# SISTEM JARINGAN KOMUNIKASI

# SISTEM JARINGAN DAN KOMUNIKASI DATA

## Arsitektur Manajemen Jaringan

Manajemen Jaringan berisikan himpunan fungsi untuk *control, plan, allocation, deploy, coordinate, dan monitor network resources.* Arsitektur Manajemen Jaringan dimulai dari analisis kebutuhan dan alurnya. Saat menganalisis, perlu diperhatikan bebarapa hal, yaitu :

- *Protokol manajemen jaringan* yang digunakan,
- Implementasi high-level manajemen asset
- *Efek* dari pemenuhan *kebutuhan* terhadap *konfigurasi* jaringan
- Perlunya *monitoring* secara *terpusat*
- *Pengujian penyedia layanan* terhadap kebijakan
- Perlunya *monitoring* secara *proaktif*

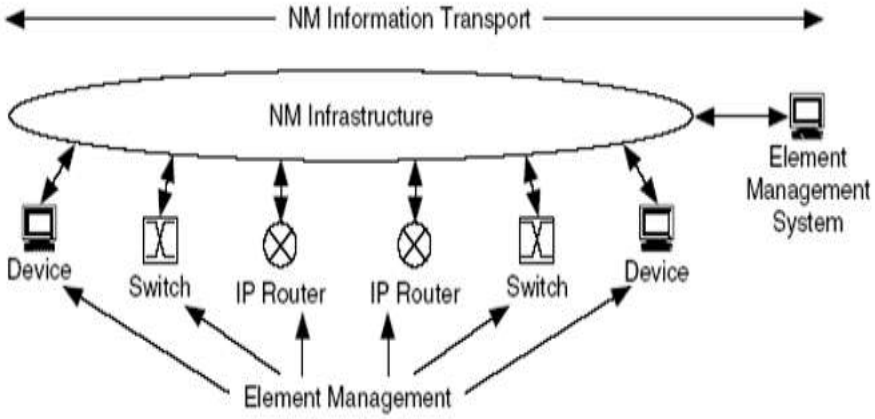
### Mendefinisikan manajemen jaringan

Manajemen jaringan bisa dipandang sebagai suatu struktur *top-down* yang berisikan lapisan-lapisan (*layer*) manajemen. Lapisan-lapisan manajemen tersebut yaitu (dari atas ke bawah):

- *Business layer*→*budget resource*, *perencanaan*, dan *persetujuan.*
- *Service layer*→*pelayanan* terhadap pengguna.
- *Network layer*→*perangkat* yang digunakan di seluruh jaringan.
- *Element layer*→*kumpulan* perangkat yang *mirip* pada lapisan *network.*
- *Network-element layer*→*instance* dari perangkat pada lapisan *network*

Manajemen Jaringan bisa dibagi menjadi dua fungsi dasar, yaitu tentang bagaimana mengirimkan informasi ke seluruh system, dan manajemen dari elemen-elemennya sendiri (seperti bagaimana alokasi router yang baik).

*Gambar 1 fungsi dasar manajemen*




### Perangkat yang digunakan dalam jaringan dan karakteristiknya

Perangkat jaringan merupakan komponen individual dari suatu jaringan yang memiliki satu atau lebih lapisan protocol. Perangkat jaringan memiliki *karakteristik* yang dapat diukur, karakteristik yaitu:

- **End-to-end**→dapat diukur dari *ketersediaan, kapasitas, delay, varians delay, hasil, banyaknya Error, dan pemanfaatan jaringan*.

- **Per-link**dapat diukur dari perambatan *delay*, pemanfaatan link
- **Per-network**dapat diukur dari perambatan *delay*, pemanfaatan link
- **Per-element**dapat diukur dari banyaknya paket IP per detik, pemanfaatan *buffer* **untuk router**, logs dari kegagalan autentikasi

**Mekanisme manajemen jaringan**

Dua protocol yang digunakan untuk manajemen jaringan:

- Simple Network Management Protocol (SNMP)
- Common Management Information Protocol (CMIIP)

Protocol jaringan menyediakan mekanisme untuk *mengembalikan*, *merubah*, dan *mengirimkan* data ke penjuru jaringan.

**SNMP** merupakan protocol standar internet untuk *mengumpulkan* dan *mengorganisir* informasi tentang perangkat yang dikelola di jaringan dan *mengubah* informasi tersebut untuk mengubah perilaku perangkat. SNMP banyak digunakan dalam manajemen jaringan untuk *monitoring* jaringan. SNMP mengorganisir data dalam bentuk *variabel* dari system yang dikelola pada *Management Information Base.* **MIB** menggambarkan *status* dan *konfigurasi* system. SNMP terdiri dari 3 bagian utama :

- **Perangkat** yang dikelola
- ***Agent***, software yang berjalan di perangkat yang dikelola. Agent bisa mengatur agent yang lain, agent yang mengatur tersebut dikenal dengan **Master Agent**.
- ***Network Management Station*** (NMS), software yang berjalan di pengelola.

**Pertimbangan arsitektur**

*Proses* manajemen terdiri dari:

- Memilih karakteristik mana yang akan dikelola
- Mengumpulkan perangkat jaringan untuk memperoleh data yang sesuai
- Me proses data untuk melihat, menampilkaan dan menyimpan data tersbeut.

*fitur* manajemen dalam pengelolaan jaringan menurut framework FCAPS:

- **Fault**me proses event, identifikasi masalah, isolasi, troubleshooting, dan keputusan, mengembalikan jaringan ke status yang stabil
- **Configuration**penyediaan jaringan, konfigurasi, backup dan pemulihan system. Mengembangkan dan mengoperasikan system database.
- **Accounting**pemantauan dan pengelolaan penggunaan layanan. Tagihan pelayanan.
- **Performance**mengimplementasi kontrol performa berdasarkkan aristektur pelayanan IP. Mengumpulkan data performa jaringan. Menganalisis data performa. Membuat laporan jangka pendek dan panjang dari data. Mengatur parameter jaringan dan performa system.
- **Security**mengimplementasi control keamanan. Mengumpulkan dan menganalisis data keamanan. Membuat laporan keamanan dan log nya.

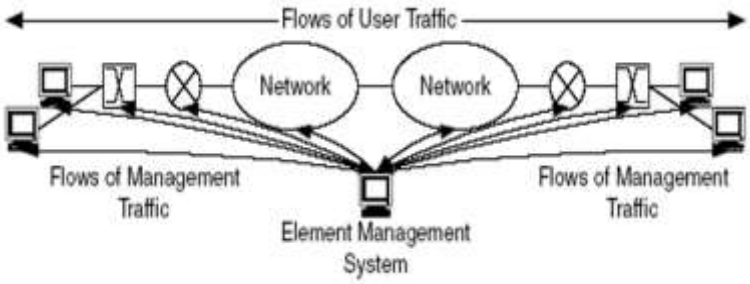
*Proses* dan *fitur* yang akan dikelola menentukan arsitektur manajemen jaringan. Hal-hal yang perlu dipertimbangan dalam manajemen jaringan yaitu:

- Manajemen In-band dan out-of-band
- Manajemen terdistribusi, terpusat dan hieararkis
- Check and balance
- Pengelolaan data manajemen jaringan
- Pemilihan MIB
- Integrasi ke dalam OSS

## Manajemen in-band dan out-of-band

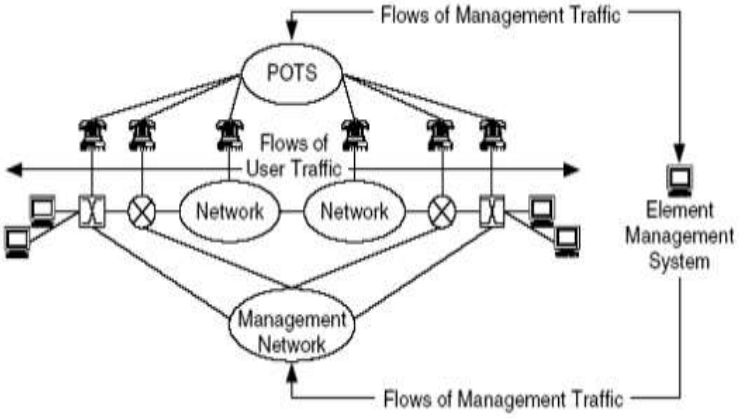
- **Manajemen in-band** muncul saat traffic flow manajemen jaringan mengikuti *jalur* yang *sama* dengan traffic flow pengguna dan aplikasi. Manajemen in-band menyederhanakan arsitektur manajemen jaringan.

*Gambar 2 manajemen in-band*




- **Manajemen out-of-band** muncul saat traffic flow manajemen jaringan dan traffic flow pengguna berada di jalur yang *berbeda.* Manajemen out-of-band menyediakan availabilitas yang tinggi dan bisa melakukan monitoring ke jalur yang berada di luar jalur normal. Namun pada manajemen out-of-bond perlu ditambahkan fitur keamanan karena letak manajemen jaringan dan pengguna yang berbeda serta menambah kompleksitas terhadap arsitektur manajemen jaringan.

*Gambar 3 manajemen out-of-band*




## Manajemen terpusat, terdistribusi dan hierarkis

- **Manajemen terpusat,** semua data manajemen berasal dari satu sumber manajemen. Manajemen terpusat hanya memerlukan satu system manajemen, sehingga menyederhanakan arsitektur dan tools yang digunakan. Namun hasilnya, jika terjadi kesalahan, satu system akan terdampak. Bisa mengakibatkan kegagalan interface jaringan.
- **Manajemen terdistributsi,** terdapat banyak komponen yang terpisah di dalam system manajemen. Hal tersebut mengakibatkan lokalisasi system manajemen sehingga sumber manajemen lebih tersebar.
- **Manajemen hieararkis.** Fungsi manajemen dipisah dan diletakan di perangkat terpisah. Fungsi yang terpisah dikenal sebagai lapisan komunikasi. Pada manajemen tipe ini, terdapat lokalisasi perangkat monitoring. perangkat monitoring berfungsi

mengumpulkan dan memfilter data manajemen. Lokalisasi perangkat monitoring mengurangi data manajemen yang melintasi jaringan. Data yang dikirim ke jaringan hanya data yang relevan. Perangkat monitoring bertindak sebagai filter dalam hal tersebut.

## Jaringan Sistem Operasi

Jaringan sistem operasi merupakan *sistem operasi* yang *menerapkan kemampuan jaringan*. Sistem operasi dengan kemampuan jaringan memungkinkan komputer *terhubung* ke arsitektur *client-server* di mana satu server menangani banyak klien. Jaringan sistem operasi berjalan di *sebuah server* dan server tersebut bisa *mengelola data, user, keamanan, aplikasi, dan fungsi jaringan lainnya.*

### Distribusi Linux

*Distribusi Linux* (distro) merupakan sebuah sistem operasi yang dibuat dari kumpulan software yang berbasis kernel linux, atau dikenal dengan package management system. Distro berisikan kernel Linux, tools GNU dan library, serta software tambahan, dokumentasi, sistem window, window manager, dan desktop environment. Salah satu contoh distro yaitu CentOS.

### Yellowdog, Updater, Modified

Yellowdog, Updater, Modified(YUM) merupakan tools command-line package-management opens-source yang digunakan untuk menjalankan komputer dengan sistem operasi linux. YUM berfungsi untuk :

- *Menginstall* package
- *Menghapus* package
- *Mengupdate* package yang sudah terinstall
- *Merinci* package yang *tersedia*
- *Merinci* package yang *terinstall*

beberapa command yang digunakan untuk menginstall apache, php, mariadb, dan GUI (opsional) pada CentOS versi 7:

- Install **Apache server**
  - `yum install httpd` (menginstall apache server)
  - `firewall-cmd --add-service=http` (membolehkan service http melewati firewall secara permanen)
  - `firewall-cmd --permanent –add-port=3221/tcp` (membuka port 3321 pada firewall secara permanen)
  - `firewall-cmd --reload` (memuat ulang firewall)
  - `systemctl restart httpd.service` (merestart server agar efek perubahan diupdate)
  - `systemctl start httpd.service`
  - `systemctl enable http.service` (memulai server setiap sistem melakukan booting)
- Install **PHP**
  - `yum install php` (menginstall PHP)
  - `systemctl restart httpd.service` (menjalankan ulang server untuk melihat perubahan)

- echo -e "<?php echo 'hello'; ?>" (menguji apakah PHP sudah bisa dijalankan)

- Install **database MariaDB**
  - yum install mariadb-server mariadb (menginstall database MariaDB)
  - systemctl start mariadb.service (menjalankan database)
  - systemctl enable mariadb.service (menjalankan database setiap sistem melakukan booting)
  - firewall-cmd --add-service=mysql (membolehkan service mysql melewati firewall)
  - /usr/bin/mysql_secure_installation (mengamankan server MariaDB)
- Install **GUI**
  - yum -y group install "GNOME Desktop" Graphical Administration Tools"
  - ln -sf /ib/systemd/system/runlevel5.target /etc/systemd/system/default.target

Untuk installasi fitur lebih lengkap, silahkan akses:

https://www.tecmint.com/things-to-do-after-minimal-rhel-centos-7-installation/

## Virtual Host

Virtual Host merupakan metode menjalankan lebih dari satu website pada satu mesin. Ini memungkinkan satu mesin membagikaan resourcenya, seperti memory dan prosesor, ke website-website tersebut. Terdapat dua tipe virtual host, **IP-based** virtual host, yang berarti alamat IP pada satu website berbeda dengan website yang lain, walaupun dijalankan pada satu mesin/server dan **name-based** virtual host, yang berarti bahwa nama pada satu website berbeda dengan nama pada website yang lain walaupun merujuk pada alamat IP yang sama.

Berikut tahapan membuat virtual host di CentOS versi 7:

1. Buat struktur direktori
   a. sudo mkdir -p /var/www/nyobavhost.com/public_html
2. Buka izin
   a. sudo chown -R $USER /var/www/nyobavhost.com/public_html
3. Buat halaman demo
   a. nano /var/www/nyobavhost.com/public_html/index.html (membuat file html bernama index, dan membukanya dengan text editor nano)
   b. tuliskan sintaks html sederhana
4. Buat file konfigurasi virtual host
   a. sudo mkdir /etc/httpd/sites-available (digunakan untuk menyimpan semua file konfigurasi virtual host)
   b. sudo mkdir /etc/httpd/sites-enabled (digunakan untuk menyimpan tautan ke virtual host yang ingin kita publish)
   c. sudo nano /etc/httpd/sites-available/nyobavhost.com.conf (membuat file konfigurasi baru dan membukanya dengan teks editor nano)
   d. masukan konfigurasi dasar virtual host, seperti namanya dan aliasnya.
5. Enable file konfigurasi
   a. sudo ln -s /etc/httpd/sites-available/nyobavhost.conf /etc/httpd/sites-enabled/nyobavhost.com.conf

6. Tambahkan ip dan hostname di file localhost (opsional)
    a. `sudo nano /etc/hosts` (membuka file local host)
    b. tambahkan alamat IP dan hostname nya
7. Uji hasilnya
    a. `httpd://nyobavhost.com`

terkadang terdapat error pada server yang diakibatkan oleh fitur keamanan selinux, untuk mengatasinya bisa dengan mengubah konfigurasi selinux dan/atau menggunakan kode setsebool:

1. `sudo nano /etc/selinux/config`
2. ubah value SELINUX menjadi "disabled"
3. restart server
4. jika belum bisa, masukan kode `setsebool -P httpd_unified l`
5. restart server

Untuk penjelasan yang lebih rinci, bisa dilihat di:

https://www.digitalocean.com/community/tutorials/how-to-set-up-apache-virtual-hosts-on-centos-7

## Keamanan Jaringan

Permasalahan keamanan jaringan (Network Security) bisa dibagi menjadi 4 bagian yang saling terkait: **secrecy** (mencegah orang yang tidak memiliki otorisasi melihat informasi), **authentication** (memastikan bahwa seseorang memiliki otorisasi), **nonrepudiation** (jaminan bahwa signature key hanya dimiliki satu orang, sehingga jika ditemukan suatu signature key di suatu tempat, maka orang yang memilikinyalah yang menggunakannya), **integrity control** (mencegah orang lain mengubah informasi). Beberapa hal yang perlu dipertimbangkan oleh perusahaan mengenai data dan informasi yang ingin diamankan:

- data:
    - Data **Availability**, berkenaan dengan perlindungan terhadap gangguan pelayanan. Apakah data tetap bisa diakses oleh pengguna yang sah.
    - Data **Integrity**, berkenaan dengan perlindungan terhadap perubahan data. Apakah data yang dikirimkan dan diterima sama.
    - Data **Confidentiality**, berkenaan dengan perlindungan dari akses data oleh unauthorized access. Seperti penyadapan dan snooping
    - **Privacy**, berkenaan dengan sebeberapa anonymous seorang pengirim. Apakah identitas pengirim diketahui.
- Informasi
    - **Accountability**, mengacu pada bagaimana mengetahui siapa yang bertanggung jawab terhadap data tertentu dan mengetahui perubahannya.
    - **Authorization**, mengacu pada bagaimana informasi yang dimiliki diberikan ke pengguna lain mengetahui siapa yang bertanggung jawab atas informasi yang diberikan, serta bagaimana orang yang bertanggung jawab atas informasi itu menyetujui akses dan perubahan informasi.

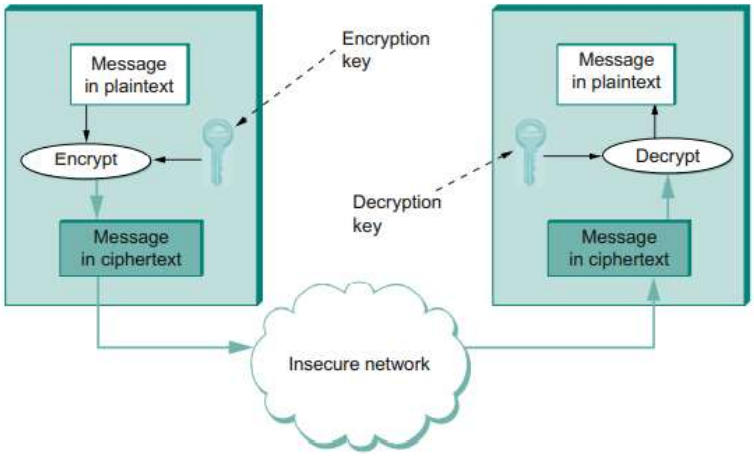
Kemanan jaringan terletak di setiap layer OSI.

- Layer **fisikal**, penyadapan bisa diatasi dengan menutup jalur transmisi dengan tabung yang memiliki gas inert bertekanan tinggi. Setiap percobaan untuk melubangi kabel transmisi akan mengeluarkan gas bertekanan tinggi dan memicu alarm.
- Layer **data link**, paket pada jalur one-to-one bisa dienkrupsi saat melewati satu mesin, dan didekripsi saat memasuki mesin yang lain, ini dikenal dengan *link encryption*.
- Layer **jaringan**, bisa dengan menginstall firewall untuk menyaring paket yang masuk dan keluar. Keamanan IP juga bisa diterapkan pada layer ini.
- Layer **Transport**, bisa dengan enkripsi end-to-end.
- Layer **Aplikasi**, bisa dengan otentikasi dan nonrepudiation.

## Kriptografi

Kriptografi berasal dari Bahasa latin yang berarti "tulisan rahasia". Terdapat dua konsep penting dalam kriptografi, yaitu **chiper** dan **code.** *Chiper* merupakan transformasi character-of-character atau bit-for-bit tanpa mengetehui bahasa apa yang digunakan. Sebaliknya, *code* mengganti *satu kata* dengan *kata lain* atau symbol. Saat ini chiper lebih banyak digunakan daripada code dalam konteks kriptografi. Penerapan kriptografi ialah dengan enkripsi dan dekripsi cipher.

*Gambar 4 alur enkripsi dan dekripsi*




Enkripsi mengubah sebuah pesan sedemikian hingga pesan yang diubah tersebut tidak akan bisa dimengerti, jika tidak mengetahui bagaimana pesan tersebut awalnya diubah. Pengirim pesan menerapkan fungsi enkripsi ke pesan plaintext, dihasilkan pesan ciphertext yang kemudian dikirimkan ke jaringan. penerima menggunakan fungsi dekripsi yang membalikan fungsi enkripsi. Ciphertect diubah menjadi plaintext dan bisa dimengerti oleh penerima. Fungsi enkripsi memiliki parameter berupa key. Key ini bisa bersifat public dan private.

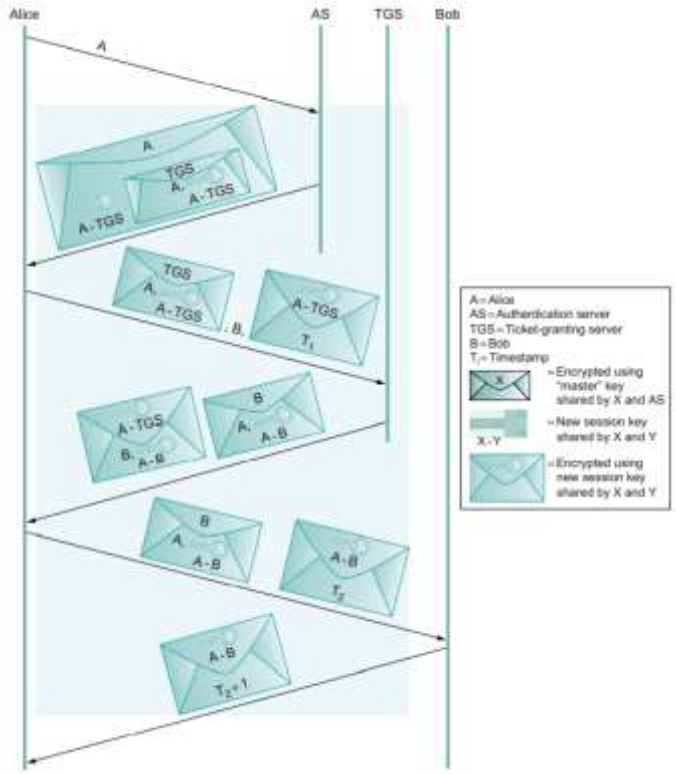
## Predistribusi Key

Predistributed Key merupakan salah satu metode mendapatkan encryption key yang digunakan pada enkripsi pesan. Selain predistributed key, ada session key yang digunakana untuk berkomunikasi secara terenkripsi di dalam jaringan. predistributed key digunakan untuk sesi komunikasi yang lebih panjang dari pada sesi komunikasi pada session.

## Protokol Otentikasi

Protocol otentikasi merupakan protocol komunikasi yang ditujukan untuk transfer data otentikasi dari dua komunikan. Protocol ini memungkinkan penerima mengotentikasi entitas penghubung (klien ke server) dan mengotentikasi dirinya sendiri ke entitas penghubung (server ke klien) dengan menyatakan jenis informasi yang dibutuhkan untuk informasi beserta sintaksnya.

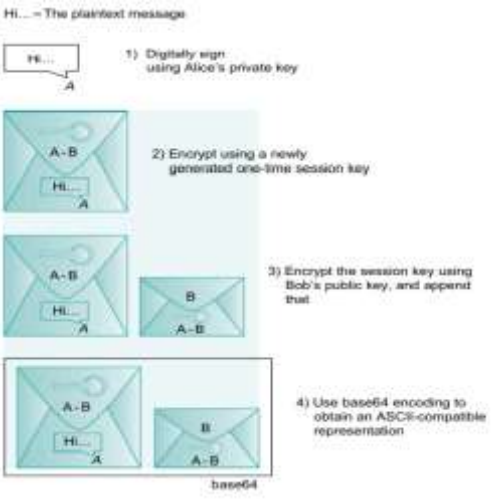
*Gambar 5 alur protokol otentikasi kerberos*




## Pretty Good Privacy (PGP)

PGP merupakan pendekatan yang digunakan untuk keamanan pada E-mail. Pendekatan ini menyajikan otentikasi, confidentiality, data integrity, dan nonrepudiation. Beberapa protocol yang terdapat pada pendekatan PGP yaitu SSH (Secure Shell), TLS (transport Layer Security), SSL, HTTPS, IPsec (IP security), wireless Security.

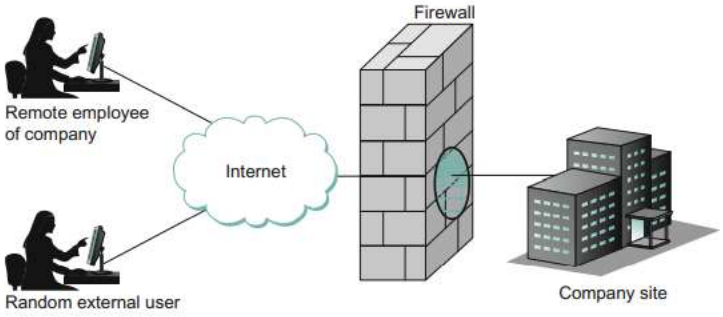
*Gambar 6 alur pendekatan PGP*



## Firewalls

Firewall merupakan sebuah sistem yang berada di suatu titik pada jalur konektivitas antara area yang dilindunginya dengan internet. Keamanan berbasis firewall berarti komunikasi antar komunikan hanya melewati firewall, tidak ada jalur yang lain. Firewall menyaring pesan yang keluar dan masuk ke dalam jaringan yang dilindunginya dengan hanya membolehkan alamat IP, port TCP, UDP tertentu saja. Akibatnya, Firewall membagi jaringan menjadi dua bagian, bagian yang terpercaya, dan bagian yang kurang terpercaya.

*Gambar 7 posisi firewall dalam jaringan*




## Information Gathering

Information gathering/Recoinnaissance (pengumpulan informasi) merupakan kegiatan untuk *mengumpulkan informasi* dari suatu *system*. Untuk bisa mendapatkan hasil yang tepat sasaran pada penetration testing, perlu diketahui terlebih dahulu bagaimana perilaku atau property yang dimiliki suatu system, karena itu Information gathering sangat penting dilakukan. Information gathering merupakan salah satu Langkah awal dalam melakukan penetration testing. Dari hasil pengumpulan informasi, didapat property, perilaku atau celah keamanan dari suatu sistem. Dua jenis information gathering, yaitu :

- **Active** information gathering, memiliki ciri sebagai berikut:
  - Kontak langsung dengan target sistem
  - Mengakses langsung target untuk mencari informasi
  - Berpotensi melanggar hukum. Illegal jika yang diakses seharusnya merupakan hal yang tidak boleh diakses. Legal apabila yang diakses memang boleh diakses dan ditujukan untuk memperbaiki bug yang ada.
  - Beberapa metodenya yaitu port scanning (NMap), directory brute-force (menebak directory yang ada pada sistem), identifikasi OS, CMS detection, dst

- **Passive** information gathering, memiliki ciri sebagai berikut:
  - Tidak kontak langsung dengna target sistem
  - Mengumpulkaan informasi berdasarkan data yang sudah tersedia secara public
  - Biasanya tidak melanggar hukum
  - Beberapa tools yang digunakan seperti google hacking, wayback machine, whois serach, nslookup, dst.

Beberapa tahapan dalam melakukan information gathering:

1. Menentukan target

2. Menggali informasi target:
    a. **pemilik target domain**, bisa dengan menggunakan whois untuk melihat informasi dasar tentang domain yang teregistrasi seperti nama domain, awal dibuat, status UNSSEC, alamat IP, dst.
    b. **teknologi yang digunakan** target, bisa dengan menggunakan webapplyzer untuk mengetahui teknologi yang digunakan, seperti library, OS, web server, keaman, dst.
    c. **subdomain target**, bisa dengan menggunakan query "site:target" pada google, atau dengan menggunakan website nmapper.com, di website tersebut akan dikembalikan banyaknya subdomain, dan list subdomain.
3. Menggali informasi subdomain target. (opsional)

POLITEKNIK STATISTIKA STIS
J A K A R T A

UJIAN AKHIR SEMESTER GASAL
TAHUN AKADEMIK 2019/2020

Mata Kuliah : SISTEM JARINGAN DAN KOMUNIKASI DATA
Tingkat : IIISI
Hari/Tanggal : Rabu, 11 Desember 2019
Sistem Ujian : Take Home

**PETUNJUK DAN ATURAN**

1. Kerjakan soal yang ada dengan menggunakan kalimat yang singkat, jelas dan mudah dipahami
2. Ilustrasi gambar rancangan yang anda buat harus jelas
3. Anda **diperbolehkan** mendiskusikan soal dengan teman anda, tetapi wajib mengerjakana ujian masing masing
4. **Dilarang** melakukan plagiarism tulisan mahasiswa lain atau siapapun, tanpa mencantumkan sumber secara tepat dan memadai.
5. jawaban *softcopy* dikumpulkan dalam format PDF dengan nama file adalah **nim.nama.pdf** menggunakan google drive melalui tautan ---
6. jawaban dicetak dalam kertas A4, tidak perlu dijilid dan dikumpulkan pada hari Rabu 11 Desember 2019 di BAAK.
7. Pelanggaran terhadap aturan yang ada akan berakibat pengurangan nilai atau anda akan dinyatakana **gagal.**

**SOAL**

Pada pelaksanaan Praktik Kerja Lapangan (PKL) akan dibuat berbagai system yang terdiri dari system pengumpulan data berbasis aplikasi android, web monitoring pelaksanaan lapangan secara *realtime, instant messaging,* dan web manajemen PKL. Sistem ini akan digunakan oleh sekitar 600 mahasiswa dan 100 dosen pembimbing. Dalam pembangunan system ini diperlukan rancangan arsitektur jaringan dan computer untuk memenuhi berbagai layanan tersebut.

Buatlah rancangan arsitektur jaringan dan komputer untuk mendukung pelaksanaan PKL dengna rincian sebagai berikut.

- Buat analisis kebutuhan system untuk pelaksanaan PKL.
- Gambarkan arsitektur meliputi server, jaringan, aplikasi, dan teknologi yang dibutuhkan unutk melayani semua kebutuhan system.
- Tentukan spesifikasi server dan layanan apa saja yang akan dijalankan di setiap server.
- Tentukan arsitektur dan strategi untuk memenuhi syarat kehandalan dan ketersediaan data dan layanan apa saja yang akan dijalankan di setiap server.
- Jelaskan strategi anda untuk menjamin keamanan jaringan dan aplikasi yang anda buat.

**PEMBAHASAN SOAL UAS GASAL**
**TAHUN AKADEMIK 2019/2020**

**Rancangan Jaringan dan Komputer untuk Pelaksanaan Praktik Kerja Lapangan**

## I. Analisis Kebutuhan Sistem

Pada pelaksanaan Praktik Kerja Lapangan (PKL) terdapat beberapa sistem informasi yang dibuat guna mendukung jalannya PKL. Adapun sistem yang dibuat adalah sistem pengumpulan data berbasis aplikasi android (CAPI), web monitoring pelaksanaan lapangan secara realtime, instant messaging (PKL Messenger), dan web manajemen PKL (SIKOKO). Dari setiap sistem tersebut perlunya analisis untuk dapat mengetahui kebutuhan dari tiap sistem yang dibuat. Analasis kebutuhan sistem dibagi menjadi dua, yaitu untuk kebutuhan fungsional dan non-fungsional. Berikut adalah analisis kebutuhan dari semua sistem yang akan dibuat.

1. Sistem Pengumpulan Data Berbasis Aplikasi Android (CAPI)
   Kebutuhan Fungsional :
   a) Sistem mampu mengambil dan mengirimkan data (kuesioner, database) dari/ke server
   b) Pengguna dapat melihat profil serta beban kerja dari pengguna itu sendiri
   c) Pengguna dapat membaca, menginput, menghapus, dan merubah data pada kuesioner
   d) Pengguna dapat membaca, menghapus, dan merubah pada fitur listing/updating
   Kebutuhan Non-Fungsional :
   a) Minimum OS Android 5.0 (Lollipop)
   b) Kapasitas Penyimpanan Aplikasi 60 MB
   c) Sistem aplikasi dan database dilengkapi dengan password
2. Web Monitoring
   Kebutuhan Fungsional :
   a) Sistem mampu mengambil dan menampilkan data dari database server
   b) Sistem mampu menampilkan berbagai macam visualisasi data (tabulasi, diagram, analisis spasial, dll)
   c) Pengguna dapat melihat seluruh progress cacah secara realtime

   Kebutuhan Non-Fungsional :

   a) Sistem dapat dijalankan oleh beberapa software web browser diantaranya Internet Explorer, Google Chrome dan Mozilla Firefox.
   b) Sistem aplikasi dan database dilengkapi dengan password
   c) Sistem dapat diakses selama 24 jam sehari selama pengguna memiliki akses Internet.
3. PKL Messenger
   Kebutuhan Fungsional :
   a) Sistem mampu mengambil dan menampilkan data dari database server
   b) Sistem mampu melakukan pemantauan chat setiap petugas PKL
   c) Pengguna dapat Mengunggah dan mengirim data/file ke dalam fitur chat
   Kebutuhan Non-Fungsional :
   a) Minimum OS Android 5.0 (Lollipop)
   b) Sistem aplikasi dan database dilengkapi dengan password
4. SIKOKO
   Kebutuhan Fungsional :
   d) Sistem mampu mengambil dan menampilkan data dari database server

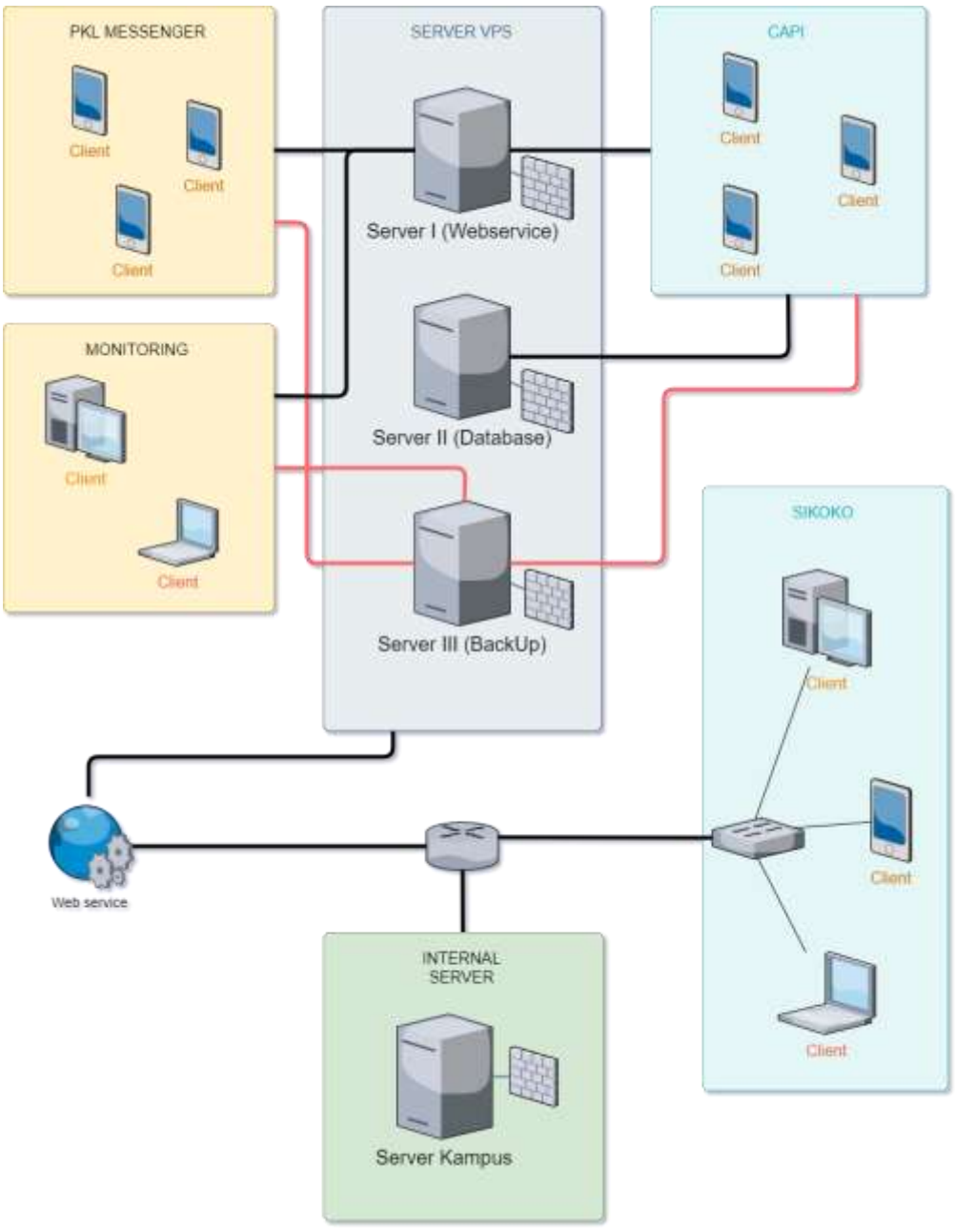
e) Sistem mampu melakukan perizinan CRUD pada pengguna, tergantung dengan status dari pengguna itu sendiri (admin, sekretaris,pubdok, dan anggota[mahasiswa,dosen])
f) Pengguna dapat Mengunggah dan mengirim data/file ke dalam fitur upload/download notulensi

Kebutuhan Non-Fungsional :

a) Sistem dapat dijalankan oleh beberapa software web browser diantaranya Internet Explorer, Google Chrome dan Mozilla Firefox.
b) Sistem aplikasi dan database dilengkapi dengan password
c) Sistem dapat diakses selama 24 jam sehari selama pengguna memiliki akses Internet.

## II. Arsitektur Jaringan

Arsitektur jaringan meliputi gambaran dari server, jaringan, aplikasi, dan teknologi yang dibutuhkan untuk melayani semua kebutuhan sistem. Berikut adalah gambaran arsitektur jaringan pada sistem Praktik Kerja Lapangan.




Gambar 1. Arsitektur jaringan server dan aplikasi

Pada gambar diatas server dibagi menjadi 4 server, dimana 3 diantaranya merupakan server VPS yang disewa dan 1 diantaranya merupakan server internal dari kampus. Pada server I melayani untuk kebutuhan sistem CAPI, PKL Messenger, serta Web Monitoring. Pada server II melayani untuk kebutuhan sistem CAPI saja. Lalu server III melayani segala kebutuhan sistem kecuali untuk sistem SIKOKO. Sistem SIKOKO itu sendiri dilayani kebutuhannya oleh server kampus

## III. Spesifikasi dan Layanan Server

Berikut adalah table spesifikasi dan layanan untuk masing-masing server.

| SERVER I (Webservice) | | |
|---|---|---|
| Spesifikasi | | Layanan |
| Storage | 120 GB | PHP |
| RAM | 6 GB | Ejabberd |
| CPU Core | 6 Core | Apache |
| Operating System | Linux | Node JS |
| SSL | Yes | PHPmyAdmin |

Tabel 1. Spesifikasi dan layanan pada Server I

| SERVER II (Database) | | |
|---|---|---|
| Spesifikasi | | Layanan |
| Storage | 120 GB | Java |
| RAM | 6 GB | Tomcat |
| CPU Core | 6 Core | ODK Aggregate |
| Operating System | Linux | My SQL |

Tabel 2. Spesifikasi dan layanan pada Server II

| SERVER III (BackUp) | | |
|---|---|---|
| Spesifikasi | | Layanan |
| Storage | 160 GB | Server I + Server II |
| RAM | 8 GB | |
| CPU Core | 8 Core | |
| Operating System | Linux | |

Tabel 3. Spesifikasi dan layanan pada Server III

| SERVER Kampus (Internal) | |
|---|---|
| Spesifikasi | Layanan |
| Pada server kampus spesifikasi serta konfigurasi dilakukan oleh pihak kampus.<br>Namun untuk SIKOKO sendiri kebutuhannya adalah dengan terinstallnya php, java, apache, dan database sebagai dasar pembuatan sistem SIKOKO itu sendiri. | |

Tabel 4. Spesifikasi dan layanan pada Server Kampus

## IV. Syarat Kehandalan dan Ketersedian Data

Kehandalan (realibility) pada server adalah suatu kondisi dimana server tersebut dapat bekerja secara optimal. Seperti dapat beroperasi 24jam/hari, tidak mengalami down-time, serta memiliki kompatibilitas tinggi terhadap software dan periferal pendukung eksternal. Dalam pelaksanaan PKL maka server dituntut untuk dapat beroperasi 24 jam nonstop. Hal tersebut dikarenakan kebutuhan dari penggunaan sistem yang padat. Jika terjadi down-time pada salah satu server, maka akan berakibat terhadap sistem yang sedang digunakan. Hilangnya data bisa menjadi hal yang sangat mungkin terjadi. Perlunya ada antisipasi dari server untuk menangani masalah tersebut.

Salah satu solusinya adalah penyediaan backup sever. Server III (Backup) dibuat dengan spesifikasi yang lebih tinggi dari pada kedua server vps lainnya. layanan pada server III juga memiliki semua layanan yang ada pada dua server utama. Hal tersebut dikarenakan server itu akan menjadi backup server yang menanggulangi permasalahan apabila server lainnya mengalami down. Dengan adanya server III ini, diharapkan kebutuhan dari sistem akan tetap terlayani sehingga kita nanti tidak memiliki adanya hambatan pada saat pelaksanaan PKL.

Solusi selain dengan menyediakan backup server adalah dengan melakukan stress test pada server utama. Stress test berguna untuk mengukur daya tahan server terhadap kondisi yang diibaratkan seperti kondisi pada saat di lapangan sesungguhnya. Dengan melakukan stress test, kita dapat mengetahui bagaimana performa dari server tersebut ketika nanti akan dijalankan di lapangan. Tindakan preventif akan bisa kita lakukan apabila kita sudah mendapatkan informasi dari bagaimana performa server tersebut berjalan.

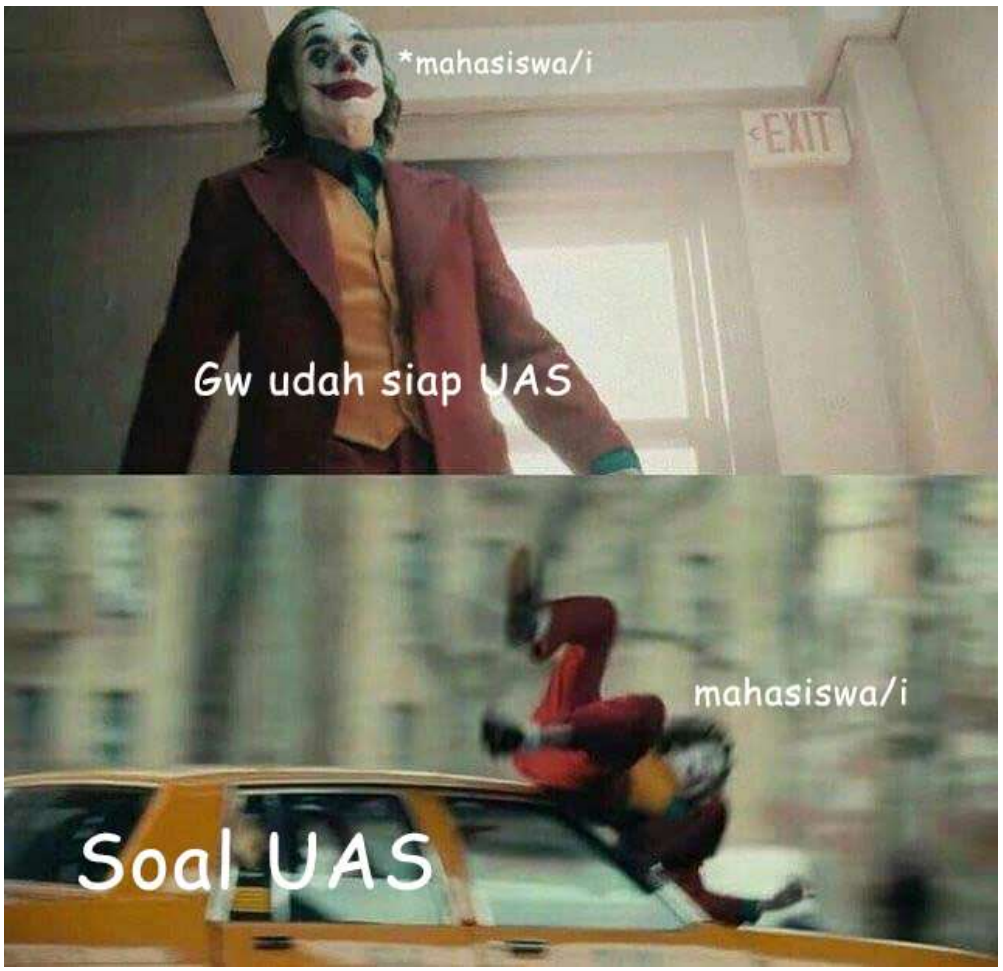
## V. Keamanan Jaringan dan Aplikasi

Keamanan jaringan merupakan aspek penting untuk menjaga validitas dan integritas data serta menjamin ketersediaanlayanan begi penggunanya. Adapun cara untuk dapat menjaga keamanan pada jaringan adalah sebagai berikut.

1. Membatasi Akses ke Jaringan
    a) Membuat tingkatan akses
    Tigkatan akses (CRUD) yang diberikan sesuai dengan akun dari pengguna sistem
    b) Mekanisme kendala akses
    Mengidentifikasi pengguna dengan melakukan aktifitas login menggunakan username dan password. Juga bisa dengan menambah sesi (session) untuk membatasi lamanya idle koneksi.
    c) Sistem otentikasi pengguna
    Melakukan autentikasi pengguna ketika akan melakukan penggantian password. Misalnya dengan memberi pertanyaan “siapa nama ibu kandungmu?”

d) Firewall
Melakukan konfigurasi firewall dengan memilih port mana saja yang dibuka. Bukan malah membuka semua port lalu memilih port mana saja yang ditutup.

2. Mengamankan aset data
   a) Melakukan backup data
   Melakukan backup data agar apabila terjadi kejadian yang tidak diinginkan seperti kehilangan data, kita tetap dapat memiliki data tersebut.
3. Melakukan pengamanan tambahan
   a) menggunakan protokol SSL (https) pada aplikasi web
   b) memakai Intrusion Detection System (IDS)
   Intrusion Detection System (IDS) adalah suatu aplikasi yang memonitor peristiwa yang terjadi pada suatu sistem atau jaringan dan menganalisanya untuk mendapatkan tanda-tanda potensi insiden yang merupakan pelanggaran atau ancaman, mengenai pelanggaran dari kebijakan pengamanan komputer, kebijakan penggunaan yang dapat diterima atau praktek pengamanan standar.
   c) Menggunakan Reverse Proxy
   Reverse proxy adalah perangkat yang ditempatkan antara suatu web server dan klien web server tersebut. Reverse proxy memiliki beberapa fungsi antara lain Encryption Accelerator, Security Gateway, Content Filter, dan Authentication Gateway.



Catatan: