

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 Kesimpulan

Hasil analisis jaringan, terdapat dua pengguna dalam jaringan UNIMA yaitu pengguna LAN dan WLAN, masalah pada infrastruktur keamanan di setiap fakultas dan kantor yang terhubung dengan server di Puskom, karena jaringan dari setiap kantor dan fakultas ke Puskom masih bersifat *flat* atau jaringan tradisional dan tidak adanya filtering atau akses kontrol dari setiap kantor dan fakultas yang terhubung dengan server yang terdapat di Puskom. Dari hasil analisis dibuat dua perancangan jaringan dengan yaitu perancangan jangka pendek (pemanfaatan piranti yang sudah ada) dan perancangan jaringan jangka panjang yang merupakan pengembangan dari rancangan jaringan jangka pendek (penambahan piranti jaringan) untuk kebutuhan masa yang akan datang.

Dengan dua perancangan ini, diharapkan nantinya pihak pengelola jaringan UNIMA dalam hal ini Pusat Komputer (Puskom) memiliki sebuah dokumentasi yang lengkap mengenai kondisi dari infrastruktur jaringan yang telah diterapkan di instansi UNIMA. Jika sewaktu-waktu akan ada pengembangan terhadap infrastruktur keamanan jaringan yang telah diimplementasikan, dokumen ini dapat membantu pihak UNIMA melihat kembali keterkaitan seluruh komponen jaringan.

Suatu sistem keamanan jaringan bisa dibuat lebih baik tapi keamanan jaringan tidak ada jaminan apakah suatu sistem jaringan dapat dikatakan *secure* atau *reliable*. Namun, keamanan dapat ditingkatkan dalam skala berkelanjutan dari 0 hingga 1, atau dari kondisi tidak *secure* menjadi *relative secure*.

## 5.2 Saran

Dengan penelitian analisis infrastruktur keamanan jaringan pada di Universitas Negeri Manado ini, ada beberapa saran yang dianjurkan peneliti yang menyangkut dengan keamanan infrastruktur jaringan UNIMA, diantaranya sebagai berikut:

Untuk perancangan jangka pendek penambahan *switch* pada setiap gedung fakultas dan kantor instansi untuk menjangkau *user* yang belum terhubung dengan jaringan LAN UNIMA.

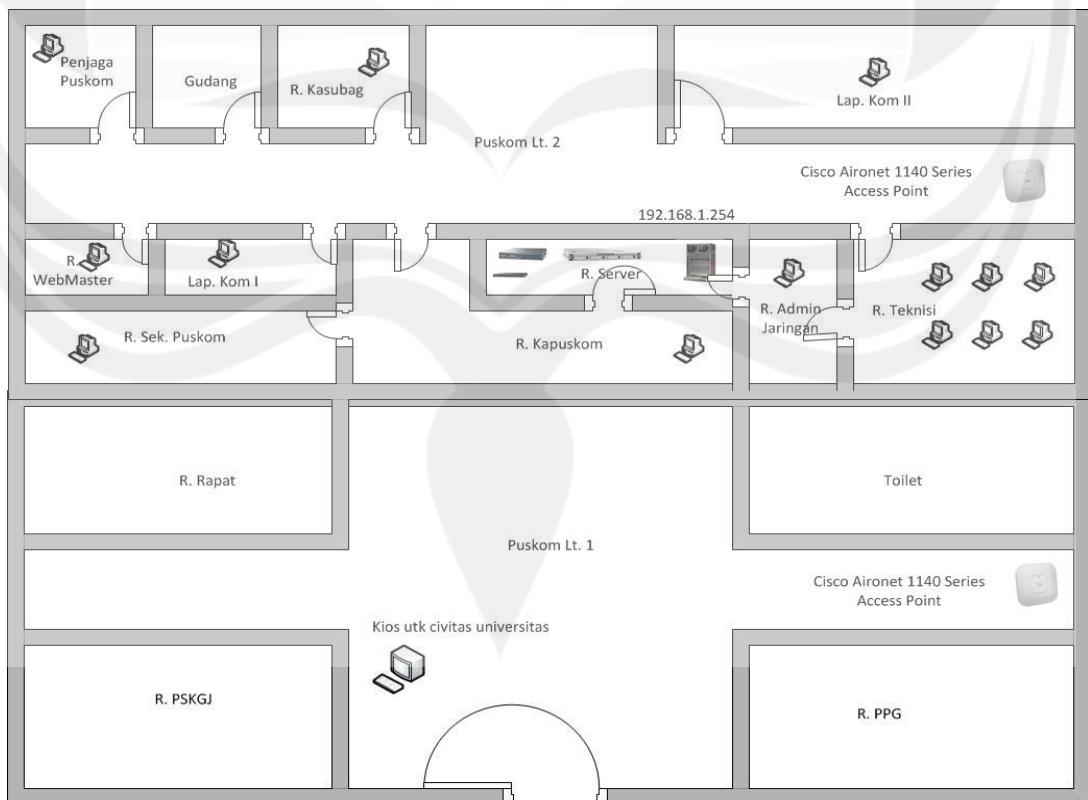
Setelah perancangan jangka panjang diimplementasikan dan akses layanan (*bandwidth*) jaringan UNIMA berjalan stabil, maka yang menjadi saran penulis yaitu mengoptimalkan akses layanan jaringan yang ada, dengan mengalihkan *bandwidth* UNIMA pada malam hari ke setiap rumah dosen dan pegawai UNIMA dengan cara mengimplementasikan teknologi VPN agar *bandwidth* tidak terbuang percuma pada malam hari.

## DAFTAR PUSTAKA

- Aswandi. (2009). Infrastruktur Jaringan Komunikasi Antar Perusahaan Menggunakan Analisa Top-Down Model Untuk Mendukung Data Center. *Jurnal Ilmiah Abdi Ilmu*, 171-181.
- Hizbullah, A. (2012). Optimalisasi Bandwiidht dan Keamanan Jaringan dengan Filterisasi pada Warung Internet menggunakan Mikrotik Routerboard. *Jurnal Komputasi*, 103-116.
- McCabe, J. D. (2007). *Network Analysis, Architecture, and Design*. Amsterdam, Boston, Tokyo, Heidelberg, London, Neew York, Oxford, Sidney: Morgan Kaufmann Publishers is an imprint of Elsevier.
- Nangoi, F. Y. (2011). Perancangan Tata Kelola Teknologi Informasi dengan Framework Cobit pada Infrastruktur dan Keamanan Jaringan di Universitas X. *Master Thesis of Magister Management Technology*, 2-5.
- Rochman, E. F. (2009). Analisa Traffic Jaringan dan Desain Jaringan untuk Optimalisasi Bandwith Internet pada Universitas Kanjuruhan Malang. *Jurnal Matematika dan Komputer Indonesia*, 25-32.
- Sembiring, I., Widiasari, I. R., & Prasetyo, S. D. (2009). Analisa dan Implementasi Sistem Keamanan Jaringan Komputer. *Jurnal Informatika*, 1-15.

- Suyatno, A. (2009). Aplikasi Model Sistem Keamanan Jaringan Berbasis De-Militarised Zone. *Jurnal Informatika Mulawarman*, 6-12.
- Wibowo, A. (2008). Perancangan Sistem Keamanan Komputer Berbasis Jaringan Waktu Nyata. *Jurnal Artificial, ICT Research Center UNAS*, 36-52.

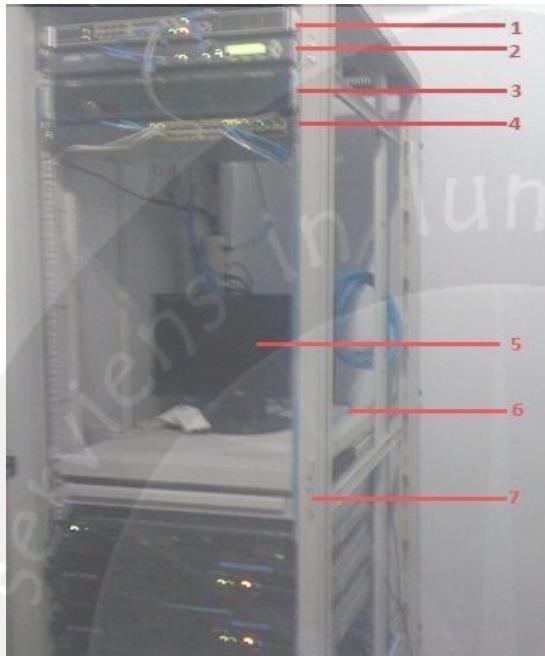




Gambar 1 Denah Jaringan Gedung Pusat Komputer (PUSKOM)



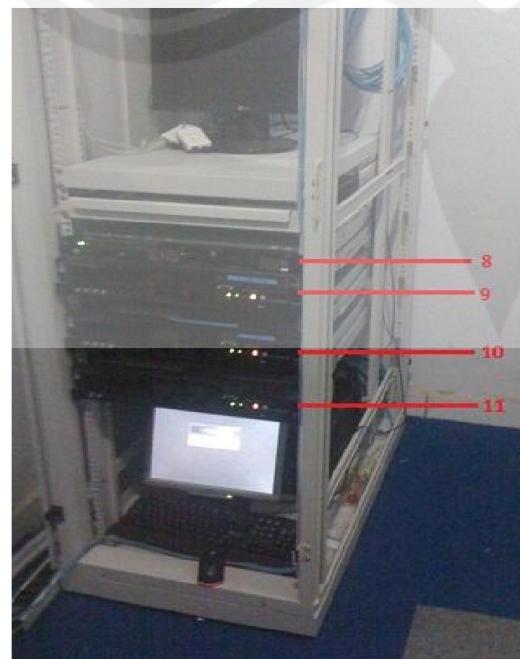
Instalasi perangkat jaringan yang ada di Ruang Server Puskom UNIMA:



Keterangan:

1. Bandwidth Management  
(Allot NetEnforcer)
2. Fortigate Firewalll UTM
3. Cisco Router (Intranet Router ke FIP Tomohon)
4. DMZ Access Catalyst Switch
5. Display Monitor LCD Flat
6. Rak Kit (Shelf)
7. Rak 42U yang sudah dirakit

Gambar 2 Rak 42U yang berisi perangkat Server (Tampak Depan)

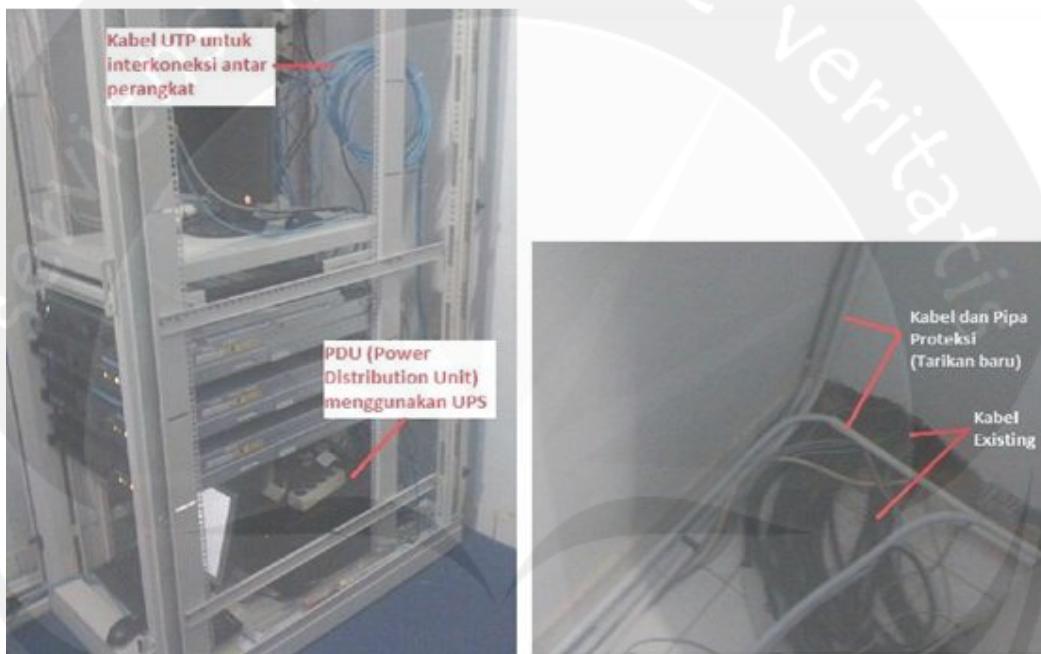


Keterangan:

7. Server NXplorer (Software Manager untuk Appliance Allot NetEnforcer)
8. Server Database SIA (Sistem Informasi Akademik)
10. Server Aplikasi dan Web SIA  
(Sistem Informasi Akademik)

## 11. Server Backup Database dan DHCP, DNS, dan Management

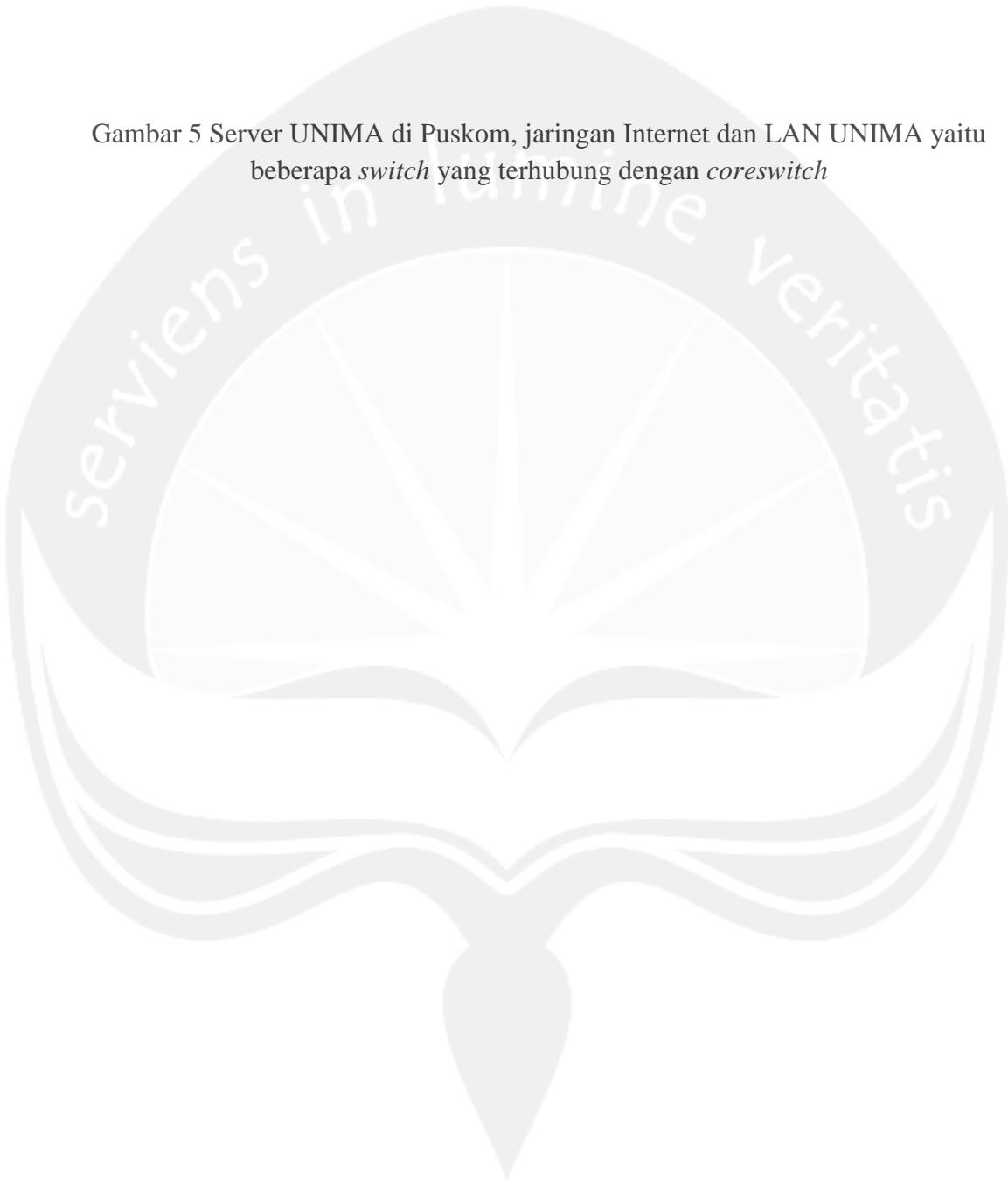
Gambar 3 Rak 42U yang berisi perangkat Server (Tampak Depan)

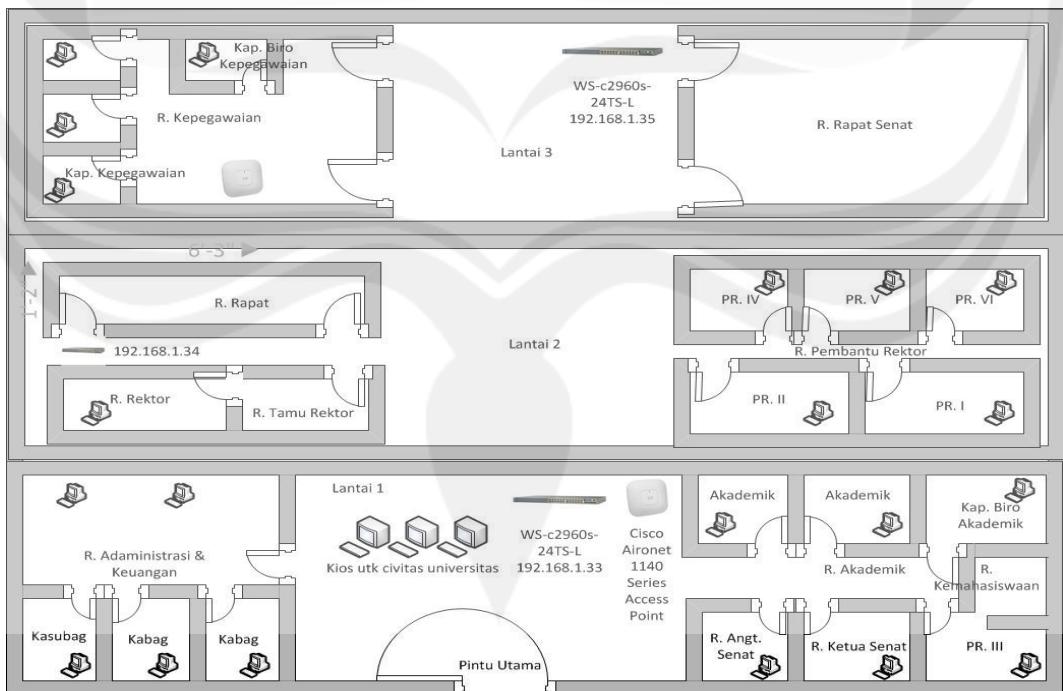


Gambar 4 Rak 42U tampak samping dan Tarikan kabel UTP yang diproteksi pipa



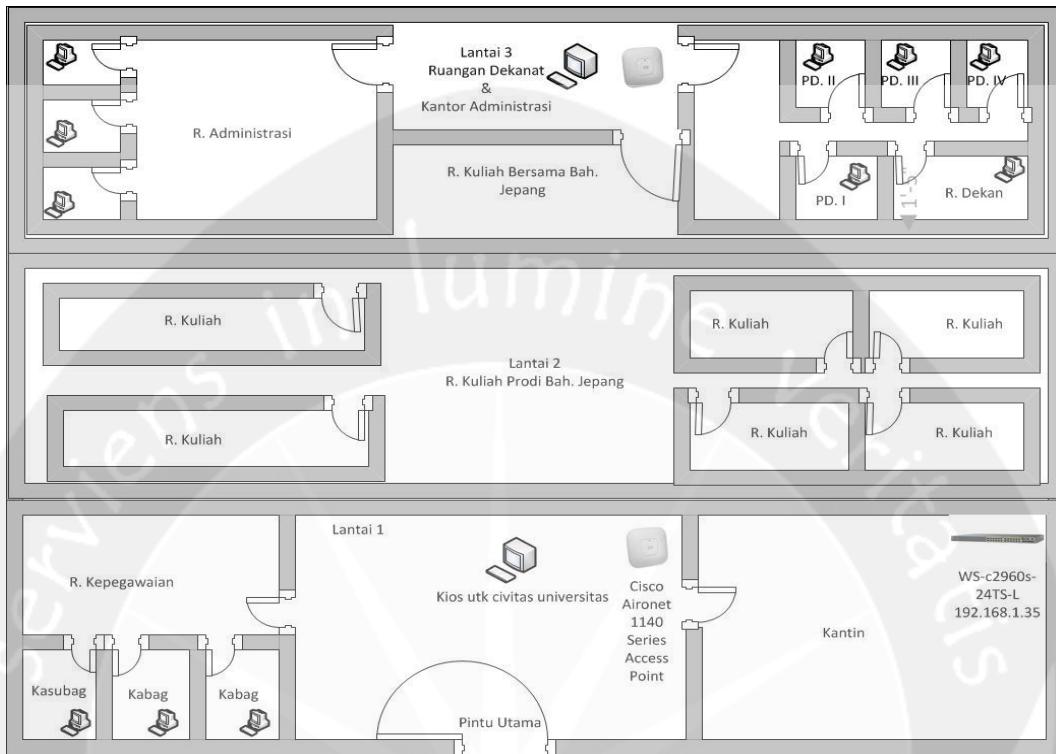
Gambar 5 Server UNIMA di Puskom, jaringan Internet dan LAN UNIMA yaitu beberapa *switch* yang terhubung dengan *coreswitch*





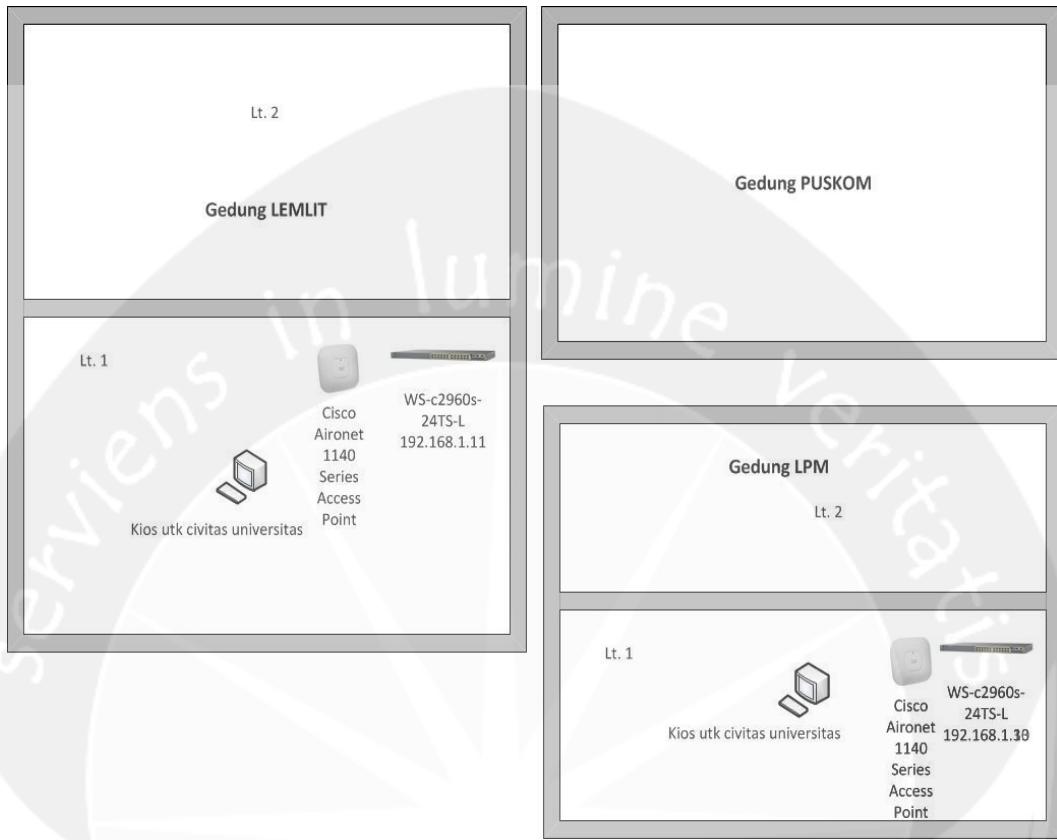
Gambar 6 Denah jaringan Gedung Kantor Pusat UNIMA



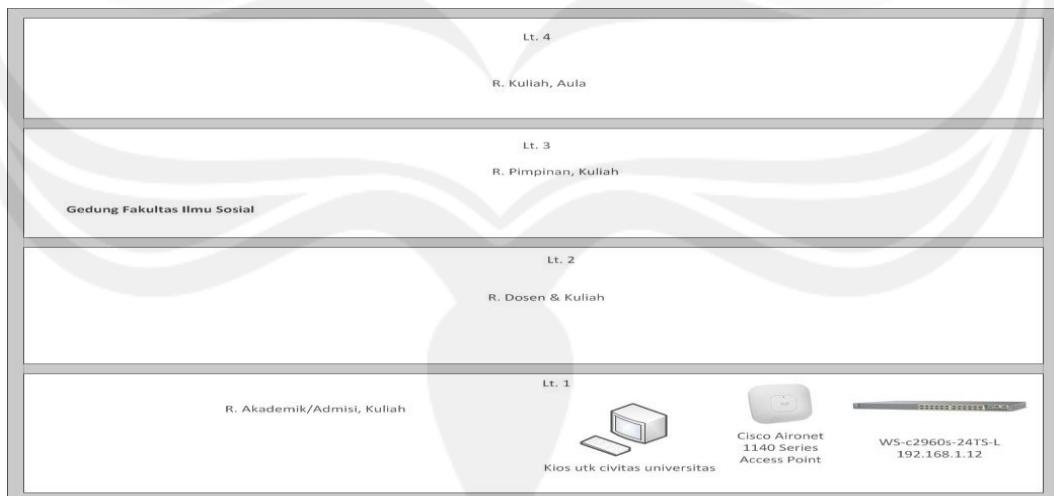


Gambar 7 Denah Jaringan Gedung Fakultas Bahasa dan Seni





Gambar 8 Denah Jaringan Gedung LPM dan LEMLIT



Gambar 9 Denah Jaringan Gedung Fakultas Ilmu Sosial (FIS)



Gambar 10 Denah Jaringan Gedung Fakultas Ekonomi





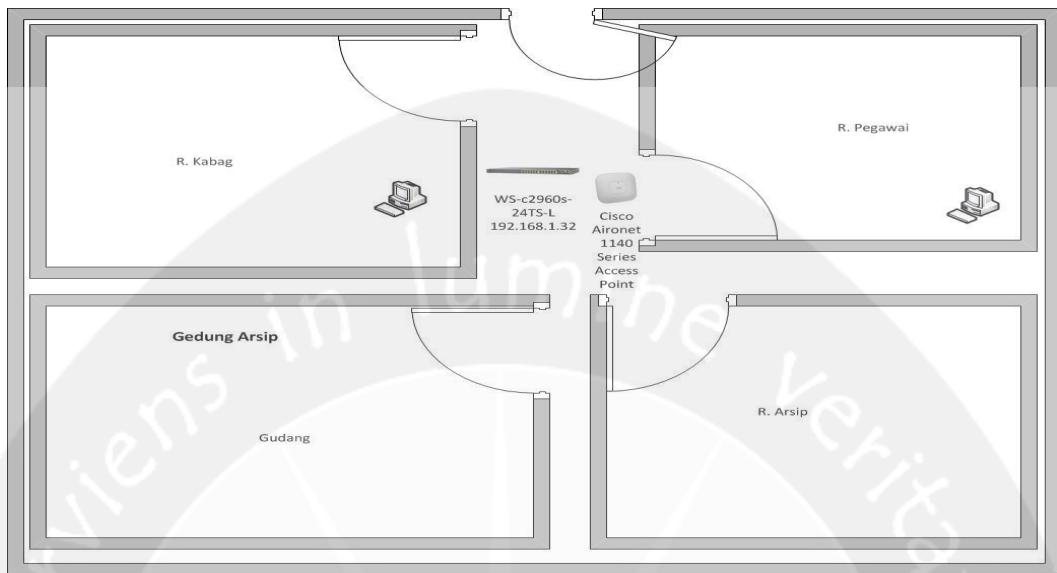
Gambar 11 Denah Gedung Jaringan LP2AI(LP3)/ SIKDIKSAT



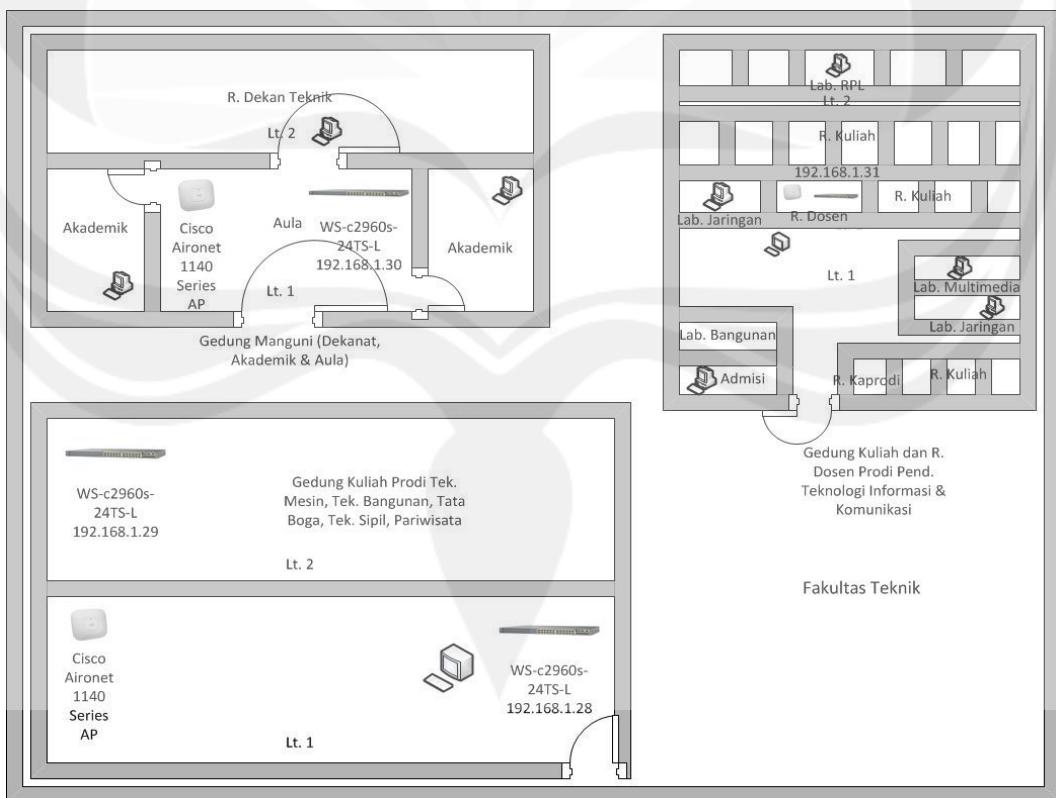


Gambar 12 Denah Jaringan Gedung Perpustakaan



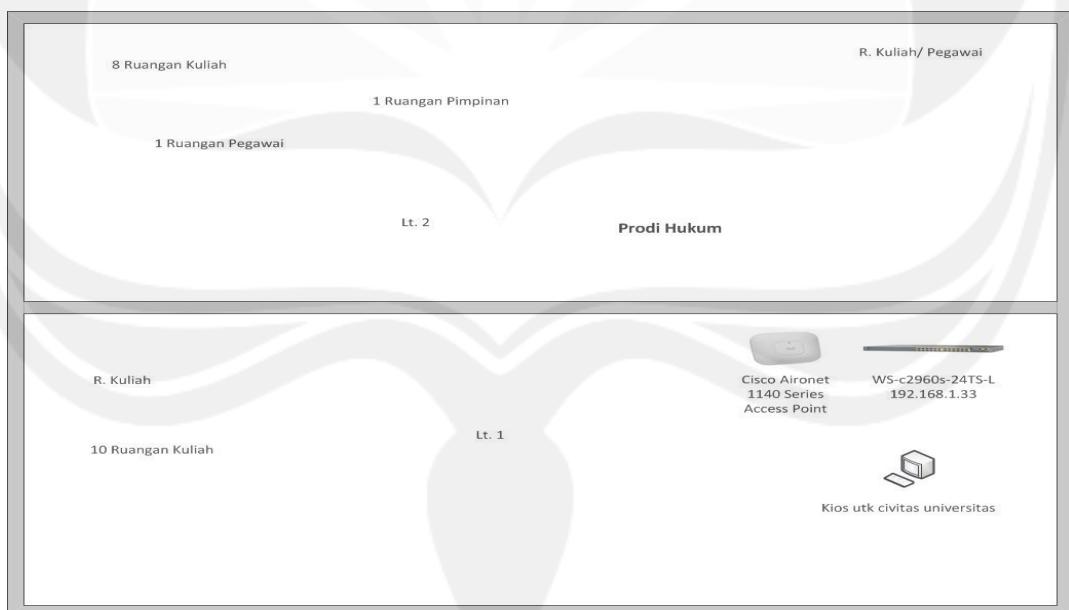


Gambar 13 Denah Jaringan Gedung Arsip



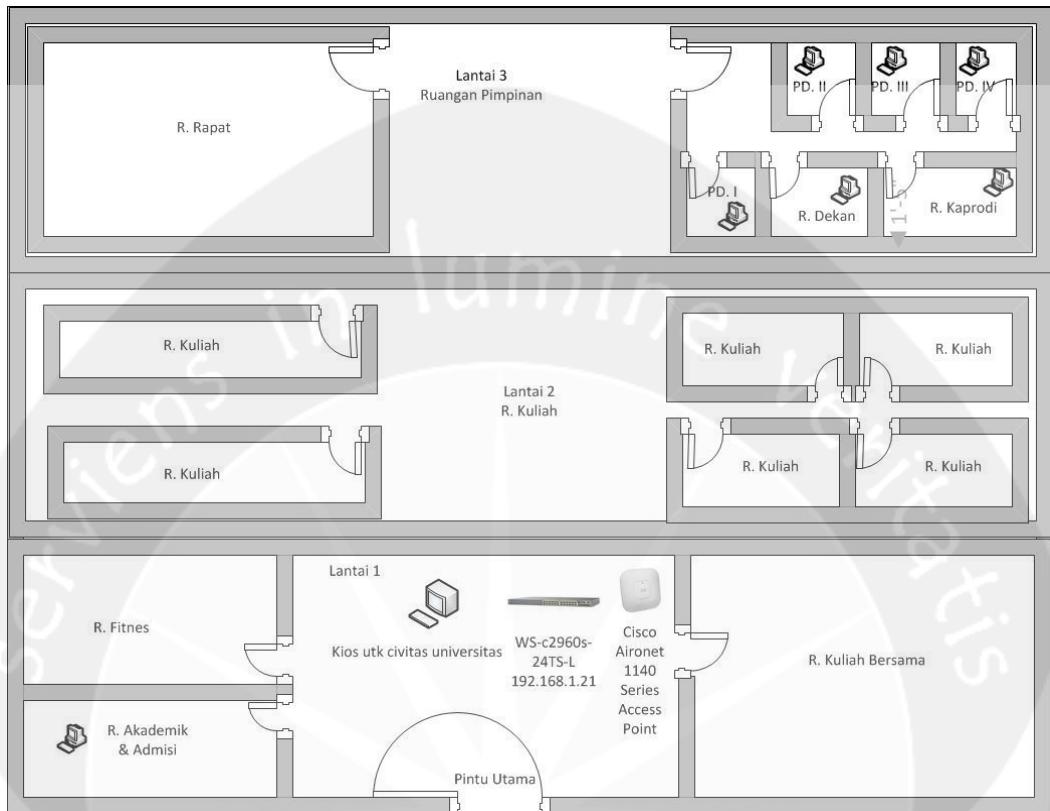
Gambar 14 Denah Jaringan Gedung Fakultas Teknik





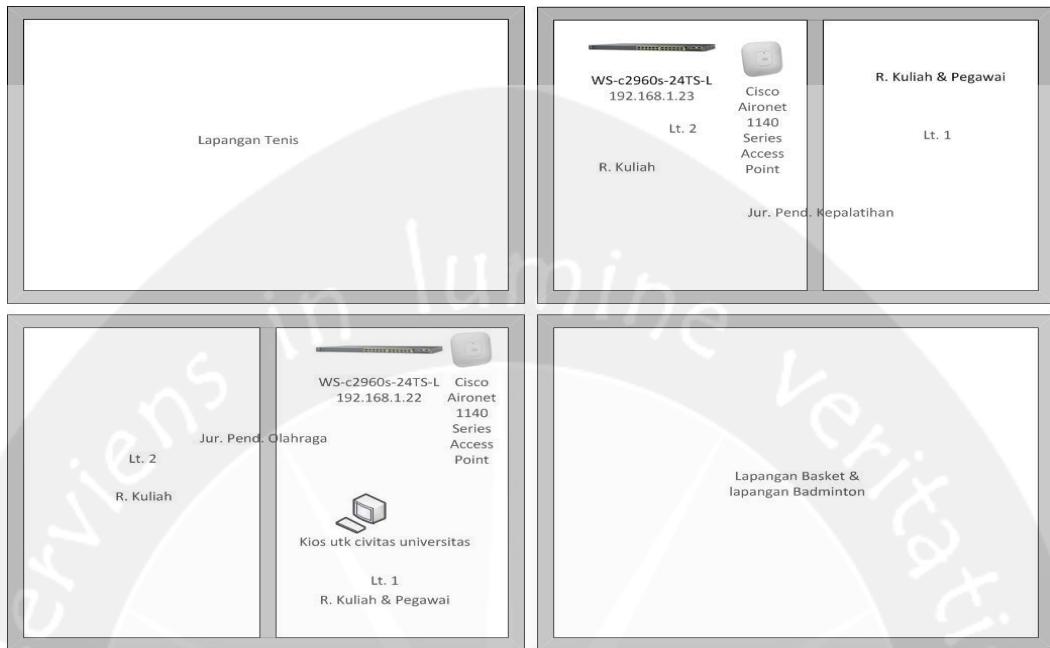
Gambar 15 Denah Jaringan Gedung Prodi Hukum



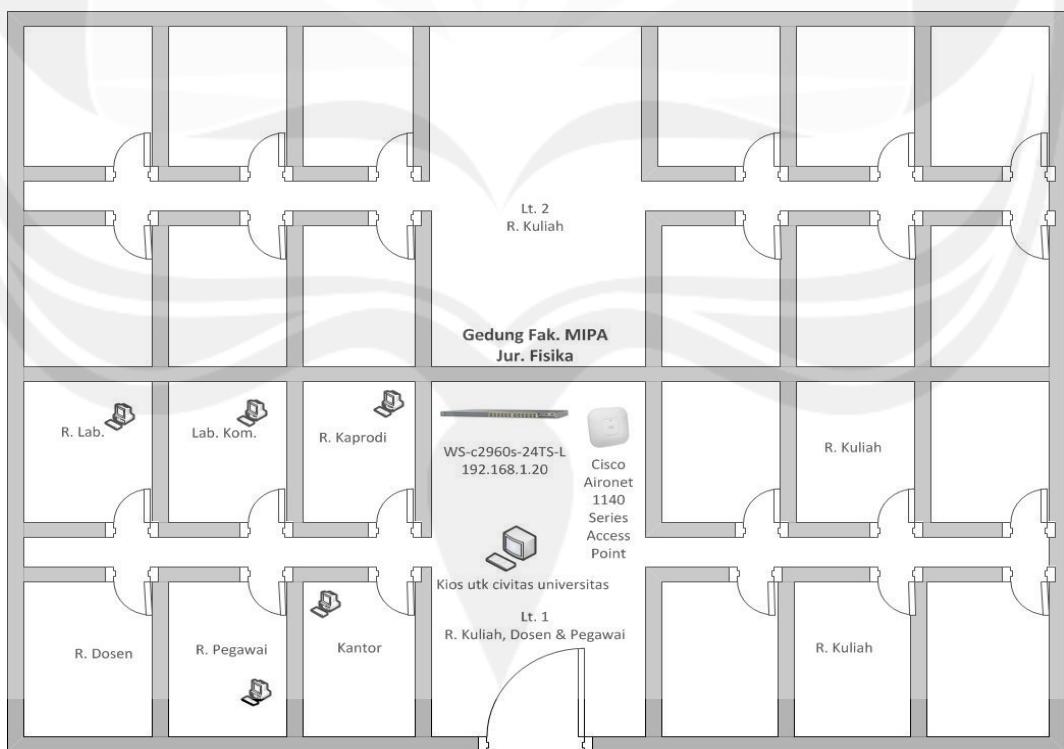


Gambar 16 Denah Jaringan Gedung Fakultas Ilmu Keolahragaan

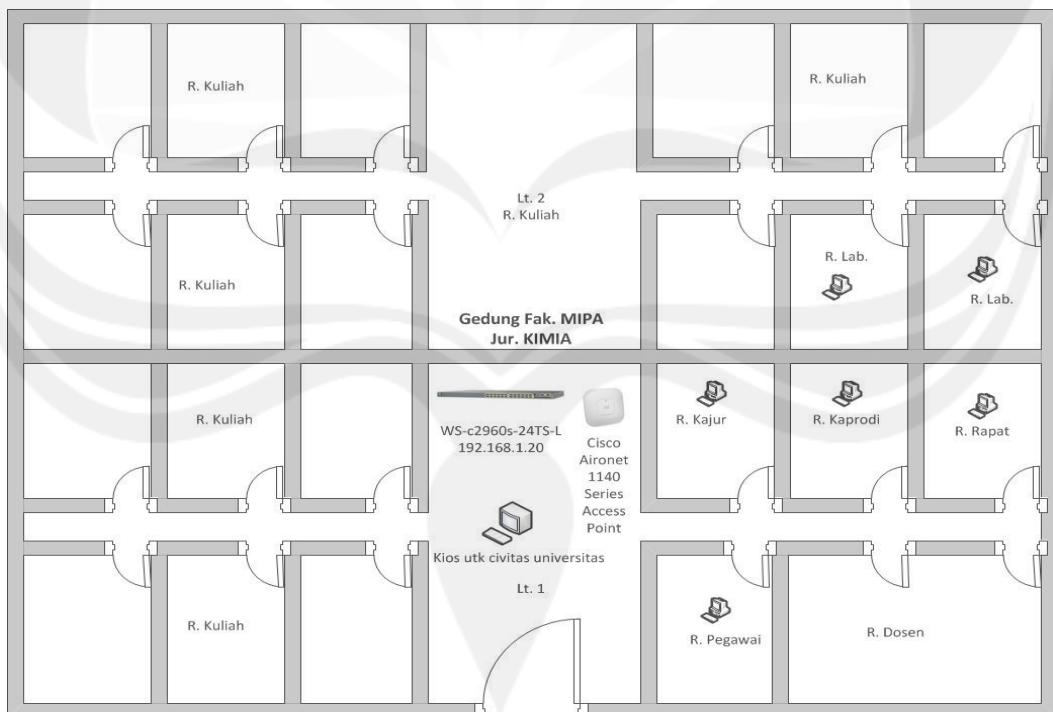




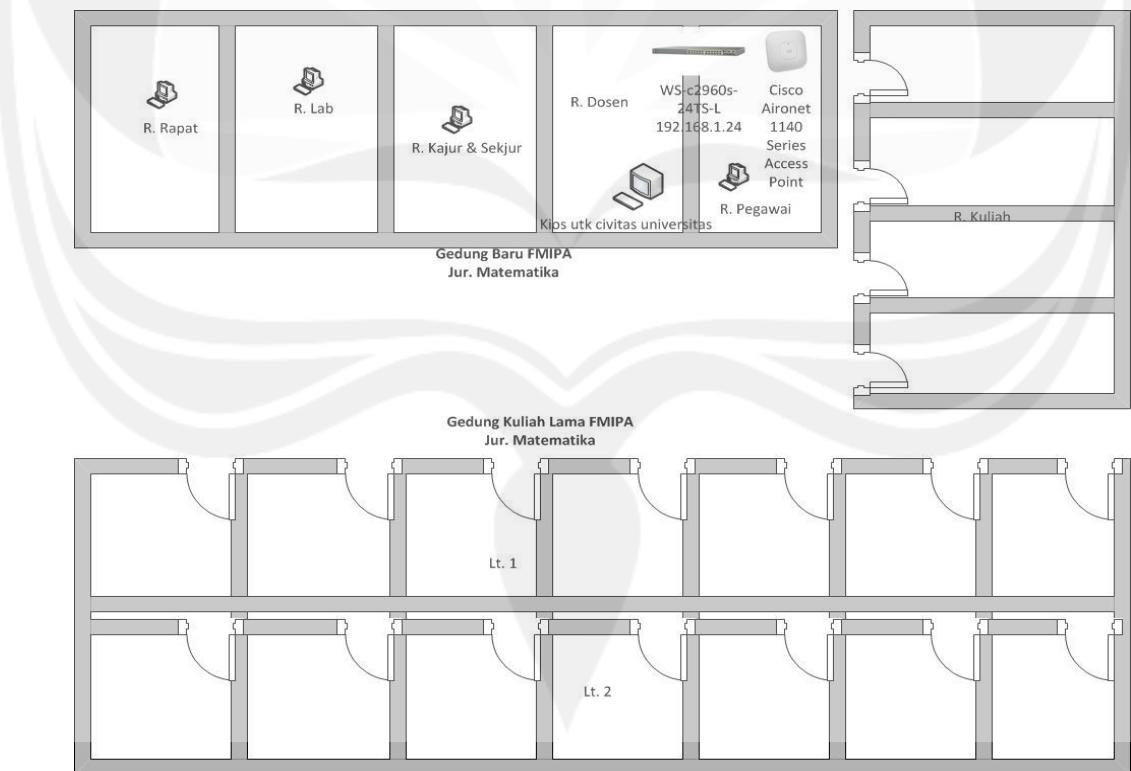
Gambar 17 Denah Jaringan Gedung Fakultas Ilmu Keolahragaan II (FIK II)



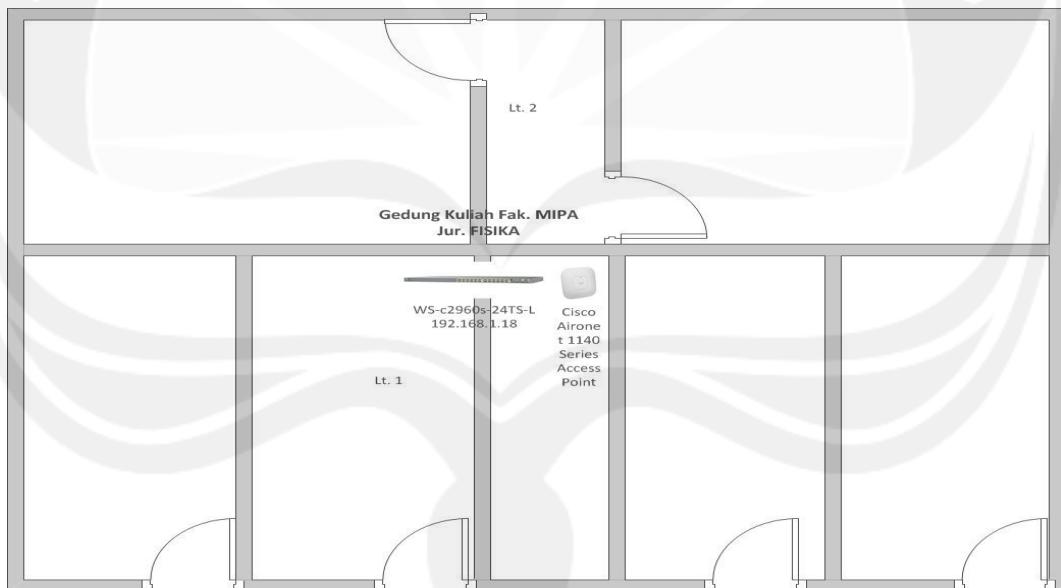
Gambar 18 Denah Jaringan Gedung Fak. MIPA Jurusan Fisika II



Gambar 19 Denah Jaringan Gedung Fak. MIPA Jurusan KIMIA

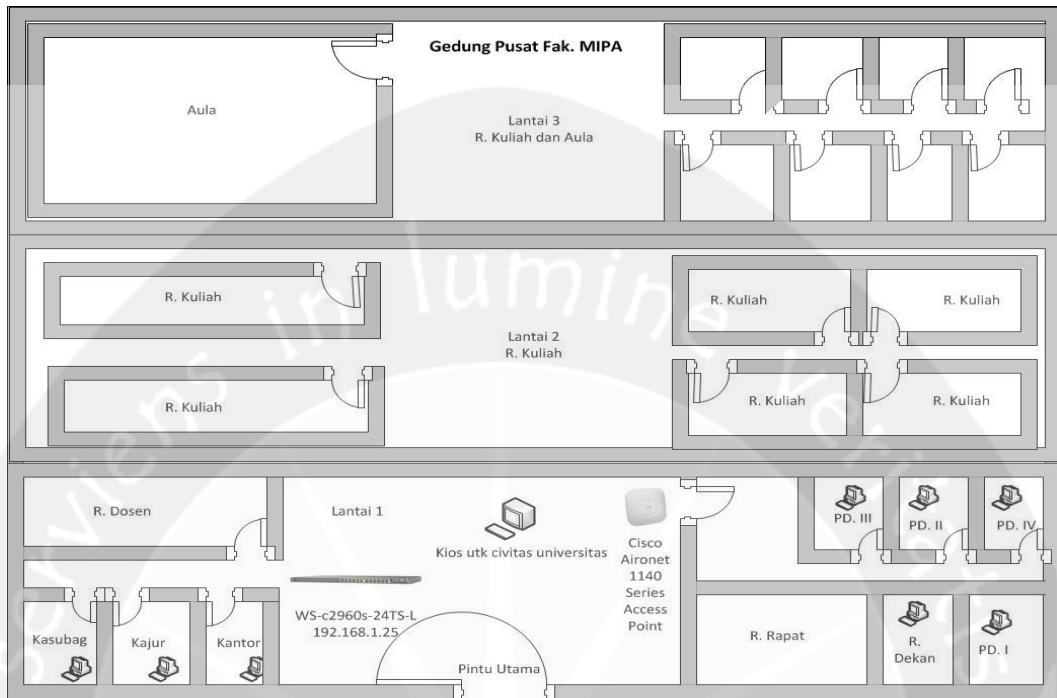


Gambar 20 Denah Jaringan Fak. MIPA Jurusan Matematika



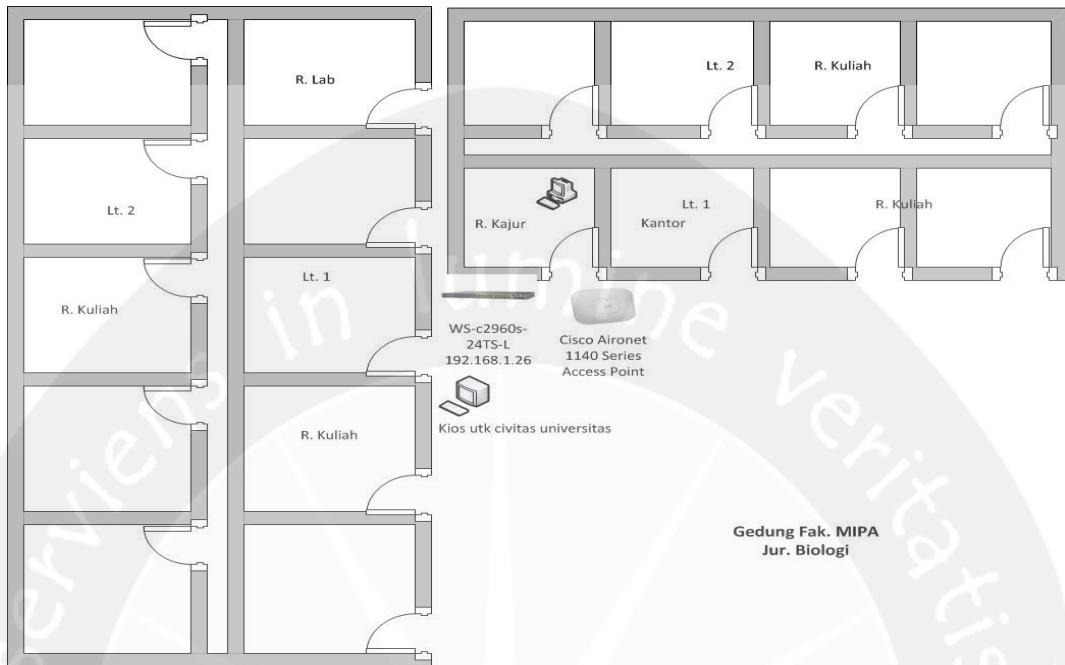
Gambar 21 Denah Jaringan Gedung Fak. MIPA Jurusan FISIKA





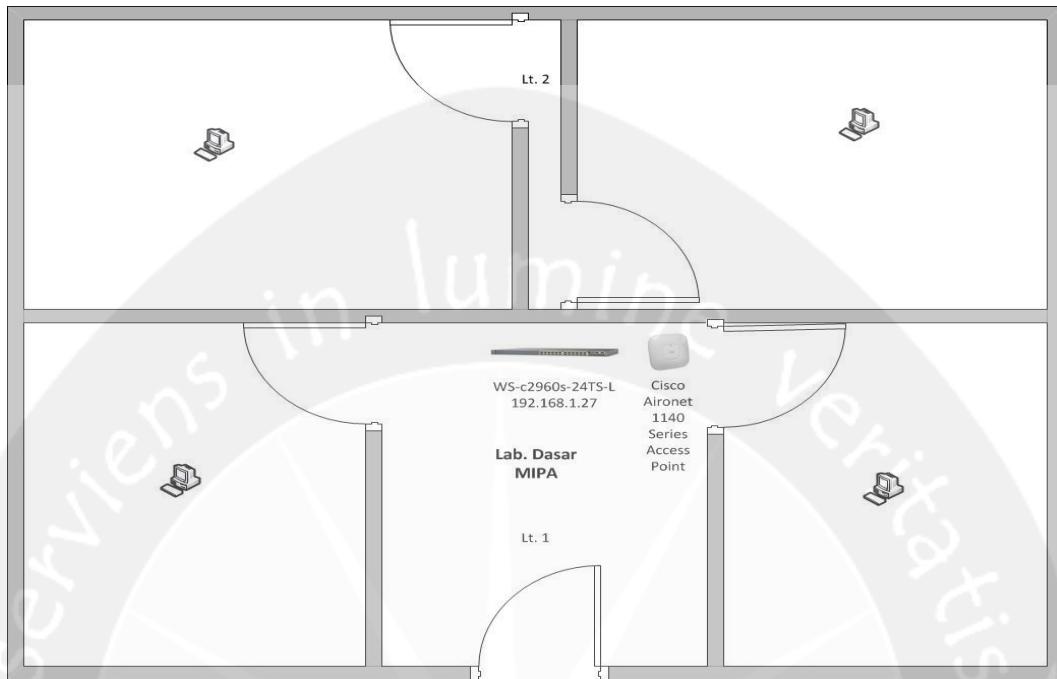
Gambar 22 Denah Jaringan Gedung Fakultas MIPA





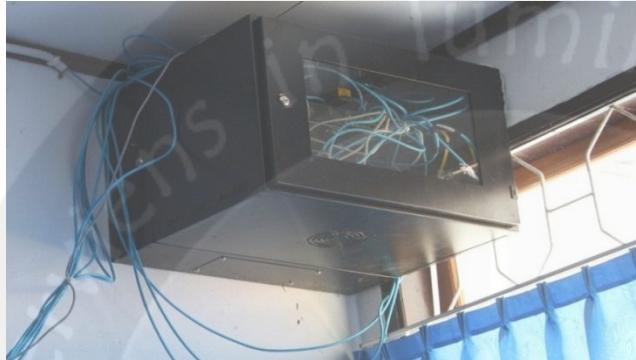
Gambar 23 Denah Jaringan Gedung Fak. MIPA Jurusan Biologi





Gambar 24 Denah Jaringan Gedung Laboratorium Dasar MIPA

Dalam observasi yang dilakukan peneliti mengambil beberapa sampel gambar *switch* yang terpasang di fakultas Teknik, fakultas Ilmu Sosial dan fakultas Ilmu Sosial.



Gambar 26 atas *switch* yang ada di Fak. Teknik

Gambar 27 kanan *switch* dan kios yang ada

di Fakultas Ilmu Sosial (FIS)



Gambar 28 bawah *switch* yang ada di Fak. Ilmu Pendidikan



## GLOSSARY

**Local-Area Network (LAN)**: komputer yang terhubung berada pada tempat yang berdekatan secara gografis (misalkan satu gedung).

**Metropolitan-Area Network (MAN)**: komputer yang terhubung berada dalam jangkauan lebih luas dari LAN. Umumnya menghubungkan antar gedung atau perkantoran dalam area satu kota.

**Wide-Area Network (WAN)**: komputer yang terhubung berada pada tempat yang berjauhan dan dihubungkan dengan line telepon atau gelombang radio. Jangkauannya luas, bisa antarnegara, bahkan antarbenua.

**Topologi** : suatu metode atau cara untuk menghubungkan komputer yang satu dengan lainnya agar terbentuk menjadi jaringan komputer.. Terdapat bermacam-macam topologi seperti bus, star, ring, mesh, dll.

**Protokol** : protokol mendefinisikan sekelompok aturan dan sinyal yang digunakan oleh komputer pada jaringan untuk berkomunikasi. Protokol LAN yang paling populer adalah Ethernet. Protokol LAN lain yang banyak digunakan adalah IBM token-ring network.c. arsitektur: jaringan dapat diklasifikasikan ke dalam arsitektur peer-to-peer atau client/server.

**NIC** : NIC (network interface card) atau biasa disebut LAN card (Local Area Network Card) adalah *expansion board* yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu.

**Backbone** : Backbone adalah saluran atau koneksi berkecepatan tinggi yang menjadi lintasan utama dalam sebuah jaringan.

**Bandwidth**: Bandwidth menunjukkan kapasitas dalam membawa informasi. Istilah ini dapat digunakan dalam banyak hal: telepon, jaringan kabel, bus, sinyal frekuensi radio, dan monitor. Paling tepat, bandwidth diukur dengan putaran perdetik (cycles per second), atau hertz (Hz), yaitu perbedaan antara frekuensi terendah dan tertinggi yang dapat ditransmisikan. Tetapi juga sering digunakan ukuran bit per second (bps).

**Bridge** : Bridge adalah peranti yang meneruskan lalu lintas antara segmen jaringan berdasar informasi pada lapisan data link. Segmen ini mempunyai alamat lapisan jaringan yang sama. Setiap jaringan seharusnya hanya mempunyai sebuah bridge utama.

**Coaxial:** Adalah suatu jenis kabel yang menggunakan dua buah konduktor. Pusatnya berupa inti kawat padat yang dilingkupi oleh sekat yang kemudian dililiti lagi oleh kawat berselaput konduktor. Jenis kabel ini biasa digunakan untuk jaringan dengan bandwidth yang tinggi.

**Collision:** Adalah suatu kondisi yang terjadi bila dua buah device mengirim data pada saat yang bersamaan. Akibat dari kejadian ini adalah hilangnya data.

**Database:** Merupakan suatu himpunan file yang terhubung secara logik yang memiliki common access. Semua besaran data ditujukan pada beberapa sistem yang berhubungan. Sebuah database dapat memiliki beberapa data item yang bisa dipasang ke dalam banyak tipe perekaman yang berbeda.

**Download:** Adalah proses untuk mengambil file dari internet.

**Downstream:** Sebuah bentuk transmisi (pengiriman sinyal) dari server kepada "end user" atau orang yang mengakses ke server, transmisi downstream dapat terbentuk didalam lalulintas jaringan komputer seperti LAN, WAN dsb yang berakhir di end user tadi. Lawan atau kebalikan dari Downstream adalah Upstream.

**DNS :** DNS (domain name sistem) adalah sistem yang menerjemahkan domain Internet, seperti www.microsoft.com menjadi alamat Internet, yaitu serangkaian nomor yang terlihat seperti 101.232.12.5. Istilah DNS berhubungan dengan konvensi untuk penamaan host pada Internet dan cara penangan nama-nama tersebut.

**Email**-Singkatan dari Electronic Mail, yang merupakan cara berinteraksi para pengguna komputer dalam berkirim surat melalui Internet.

**Ethernet :** Ethernet adalah protokol LAN yang dikembangkan oleh Xerox Corporation yang bekerjasama dengan DEC dan Intel pada tahun 1976. Ethernet menggunakan topologi bus atau star dan mendukung transfer data sampai dengan 10 Mbps. Versi Ethernet yang lebih baru yang disebut 100Base-T (atau Fast Ethernet), mendukung transfer data sampai dengan 100 Mbps, dan versi terbarunya, Gigabit Ethernet, mendukung transfer data sampai dengan 1 Gigabit per detik atau 1000 Mbps.

**Fast Ethernet :** Fast Ethernet seperti Ethernet biasa, namun dengan kecepatan transfer data yang lebih cepat, sampai dengan 100 mbps. Ethernet ini juga disebut 100BaseT.

**Fiber Optic Kabel:** yang memiliki inti serat kaca sebagai saluran untuk menyalurkan sinyal antar terminal, sering dipakai sebagai saluran BACKBONE karena keandalannya yang tinggi dibandingkan dengan coaxial cable atau kabel UTP.

**Firewall:** Suatu program yang diterapkan untuk melindungi jaringan komputer terhadap akses-akses tertentu dari luar jaringan.

**FTP:** atau File Transfer Protokol adalah suatu protokol internet yang digunakan untuk mentransfer file ke sebuah web server di internet sehingga file tersebut bisa diakses dari mana pun juga. Untuk memasuki FTP web server, seseorang harus mempunyai username dan password. FTP juga bisa disetting "Anonymous", sehingga orang yang memasuki suatu alamat FTP, tidak memerlukan username dan password. FTP di internet dikenali pada port 21.

**Gateway:** Istilah gateway merujuk kepada hardware atau software yang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga data dapat ditransfer antar komputer yang berbeda-beda. Salah satu contoh penggunaan gateway adalah pada email, sehingga pertukaran email dapat dilakukan pada sistem yang berbeda.

**GPS:** GPS (Global Positioning System) adalah sistem navigasi menggunakan 24 satelit MEO (medium earth orbit atau middle earth orbit) yang mengelilingi bumi dan penerima-penerima di bumi. Satelit mengorbit pada ketinggian sekitar 12.000 mil di atas bumi dan mampu mengelilingi bumi dua kali dalam 24 jam. Satelit GPS secara kontinu mengirimkan sinyal radio digital yang mengandung data lokasi satelit dan waktu pada penerima yang berhubungan. Satelit GPS dilengkapi dengan jam atom dengan ketepatan satu per satu juta detik. Berdasar informasi ini, stasiun penerima mengetahui berapa lama waktu yang digunakan untuk mengirim sinyal sampai ke penerima di bumi. Semakin lama waktu yang digunakan untuk sampai ke penerima, semakin jauh posisi satelit dari stasiun penerima. dengan mengetahui posisi satelit, penerima mengetahui bahwa satelit terletak pada posisi tertentu pada permukaan bola imajiner yang berpusat pada satelit. Dengan menggunakan tiga satelit, GPS dapat menghitung lintang dan bujur penerima berdasar perpotongan ketiga bola imajiner. Dengan menggunakan empat satelit, dapat juga ditentukan ketinggian. GPS dikembangkan dan dioperasikan oleh Departemen Pertahanan Amerika. GPS, asalnya dikenal dengan NAVSTAR (Navigation System with Timing and Ranging). Sebelum untuk keperluan yang lebih luas, GPS digunakan untuk menyediakan kemampuan navigasi sepanjang waktu dan dalam segala cuaca untuk militer darat, laut, dan angkatan udara. Disamping untuk navigasi dan penentuan posisi geografik, GPS dapat juga digunakan di antaranya untuk pemetaan, kehutanan, eksplorasi mineral, manajemen habitat liar, dan pengawasan perpindahan penduduk.

**Host:** Host adalah sistem komputer yang diakses oleh pengguna yang bekerja pada lokasi yang jauh. Biasanya, istilah ini digunakan jika ada dua sistem komputer yang terhubung dengan modem dan saluran telepon. Sistem mengandung data yang disebut host, sedang sistem yang digunakan untuk mengakses dari jarak jauh disebut remote terminal. Istilah host juga digunakan untuk menyebut komputer yang terhubung dengan jaringan TCP/IP, termasuk

**Internet:** Setiap host mempunyai alamat IP yang unik. Selain itu, istilah host juga merujuk pada penyediaan infrastruktur layanan komputer. Sebagai contoh, banyak perusahaan yang menjadi host Web server, yang berarti bahwa perusahaan tersebut menyediakan hardware, software, dan saluran komunikasi yang dibutuhkan oleh server, tetapi isi server (data) dikendalikan oleh pihak lain. ISP (Internet Service Provider) : ISP (Internet service provider) adalah penyedia layanan Internet. Sebagian besar ISP mempunyai jaringan server (mail, berita, Web), router, modem yang dihubungkan dengan koneksi "backbone" Internet yang permanen dan berkecepatan tinggi. Pelanggan ISP dapat mendapatkan koneksi Internet dengan modem dan telepon. Untuk mengakses Internet pelanggan ISP harus melakukan dial ke jaringan dengan menekan nomor telepon tertentu milik ISP.

**ICMP:** atau Internet Control Message Protocol adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan atau paket ICMP dikirim jika terjadi masalah pada layer IP dan layer atasnya (TCP/UDP). IEEEICMP atau Institute of Electrical and Electronic Engineers adalah institut yang membuat standarisasi jaringan untuk pengkabelan, topologi fisik dan skema pengaksesan.

**Internet:** Internet adalah jaringan global yang menghubungkan jutaan komputer. Sejak 1999 Internet telah memiliki 200 juta pemakai di seluruh dunia, dan jumlah ini meningkat cepat. Lebih dari 100 negara terhubung dengan Internet untuk menukar data, berita, dan informasi lainnya. Setiap komputer yang terhubung dengan Internet disebut host.

**IP:** atau Internet Protocol adalah protokol di internet yang mengurus masalah pengalamatan dan mengatur pengiriman paket data sehingga ia sampai ke alamat yang benar

**ISDN:** ISDN (Integrated Services Digital Network) adalah standard komunikasi internasional untuk pengiriman suara, video dan data melalui line telepon digital atau telepon kawat biasa. ISDN mempunyai kecepatan transfer data 64 Kbps. Sebagian besar saluran ISDN ditawarkan oleh perusahaan telepon yang memungkinkan dua saluran, yang disebut kanal B (B channel). Satu line dapat

digunakan untuk suara dan yang lain untuk data lain dan keduanya mempunyai kecepatan transfer 128 Kbps. Versi awal ISDN menggunakan transmisi baseband. Versi lain ISDN, yaitu B-ISDN, menggunakan transmisi broadband dan dapat mendukung transmisi data dengan kecepatan 1,5 Mbps.

**Network:** Sekumpulan dari komputer-komputer yang saling terkoneksi dan dapat berinteraksi/berkomunikasi satu dengan yang lainnya. OS/2 adalah sistem operasi yang dikeluarkan oleh perusahaan komputer IBM.

**Ping:** Adalah suatu aplikasi yang digunakan untuk menguji hubungan antara dua system. Contoh, pada DOS prompt ketikkan ping www.klik-kanan.com dan akhiri dengan enter untuk menguji koneksi dari Anda ke situs Klik Kanan.

**Protocol** (protokol) : Bahasa atau prosedur hubungan yang digunakan oleh dua sistem komputer dengan sistem lainnya sehingga antara keduanya dapat saling berhubungan. Untuk dapat berkomunikasi. Kedua system harus menggunakan protokol yang sama. PPP (Point To Point Protocol) : Protokol TCP/IP yang memungkinkan hubungan antara host dengan jaringan dan antara router dengan router atau dapat pula digunakan untuk hubungan serial antara 2 system.

**Repeater:** Suatu perangkat yang dipasang di titik-titik tertentu dalam jaringan untuk memperbarui sinyal-sinyal yang di transmisikan agar mencapai kembali kekuatan dan bentuknya yang semula, guna memperpanjang jarak yang dapat di tempuh. Ini dibutuhkan karena sinyal-sinyal mengalami perlemahan dan perubahan bentuk selama transmisi.

**Router:** Suatu perangkat yang berfungsi menghubungkan suatu LAN ke suatu internetworking/WAN dan mengelola penyaluran lalu-lintas data di dalamnya. Routing : Proses dari penentuan sebuah path yang dipakai untuk mengirim data ke tujuan tertentu.

**RJ-45:** RJ-45 (Registered Jack-45) adalah konektor delapan kabel yang biasanya digunakan untuk menghubungkan komputer ke sebuah local-area network (LAN), khususnya Ethernets. Konektor RJ-45 mirip dengan konektor RJ-11 yang digunakan dalam koneksi telepon, tetapi lebih besar.

**Server:** Suatu unit yang berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. Komputer server akan melayani seluruh client atau workstation yang terhubung ke jaringannya.

**Subnet Mask:** Adalah angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar.

**TCP/IP:** TCP/IP Transmission Control Protokol adalah dua buah protokol yang dikembangkan oleh militer AS yang memungkinkan komputer pada jaringan dapat saling berhubungan. IP digunakan untuk memindahkan paket data antarsimpul. TCP digunakan untuk memverifikasi pengiriman dari client ke server. TCP/IP adalah dasar internet dan dapat ditemukan pada semua sistem operasi modern, seperti Unix dan Windows.

**Telnet:** Adalah protokol yang digunakan untuk melakukan remote access, yaitu mengakses suatu "machine" dari jarak jauh. Dan "machine" ini memakai OS berbasis \*NIX (linux, BSD maupun Unix). Akses telnet di internet dikenali pada port 23. UDP atau user datagram protocol adalah suatu protokol pada lapisan Transport yang menyediakan layanan pengantaran datagram connectionless dengan usaha yang terbaik.

**Topologi:** Dalam jaringan komputer topologi adalah bentuk pengaturan keterhubungan antar sistem komputer. terdapat bermacam-macam topologi seperti bus, star, ring.

**UTP:** UTP (Unshielded Twisted Pair) adalah jenis kabel yang terdiri dari dua kawat tak terbungkus yang berpilin. Kabel UTP banyak digunakan pada local-area networks (LANs) dan sambungan telepon karena harganya lebih murah. Kabel UTP tidak sebaik kabel koaksial dan serat optik dalam hal penyediaan bandwidth dan ketahanan terhadap interferensi.

**VLAN:** VLAN (virtual local-area network) adalah jaringan komputer yang seakan terhubung menggunakan kabel yang sama meskipun mungkin secara fisik berada pada bagian LAN yang lain. VLAN dikonfigurasi melalui software dan tidak hardware, yang membuatnya sangat fleksible. Salah satu keunggulan VLAN adalah jika sebuah komputer secara fisik dipindah ke lokasi lain, komputer tersebut tetap pada VLAN yang sama tanpa melakukan konfigurasi ulang hardware.

**VPN:** VPN (virtual private network) adalah koneksi internet pribadi yang aman dan terenkripsi untuk menjamin bahwa hanya pengguna yang berhak yang dapat mengaksesnya dan trasfer data yang dilakukan tidak dapat diganggu.

**VSAT:** VSAT (Very Small Aperture Terminal) stasiun bumi yang digunakan pada satelit komunikasi sinyal data, suara, dan video, kecuali pemancaran televisi.

VSAT terdiri dari dua bagian: sebuah transceiver yang diletakkan di tempat terbuka sehingga dapat secara langsung menerima sinyal dari satelit dan sebuah perangkat yang diletakkan dalam ruangan untuk menghubungkan transceiver dan perangkat komunikasi pengguna akhir (end user), seperti PC. Transceiver menerima dan mengirim sinyal ke transponder satelit diluar angkasa. Satelit mengirimkan dan menerima sinyal dari komputer stasiun bumi yang berfungsi sebagai hub sistem. Setiap pengguna yang saling terhubung dengan stasiun hub melalui satelit, membentuk topologi bintang. Hub mengendalikan semua operasi pada jaringan. Semua transmisi untuk komunikasi antar pengguna harus melalui stasiun hub yang meneruskannya ke satelit dan ke pengguna VSAT lainnya. VSAT dapat mengirimkan data sampai dengan kecepatan 56 Kbps.

**WAN:** WAN wide area network adalah komputer yang terhubung berada pada tempat yang berjauhan dan hubungan dengan line telepon atau gelombang radio. Lihat juga LAN dan jaringan.

**Wi-Fi:** Wi-Fi Wireless Fidelity adalah nama dagang resmi untuk IEEE 802.11b yang dibuat oleh Wireless Ethernet Compatibility Alliance (WECA). Istilah Wi-Fi menggantikan 802.11b seperti halnya istilah Ethernet menggantikan IEEE 802.3. Produk yang disertifikasi oleh WECA sebagai Wi-Fi dapat beroperasi bersama meskipun dibuat oleh perusahaan yang berbeda.

**Workstation:** Pada jaringan komputer, workstation adalah komputer yang terhubung dengan sebuah local-area network (LAN). Istilah workstation juga digunakan untuk menyebut komputer yang digunakan untuk aplikasi teknik (CAD/CAM), desktop publishing, pengembangan software, dan aplikasi lainnya yang membutuhkan tingkat komputasi dan kemampuan grafis yang cukup tinggi. Workstation biasanya terdiri dari layar grafik yang besar dengan resolusi tinggi, RAM minimal 64 MB, dukungan jaringan built-in, dan graphical user interface. Sebagian besar workstation juga mempunyai perangkat penyimpanan seperti disk drive, tetapi jenis workstation khusus, yang disebut diskless workstation, tidak mempunyai disk drive. Sistem operasi yang banyak digunakan untuk workstation adalah UNIX dan windows NT. Seperti halnya PC, sebagian besar workstation adalah komputer single user, Meski demikian, workstation pada dasarnya dihubungkan dengan local area network, meskipun dapat juga sebagai sistem yang berdiri sendiri stand alone.

**100BaseT:** 100BaseT adalah nama lain fast Ethernet yang mempunyai kecepatan transmisi sampai dengan 100 mbps. Jenis 100BaseT ini lebih mahal daripada 10BaseT dan lebih jarang digunakan pada local area network (LAN).

**10Base2:** 10Base2 adalah satu jenis standar Ethernet (IEEE802.3) untuk lokal area network (LAN). Standard 10 Base-2 (yang juga disebut Thinnet)

menggunakan kabel koasial 50 ohm (RG-58A/U) dengan panjang maksimal 185 meter. Kabel ini lebih kecil dan lebih fleksibel daripada yang digunakan untuk standard 10 Base 5. Sistem 10 Base-2 beroperasi pada 10 Mbps dan menggunakan metode transmisi baseband.

**10 Base5:** 10 Base-5 adalah standard awal untuk Ethernet yang menggunakan kabel koasial. Nama 10 Base5 didasarkan pada fakta bahwa kecepatan transfer data maksimum adalah 10 Mbps, menggunakan transmisi Baseband, dan panjang kabel maksimal adalah 500 meter. 10 Base5 juga disebut Thick Wire atau thick Net.

**10BaseT:** 10BaseT adalah jenis Ethernet yang paling umum. Nama tersebut menunjukkan bahwa kecepatan transmisi maksimum adalah 10Mbps. 10BaseT menggunakan kabel tembaga dan merupakan card standard untuk menghubungkan komputer pada lokal area network (LAN).

**REKOMENDASI UNTUK PENGELOLA JARINGAN UNIMA**

## **Rekomendasi Standar Kebijakan (*Policy*) Dan Prosedur Akses Sistem Informasi**

Akses sistem informasi atau jaringan internet di lingkungan Kampus UNIMA seharusnya sudah memiliki kebijakan (*policy*) dan prosedur (*procedure*) yang sejalan dengan visi misi kampus. Oleh karena itu rekomendasi yang diusulkan adalah sebagai Pembuatan Kebijakan (*policy*) dan prosedur (*procedure*) pemanfaatan dan penggunaan sistem informasi secara tertulis untuk dipublikasikan serta disosialisasikan kepada seluruh civitas akademika Kampus UNIMA. Kebijakan dan prosedur harus mencakup topik area keamanan kunci atau *password*, manajemen resiko, identifikasi aset kritis, keamanan fisik, manajemen sistem dan jaringan, otentikasi dan otorisasi, kontrol akses (*access-control*), manajemen kelemahan (*weakness management*), manajemen insiden (incident response), kesadaran (*awareness*) dan pelatihan (training), dan privasi (*privacy*).

## **Usulan Kebijakan (*Policy*) Manajemen Infrastruktur Teknologi Informasi**

Berdasarkan skema rancangan pengembangan jaringan yang akan di implementasikan beberapa point penting sebagai kebijakan kedepan antara lain:

1. Komunikasi antar VLAN yang terbentuk harus melalui proses filtering berbasis ACL (*access control-lists*) yang dilakukan pada *distribution switch*. Hal ini untuk menjamin keamanan komunikasi antar VLAN, seperti proteksi *file sharing*, penyebaran malware (*virus, trojan* dan

*worm*), broadcast berlebihan, dan serangan para cracker. Pembatasan yang diusulkan adalah ACL sebagai *Packet Statefull Firewall* yang kemungkinan akan berbeda antara komunikasi VLAN yang satu dengan yang lainnya.

2. Setiap VLAN yang akan mengakses jaringan internet secara direct, akan di translasikan ke sebuah IP *Public* sebagai indentitas di internet. Dengan translasi ini diharapkan dapat dilakukan *managemen bandwidth* dan *monitoring* di perangkat *shapper*.
3. Pada Jaringan sudah seharusnya terdapat *proxy cache server* yang mampu melayani seluruh civitas akademik UNIMA. *Proxy Cache server* selain difungsikan sebagai *Caching Content* untuk *Accelerator* koneksi internet sehingga menghemat *bandwitzh*, *proxy cache server* juga dapat difungsikan sebagai *firewall* atau *filtering content* di level aplikasi. Hal ini untuk menjamin penggunaan koneksi internet Kampus UNIMAbenar benar sesuai dengan peruntukannya dan tidak disalahgunakan oleh para pengguna.

Terdapat dua pilihan cara implementasi penggunaan *Proxy Cache server*, yakni sebagai *Server Proxy* atau *Transparent Proxy*. Penggunaan *Server Proxy* berarti setiap *client* melakukan konfigurasi *Proxy Client* secara manual pada *browser/internet tools* masing-masing untuk dapat terhubung internet. Sedangkan *Transparent Proxy*, *client* tidak perlu melakukan setting atau bahkan tidak perlu tahu jika akses yang mereka lakukan telah

di belokkan melalui *proxy server*. Keuntungan menggunakan sistem *Server Proxy* adalah dapat memanfaatkan fitur Otentikasi dan *monitoring* yang lebih baik dibanding sistem *transparent proxy*.

4. Komunikasi antar VLAN untuk protokol tertentu dapat dimonitor dengan menggunakan *System Logging* melalui ACL yang akan diimplementasikan pada *Distribution Switch*. *System Logging* yang dimaksud adalah, rekaman komunikasi antar VLAN harus dapat disimpan di server SysLog untuk keperluan audit atau monitoring bilamana diperlukan.
5. Untuk kemudahan managemen VLAN berbasis perangkat Cisco, dapat di implementasikan VTP (*Vlan Trunking Protokol*), sehingga penambahan atau perubahan VLAN dapat dilakukan secara terpusat.
6. *Policy* atau *filtering* untuk VLAN *wireless* sebaiknya lebih ketat dibanding jaringan VLAN yang menggunakan kabel (*wired network*), karena tingginya tingkat *vulnerable* dari teknologi *wireless* saat ini.

## **STRATEGI KOMUNIKASI DAN PENGAMANAN DATA (KONSEP DATA CENTER)**

### **Prinsip Keamanan Informasi**

Strategi komunikasi dan pengamanan data harus sesuai dengan prinsip-prinsip keamanan. Ada empat prinsip utama dalam keamanan informasi.

1. *Privacy/Confidentiality* yaitu usaha menjaga informasi dari orang yang tidak berhak mengakses (mengaransi bahwa data pribadi tetap pribadi).
2. *Integrity* yaitu usaha untuk menjaga data atau sistem tidak diubah oleh yang tidak berhak.
3. *Authentication* yaitu usaha atau metoda untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari server yang diberikan benar berasal dari server yang dimaksud.
4. *Availability* berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Keempat aspek diatas menjadi dasar untuk melakukan pengamanan terhadap sistem atau data. Keamanan komputer adalah sebuah proses, yang harus dijalankan untuk mengamankan sistem dan dalam penerapannya harus dilakukan dengan menyeluruh. Bagian-bagian keamanan yang ada pada *Data Center* mengacu pada empat aspek dasar keamanan yang disebutkan sebelumnya.

## **Aspek keamanan pada data center**

Aspek keamanan data/informasi atau disebut juga keamanan virtual pada data center berkaitan dengan hal-hal sebagai berikut:

- I. Kontrol akses logikal, menyangkut apa, siapa dan bagaimana data diakses secara virtual. Contohnya seperti password untuk menentukan hak akses.
- II. Kontrol penyimpanan, menyangkut berapa lama data disimpan dan jenis keamanan apa yang digunakan pada media penyimpanan dan data yang disimpan.  
Contohnya sistem backup data yang dipakai dan enkripsi yang digunakan.
- III. Keamanan jaringan baik jaringan intranet maupun internet terkait dengan konfigurasi jaringan, hak akses jaringan, firewall, intrusion detection dan lainnya.
- IV. Keamanan sistem terkait dengan sistem operasi yang digunakan.

## **Kebijakan keamanan data center**

Keamanan fisik dan keamanan virtual dalam data center tidak terlepas dari kebijakan keamanan yang diterapkan di sebuah *data center*. Prosedur dan kebijakan yang diterapkan harus dapat berhasil dengan efektif. Namun kebijakan dan prosedur yang diterapkan sangat terkait sumber daya manusia yang akan melakukan kebijakan. Secara umum kebijakan keamanan menyangkut pengaturan terhadap sistem, pengaturan terhadap hak akses dan pengguna, pengaturan pengoperasian, prosedur backup dan pengaturan penyimpanan, serta kebijakan

yang terkait dengan kontrol akses fisik dan lainnya. Memberikan pelatihan kepada staf tentang pentingnya mematuhi dan menjalankan prosedur serta kebijakan yang berlaku merupakan sebuah cara yang dapat dilakukan agar kebijakan keamanan dapat mencapai tujuannya.

### **Pengamanan Data Center secara Fisik**

Beberapa ancaman dan resiko pada data center adalah sebagai berikut:

a) Keamanan fisik dan faktor lingkungan

Penerapan keamanan fisik harus memperhatikan faktor lingkungan dan menerapkan kontrol keamanan lingkungan. Bahaya lingkungan ini berupa kebakaran, banjir, embun, suhu, listrik, gempa bumi dan bentuk-bentuk bencana alam lainnya yang memberikan pengaruh negatif untuk peralatan yang ada dalam data center. Namun banyak yang belum siap untuk mengatasi bahaya ini, karena menganggap bahwa bencana belum tentu akan terjadi.

b) Keamanan fisik dan faktor manusia

Manusia merupakan faktor penting dalam keamanan fisik. Eksplorasi keamanan komputer kebanyakan dilakukan oleh manusia. Jika menganggap bahwa seseorang yang tidak sah tidak mungkin masuk ke ruang server atau ruang penyimpanan data adalah sebuah hal yang salah. Hal ini dapat menjadi ancaman terbesar untuk data center. Namun demikian kita tidak hanya memperhatikan eksplorasi keamanan oleh

orang dari luar, namun harus peduli pula dengan orang yang berasal dari dalam. Hal ini adalah ancaman terbesar karena orang berasal dari dalam dan lebih mengetahui dibandingkan penyusup dari luar.



c) Keamanan fisik dan faktor finansial

Perlu investasi yang cukup lumayan untuk mengimplementasikan keamanan fisik yang terintegrasi di sebuah data center. Namun terkadang karena alasan keuangan pengimplementasian tidak jadi dilakukan. Jika para menejer mengabaikan hal tersebut bisa jadi hal tersebut merupakan tindakan yang benar. Namun pandangan yang demikian adalah salah, pengimplementasian keamanan fisik harus diinvestasikan seefisien dan seefektif mungkin, karena jika terjadi sesuatu karena faktor lingkungan atau faktor manusia telah ada pencegahan dan penanggulangannya. Dengan penerapan keamanan fisik resiko kehilangan baik pada data ataupun perangkat keras menjadi lebih kecil, kerugian yang didapat tidak sebesar tanpa penerapan keamanan fisik. Jadi wajar saja jika diinvestasikan untuk keamanan fisik.

### **Rekomendasi langkah pengamanan Data**

Beberapa rekomendasi yang masing terkait dengan strategi pengamanan sistem informasi dan data pada kampus UNIMA antara lain:

- a. Melakukan identifikasi aset sistem informasi milik kampus Aset sistem informasi milik kampus memiliki tingkat
- b. Melakukan analisa resiko terhadap sistem informasi milik kampus.
- c. Membuat kebijakan keamanan sistem informasi dalam kampus.
- d. Meningkatkan kesadaran keamanan sistem informasi dalam kampus

Kesadaran akan keamanan sistem informasi sebaiknya dilakukan dengan cara :

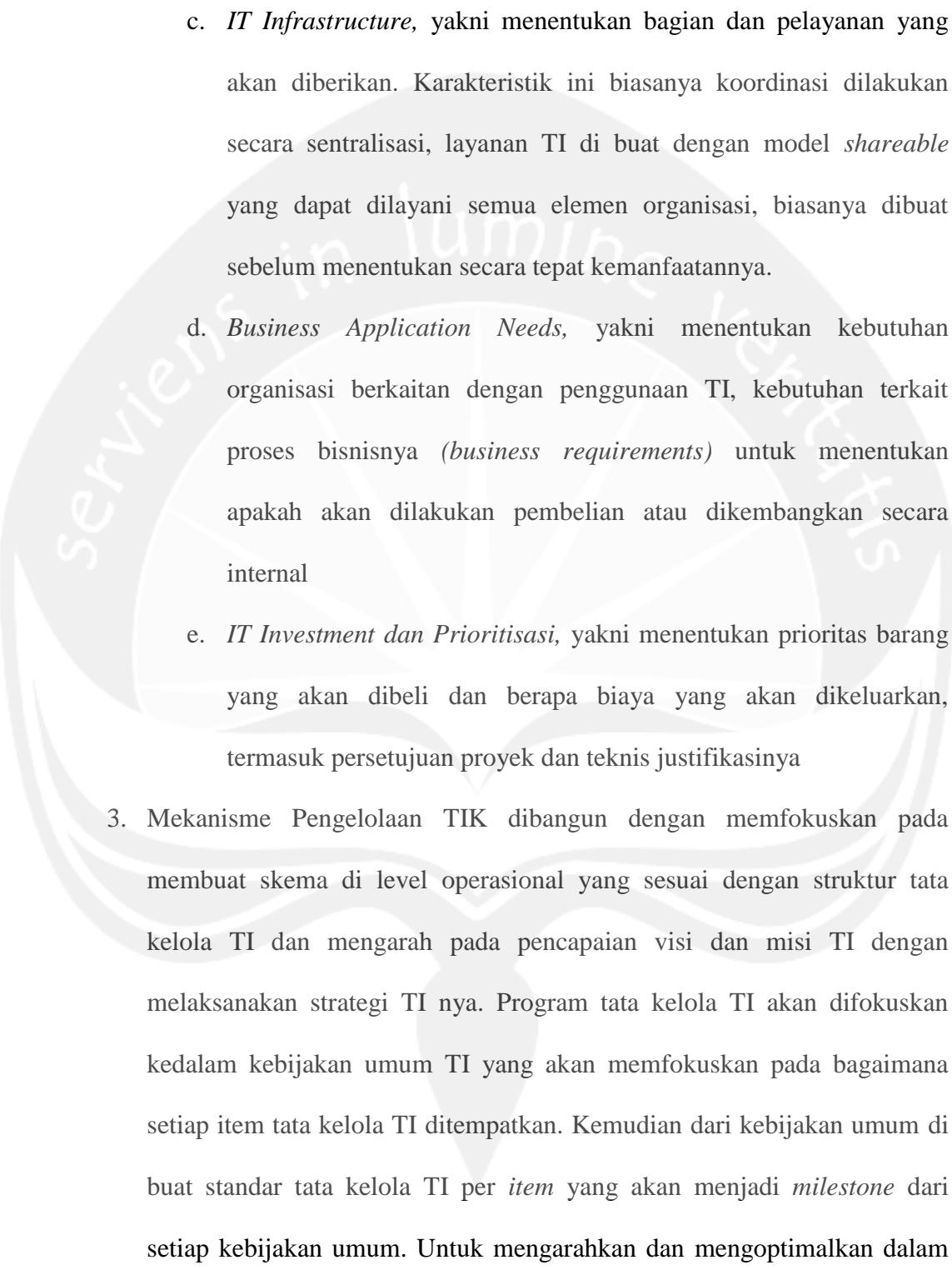
1. Mengikutsertakan pengelola/pimpinan kampus atau unit kerja serta pengurus departemen dalam pelatihan keamanan sistem informasi.
2. Mengikutsertakan staf TIK Kampus dalam pelatihan keamanan sistem informasi tingkat lanjut.
3. Membuat remainder bagi para user agar peduli dengan masalah keamanan sistem informasi.

## **PENGELOLAAN INFRASTRUKTUR TEKNOLOGI INFORMASI DAN SISTEM INFORMASI**

### **Skema Pengelolaan Teknologi Informasi**

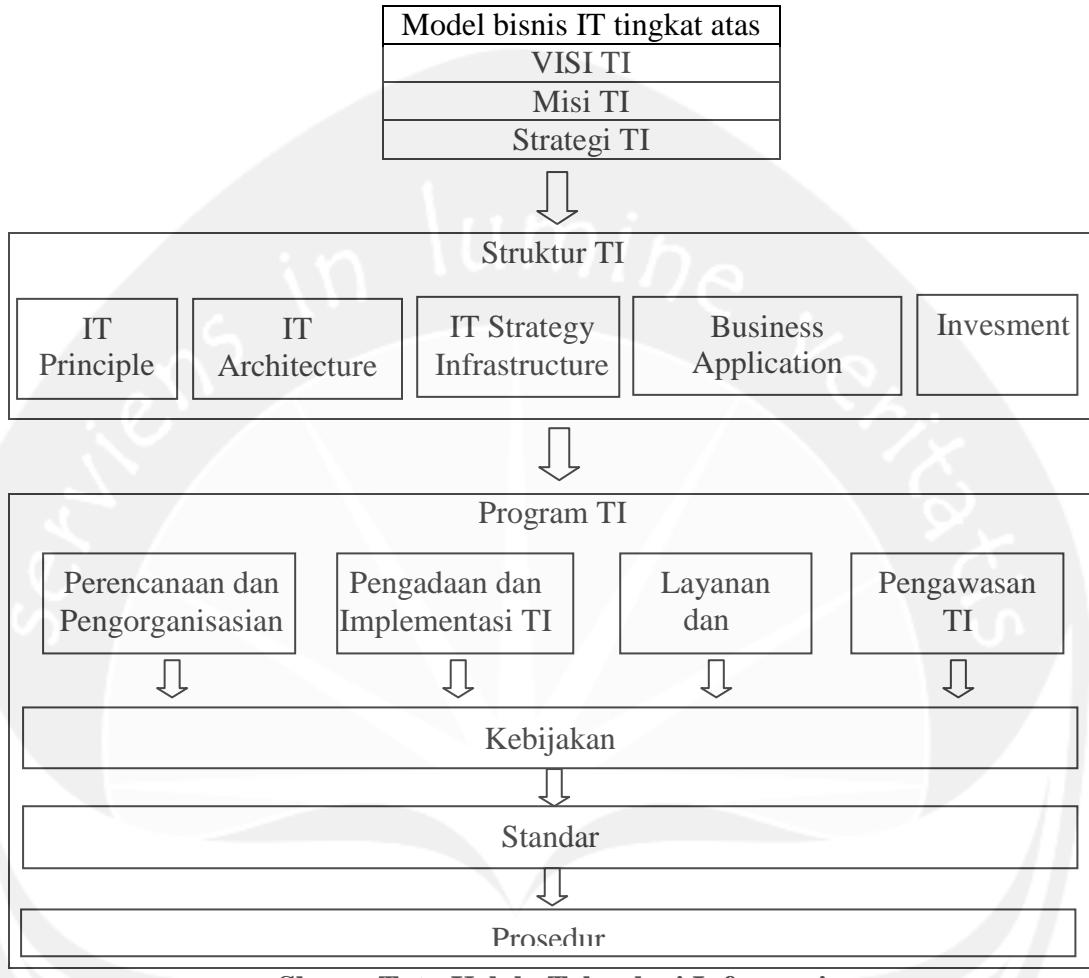
Untuk melakukan pengelolaan Teknologi Informasi Kampus UNIMA membutuhkan skema pengelolaan teknologi informasi sebagai berikut :

1. Perumusan Visi, Misi dan Strategi TIK yang merupakan harmonisasi antara visi, misi dan strategi organisasi dengan visi, misi dan strategi TI. Hal ini dilakukan dengan membuat dan memfokuskan visi, misi dan strategi TI yang dapat menunjang tercapainya visi, misi dan strategi universitas.
2. Struktur TI yang mengatur siapa yang terlibat dan pengambilan keputusan terhadap area tata kelola TI yang memiliki karakteristik sebagai berikut :
  - a. *IT Principles*, yakni mengklarifikasi peranan TI pada organisasi. Karakteristik ini merupakan keputusan tingkat tinggi (*high-level decision*) tentang *IT strategic role* dalam bisnis prosesnya.
  - b. *IT Architecture*, yakni mendefinisikan standar-standar TI yang akan dilakukan dan diwujudkan dalam keputusan-keputusan tentang pengaturan data dan aplikasi dalam penggunaan TI. Karakteristik ini juga akan mengintegrasikan pilihan teknis yang dapat mengarahkan organisasi dalam memenuhi kebutuhan teknisnya.

- 
- c. *IT Infrastructure*, yakni menentukan bagian dan pelayanan yang akan diberikan. Karakteristik ini biasanya koordinasi dilakukan secara sentralisasi, layanan TI dibuat dengan model *shareable* yang dapat dilayani semua elemen organisasi, biasanya dibuat sebelum menentukan secara tepat kemanfaatannya.
  - d. *Business Application Needs*, yakni menentukan kebutuhan organisasi berkaitan dengan penggunaan TI, kebutuhan terkait proses bisnisnya (*business requirements*) untuk menentukan apakah akan dilakukan pembelian atau dikembangkan secara internal
  - e. *IT Investment dan Prioritisasi*, yakni menentukan prioritas barang yang akan dibeli dan berapa biaya yang akan dikeluarkan, termasuk persetujuan proyek dan teknis justifikasinya
3. Mekanisme Pengelolaan TIK dibangun dengan memfokuskan pada membuat skema di level operasional yang sesuai dengan struktur tata kelola TI dan mengarah pada pencapaian visi dan misi TI dengan melaksanakan strategi TI nya. Program tata kelola TI akan difokuskan kedalam kebijakan umum TI yang akan memfokuskan pada bagaimana setiap item tata kelola TI ditempatkan. Kemudian dari kebijakan umum dibuat standar tata kelola TI per *item* yang akan menjadi *milestone* dari setiap kebijakan umum. Untuk mengarahkan dan mengoptimalkan dalam pelaksanaannya, standar tersebut akan didukung oleh prosedur

operasionalnya. Program TI akan terdiri atas Kebijakan TI, Standar TI dan Prosedur TI.





**Skema Tata Kelola Teknologi Informasi**

### Team Pengelola dan Staff TIK

Pengelolaan infrastruktur teknologi informasi dan sistem informasi membutuhkan tim yang solid dan mau bekerja sama dengan baik. Setiap Anggota team dapat memiliki tanggung-jawab khusus yang berbeda, sesuai bidang kerja atau fungsi kerja masing masing, tetapi haruslah saling dapat berbagi pengetahuan dan informasi satu sama lain.

Disamping team yang solid, dalam pengelolaan sistem dan teknologi informasi khususnya infrastruktur diperlukan standard dan procedure atau sering disebut dengan SOP (*Standart Operational Procedure*). Procedur standard yang umum dalam pengelolaan sistem jaringan ataupun sistem informasi adalah adanya dokumentasi setiap terdapat perubahan atau kejadian pada sebuah sistem atau jaringan komputer. Dokumentasi inilah yang diharapkan mampu dijadikan acuan kerja bagi rekan-rekan dalam team. Dengan adanya dokumentasi yang lengkap dan dicatat secara sistematis sesuai prosedur tertentu, maka proses pembelajaran dan pertanggungjawaban dapat dilaksanakan lebih baik.

## **PENGEMBANGAN SDM TIK KAMPUS UNIMA**

Agar pengelolaan TIK kampus UNIMA dapat berlangsung dengan baik dan mengalami kemajuan melalui inovasi dan kreatifitas, maka dapat dilakukan beberapa perencanaan yang berkaitan dengan pengembangan kemampuan SDM TIK seperti :

1. Bekerjasama dengan Pengelola Sumber Daya Manusia UNIMA untuk merancang dan membuat sistem pengembangan skill khusus Sumber Daya Manusia Teknologi Informasi yang memenuhi kebutuhan kampus.
2. Menyelenggarakan jalur pendidikan pelatihan, seminar dan *workshop* yang dapat digunakan untuk meningkatkan keahlian dan mengupgrade kemampuan para pengelola dan staf teknologi informasi kampus khususnya dibidang jaringan komputer.

3. Bekerja sama dengan lembaga/konsultan atau organisasi yang sesuai dalam pengembangan sumber daya manusia melalui kerja sama kunjungan atau study banding agar dapat memberi wawasan lebih serta pembandingan pemanfaatan teknologi informasi di kampus.
4. Melakukan proses *review* berkala untuk memastikan bahwa pengelola dan staff TI sudah berkontribusi dalam pengembangan Teknologi Informasi secara professional serta memastikan bahwa setiap pengelola & staf TI mendapatkan fasilitas pengembangan keahlian dan pembelajaran TI yang layak