>enable

Switch0#conf ter

Switch0(config)#line vty 0 1

Switch0(config-line)#transport input telnet

Switch0(config-line)#password walikota

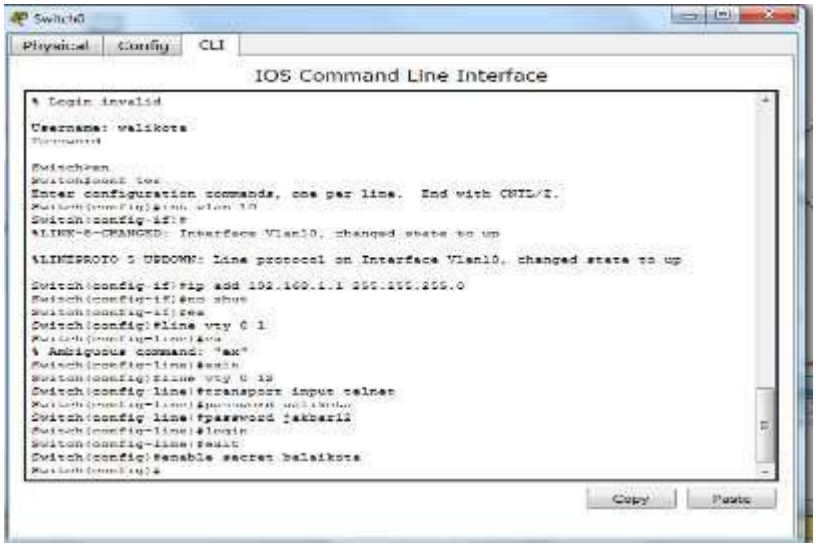
Switch0(config-line)#password jakbar12

Switch0(config-line)#login

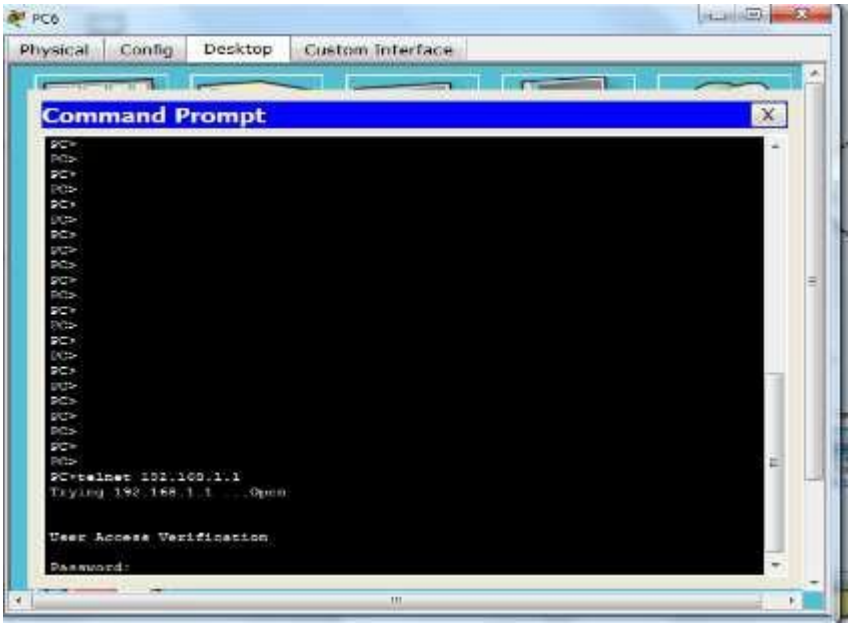
Switch0(config-line)#exit

Switch0(config)#enable secret balaikota

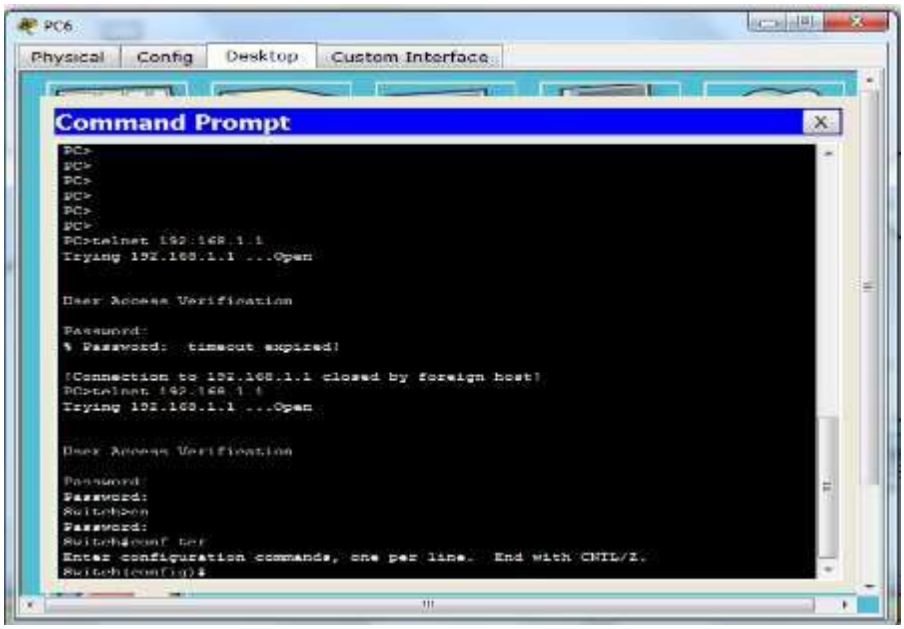
Switch0(config)#exit



Setelah di konfigurasi pada *switch*, cek pada PC 6



Berhasil, selanjutnya masukan password yang telah di konfigurasi pada *switch*.



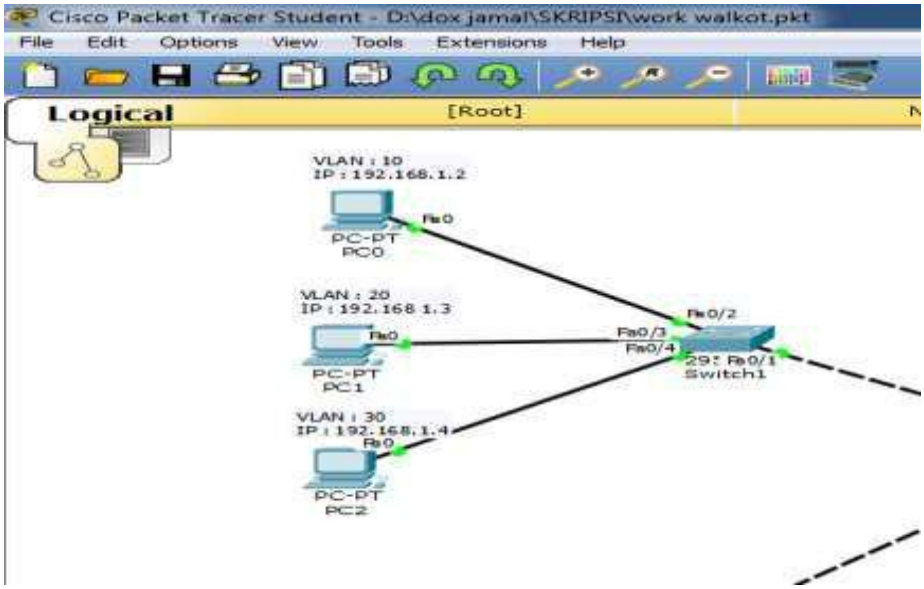
Sukses

4.2.5 Konfigurasi VLAN pada Walikota Jakbar

Tujuannya dibuta VLAN adalah untuk membuat segmentasi tiap divisi, mengindari tabrakan data, menghemat bandwidth dan lebih banyak lagi.

Semua PC di Walikota telah dibari IP selanjut nya lakukan konfigirasi di *switch*.

Switch1



Switch1>enable

Switch1#conf ter

Switch1(config)#int fa0/2

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 10

Switch1(config-if)#exit

Switch1(config)#int fa0/3

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 20

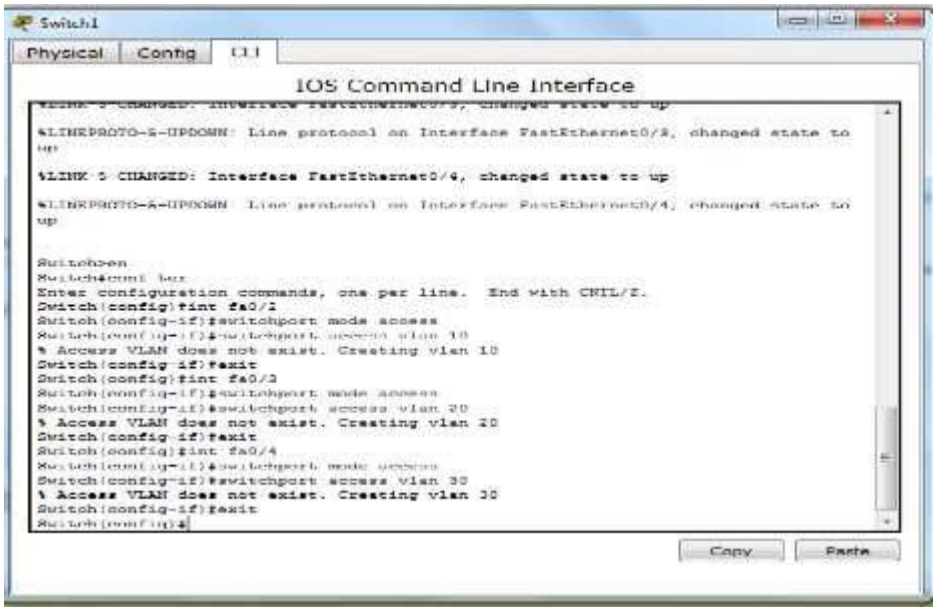
Switch1(config-if)#exit

Switch1(config)#int fa0/4

Switch1(config-if)#switchport mode access vlan

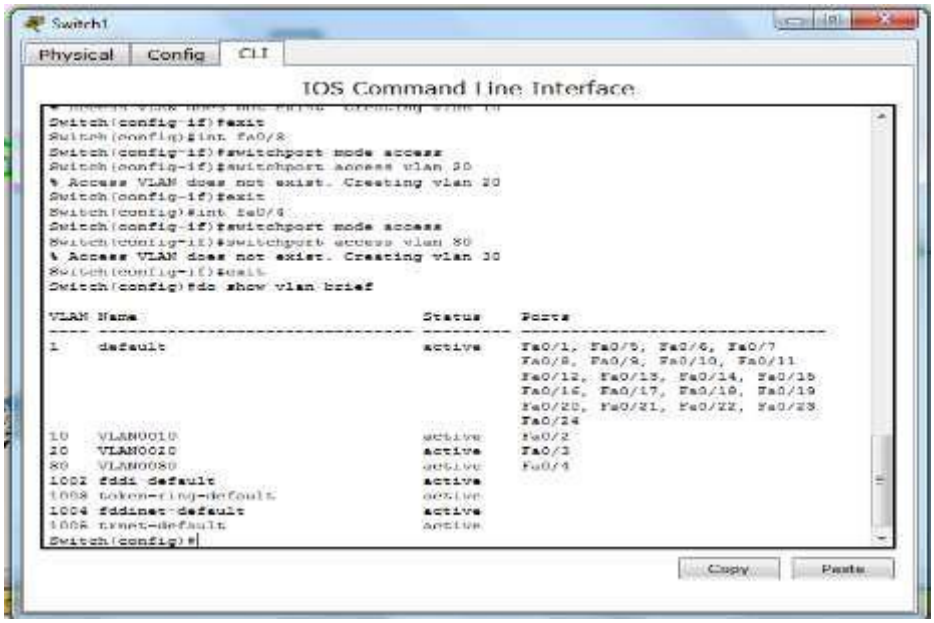
Switch1(config-if)#switchport access vlan 30

Switch1(config-if)#exit

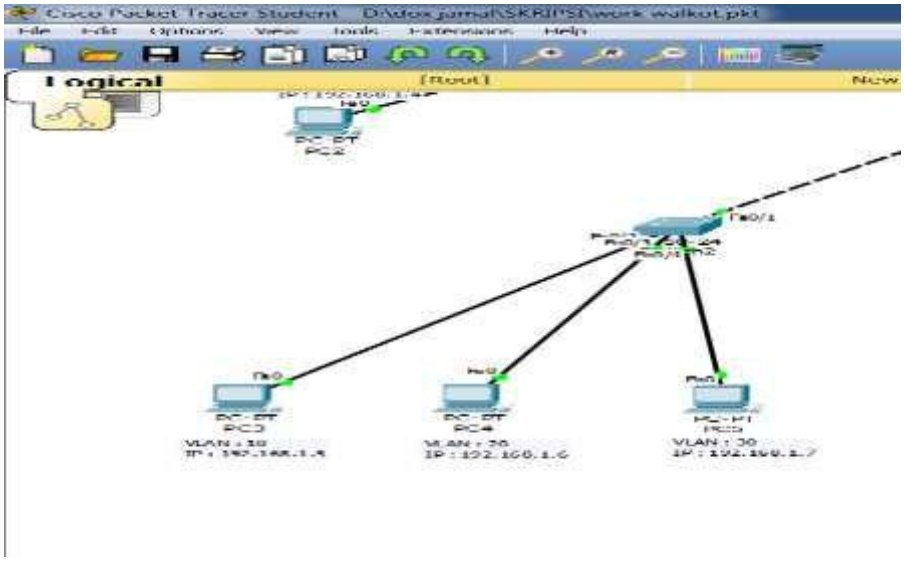


Untuk melihat VLAN

Switch1(config)#do show vlan brief



Switch2



Switch2>enable

Switch2#conf ter

Switch(config)#int fa0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

Switch(config)#int fa0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

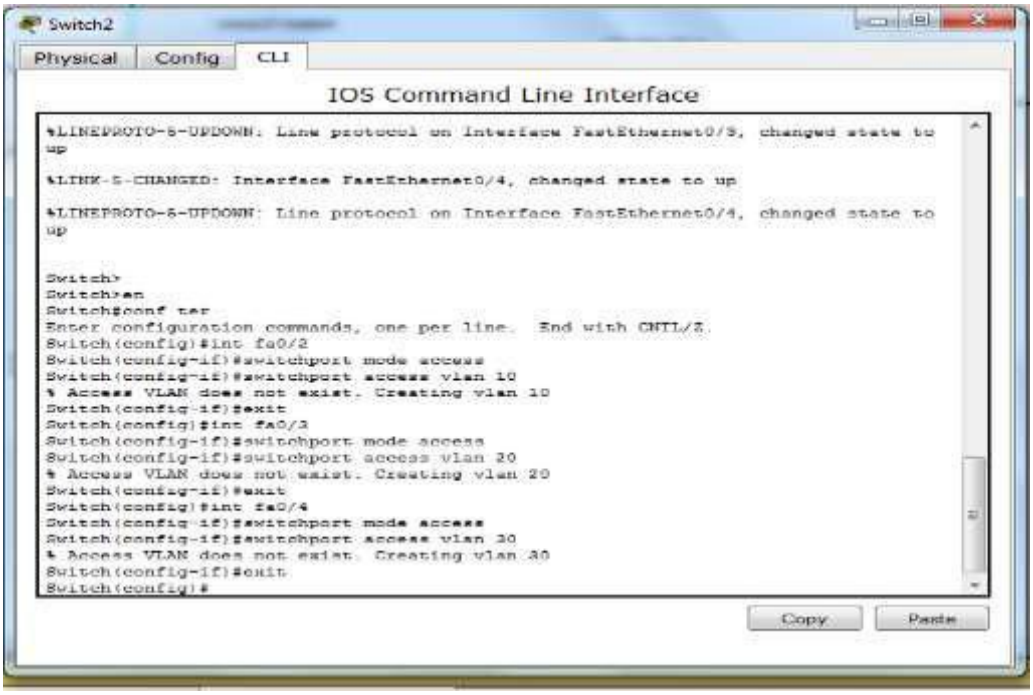
Switch(config)#exit

Switch(config)#int fa0/4

Switch(config-if)#switchport mode access

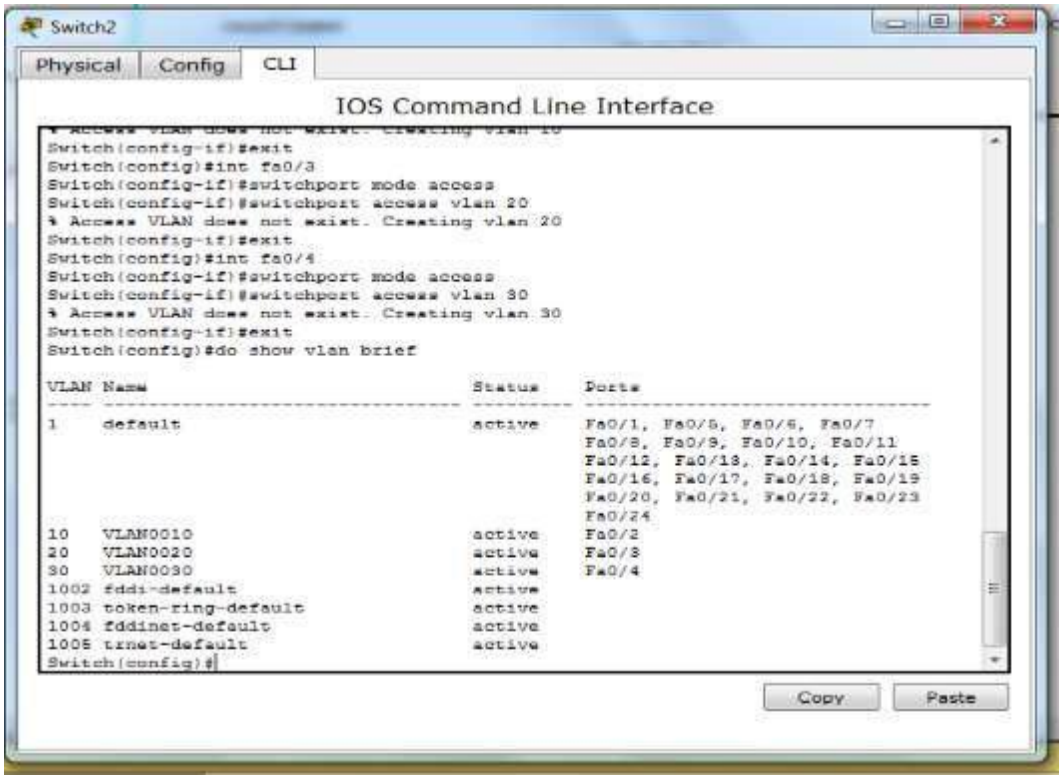
Switch(config-if)#switchport access vlan 30

Switch(config-if)#exit

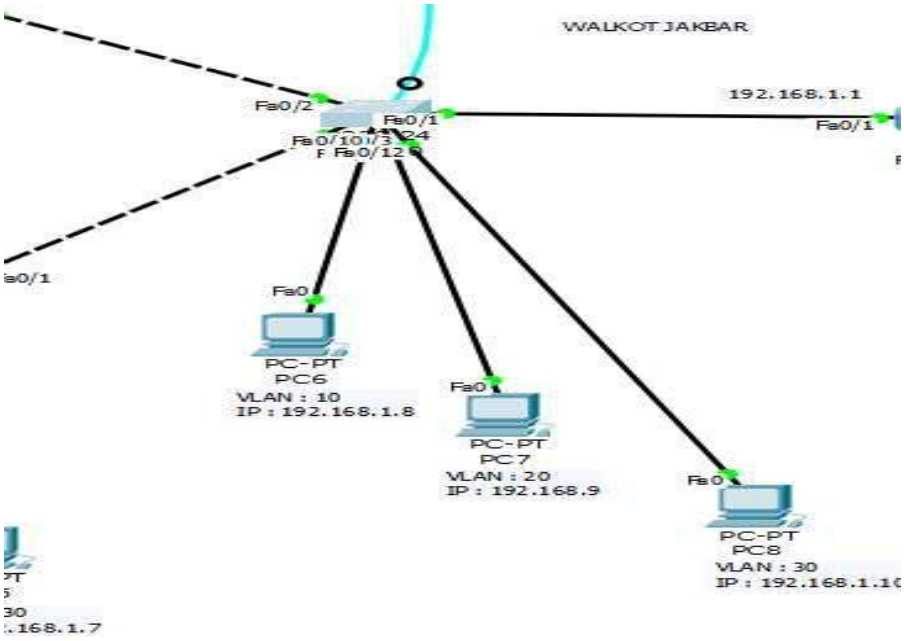


Untuk melihat VLAN

Switch2(config)#do show vlan brief



Switch0



Switch0>enable

Switch0#conf ter

Switch0(config)#int fa0/10

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 10

Switch0(config-if)#exit

Switch0(config)#int fa0/11

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 20

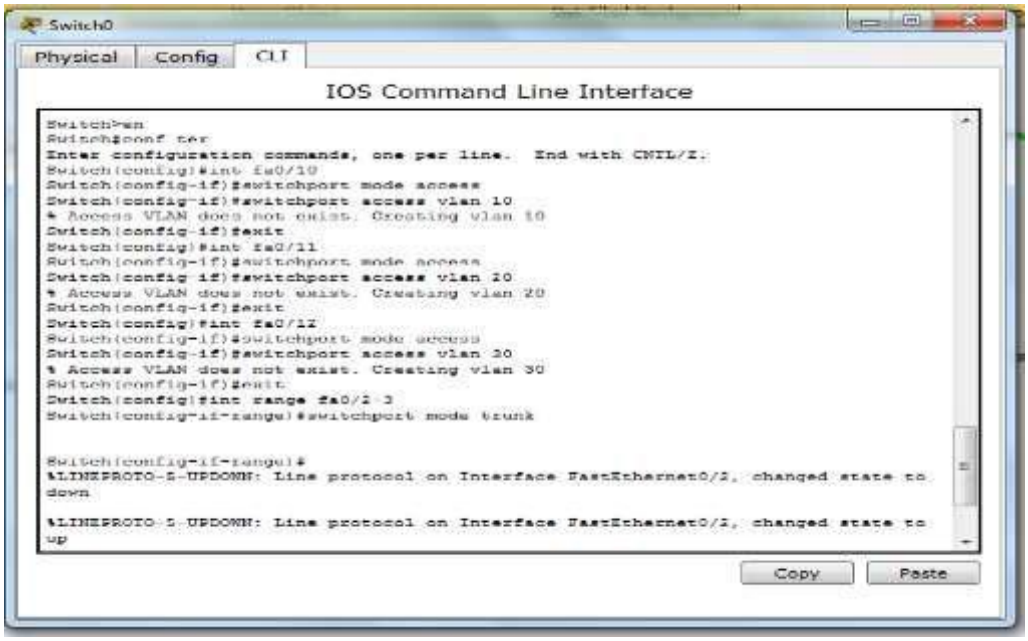
Switch0(config-if)#exit

Switch0(config)#int fa0/12

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 30

Switch0(config-if)#exit



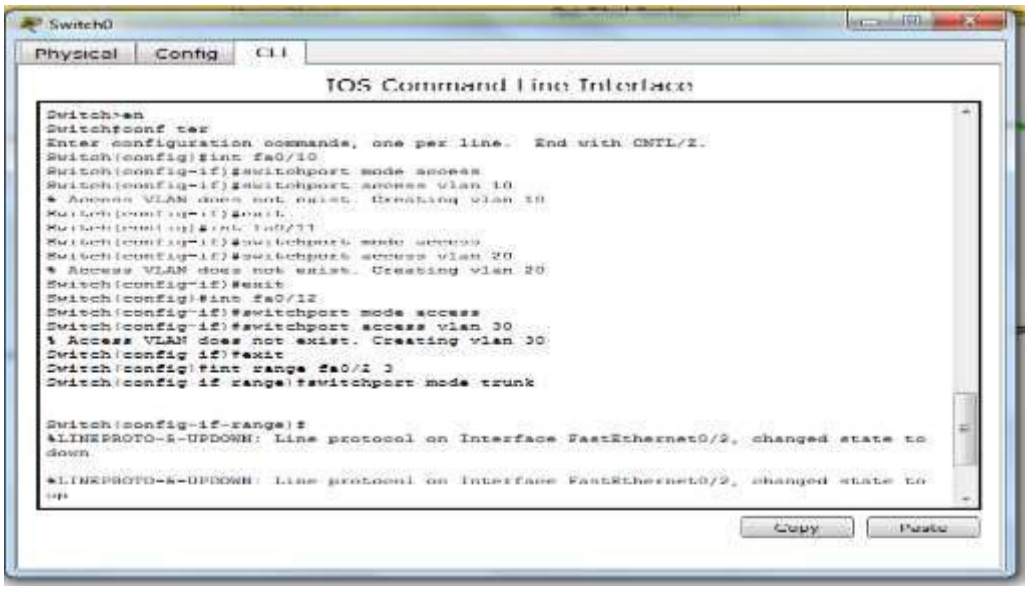
Switch0, switch trunk

Switch0>enable

Switch0#conf ter

Switch0(config)#int range fa0/2-3

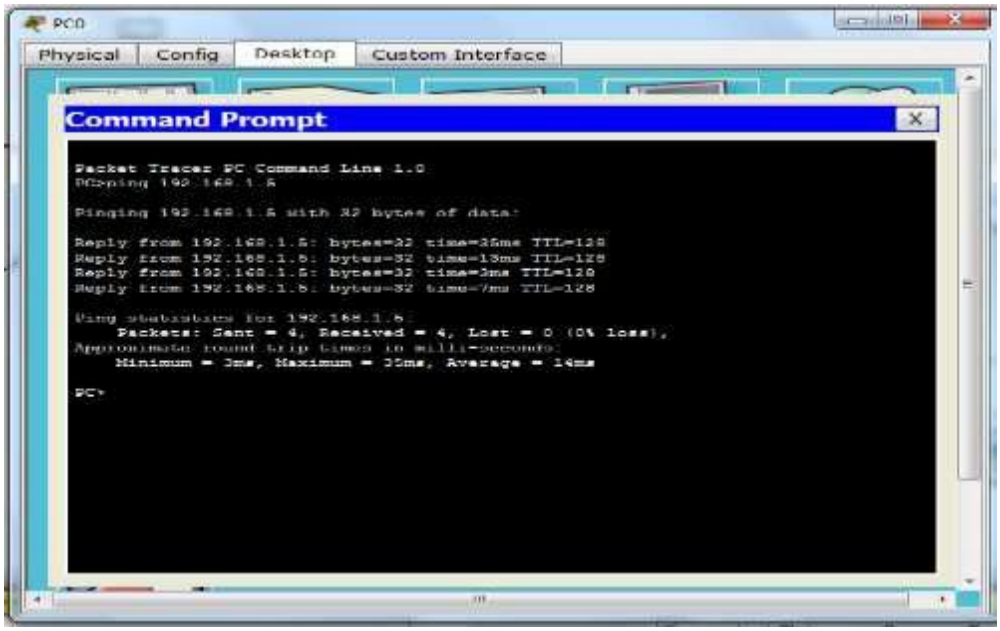
Switch0(config-if-range)#switchport mode trunk



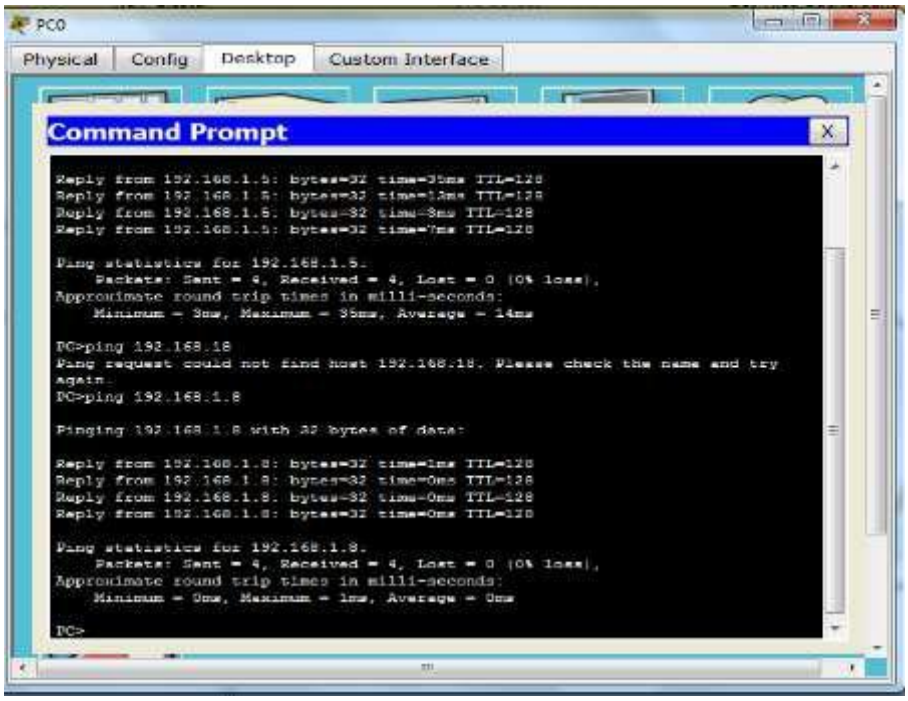
Selanjutnya tek koneksi mulai dari vlan 10 sampai vlan 30

Vlan 10

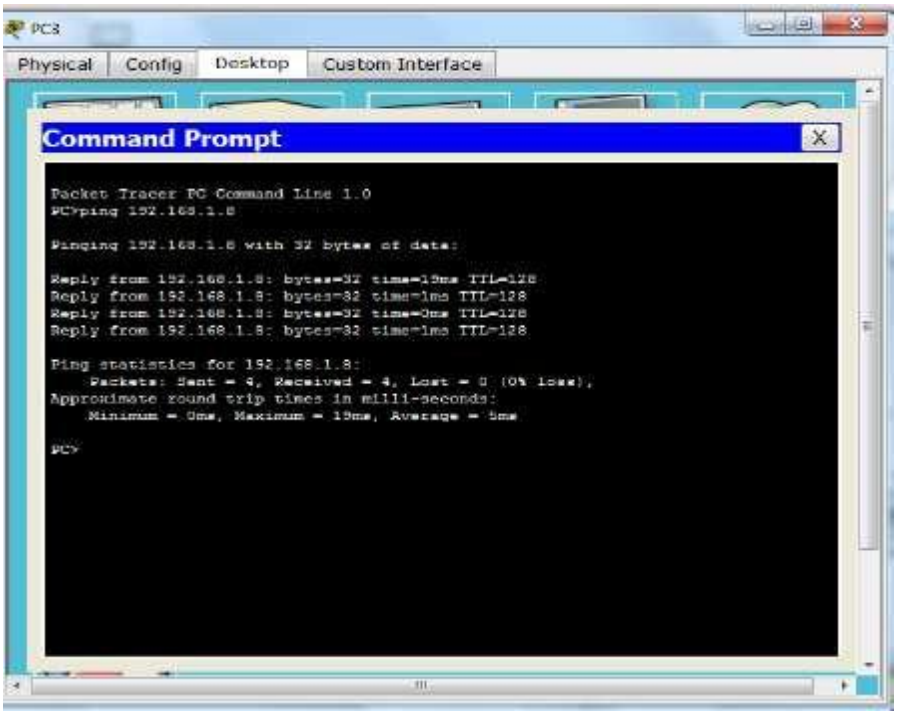
Ping PC0 ke PC3 sama-sama vlan 10



Ping PC0 ke PC6 sama-sama vlan 10

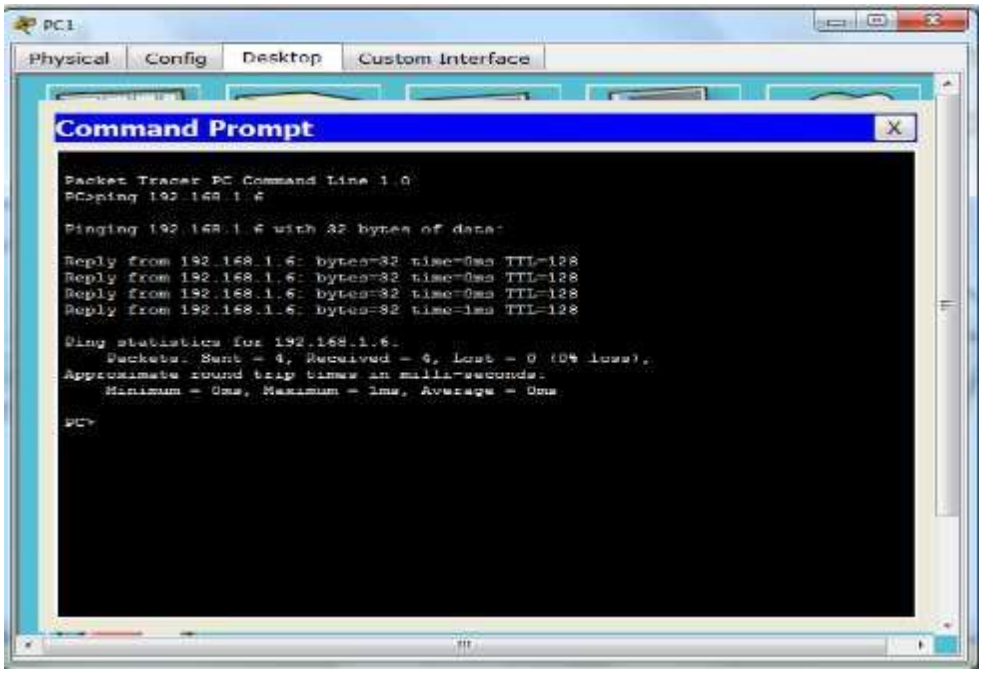


Ping PC3 ke PC6 sama-sama vlan 10

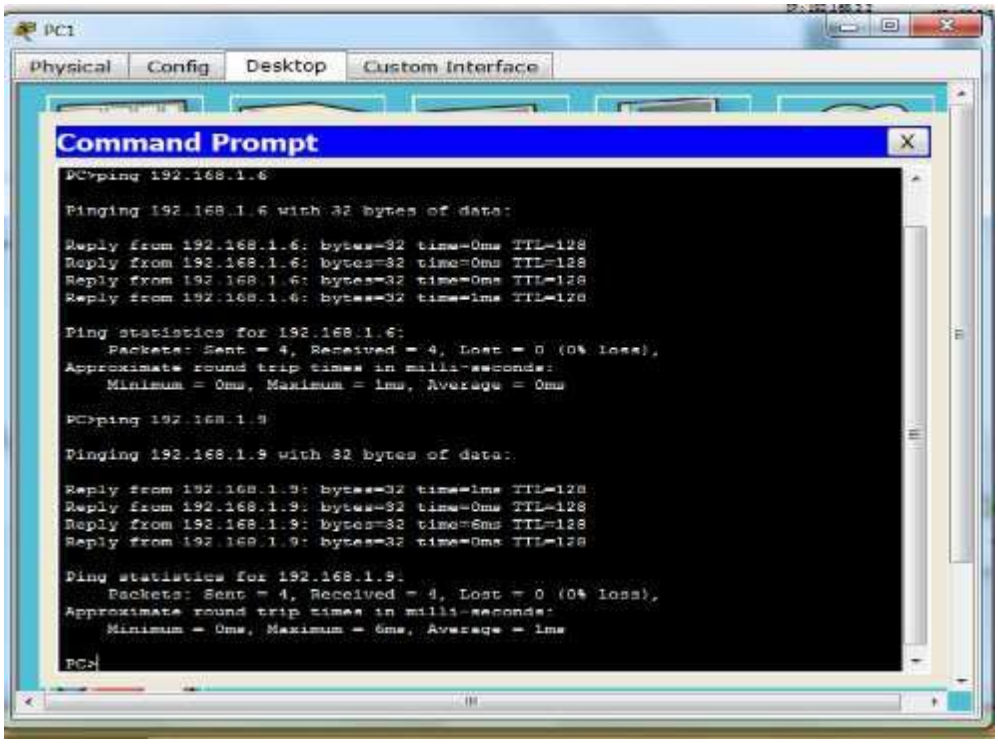


Vlan 20

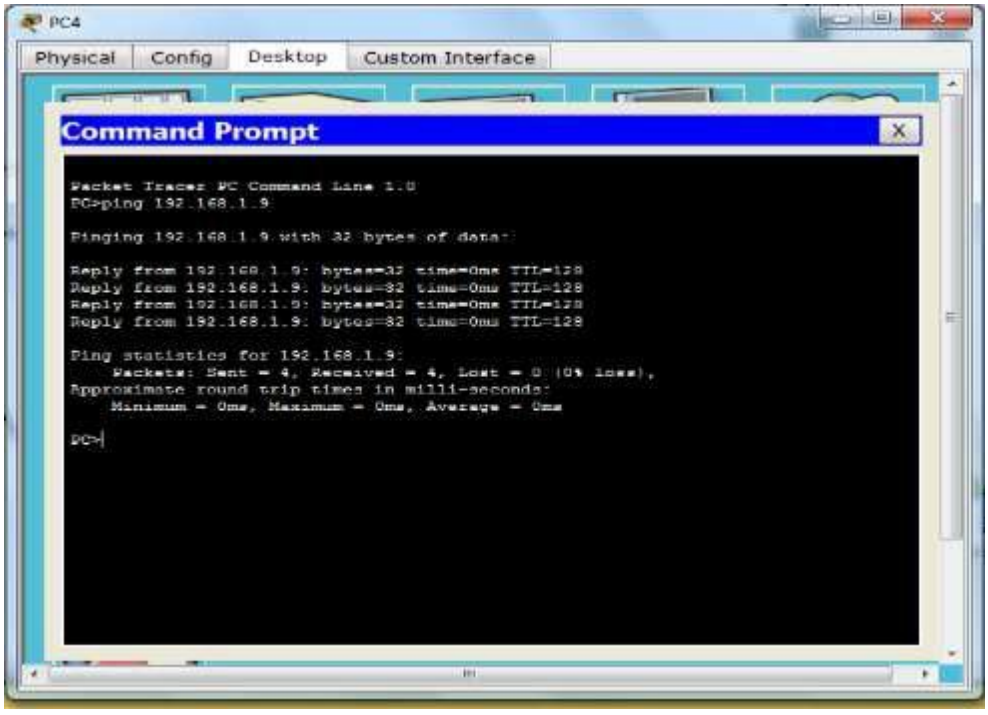
Ping PC1 ke PC4 sama-sama vlan 20



Ping PC1 ke PC7 sama-sama vlan 20

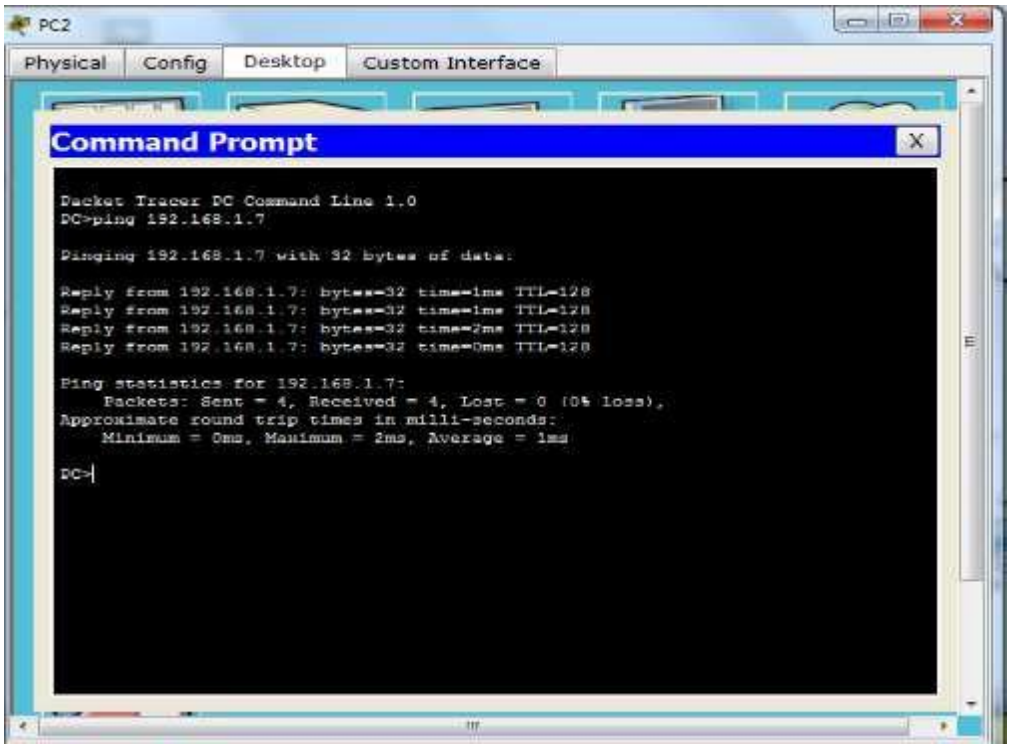


Ping PC4 ke PC7 sama-sama vlan 20

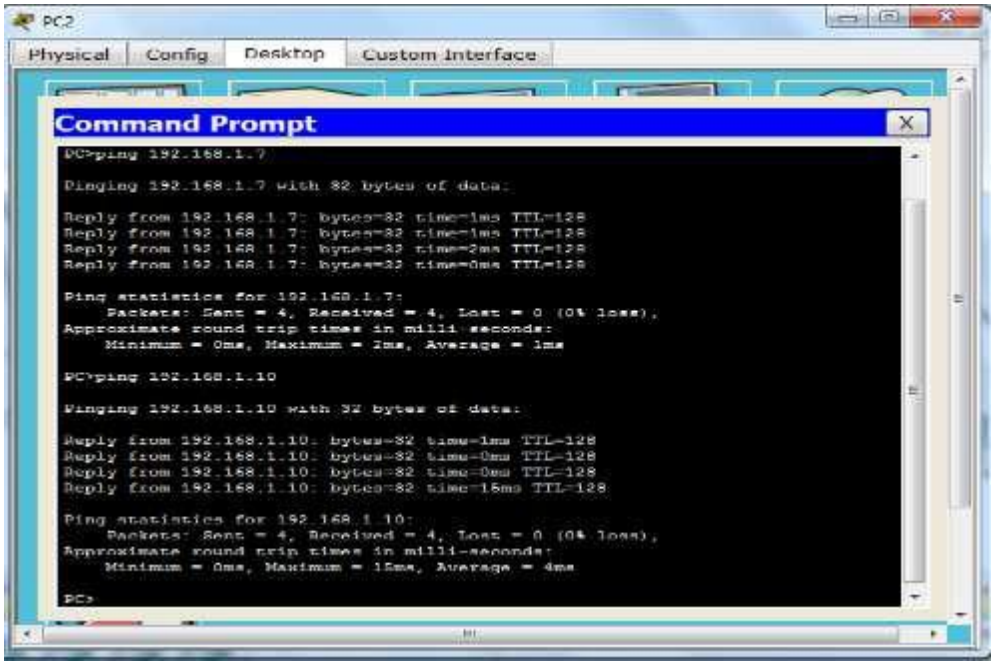


Vlan 30

Ping PC2 ke PC5 sama-sama vlan 30

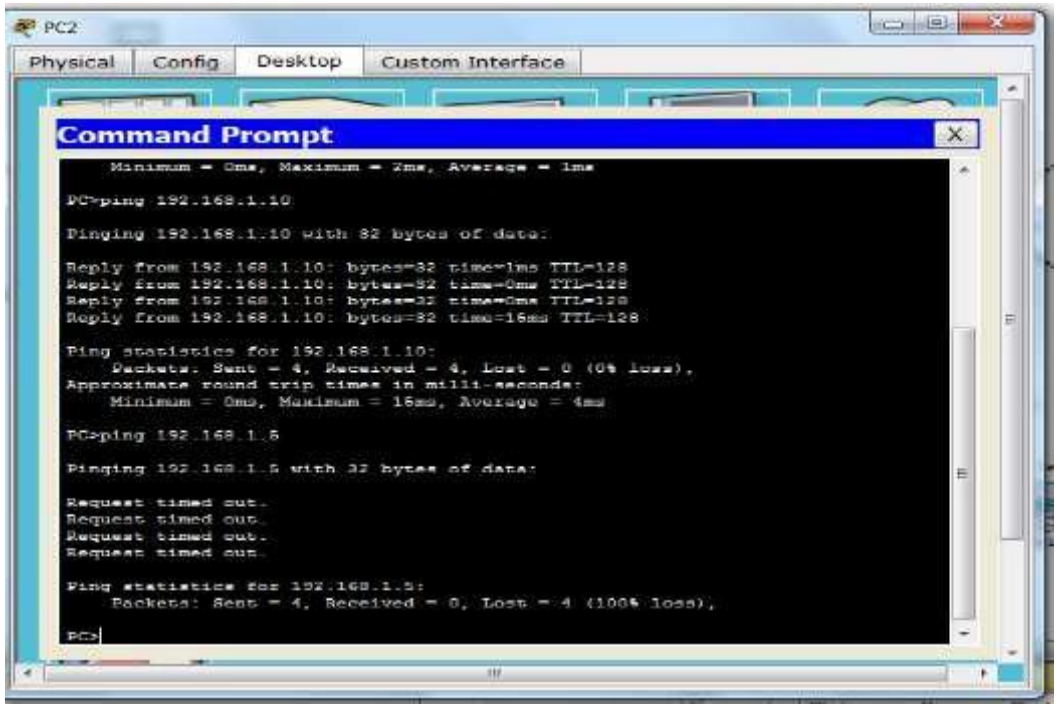


Ping PC5 ke PC8 sama-sama vlan30

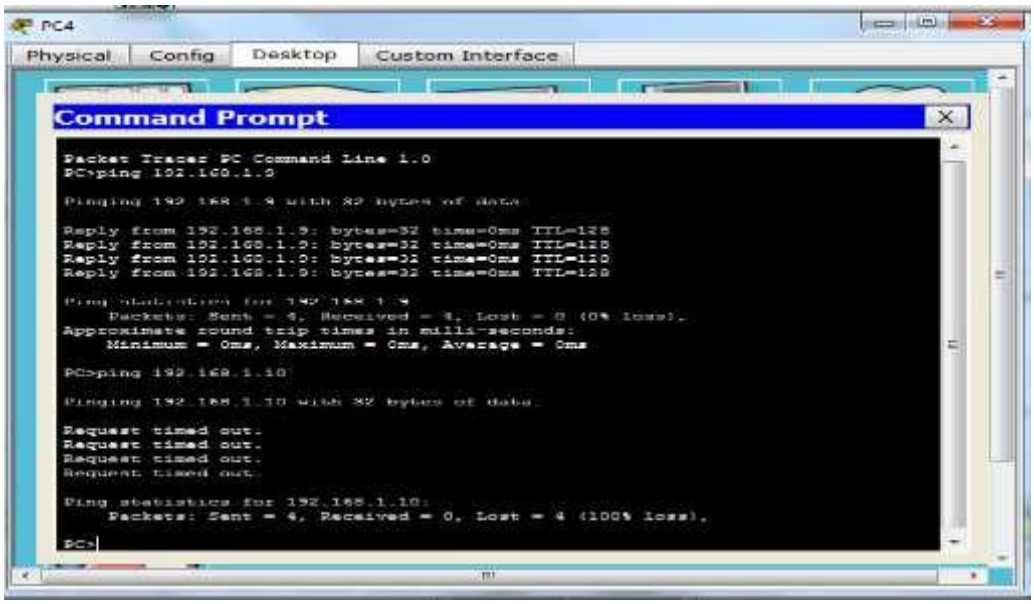


Selanjutnya coba ping antar vlan yang berbeda

Ping PC2 vlan 30 ke PC3 vlan 10 antar vlan yang berbeda



Ping PC4 vlan 20 ke PC8 vlan 30 antar vlan yang berbeda



BAB V

PENUTUP

5.1 Simpulan

1. Peneraan VLAN dalam jaringan SUDIN Walikota Jakarta Barat mempermudah karyawan tiap divisi saling berinteraksi dalam pertukaran data, selain itu memermudah staf IT dalam mengontrol jaringan.
2. Penerapan *password* pada *switch* tak kalah penting, supaya keamanan yang telah di konfigurasi di *switch* menjadi aman, dan tidak semua *user* bisa merubah konfigurasi yang telah dibuat.
3. Dan penerapan keamanan seprti remot jaringan menggunakan telnet dan lain lain tergantung kebutuahan yang ada pada SUDIN Walikota Jakarta Barat.

5.2 Saran

1. Staf IT Suku dinas Komunikasi dan Informatika Walikota Jakarta Barat disaran kan untuk melakukan *maintenance*(perawatan) secara berkala, seperti pengaturan *port* yang telah di tentukan pada *switch*,supaya kemanan jaringan lebih terkontrol.
2. Dan dilakuakn juga pembaharuan *hardware* khusus nya *switch* supaya dengan teknologi terbaru supaya lebih memudahkan mengontrol *port* dan optimal dalam menjaga perofma keamanan jaringan.

DAFTAR PUSTAKA

Dewanto, Y., & Andiani. (2015). Konfigurasi VLAN pada Cisco Switch di Gedung Indosat dengan Menggunakan Program Simulasi. *Ticom*, *3*(3), 1–5.

Hidayatulloh, S. (2014). Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol Ipsec. *Informatika*, *I*(2), 93–104.

Irwan Agus Sobari. (2015). Rancangan Wireless Intrusion Detection System Menggunakan Snort, *XII*(1), 1–9.

Natali, J., Fajrillah, & Diansyah, T. M. (2016). Implementasi Static Nat Terhadap Jaringan Vlan Menggunakan Ip Dynamic Host Configuration Protocol (Dhcp). *Jurnal Ilmiah Informatika*, *1*(1), 51–58. Retrieved from http://ejournal.amiki.ac.id/index.php/JIMI/article/view/10/8

Nurmanina, A. (2013). Jurnal (11-07-13-09-58-07). *Sosiology*.

Prasetyo, T. F., & Hikmawan, A. (201AD). Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA dan MD5. *Infotech*, *60*(18), 41–46. Retrieved from https://anzdoc.com/analisa-dan-implementasi-sistem-keamanan-data-dengan-menggun.html

Primartha, R. (2013). Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES). *Journal of Research in Computer Science and Applications*, *2*(1), 13–18. https://doi.org/2301-8488

Sakti, B., Aziz, A., & Doewes, A. (2013). Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing. *Jurnal Itsmart*, *2*(1).

Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. *Jaringan Komputer*, *1*(1), 9–14.

T.Putra Ning, A. S. B. (2016). Implementasi Virtual LAN pada Gedung MPC Jakarta PT . Pos Indonesia (Persero), 56–61.

Zuhri, M., & Sobari, I. A. (2017). Optimalisasi Jaringan Wide Area Network Dengan Teknik Multiprotocol Label Switching. *Prosiding SIMNASIPTEK*, 190–194.

LEMBAR KONSULTASI BIMBINGAN SKRIPSI

STMIK NUSA MANDIRI JAKARTA

NIM : 12140391
Nama Lengkap : Syaiful Jamal
Dosen Pembimbing I : Irwan Agus Sobari, M.Kom
Judul Skripsi : Analisa Sistem Keamanan Jaringan dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat

No	Tanggal Bimbingan	Pokok Bahasan	Paraf Dosen Pembimbing
1.	5 April 2018	Bimbingan Predana	
2.	26 April 2018	Pengajuan Judul	
3.	23 Mei 2018	Pengajuan Bab 1	
4.	28 Juni 2018	Perbaikan Bab 1 dan Pengajuan Bab 2	
5.	4 Juli 2018	Perbaikan Bab 2 dan Pengajuan Bab 3	
6.	19 Juli 2018	Perbaikan Bab 3 dan Pengajuan Bab 4	
7.	2 Agustus 2018	Perbaikan Bab 4 dan Simulasi Jaringan	
8.	6 Agustus 2018	Perbaikan Bab 4 dan Pengajuan Bab 5	

Catatan untuk Dosen Pembimbing.
Bimbingan Skripsi

- Dimulai pada tanggal : 5 April 2018
- Diakhiri pada tanggal : 6 Agustus 2018
- Jumlah pertemuan bimbingan :8 kali

Disetujui oleh,
Dosen Pembimbing I

(Irwan Agus Sobari, M.Kom)

	LEMBAR KONSULTASI BIMBINGAN SKRIPSI
STMIK NUSA MANDIRI	STMIK NUSA MANDIRI JAKARTA

NIM : 12140391
Nama Lengkap : Syaiful Jamal
Dosen Pembimbing I : Bambang Wijonarko, M.Kom
Judul Skripsi : Analisa Sistem Keamanan Jaringan dengan Menggunakan *Switch Port Security* Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat

No	Tanggal Bimbingan	Pokok Bahasan	Paraf Dosen Pembimbing
1.	5 April 2018	Bimbingan Predana	
2.	26 April 2018	Pengajuan Judul	
3.	23 Mei 2018	Pengajuan Bab 1	
4.	28 Juni 2018	Perbaikan Bab 1 dan Pengajuan Bab 2	
5.	4 Juli 2018	Perbaikan Bab 2 dan Pengajuan Bab 3	
6.	19 Juli 2018	Perbaikan Bab 3 dan Pengajuan Bab 4	
7.	2 Agustus 2018	Perbaikan Bab 4 dan Simulasi Jaringan	
8.	6 Agustus 2018	Perbaikan Bab 4 dan Pengajuan Bab 5	

Catatan untuk Dosen Pembimbing.
Bimbingan Skripsi

- Dimulai pada tanggal : 5 April 2018
- Diakhiri pada tanggal : 6 Agustus 2018
- Jumlah pertemuan bimbingan :8 kali

Disetujui oleh,
Dosen Pembimbing II

(Bambang Wijonarko, M.Kom)

PEMERINTAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA
DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK
SUKU DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK
KOTA ADMINISTRASI JAKARTA BARAT
Jalan Raya Kembangan No. 2 Blok A Lantai 9 Telepon 021-5821756
Faximile 021-5825106 Email : komunfotikjb@jakarta.go.id
JAKARTA
Kode Pos 11610

SURAT KETERANGAN
Nomor 827 / -074

Menindaklanjuti surat dari STMIK NUSA MANDIRI JAKARTA nomor 25519/PKL/TI-NM/B3/VIII/2018/PKL/S1-NM/B3/I/2018 Tanggal 09 Juli 2018 perihal Permohonan Riset, yang bertanda tangan dibawah ini, Kepala Suku Dinas Komunikasi, Informatika dan Statistik Kota Administrasi Jakarta Barat menerangkan bahwa

Nama	Syaiful Jamal
NIM	12140391
Jurusan	Teknik Informatika

Telah menyelesaikan Riset dengan baik di Suku Dinas Komunikasi Informatika dan Statistik Kota Administrasi Jakarta Barat selama 1 (satu) bulan mulai dari tanggal 02 Juli s/d tanggal 02 Agustus 2018

Demikian surat ini dibuat untuk dapat dipergunakan sebagaimana mestinya

Jakarta, 13 Agustus 2018

Kepala Suku Dinas
Komunikasi Informatika Dan Statistik
Kota Administrasi Jakarta Barat

Drs. Sugiono, MM
NIP. 196606281997031002