IMPLEMENTASI RASPBERRY PORTABLE SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN NETWORK MONITORING

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Viriyadharma Gopama
140210033

FAKULTAS TEKNIK DAN KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2018

IMPLEMENTASI RASPBERRY PORTABLE SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN NETWORK MONITORING

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Viriyadharma Gopama
140210033

FAKULTAS TEKNIK DAN KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2018

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Viriyadharma Gopama

NPM/NIP : 140210033

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

IMPLEMENTASI RASPBERRY PORTABLE SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN NETWORK MONITORING

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun

Batam, 15 Febuari 2018

Materai 6000

Viriyadharma Gopama

140210033

IMPLEMENTASI RASPBERRY PORTABLE SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN NETWORK MONITORING

Oleh:
Viriyadharma Gopama
140210033

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam, 03 Feb 2018

Cosmas Eko Suharyanto, S.Kom., M.MSI
Pembimbing

ABSTRAK

Teknologi sangat mempengaruhi proses aktivitas atau kinerja untuk organisasi besar seperti PT. LFC Teknologi Indonesia. Dengan bekerja sama dengan perusahaan yang berada di luar negara tentunya dibutuhkan alat bantu komunikasi jarak jauh seperti *e-mail, Cisco WebEx*, *Skype* maupun di *remote* secara langung menggunakan aplikasi *teamviewer*. Dengan alat komunikasi yang ada memerlukan koneksi internet yang stabil dan cepat sehingga proses komunikasi antar perusahaan bisa berjalan lancar. Akan tetapi sering ditemukannya masalah pada saat berkomunisi dengan pelanggan karena koneksi internet yang tidak stabil yang biasanya kita sebut sebagai *packet loss*. Pada saat PT. LFC Teknologi Indonesia baru berjalan mengalami masalah dalam kinerja mereka seperti *data crash,* internet tidak jalan, tidak bisa *sharing file* satu antar lain beserta pernah di retas oleh pihak luar. Penelitian ini dilakukan dengan alat *Raspberry Pi* dengan bantuan aplikasi *Wireshark* untuk memonitoring aktivitas jaringan beserta juga keamanan jaringan dan *Nagios* digunakan untuk memonitoring *user* untuk mengetahui status komputer mereka. Kualitas keamanan jaringan lokal yang berada pada perusahaan pada tahap pertama pelaksanaan penelitian ditemukan banyaknya masalah seperti *broadcasting* dari *switch* itu sendiri sehingga lalu lintas pada jaringan sangat padat, tetapi bagian TI perusahaan sangat bagus dalam mengatasi masalah yang ada pada tahap kedua pelaksanaan penelitian masalah tersebut sudah berkurang. Dari pantauan menggunakan *nagios* dapat dikatakan komputer pada perusahaan dapat dikatakan bagus atau terjaga. Celah cybercrime yang ditemukan pada tahap pertama dapat mengetahui *id* dan *password user* akhirnya diperbaiki oleh TI perusahaan sehingga tidak serang dari luar tidak begitu mudah masuk. Paket *loss, ping* dan *jitter* dalam tahap pertama penelitian ditemukan banyak masalah berhubungan dengan koneksi internet. Pada tahap kedua semua masalah telah diperbaiki oleh bagian TI perusahaan sehingga kinerja perusahaan lebih bagus dari sebelumnya.

Kata Kunci : Keamanan Jaringan, *Nagios, Monitoring, Raspberry, Wireshark*

ABSTRACT

Technology greatly affects the process of activity or performance for large organizations such as PT. LFC Teknologi Indonesia. Working closely with companies outside the country would require remote communications tools such as e-mail, Cisco WebEx, Skype or remote using the teamviewer application. With the existing communication tools require a stable and fast Internet connection so that the communication process between companies can run smoothly. However, the problem is often found when communicating with customers due to unstable internet connection which we usually call as packet loss. At the time of PT. LFC Teknologi Indonesia runs experiencing problems in their performance such as data crashes, the internet is not running, can not share files between one another and have been in retas by outsiders. This research is done with Raspberry Pi tool with the help of Wireshark application to monitor network activity along with network security and Nagios used to monitor user to know their computer status. The quality of the local network security at the company in the first phase of the research implementation found many problems such as broadcasting of the switch itself so that traffic on the network is very solid, but the company's IT department is very good in overcoming the problems that exist in the second phase of research the problem has been reduced . From monitoring using Nagios can be said on the computer company can be said good or awake. The cybercrime gap found in the first stage can find out the user's id and password are finally fixed by the company's IT so that it does not attack from outside is not so easy to enter. Package loss, ping and jitter in the first stage of the study found many problems related to internet connection. In the second stage all the problems have been fixed by the company's IT department so that the company's performance is better than ever.

Keyword : *Network Security, Nagios, Monitoring, Raspberry, Wireshark*

KATA PENGANTAR

Puji dan syukur kepada tuhan yang maha esa yang telah melimpahkan berkat dan rahmat-nya, sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Implementasi *Raspberry Portable* Sebagai Pengukuran Keamanan Jaringan Dan *Network Monitoring*" yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi. Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa dalam penulisan skripsi ini penulis mendapat bantuan dari berbagai pihak, maka dalam kesempatan ini penulis ingin menyampaikan ucapan terima kepada:

1. Ibu Nur Elfi Husda, S.Kom,. M.SI. selaku Rektor Universitas Putera Batam.
2. Bapak Andi Maslan, S.T, M.SI selaku Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Bapak Cosmas Eko Suharyanto, S.Kom., M.MSI selaku pembimbing proposal pada Program Studi Metode Penelitian Teknik Informatika Universitas Putera Batam.
4. Dosen dan staff Universitas Putera Batam yang selama ini sudah memberikan ilmu dan pengetahuan serta bimbingan kepada penulis.
5. Kedua orang tua yang memberikan kasih sayang dan cinta yang tulus serta menjadi tempat curahan hati penulis, atas doa, nasihat, serta dukungan yang mereka berikan.

6. PT. LFC Teknologi Indonesia yang memberikan kesempatan kepada penulis untuk dapat melaksanakan penelitian ini.
7. Teman-teman seperjuangan yang sudah memberikan masukan dan semangat dalam penyusunan skripsi.
8. Serta kepada semua pihak yang tidak dapat disebutkan satu per satu yang telah membantu hingga terselesaikannya skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna mengingat keterbatasan pengetahuan yang penulis peroleh hingga saat ini. Oleh karena itu, penulis mengharapkan kritik dan saran dari para pembaca. Semoga skripsi ini bermanfaat bagi pihak-pihak yang membacanya. Akhir kata, terima kasih.

Batam, Febuari 2018

Viriyadharma Gopama

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer menelusuri awal tahun 1960an. Sudah disepakati secara luas bahwa Internet global saat ini dimulai dari Advanced Research Projects Agency Network (ARPANet) Departemen Pertahanan A.S. pada tahun 1969, berdasarkan konsep yang diterbitkan pada tahun 1967. (Zeng, Gu, & Guo, 2015).

Indonesia merupakan salah satu negara dengan rata-rata *traffic* internet paling tinggi di dunia dalam beberapa tahun terakhir, berdasarkan informasi dari *detik.com* sekitar 38% dari seluruh lalu lintas di dunia berasal dari indonesia. Ini menunjukkan tingkat konektivitas dan penggunaan yang sangat tinggi. Teknologi sangat mempengaruhi proses aktivitas atau kinerja untuk organisasi besar seperti PT. LFC Teknologi Indonesia.

Menurut *Techrepublic.com* pada tahun 2007, sebuah pemadaman komputer di Bandara Internasional Los Angeles menyebabkan 17.000 penumpang berdiri pada penerbangan internasional selama 10 jam. Masalahnya terjadi karena otoritas Bea Cukai AS tidak bisa menyaring penumpang tanpa perangkat lunak. Menurut berita dari Techrepublic.com, cacat jaringan memungkinkan peretas mencuri hampir 46 juta nomor kartu kredit pada tahun 2007 dari TJX, perusahaan induk T.J. Maxx, Marshalls, HomeGoods, A.J. Wright, dan lainnya. Dipercaya bahwa keamanan yang lemah di sekitar LAN nirkabel perusahaan adalah masalahnya.

Menurut csoonline.com awalnya dilaporkan pada awal Oktober oleh blogger keamanan Brian Krebs, butuh beberapa minggu untuk mengetahui skala pelanggaran dan apa yang disertakan. Perusahaan tersebut awalnya melaporkan bahwa peretas telah mencuri hampir 3 juta catatan kartu kredit pelanggan terenkripsi, ditambah data masuk untuk sejumlah akun pengguna yang belum ditentukan.

Kemudian di bulan tersebut, Adobe mengatakan bahwa penyerang telah mengakses ID dan kata sandi terenkripsi untuk 38 juta pengguna aktif. Namun Krebs melaporkan bahwa sebuah file yang diposkan beberapa hari sebelumnya, "tampaknya menyertakan lebih dari 150 juta *username* dan *password hash* yang diambil dari Adobe "Setelah berminggu-minggu penelitian, akhirnya ternyata, begitu juga kode sumber beberapa produk Adobe, hack juga telah membuka nama pelanggan, *ID*, *password* dan informasi debit dan kartu kredit.

Berdasarkan berita dari *csoonline.com* pada bulan September 2016, raksasa internet yang dulu dominan, saat melakukan negosiasi untuk menjual dirinya ke Verizon, mengumumkan bahwa mereka telah menjadi korban pelanggaran data terbesar dalam sejarah, kemungkinan oleh "aktor yang disponsori negara," pada tahun 2014. Serangan tersebut membahayakan nama asli, alamat email, tanggal lahir dan nomor telepon dari 500 juta pengguna. Perusahaan mengatakan "mayoritas besar" kata kunci yang terlibat telah digabung menggunakan algoritma *bcrypt* yang kuat.

Beberapa bulan kemudian, pada bulan Desember, ia mengubur catatan sebelumnya dengan pengungkapan bahwa sebuah pelanggaran pada tahun 2013,

oleh sekelompok *hacker* yang berbeda telah membahayakan 1 miliar akun. Selain nama, tanggal lahir, alamat email dan kata kunci yang tidak terlindungi dengan baik seperti pada tahun 2014, pertanyaan dan jawaban keamanan juga dikompromikan. Pada bulan Oktober 2017, Yahoo merevisi perkiraan tersebut, dengan mengatakan bahwa, pada kenyataannya, semua 3 miliar akun pengguna telah disusupi.

Berdasarkan artikel dari *csoonline.com* Sony's Playstation Network dipandang sebagai pelanggaran data game terburuk yang pernah terjadi sepanjang masa. Dari lebih dari 77 juta akun terpengaruh, 12 juta memiliki nomor kartu kredit yang tidak dienkripsi. Hacker mendapatkan akses ke nama lengkap, kata sandi, *e-mail*, alamat rumah, riwayat pembelian, nomor kartu kredit dan login dan kata kunci *PSN / Qriocity*. "Cukup untuk membuat setiap orang keamanan yang baik bertanya-tanya, 'Jika seperti apa rasanya di Sony, seperti apa di perusahaan multi nasional lainnya yang duduk di jutaan catatan data pengguna?'" Kata John Linkous dari John. Dia mengatakan bahwa pihaknya harus mengingatkan mereka pada keamanan TI untuk mengidentifikasi dan menerapkan kontrol keamanan secara konsisten di seluruh organisasi mereka. Bagi pelanggan, "Hati-hati dengan siapa Anda memberikan data Anda. Mungkin tidak sepadan dengan harga untuk mendapatkan akses ke game online atau aset virtual lainnya."

(Prihantono dan dkk, 2013) *Raspberry* Pi adalah komputer berukuran kartu kredit yang dihubungkan ke TV dan *keyboard* Anda. Ini adalah komputer kecil yang mumpuni yang bisa digunakan dalam proyek elektronik, dan untuk banyak hal yang dilakukan PC *desktop* Anda, seperti *spreadsheet*, pengolah kata, *browsing* internet, dan permainan. Ini juga memainkan video berdefinisi tinggi. Kami ingin

melihatnya digunakan oleh orang dewasa dan anak-anak di seluruh dunia untuk belajar pemrograman dan pembuatan *digital*. Berdasarkan informasi dari *alphr.com* pada Februari 2016, generasi ketiga dari Model B *Raspberry* Pi telah dirilis. Di luar revisi ini, yang *mengupgrade* prosesor utama di papan tulis ke versi 64-bit, tidak ada rencana segera untuk merilis model baru lagi.

PT. LFC Teknologi Indonesia adalah sebuah perusahaan penanaman modal asing yang bergerak pada bidang distribusi, pemeliharaan dan penyedia solusi di bidang metrologi, pemotongan, *laser* dan mesin industri berat. Banyak perusahaan pokok dari berbagai negara seperti Belanda, China, Italia, Jepang, Jepang, beserta Taiwan dan lain-lain bekerja sama dengan PT.LFC Teknologi Indonesia. Dengan bekerja sama dengan perusahaan yang berada di luar negara tentunya dibutuhkan alat bantu komunikasi jarak jauh seperti *e-mail*, *Cisco WebEx*, *Skype* maupun di *remote* secara langung menggunakan aplikasi *teamviewer*. Dengan alat komunikasi yang ada memerlukan koneksi internet yang stabil dan cepat sehingga proses komunikasi antar perusahaan bisa berjalan lancar. Akan tetapi sering ditemukannya masalah pada saat berkomunisi dengan pelanggan karena koneksi internet yang tidak stabil yang biasanya kita sebut sebagai *packet loss*.

Pada tahun 2000-2007 banyak terjadinya kejahatan komputer yang merugikan aktivitas manusia dan dari situlah banyak yang melihat sisi negatif dari perkembangan teknologi, maka dari itu kita membutuhkan Keamanan Jaringan. Keamanan Jaringan sangatlah penting dalam kehidupan keseharian kita. Setiap individu memiliki privasi dan privasi itu akan berbahaya jika diketahui oleh orang lain, misalnya pin kartu kredit maupun KTP. Asal mula kejahatan komputer itu

sendiri berawal dari “iseng”, karena pertama kali kesalahan sesuatu ditemukan karena kesengajaan. Seiring perkembangan waktu rasa ingin tahu akan muncul dan mereka mulai mencoba meretas keamanan sekolah, kantor dan bank.

PT. LFC Teknologi Indonesia juga memiliki masalah yang sama seperti beberapa perusahaan yang ada diatas. Pada saat PT. LFC Teknologi Indonesia baru berjalan mengalami masalah dalam kinerja mereka seperti *data crash,* internet tidak jalan, tidak bisa *sharing file* satu antar lain beserta pernah di retas oleh pihak luar. Maka dari itu mereka membangun TI yang berfungsi dalam mengatasi masalah yang ada pada aktivitas jaringan dalam perusahaan. Untuk dapat memastikan perbaikan yang telah dilakukan oleh bagian TI perusahaan tersebut perusahaan memberikan penelit akses untuk melaksanakan penelitian ini untuk mengukur sejauh mana keamanan jaringan dan *network monitoring* yang telah ada berjalan.

Dalam jaringan data hari ini, analisis lalu lintas - menentukan tautan mana yang semakin padat dan mengapa - biasanya dilakukan oleh komputer di tepi jaringan, yang mencoba menyimpulkan keadaan jaringan dari waktu paket data yang berbeda mencapai tujuan mereka. Layanan pemantauan media telah banyak disebut dari waktu ke waktu, karena pemeran baru memasuki pasar, bentuk baru media diciptakan, dan karena penggunaan baru dari konten yang tersedia dikembangkan. Kelompok yang ada dapat menyediakan layanan pemantauan semacam itu, yang berkaitan dengan tujuan utama mereka, sementara lembaga pemantau umumnya menyediakan seperti bisnis utama mereka. *Packet loss* yang ada pada PT.LFC Indonesia dapat disebabkan juga banyaknya aktivitas yang sedang berjalan dalam jaringan perusahaan pada waktu yang bersamaan. Untuk

memastikan apakah aktivitas yang sedang dalam jaringan perusahan yang menyebabkan terjadinya *packet loss* maka peneliti menggunakan aplikasi *Wireshark* untuk memonitoring aktivitas jaringan yang ada pada PT. LFC Teknologi Indonesia.

Peneliti memakai *Raspberry Pi* karena mengikuti persetujuan dengan PT. LFC, dimana alat peneliti perlu ditinggalkan didalam perusahaan sebagai jaminan untuk memastikan bahwa peneliti tidak melakukan manipulasi data. Beserta *Raspberry Pi* yang peneliti gunakan adalah baru tidak ada cantum tangan dari pihak luar sehingga dapat dipastikan alat yang peneliti pakai bersih dari *virus* ataupun *malware*. Peneliti juga memberikan perusahaan akses untuk memakai atau menggunakan fitur dari alat yang peneliti siapkan sehingga pihak TI perusahaan dapat memperbaiki masalah yang ditemukan.

Sistem pengamanan yang dapat menangani ancaman dari pihak luar melalui jaringan internet menjadi suatu hal yang mutlak dimiliki sebuah perusahaan atau organisasi. Dibalik itu, pengawasan atas pengguna koneksi internet dalam organisasi tersebut juga harus diperhatikan. Akses berlebih yang diberikan kepada pengguna akan mengakibatkan penyimpangan di luar kepentingan organisasi. Dalam hal ini, diperlukan pembatasan hak akses pengguna ke situs berisiko dan yang tidak diperkenankan oleh pihak organisasi. Maka dari kutipan diatas penulis mengangkat judul "**IMPLEMENTASI *RASPBERRY PORTABLE* SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN *NETWORK MONITORING***".

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan diatas, masalah dapat di identifikasikan sebagai berikut:

1. Adanya ancaman berupa usaha untuk mengakes data pada *server* perusahaan yang dilakukan pengamanan berupa *password security*
2. PT. LFC Teknologi Indonesia pernah terjadi *data crash,* internet tidak jalan, tidak dapat *sharing file*.
3. Terdapat banyaknya instasi yang tidak kebal terhadap serangan *cybercrime*
4. Seringnya terjadi paket *loss*, *ping* dan *jitter yang tinggi*

1.3 Pembatasan Masalah

Mengingat banyaknya perkembangan yang bisa ditemukan dalam permasalahan ini, maka penulis membatasi lingkup penelitian sebagai berikut:

1. Hanya berfokus dalam pengukuran keamanan jaringan *LAN/WLAN* tentang *Authentication*, *Privacy* dan *Availability*.
2. Hanya menggunakan aplikasi *Wireshark* dan *Nagios* sebagai alat bantu menganalisis keamanan jaringan dan *network monitoring*.
3. Penelitian ini akan dilakukan PT.LFC Teknologi Indonesia.
4. Aplikasi *Nagios* yang dipakai adalah *Nagios Core* (*Open Source*).
5. *Nagios* hanya menganalisis servis *basic* tiap *host*.

6. Aplikasi *website speedtest.net*

1.4 Rumusan Masalah

Berdasarkan identifikasi masalah yang diatas, maka penulis dapat merumuskan masalah penelitian sebagai berikut:

1. Bagaimana mendeteksi sejauh mana kualitas keamanan jaringan topologi lama pada PT.LFC Teknologi Indonesia secara lokal?
2. Bagaimana kondisi komputer setiap user setelah sejak diterapkan TI untuk perusahaan?
3. Bagaimana kita dapat mendeteksi adanya celah *cybercrime*?
4. Bagaimana kita dapat mengetahui adanya paket *loss*, *ping* dan *jitter yang tinggi?*

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada diatas, maka tujuan penelitian ini adalah:

1. Untuk mengetahui sejauh mana kualitas keamanan jaringan dengan memakai topologi yang sudah ada pada PT.LFC Teknologi Indonesia dalam lokal.
2. Untuk mengetahui apakah masalah komputer yang ada pada *user* yang terjadi sebelumnya akan terjadi lagi
3. Untuk mengetahui cara mendeteksi adanya celah *cybercrime*.

4. Untuk mengetahui cara mendeteksi paket *loss*, *ping* dan *jitter yang tinggi*

1.6 Manfaat/kegunaan

Penelitian yang penulis lakukan ini diharapkan memberikan manfaat secara teoretis maupun praktis.:

1. Manfaat teoritis

   Penelitian memuat ilmu pengetahuan tentang kegunaan fungsi dari menganalisis keamanan jaringan menggunakan *Wireshark* dan *Nagios*

2. Manfaat Praktis

   a) Bagi Lembaga Pendidikan

      Penelitian ini dapat digunakan sebagai masukan untuk pengembangan keamanan jaringan dan network monitoring yang akan datang.

   b) Bagi Kantor/Perusahaan

      Penelitian ini bermanfaat untuk mengetahui betapa bahayanya kejahatan komputer dan kantor/perusahaan akan lebih teliti dalam mengatur keamanan jaringan dan melakukan *network monitoring*.

BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan Komputer

Jaringan komputer adalah sistem yang terdiri dari komputer-komputer, serta piranti-piranti yang saling terhubung sebagai satu kesatuan. Dengan dihubungkannya piranti-piranti tersebut, alhasil dapat saling berbagi sumber daya antar satu piranti dengan piranti lainnya. (Wahana Komputer, 2010: 2). Jaringan komputer merupakan sekumpulan perangkat jaringan yang bisa dihubungkan melalui media transmisi.(Leanna dan Indrarini, 2015).

Jaringan komputer (*computer network*) diartikan sebagai koneksi dua atau lebih komputer yang dihubungkan dengan menggunakan sebuah sistem komunikasi. (Yani, 2009: 1). Dari beberapa sumber para ahli komputer diatas, maka dalam hal ini dapat disimpulkan bahwa jaringan komputer adalah suatu sistem yang saling berkaitan antar piranti satu sama sebagai satu media transmisi.

2.1.1.1. Manfaat Jaringan Komputer

Menurut Yani (2009: 4) Banyak sekali manfaat yang dapat diperoleh dalam suatu jaringan komputer sebagai berikut :

1. Jaringan komputer memungkinkan seseorang dapat mengakses *file* yang dimilikinya (*upload*) atau file orang lain yang telah diizinkan untuk diakses (*download*), di mana pun dan kapan pun
2. Jaringan komputer memungkinkan proses pengiriman data dapat berlangsung cepat dan efisien.
3. Jaringan komputer memungkinkan adanya *sharing hardware* antar-*client*-nya.
4. Jaringan komputer memungkinkan seseorang berhubungan dengan orang lain di berbagai negara dengan berupa teks, gambar, audio, dan video secara *real time*.
5. Jaringan komputer dapat menekan biaya operasional, seperti pemakaian kerta, pengiriman surat atau berkas, telepon serta pembelian *hardware* jaringan

2.1.2 Mengenal Jenis Jaringan Komputer

Jaringan komputer mempunyai berbagai macam tipe yang masing-masing memiliki kelebihan dan kekurangan, yaitu sebagai berikut : berdasarkan ruang lingkup, berdasarkan topologi, dan berdasarkan medium penghantar jaringan. (Wahana Komputer, 2010: 3)

1. **Berdasarkan Ruang Lingkup**

   Ada banyak tipe jaringan komputer, itu juga bisa dibedakan berdasarkam beberapa parameter yang berbeda. Parameter pertama adalah berdasarkan ruang lingkup.(Wahana Komputer, 2010: 3). Menurut Sofana (2012: 108)

Berdasarkan luas areanya maka jaringan komputer dpat dibedakan menjadi :

a. PAN (*Personal Area Network*)

   PAN merupakan jaringan komputer yang diebntuk ole beberapa buah komputer atau antara komputer dengan peralatan non-komputer (seperti: printer, mesin fax, telepon seluler, *PDA*, *handphone*) (Wahana Komputer, 2010: 3).

b. LAN (*Local Area Network*)

   Local area network adalah sebuah jaringan komputer yang cakupan areanya kecil, seperti di sebuah rumah, kantor, atau sekolah. Karakteristik khusus dari LAN yang membedakannya dengan jaringan WAN adalah transfer data yang lebih besar, cakupan area geografis yang lebih sempit, dan tidak perlunya jalur komunikasi *leased line*.(Sofana, 2012: 111)

c. MAN (*Metropolitan Area Network*)

   MAN merupakan jaringan komputer yang meliputi area seukuran kota atau gabungan beberapa *LAN* yang dihubungkan menjadi sebuah jaringan besar. (Sofana, 2012: 111)

d. WAN (*Wide Area Network*)

   WAN merupakan manakala beberapa *LAN* dihubungkan dengan media komunikasi publik atau media lainnya, seperti jaringan telepon dan melibatkan area geografis yang cukup besar, seperti antarnegara antarbenua, maka model jaringan berskala besar (Sofana, 2012: 111)

2. Berdasarkan Topologi

Menurut Wahana Komputer (2010: 5). Selain berdasarkan ruang lingkup, jaringan juga bisa dikelompokkan berdasarkan topologi. Paling tidak ada

beberapa jenis jaringan yang dikelompokkan berdasarkan topologi, sebagai berikut:

a. Topologi Bus

Topologi Bus merupakan arsitektur jaringan di mana *client-client* yang ada di jaringan dihubungkan melalui line komunikasi yang ter-*share* yang disebut bus. Jaringan tipe Bus ini merupakan metode yang paling sederhana untuk menghubungkan banyak *client*. (Wahana Komputer, 2010: 5).

b. Topologi Star

Topologi Star merupakan topologi yang paling lazim digunakan di jaringan komputer. Topologi star memiliki satu pusat berupa *switch*, hub atau komputer yang berfungsi sebagai pusat untuk mentransmisi data. Topologi star ini mengurangi kegaglan jaringan karena semua jaringan dihubungkan ke bagian pusat. (Wahana Komputer, 2010: 6).

c. Topologi Ring

Jaringan dengan topologi Ring adalah jaringan dimana tiap simpul terhubung ke 2 *node* lainnya. Dengan demikian, topografi jaringan mirip dengan lingkaran di mana simpul-simpul jaringan ada di sekelilingnya. (Wahana Komputer, 2010: 6).

3. Berdasarkan Medium Penghantar Jaringan

Pembagian jaringan tipe ketiga adalah berdasarkan medium penghantar jaringan. Secara garis besar, medium penghantar jaringan bisa dibagi

menjadi 2, yaitu kabel/*wire* dan nirkabel/*wireless*. (Wahana Komputer, 2010: 7).

a. Kabel membentuk jaringan berkabel atau sering disebut *wired network*. Jaringan kabel dan nirkabel masing-masin memiliki keuntungan dan kerugian. Anda dapat memilih antara keduanya tergantung kepada kebutuhan. (Wahana Komputer, 2010: 8).

   Jaringan kabel memiliki kelebihan dalam aspek keamanan, dan transfer data yang lebih cepat. Sehingga dengan demikian, Anda bisa mentransfer data lebih cepat dalam waktu yang lebih singkat jika dibandingkan dengan *wireless*. Selain itu, jaringan kabel juga cenderung lebih murah untuk membangun *LAN* sederhana. Namun, jika jumlah komputer sangat banyak, jaringan berkabel justru lebih mahal dibandingkan jaringan *wireless*. (Wahana Komputer, 2010: 8).

b. Jenis jaringan komputer kedua adalah nirkabel atau sering disebut *wireless*. Jaringan *wireless* adalah jaringan yang lebih mudah dibuat seta perawatannya tidak mahal. Jika jumlah komputer banyak, jaringan *wireless* ini lebih murah jika dibandingkan jaringan kabel. Tidak adanya kabel digantikan dengan gelombang radio. (Wahana Komputer, 2010: 8).

4. Berdasarkan Fungsi

Menurut Sofana (2012: 110) Berdasarkan pola pengoperasian atau fungsi masing-masing komputer maka jaringan komputer dapat dibagi menjadi :

a. *Peer to Peer*

Peer to Peer adalah jenis jaringan komputer di mana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan *access* dari/ke komputer lain. *Peer to Peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan pada MAN, WAN, atau Internet, namum hal ini kurang lazim. Cukup sulit mengawasi *security* pada jaringan *peer to peer* manakala pengguna jaringan komputer sudah sangat banyak. (Sofana, 2012: 110)

b. *Client Server*

Client server adalah jaringan komputer yang salah satu (boleh lebih) komputernya difungsikan sebagai *server* untuk melayani komputer lain. Komputer yang dilayani oleh server disebut *client*. Layanan yang diberikan bisa berupa akses *Web*, *e-mail*, *file*, atau yang lain. *Client Server* banyak dipakai oleh Internet dan Intranet (Sofana, 2012: 110)

2.1.3 Standar Jaringan Komputer

1. *Internasional Standards Organization* (ISO)

Organisasi Standar Internasional (ISO, juga disebut sebagai *International Organization for Standardization*) adalah badan multinasional yang keanggotaannya diambil terutama dari komite pembuatan standar dari berbagai pemerintah di seluruh dunia. Dibuat pada tahun 1947, ISO adalah organisasi sukarela yang sepenuhnya didedikasikan untuk kesepakatan

internasional mengenai standar internasional. Dengan keanggotaan yang saat ini mencakup badan perwakilan dari banyak negara industri, ini bertujuan untuk memfasilitasi pertukaran barang dan jasa internasional dengan menyediakan model untuk kompatibilitas, peningkatan kualitas, peningkatan produktivitas, dan penurunan harga. ISO aktif dalam mengembangkan kerjasama di bidang kegiatan ilmiah, teknologi, dan ekonomi. Yang menjadi perhatian utama buku ini adalah upaya ISO di bidang teknologi informasi, yang menghasilkan pembuatan model *Open System Interconnection* (OSI) untuk komunikasi jaringan. Amerika Serikat diwakili dalam ISO oleh ANSI.

2. ***Internasional Telecommunications Union-Telecommunications Standarts Sector* (ITU-T)**

   Pada awal 1970-an, sejumlah negara mendefinisikan standar nasional untuk telekomunikasi, namun masih ada sedikit kecocokan internasional. Perserikatan Bangsa-Bangsa menanggapi dengan membentuk, sebagai bagian dari *International Telecommunications Union* (ITU), sebuah komite, Komite Konsultatif untuk Telegraf dan *Telephony Internasional* (CCITT). Panitia ini dikhususkan untuk penelitian dan penetapan standar telekomunikasi pada umumnya dan sistem telepon dan data pada khususnya. Pada tanggal 1 Maret 1993, nama komite ini diubah menjadi *International Telecommunications Union-Telecommunications Standards Sector* (ITU-T)

3. *American National Standards Insitute* (ANSI)

Meskipun namanya, *American National Standards Institute* (ANSI) adalah perusahaan nirlaba pribadi yang sepenuhnya tidak berafiliasi dengan pemerintah federal A.S. Namun, semua aktivitas ANSI dilakukan dengan kesejahteraan Amerika Serikat dan warganya yang paling penting. Tujuan ANSI yang diungkapkan termasuk melayani sebagai lembaga koordinasi nasional untuk standarisasi sukarela di Amerika Serikat, melanjutkan penerapan standar sebagai cara untuk memajukan ekonomi A.S., dan memastikan partisipasi dan perlindungan kepentingan publik. Anggota ANSI meliputi masyarakat profesional, asosiasi industri, badan pemerintah dan peraturan, dan kelompok konsumen.

4. *Institute of Electrical and Electronic Engineers* (IEEE)

Institute of Electrical and Electronics Engineers (IEEE) adalah masyarakat teknik profesional terbesar di dunia. Internasional dalam lingkupnya, ini bertujuan untuk memajukan teori, kreativitas, dan kualitas produk di bidang teknik elektro, elektronika, dan radio serta di semua cabang teknik terkait. Sebagai salah satu tujuannya, IEEE mengawasi pengembangan dan penerapan standar internasional untuk komputasi dan komunikasi

5. *Electronic Industries Associations* (EIA)

Sejalan dengan ANSI, *Electronic Industries Association* (EIA) adalah sebuah organisasi nirlaba yang ditujukan untuk mempromosikan masalah manufaktur elektronik. Kegiatannya meliputi pendidikan kesadaran

masyarakat dan upaya pelobi disamping pengembangan standar. Di bidang teknologi informasi, AMDAL telah memberikan kontribusi signifikan dengan menentukan antarmuka koneksi fisik dan spesifikasi sinyal elektronik untuk komunikasi data.

6. ***World Wide Web Consortium*** **(W3C)**

   Tim Berners-Lee mendirikan konsorsium ini di Massachusetts Institut Teknologi Teknologi untuk Ilmu Komputer. Ini didirikan untuk memberikan kemampuan komputasi dalam industri untuk standar baru. W3C telah menciptakan kantor regional di seluruh dunia.

7. ***Open Mobile Alliance*** **(OMA)**

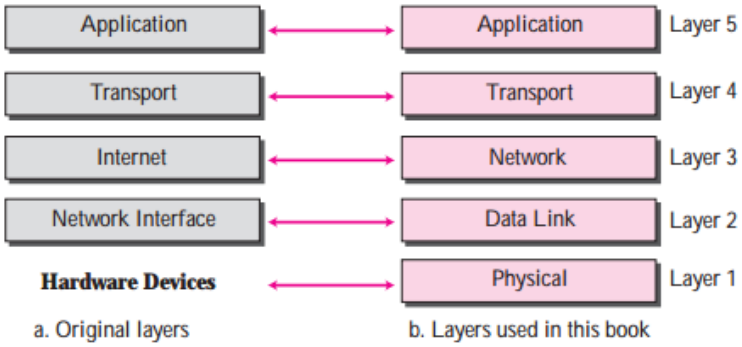
   Organisasi standar OMA diciptakan untuk mengumpulkan berbagai forum dalam jaringan komputer dan teknologi nirkabel di bawah naungan satu otoritas tunggal. Misinya adalah untuk menyediakan standar terpadu untuk protokol aplikasi

2.1.4 Arsitiketur Protokol

Menurut Forouzan (2010:28) Protokol TCP / IP dikembangkan sebelum model OSI. Oleh karena itu, lapisan dalam paket protokol TCP / IP tidak sesuai persis dengan model OSI.

Suite protokol TCP / IP asli didefinisikan sebagai empat lapisan perangkat lunak yang dibangun di atas perangkat keras. Hari ini, bagaimanapun, TCP / IP

dianggap sebagai model lima lapisan dengan lapisan yang dinamai serupa dengan model OSI. Gambar 2.1 menunjukkan kedua konfigurasi. (Forouzan, 2010:28)



Gambar 2.1 Lapisan di protokol TCP / IP Protocol

Sumber (Forouzan, 2010:29)

1. ***Process/ Application Layer***

   Sesuai namanya, lapisan ini mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Cukup banyak protocol yang telah dikembangkan pada lapisan ini. Contohnya adalah SMTP (*Simple Mail Transfer Protocol*) untuk pengiriman *electronic mail*, FTP (*File Transfer Protocol*) untuk transfer file, HTTP (*Hyper Text Transfer Protocol*) untuk aplikasi berbasis *Web* atau WWW (*World Wide Web*), NNTP (*Network News Transfer Protocol*) untuk distribusi news group dan sebagainya. (Sofana, 2012: 110)

2. ***Host-to-Host Layer / Transport Layer***

   Menurut Sofana (2012: 110) pada lapisan ini mendefinisikan cara-cara untuk melakuksan pengiriman data anatara *end to end host.* Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima akan sama

dengan informasi yang dikirim oleh pengirim. Lapisan ini juga memiliki beberapa fungsi penting antara lain:

a. *Flow Control*.

Pengirim data yang telah dipecah menjadi paket-paket data harus diatur sedemikian rupa agar pengirim tidak sampai mengirimkan daa dengan kecepatan yang melebihi kemampuan penerima dalam menerima data. (Sofana, 2012: 110)

b. *Error Detection*.

Pengirim dan penerima juga melengkapi memeriksa apakah data yang dikirimkan telah bebas dari kesalahan. Jika ditemuka kesalahan pada paket yang mengandung kesalahan tadi. Dengan demikian, data dijamin bebas dari kesalahan (error free) pada saat diteruskan ke lapisan aplikasi. (Sofana, 2012: 110)

3. *Internet Layer*

Menurut Sofana 2012: 110 pada laposan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya. Lapisan ini memiliki peran penting terutam dalam mewujudkan *internetworking* yang meliputi wilayah luas (*worldwide Internet*). Beberapa tugas penting pada lapisan ini adalah:

a. ***Addressing***, yakni melengkapi setiap paket data dengan alamat Internet atau yang dikenal dengan *Internet Protocol address* (IP *address*). Karena pengalamatan (addressing) berada pada level ini, maka jaringan TCP/IP- independen dari jenis media, sistem operasi, dan komputer yang digunakan.

b. ***Routing***, yakni menetukan rute ke mana paket data akan dikirim agar mencapai tujuan yang diinginkan. *Routing* merupakan fungsi penting dari *Internet Protocol* (IP). Proses *routing* sepenuhnya ditentuukan oleh jaringan. Pengirim tidak memiliki kendali terhadap paket yang dikirimkannya. *Router-router* pada jaringan TCP/IP-lah yang menentukan penyampaian paket data dari pengirim ke penerima.

4. ***Network Access layer / Link Layer***

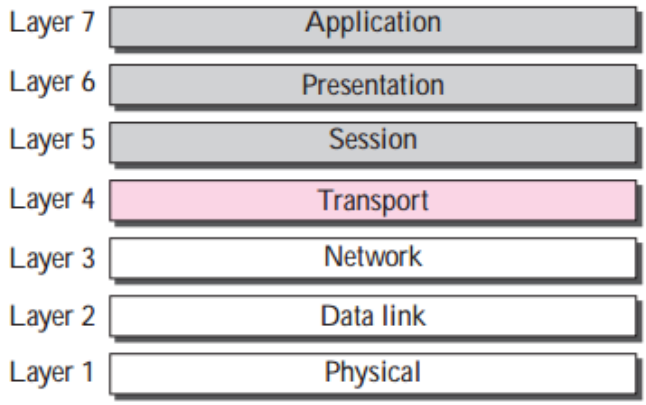
Pada lapisan ini, didefisinikan bagaimana penyaluran data dalam bentuk frame-frame data pada media fisik yang digunakan secara andal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberpa contoh protokol yang digunakan pada lapisan ini adalah X.25 untuk jaringan public, *Ethernet* untuk jaringan *Ethernet*, dan sebagainya. (Sofana, 2012: 110)

2.1.5 OSI (*Open Systems Interconnection*) Model

Menurut Forouzan (2010:20) Didirikan pada tahun 1947, *International Standards Organization* (ISO) adalah badan multinasional yang didedikasikan untuk kesepakatan internasional mengenai standar internasional. Hampir tiga perempat negara di dunia terwakili dalam ISO. Standar ISO yang mencakup semua aspek komunikasi jaringan adalah model *Open System Interconnection* (OSI). Ini pertama kali diperkenalkan pada akhir 1970-an. ISO adalah organisasi dn OSI adalah model system tersebut.

Sebuah Sistem terbuka adalah seperangkat protokol yang memungkinkan dua sistem yang berbeda untuk berkomunikasi terlepas dari arsitektur dasarnya. Tujuan dari model OSI adalah untuk menunjukkan bagaimana memfasilitasi komunikasi antara sistem yang berbeda tanpa memerlukan perubahan pada logika perangkat keras dan perangkat lunak yang mendasarinya. Model OSI bukanlah sebuah protokol; Ini adalah model untuk memahami dan merancang arsitektur jaringan yang fleksibel, kokoh, dan dapat dioperasikan. Model OSI dimaksudkan untuk menjadi dasar pembuatan protokol di tumpukan OSI. (Forouzan, 2010:21)

Model OSI adalah *framework* berlapis untuk perancangan sistem jaringan yang memungkinkan komunikasi antar semua jenis sistem komputer. Ini terdiri dari tujuh lapisan yang terpisah namun saling terkait, yang masing-masing mendefinisikan bagian dari proses pemindahan informasi di seluruh jaringan (lihat Gambar 2.2). Memahami dasar-dasar model OSI memberikan dasar yang kuat untuk mengeksplorasi komunikasi data. (Forouzan, 2010:21)



Gambar 2.2 OSI Model

Sumber (Forouzan, 2010:21)

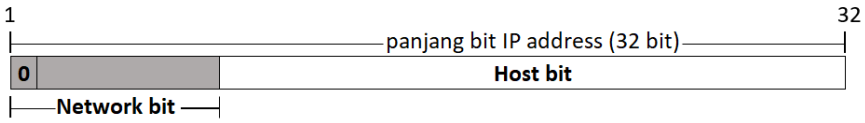
2.1.6 *Internet Protocol* (IP)

Salah satu topik terpenting dalam pembahasan TCP / IP adalah pengalamatan IP. Alamat IP adalah pengenal numerik yang diberikan ke setiap mesin pada jaringan IP. Ini menunjuk lokasi spesifik perangkat pada jaringan. (Lammle, 2018:54)

Alamat IP adalah alamat perangkat lunak, bukan alamat perangkat keras-yang terakhir sulit dikodekan pada kartu antarmuka jaringan (NIC) dan digunakan untuk menemukan host di jaringan lokal. Pengalamatan IP dirancang untuk memungkinkan host pada satu jaringan berkomunikasi dengan host pada jaringan yang berbeda terlepas dari jenis LAN yang diikuti oleh host. (Lammle, 2018:54)

Menurut Sofana (2012: 263-265) Berikut ini penjelasan masing-masing kelas IP *address*.

a Kelas A



Gambar 2.3 *IP Address Class* A

Sumber (Sofana, 2012:263)

Bit pertama bernilai 0. Bit ini dan 7 *bit* berikutnya (8 *bit* pertama) merupakan *bit-bit network* (*network bit*) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 24 *bit* terakhir merupakan *bit-bit* untuk host.

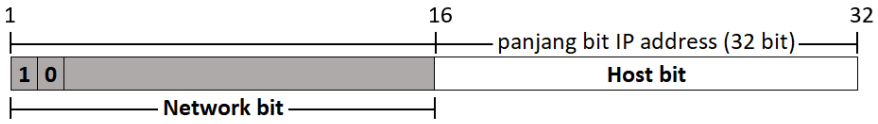
IP address kelas A dapat dituliskan sebagai :

nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

n menyatakan *network*, sedangkan *h* menyatakan *host.*

b Kelas B

Bagan IP address kelas B sebagai berikut:



Gambar 2.4 *IP Address Class* B

Sumber (Sofana, 2012:264)

Dua *bit* pertama bernilai 10. Dua bit ini dan 14 bit berikutnya (16 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kominasi angka 1 dan 0). Sisanya, yaitu 16 *bit* terakhir merupakan *bit-bit host*.

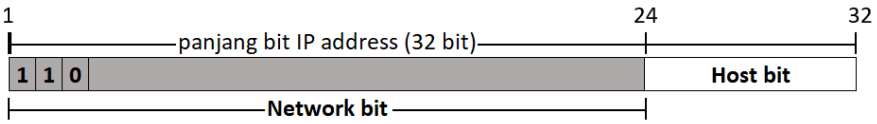
IP addres kelas B dapat dituliskan sebagai:

nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

n menyatakan *network*, sedangkan *h* menyatakan *host.*

c Kelas C

Bagan IP address kelas C sebagai berikut:



Gambar 2.5 *IP Address Class* C

Sumber (Sofana, 2012:264)

Tiga *bit* pertama bernilai 110. Tiga *bit* ini dan 21 *bit* berikutnya (24 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 8 *bit* terakhir merupakan *bit-bit host*.

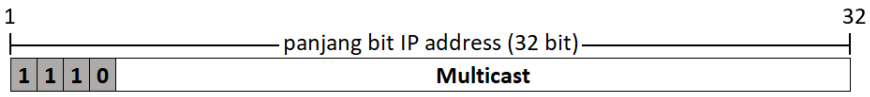
IP *address* kelas C dapat dituliskan sebagai:

nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

n menyatakan *network*, sedangkan *h* menyatakan *host.*

d Kelas D

Bagan IP address kelas D sebagai berikut :



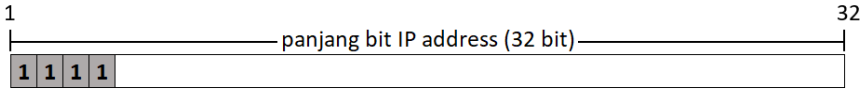
Gambar 2.6 *IP Address Class* D

Sumber (Sofana, 2012:265)

Empat bit pertama bernilai 1110. IP address kelas D merupakan *multicast address*. Salah satu aplikasi yang memanfaatkan *multicast address* adalah *real time video conferencing*. Pada *address* kelas D tidak dikenal *bit-bit nework* dan *host*.

e Kelas E

Bagan IP address kelas DE sebagai berikut:



Gambar 2.7 *IP Address Class* E

Sumber (Sofana, 2012:265)

Empat *bit* pertama adalah 111. IP *address* kelas E dicadangkan untuk kegiatan riset atau eksperimental. Pada IP *address* kelas E juga tidak dikenal *bit-bit network* dan *host*.

2.2 Teori Khusus

2.2.1 Keamanan Jaringan

Keamanan jaringan komputer merupakan isu yang sangat penting, seiring dengan pentingnya informasi yang terkandung pada jaringan. (Anif, 2015:25). Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*,

mempunyai ancaman kemanan lebih besar dari pada komputer yang berdiri sendiri (standalone). (Diansyah, Informatika, Tinggi, & Harapan, 2015:20).

Keamanan Jaringan adalah komponen yang paling vital dalam keamanan informasi karena bertanggung jawab untuk mengamankan semua informasi yang melalui komputer berjejaring. Keamanan Jaringan mengacu pada semua fungsi perangkat keras dan perangkat lunak, karakteristik, fitur, prosedur operasional, akuntabilitas, tindakan, kontrol akses, dan kebijakan administratif dan manajemen yang diperlukan untuk memberikan tingkat perlindungan yang dapat diterima untuk perangkat keras dan perangkat lunak, dan informasi dalam jaringan. Masalah keamanan jaringan dapat dibagi secara kasar menjadi empat bidang yang saling terkait: kerahasiaan, otentikasi, nonrepudiasi, dan kontrol integritas. Kerahasiaan, juga disebut kerahasiaan, berkaitan dengan menjaga informasi dari tangan pengguna yang tidak sah. Inilah yang biasanya terlintas dalam pikiran ketika orang memikirkan keamanan jaringan. (Joshi & Avinash Karkade, 2015:201)

2.2.2.1 Ancaman Terhadap Keamanan

Menurut Ariyus (2008: 8) Terjadinya banyak penukaran informasi setiap detiknya di internet. Juga banyak terjadinya pencurian ata informasi oleh pihak-pihak yang tidak bertanggung jawab. Ancaman keamanan yang terjadi terhadap informasi adalah:

1. *Interruption*: merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data

atau informasi tersebut dibutuhkan maka pemiliknya akan mengalamin kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang.

2. *Interception*: merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer dimana informasi tersebut disimpan
3. *Modification*: merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut.
4. *Fabrication*: merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan informasi sehingga orag yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi.

2.2.2.2 Aspek-aspek Keamanan Komputer

Menurut Ariyus, (2008:9-10) Keamanan komputer meliputi 8 aspek, antara lain:

1. *Authentication*: agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.
2. *Intergrity*: keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.

3. *Non-repudiation*: merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengalak bahwa dialah yang mengirim informasi tersebut.
4. *Authority*: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihan yang tidak berhak untuk mengaksesnya.
5. *Confidentiality*: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
6. *Privacy*: lebih ke arah data-data yang bersifat pribadi.
7. *Availability*: aspek *availabilitas* berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses informasi.
8. *Access Control*: aspek ini berhubungan dengan cara pengaturan akses dengan informasi. Hal ini biasanya berhubugan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan *user id* dan *password* ataupun dengan mekanisme lain

2.2.2 Monitoring

Peran *monitoring* adalah untuk mengenali dan mengevaluasi perkembangan yang terjadi akibat tindakan yaitu mengenali apakah pelaksanaan tindakan sesuai dengan rencana tindakan dan apakah telah terjadi peningkatan dengan adanya tindakan. (Herliana & Rasyid, 2016:41) Manajemen jaringan adalah kemampuan

untuk memonitor, mengontrol, dan merencanakan suatu jaringan komputer dan komponen sistem. *Monitoring* jaringan merupakan bagian dari manajemen jaringan. Hal yang paling mendasar dalam konsep manajemen jaringan adalah tentang adanya manajer atau perangkat yang memanajemen dan agen atau perangkat yang dimanajemen. (Pradikta, Affandi, & Setijadi, 2013:154) Memonitor kejadian yang berkaitan dengan keamanan sangat penting untuk upaya keamanan berkelanjutan. (Stephen R.Davis, 2010:330)

2.3 Tools/software/aplikasi/system

2.3.1 Wireshark

Menurut (Ali & Heriyanto, 2011:296) Wireshark adalah penganalisis protokol jaringan. Keuntungan utama Wireshark dibandingkan dengan *tcpdump* adalah bahwa Wireshark dapat memahami berbagai protokol, tidak hanya TCP / IP. Antarmuka pengguna memungkinkan pengguna memahami informasi yang terdapat dalam paket jaringan yang ditangkap dengan lebih mudah.

Wireshark adalah sebuah aplikasi penyerangan dengan tipe *sniffer*. Wireshark mampu mendeteksi paket yang melintas tanpa melakukan tindakan yang mencurigakan. Wireshark adalah salah satu peralatan serang yang sulit untuk dideteksi oleh sebuah *Intrusion Detection System* (IDS).(Anif et al., 2015:27)

2.3.2 Nagios

Nagios adalah aplikasi *monitoring* sistem dan jaringan yang berbasis *opensource*. Dari hasil *monitoring nagios* tersebut, selanjutnya akan tercatat pada *Nagios Log* dan diolah oleh sistem *Nagios*, sehingga apabila terdapat notifikasi *error* berupa gangguan *service* maupun *host* sistem, maka status akan dikirim ke admin melalui sms *gateway* dan memasukkan status ke *database* untuk diolah lebih lanjut. (Asri, Hamzah, & Sholeh, 2014:152)

Menurut Endah Mardiyani (Amnur, Prayama, & Agustin, 2014:43) *Nagios* adalah aplikasi *monitoring* yang dapat digunakan untuk *monitoring* sistem komputer, *monitoring* jaringan dan monitoring infrastruktur jaringan. Nagios berbasis *opensource* yang dapat dijalankan pada sistem operasi Linux. Sistem monitoring *Nagios* memonitor seluruh infrastruktur IT untuk memastikan sistem, aplikasi, layanan, dan proses bisnis yang berfungsi dengan baik. Jika jaringan mengalami masalah, *Nagios* dapat langsung memberikan *alert* kepada teknisi jaringan sehingga memungkinkan teknisi untuk mengatasi masalah tersebut lebih awal.

2.3.3 *Raspberry*

Menurut (Anif et al., 2015) *Raspberry* Pi 3 adalah komputer mikro indah yang penuh dengan potensi. Papan *Raspberry* Pi 3 sedikit lebih besar daripada Pi Zero W gratis yang disertakan dalam *Starter Kit* Anda. Ini memiliki CPU ARM 1.2GHz

yang lebih cepat, dan RAM sedikit lebih banyak (1GB vs 512MB di Pi Zero W). Ini juga memiliki empat port USB standar, sehingga memudahkan untuk menghubungkan perangkat USB, dan soket *Ethernet*. Terakhir, namun tidak kalah pentingnya, ia memiliki pin GPIO yang disolder ke papan tulis, untuk memudahkan elektronik. (Hattersley, 2016:8)

Namun, dengan baik Raspberry Pi 3 atau Pi Zero W Anda membangun robot, belajar untuk kode, dan menciptakan semua jenis proyek yang aneh dan indah. Peretas dan peminat telah mengubah papan *Raspberry* Pi menjadi stasiun cuaca otomatis, sarang terhubung internet, skateboard bermotor, dan banyak lagi. Batas satunya adalah imajinasi Anda. Membuat proyek dengan *Raspberry* Pi sangat menyenangkan begitu Anda menguasai dasar-dasarnya. Jadi dalam panduan berikut, kami akan membawa Anda dari *newbie* nol ke pahlawan *Raspberry* Pi. Ambil Pi Zero W dan mari kita mulai. (Hattersley, 2016:8)

Raspberry Pi 3 adalah model terbaru, dan versinya dengan fitur terbanyak. Di bagian bawah papan *Raspberry* Pi 3 adalah slot kartu SD. Anda memasukkan kembali sistem operasi ke kartu microSD dan menggunakannya untuk boot Pi *Raspberry*. Pi 3 dan Pi Zero W keduanya memiliki fitur built-in *wireless* LAN dan *Bluetooth*. Ini memungkinkan Anda terhubung ke router nirkabel dan *online* tanpa menggunakan dongle WiFi Menampilkan CPU ARM 1.2GHz *quad-core* (central processing unit) terbaru, Raspberry Pi 3 lebih cepat daripada banyak *smartphone*, dan cukup kuat untuk digunakan sebagai sebuah komputer *desktop*. (Hattersley, 2016:9)

2.4 Penelitian Terdahulu

Berdasarkan dasar atau ancuan teori-teori yang pernah dilaksanakan pada penelitian sebelum menggunakan aplikasi wireshark atau mengabungkan *wireshark* dan aplikasi monitoring lainnya yang lain diperlukan untuk mengubah cara monitoring jaringan dengan cara yang baru untuk diketahui apakah lebih efisien atau lebih lemah dari yang pernah diteliti sebelumnya.

Berikut ini adalah jurnal yang pernah dilakukan untuk penelitian:

1. Pradikta et al. (2013), Vol 2 no 1 dipublikasikan oleh JURNAL TEKNIK POMITS, ISSN: 2337-3539 dengan judul "**Rancang Bangun Aplikasi *Monitoring* Jaringan dengan Menggunakan *Simple Network Management Protocol***". Penelitian ini dilakukan untuk perancangan dan pembuatan aplikasi *monitoring* jaringan yang dapat digunakan sebagai perantara untuk mengambil dan mengolah nilai SNMP sekaligus terdapat sistem penyimpanan atau *database* sehingga dapat ditampilkan laporan informasi tentang kondisi jaringan yang meliputi availability perangkat dan trafik pada transport TCP. Hasilnya Penerapan sistem database pada aplikasi yang dibuat berhasil dilakukan dan nilai *availability* dipengaruhi oleh *Uptime* dan *Downtime* suatu perangkat.
2. Diansyah et al. (2015), Vol. IV No.2 dipublikasikan oleh Jurnal TIMES, ISSN: 2337-3601 dengan judul "**Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan *Wireshark***". Penelitian ini lakukan untuk menganalisis sistem aktivitas illegal didalam jaringan dan juga

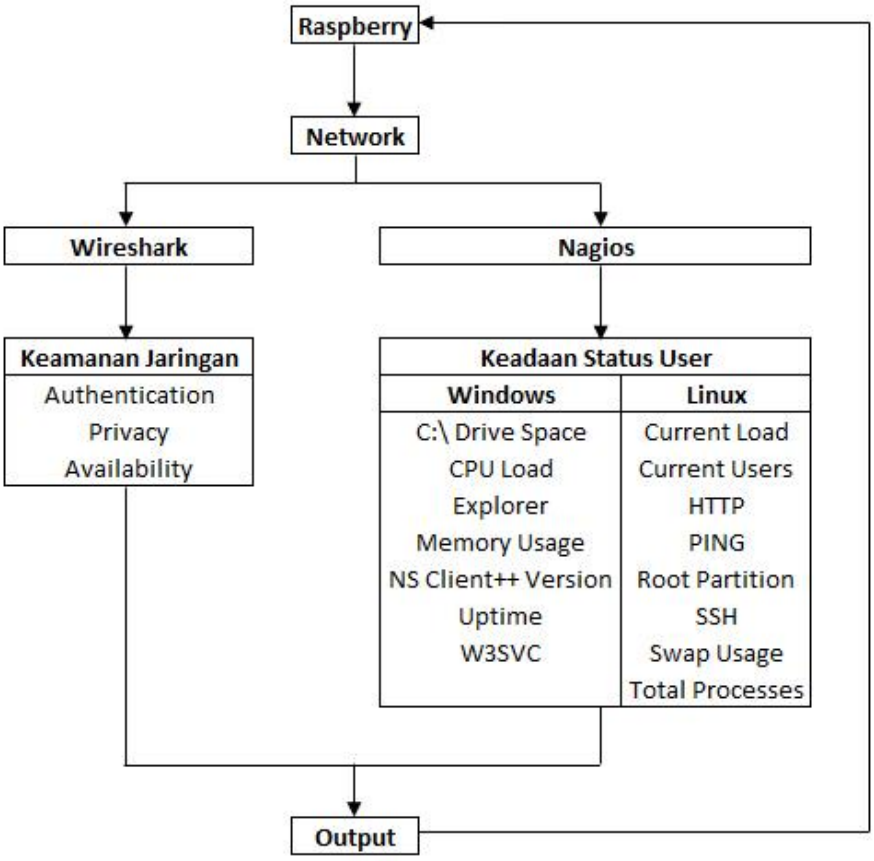
merancang sistem untuk aktivitas illegal. Hasil pengujian ini berhasil dilakukan lebih mudahdengan bantuan dari *tools* wireshark dibandingkan aplikasi lain seperti *forensic tools snort* terhadap informasi sumber, tujual *protocol*, dan waktu *capture*-nya.

3. Anif, Hws, & Huri (2015), Volume 13 No.1 Edisi Maret dipulblikasikan oleh Jurnal TELE, ISSN: 0852-5048 dengan judul "**Penerapan *Intrusion Detection System* (IDS) dengan metode Deteksi *Port Scanning* pada Jaringan Komputer di Politeknik Negeri Semarang**" Penelitian ini bertujuan menciptakan sistem keamanan jaringan komputer yang ringan, berbasis open source, mudah diatur dan dianalisis oleh administrator jaringan dengan bantuan IDS. Dari penelitian ini diketahui bahwa portsentry efektif dalam menangkal serangan port scanning namun tidak mampu memblokir serangan jenis *sniffer*, IP *spoofing* dan *Denial* of *Service* (DoS) karena bersifat tersembunyi dan tidak dianggap sebagai tindakan berbahaya.
4. Pranata, Abdillah, & Ependi, (2015) dalam Student Colloquium Sistem Informasi & Teknik Informatika, ISSN: 2443-2229 dengan judul "**Analisis Keamanan Protokol *Secure Socket Layer* (SSL) Terhadap Proses *Sniffing* di Jaringan**". Penelitian ini dilakukan untuk menganalisis dan uji coba menunjukan pada HTTPS dan HTTP yang menggunakan SSL data dilindungi sebelum dikirim ke tujuan, perbedaanya sebelum menggunakan SSL cara kerjanya langsung mengirimkan data dalam bentuk plaint-text tanpa adanya perlindungan lebih. Hasil penelitian ini

adalah *protocol* SSL merupakan protokol yang aman dari tindakan *sniffing* dan penggunaan protokol SSL pada jaringan juga sangat penting guna mengamankan data di jaringan ini

5. (Sofana, 2012) dengan judul "**Sistem Informasi *Monitoring* Pengembangan *Software* Pada Tahap *Development* Berbasis Web**" Penelitian ini dilakukan membuat sistem pemantauan aktifitas dalam setiap tahapan pengembangan perangkat lunak supaya lebih efektif dan mencegah hambatan yang ada. Hasil penelitian ini kita dapat mengetahui bahwa sistem informasi *monitoring* pengembangan perangkat lunak dapat membantu mendokumentasikan proyek dengan baik sehingga dapat dipantau secara realtime sistem analisi berserta mempermudahkan *programmer* dalam mengambil modul yang akan dikerjakan terlebih dahulu dan tersimpan informasi *monitoring* yang harus diperbaiki dari sistem analis untuk diberikan kepada *programmer*.

2.5 Kerangka Pemikiran



Gambar 2.8. Kerangka Pemikiran

Berikut ini adalah cara kerja kerangka penelitian, sebagai berikut:

1. Kerangka pemikiran ini dimulai dari *input*, *proses* dimana *Raspberry* pi dinyalakan dan terkoneksi dengan jaringan perusahaan.
2. Tahap selanjutnya memulai aplikasi *Wireshark* dan *Nagios* (tahap proses) dan biarkan aplikasi tersebut me-*monitor* jaringan tersebut dan sekitar 1 jam

3. Kemudian lihat *output file* tersebut dan dari *output file* tersebut peneliti dapat mengetahui masalah yang ditemukan dan diperbaiki.

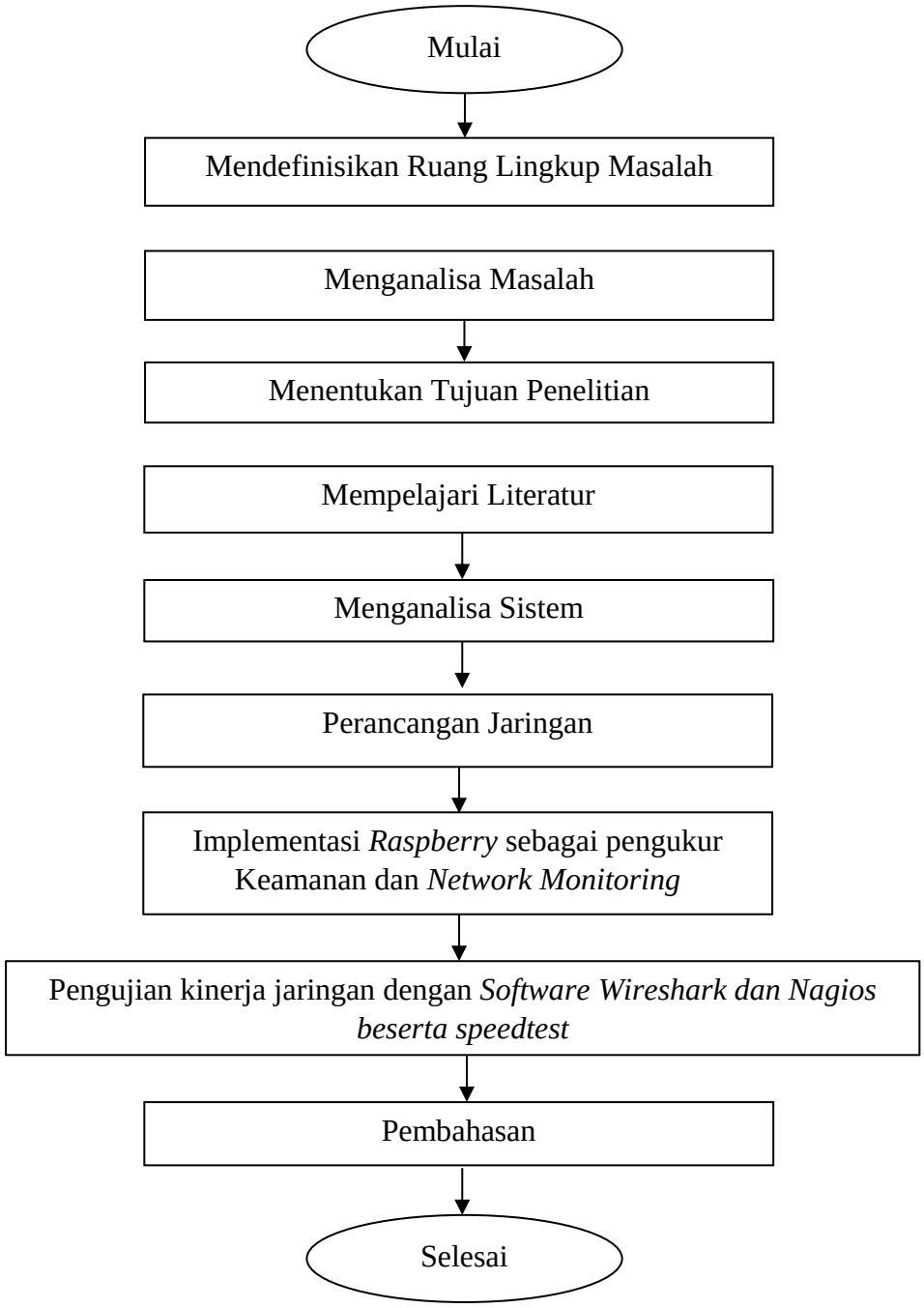
BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Menurut Nachmias & Nachmias sebagaimana disunting oleh Ambraita & Muharto (2016:27) menyatakan bahwa suatu desain penelitian adalah strategi yang memandu dan digunakan peyelidik dalam pengumpulan data, penganalisaan temuan-temuan, dan penginterpretasian data dari mana kemudian digambarkan kesimpulan-kesimpulan. Perbedaan materi proposal penelitian dengan desain penelitian hanyalah karena proposal penelitian dibuat dalam rangka mencari sponsor terutama masalah anggaran, sedangkan desain penelitian dibuat sebagai rancangan, format, pedoman, aturan main, atau acuan penelitian yang akan dikerjakan.

Dalam penelitian ini digunakan penelitian Action research. Action research merupakan penelitian yang bertujuan untuk mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan dan produktifitas lembaga dapat meningkat. (Maturidi, 2012:12). Penelitian tindakan (*action research*) atau disingkat AR ditandai dengan pendekatan *systematic inquiry* yang memiliki ciri, prinsip, pedoman, prosedur yang harus memenuhi kriteria terterntu. Menurut Semiawan dalam kutipan Muhammad & Domopolli (2014:3) Penelitian tindakan harus jelas membedakan perbedaan ciri tindakan dan penelitian, harus terlibat langsung dan bukan hanya sekedar sebagai penonton.

Adapun rancangan penelitian dapat dilihat sebagai berikut:



Gambar 3.1 Desain Penelitian (Sumber: Penelitian 2018)

1. Mendefinisikan Ruang Lingkup Masalah

   Tahap ini untuk menentukan masalah yang terdapat dalam penelitian tersebut, yaitu perusahaan masih mempunyai hambatan dalam jaringan lokal yang sering terjadinya ketidakstabilan dalam manajemen komunikasi sehingga membuat user atau karyawan mengalami kesulitan dalam melakukan kerjanya

2. Menganalisa Masalah

   Setelah tahap mengidentifikasi masalah, tahap berikutnya yaitu menganalisa masalah. Tahap ini untuk mengetahui faktor penyebab masalah. Faktor diantaranya, yaitu belum adanya *software* keamanan jaringan dan monitoring jaringan seperti "*Wireshark*" dan "*Nagios*" server. Sehingga sering terjadi *crash* dan *error* pada jaringan perusahaan.

3. Menentukan Tujuan Penelitian

   Tahap ini merupakan penentuan tujuan dari penelitian yang akan dilakukan terhadap kinerja jaringan di PT. LFC Teknologi Indonesia. Tujuannya yaitu ingin diketahui apakah kinerja jaringan dapat lebih optiomal setelah diimplementasi *Raspberry* dengan bantuan *software Wireshark* dan *Nagios* di PT. LFC Teknologi Indonesia.

4. Mempelajari Literatur

   Tahap selanjutnya yaitu menentukan literatur atau sumber ilmiah yang digunakan dalam penelitian. Sumber literatur diambil dari buku yang membahas tentang jaringan lokal, *Raspberry, Wireshark, Nagios* dan teori-teori lainnya yang mendukung penelitian tersebut.

5. Menganalisa Sistem

   Setelah tahap mempelajari literatur, selanjutnya ialah menganalisa sistem jaringan di PT. LFC Teknologi Indonesia. Diketahui bahwa sistem di perusahaan ialah dengan menggunakan satu modem ZTE F606 sebagai wireless router utama yang disambungan *WAN* port-nya dengan ISP Telkom dan disalurkan jaringan *Wi-Fi* melalui modem tersebut yang terhubung dengan sebuah switch dan 6 buah *personal computer* dan 4 laptop dari *user*.

6. Perancangan Jaringan dan Implementasi

   Setelah menganalisa sistem jaringan, tahap selanjutnya yaitu perancangan jaringan yang akan diimplementasikan. Pada perancangan ini, akan digunakan alat Raspberry dengan software-software yang telah diinstal jika ada masalah maka peneliti harus mencatat / memberitahu kepada pemilik perusahaan tentang apa saja yang perlu dikembangkan kedepannya.

7. Pengujian Kinerja

   Tahap selanjutnya setelah implementasi ialah pengujian kinerja jaringan internet. Pengujian dilakukan dengan menggunakan beberapa *software* seperti *Wireshark* dan *Nagios*. *Wireshark* digunakan untuk menangkap paket-paket yang sedang berjalan dalam jaringan mengetahui apakah adanya serangan dari luar dan mengecek keamanan jaringan lokal. Nagios digunakan untuk memonitoring pengguna yang ada dijaringan untuk mengetahui apakah pengguna terjadi crash pada saat melaksanakan

aktivitas mereka. Menggunakan aplikasi speedtest untuk mengetahui paket *ping* dan *jitter*

8. Pembahasan

   Setelah tahapan pengujian, tahapan terakhir ialah pembahasan mengenai perbedaan antara kinerja jaringan internet sebelum dan sesudah implementasi. Pembahasan tersebut memerlukan data yang valid yang diambil dalam waktu implementasi dan pengujian sistem.

3.2 Analisis Jaringan Lama/ yang sedang berjalan

3.2.1 Analisis Penguna (User)

Analisis user dimaksudkan untuk mengetahui siapa saja user yang terlibat beserta karakteristiknya sehingga dapat diketahui tingkat pengalaman dan pemahaman user terhadap komputer. *User* atau pengguna yang ada di PT. LFC Teknologi Indonesia mempunyai karakteristik user sebagai berikut:

1. *Admin*

Nama	: Noni
Pendidikan Terakhir	: S2
Jabatan	: *Admin*
Pengalaman menggunakan komputer	: 5 Tahun
Sistem operasi yang pernah/sering digunakan	: *Windows 10 Home*
Software yang pernah/sering digunakan	: *Microsoft Office*

2. *Accounting*

Nama	: Valen
Pendidikan terakhir	: S2
Jabatan	: *Accounting*
Pengalaman menggunakan komputer	: 6 Tahun
Sistem operasi yang pernah/sering digunakan	: Windows 7 Pro
Software yang pernah/sering digunakan	: *Quickbook*
	Microsoft Office

3. *Marketing*

Nama	: Atiqa
Pendidikan terakhir	: S2
Jabatan	: Marketing Pro
Pengalaman menggunakan komputer	: 8 tahun
Sistem operasi yang pernah/sering digunakan	: Windows 7
Software yang pernah/sering digunakan	: *Microsoft Office*
	Mailchimp

4. Desain Grafis

Nama	: Panca
Pendidikan terakhir	: S2
Jabatan	: Desain Grafis
Pengalaman menggunakan komputer	: 8 Tahun
Sistem operasi yang pernah/sering digunakan	: *Windows 10 Pro*
Software yang pernah/sering digunakan	: *Adobe Photoshop*

CorelDraw

5. Sales 1

Nama	: Eric Ardrianto
Pendidikan terakhir	: SMA
Jabatan	: Sale
Pengalaman menggunakan komputer	: 4 Tahun
Sistem operasi yang pernah/sering digunakan	: Windows 10 Pro
Software yang pernah/sering digunakan	: *Microsoft Office*
	Odoo

6. Sales 2

Nama	: Nora
Pendidikan terakhir	: S1
Jabatan	: Sale
Pengalaman menggunakan komputer	: 6 Tahun
Sistem operasi yang pernah/sering digunakan	: *Windows 10 Pro*
Software yang pernah/sering digunakan	: *Microsoft Office*
	Odoo

7. Sales 3

Nama	: Rendy
Pendidikan terakhir	: S2
Jabatan	: Sale
Pengalaman menggunakan komputer	: 8 Tahun
Sistem operasi yang pernah/sering digunakan	: *Windows 10 Pro*

Software yang pernah/sering digunakan : *Microsoft Office*

Odoo

3.2.2 Analisis Perangkat Lunak (*Software*)

Secara keseluruhan sistem operasi yang digunakan pada setiap komputer adalah Windows 10 dan perangkat kerja yang digunakan di PT.LFC Teknologi Indonesia antara lain:

1. *Microsoft Office* (perangkat lunak paket aplikasi perkantoran yang dibuat oleh perusahaan perangkat lunak Microsoft Corporation dan dirancang untuk dijalankan di bawah sistem operasi *Microsoft Window*s dan *Mac OS X* perangkat lunak *Office* yang dipakai antara lain adalah
   a) *Word* untuk membuat dan mengedit suatu dokumentasi
   b) *Excel* untuk membuat dan mengedit sebuah laporan
   c) *Powerpoint* untuk membuat dan mengedit presentasi
   d) *Outlook* merupakan program program *personal information manager (*management informasi pribadi) yang bisa dipakai untuk mengirim *e-mail*
2. Quickbook adalah paket perangkat lunak akuntansi yang dikembangkan dan dipasarkan oleh Intuit
3. Mailchip adalah platform otomatisasi pemasaran dan layanan pemasaran email dan nama dagang operatornya

4. Adobe Photoshop adalah perangkat lunak editor citra buatan Adobe Systems yang dikhususkan untuk pengeditan foto/gambar dan pembuatan efek
5. CorelDraw adalah editor grafik vektor yang dikembangkan oleh Corel
6. Odoo adalah perangkat lunak manajemen *all-in-one* yang menawarkan berbagai aplikasi bisnis yang membentuk rangkaian lengkap aplikasi manajemen perusahaan yang menargetkan perusahaan dari semua ukuran

3.2.3 Analisis Perangkat Keras (*Hardware*)

Adapun spesifikasi perangkat keras dari komputer-komputer yang ada di PT.LFC Teknologi Indonesia adalah sebagai berikut:

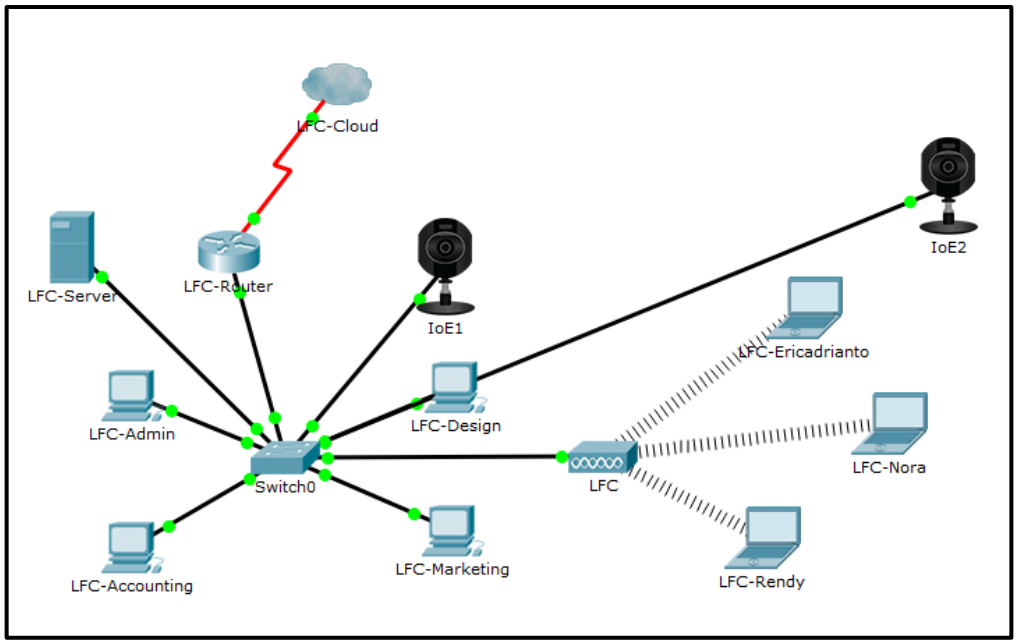
Tabel 3.1 Spesifikasi Perangkat Keras

No	Nama Komputer	Spesifikasi
1	LFC-Admin	*Processor* Intel Core i5 2.67 GHz *Monitor* Dell 14” *Harddisk* 500 GB *Memory* 6 GB *CD Room Drive* *Keyboard* dan Mouse
2	LFC-valen	*Processor* Intel Core i5 3.2 GHz *Monitor* Dell 14” *Harddisk* 500 GB *Memory* 8 GB *CD Room Drive* *Keyboard* dan Mouse
3	LFC-Design	*Processor* Intel Xeon 3.50 GHz

No	Nama Komputer	Spesifikasi
		Monitor Dell 14” *Harddisk* 1 TB *Memory* 32 GB *CD Room Drive* *Keyboard* dan *Mouse*
4	LFC-Marketing	*Processor* Intel Core i5 3.00 GHz *Monitor* Dell 14” *Harddisk* 250 GB *Memory* 4 GB *CD Room Drive* *Keyboard* dan *Mouse*
5	LFC-Ericadrianto	*Processor* Intel Cerelon 2.58 GHz LCD *Monitor* 14” *Harddisk* 500 GB *Memory* 4 GB DVDRW *Keyboard* dan *Mousepad*
6	LFC-Nora	*Processor* Intel i3 2.4 GHz LCD *Monitor* 14” *Harddisk* 500 GB *Memory* 4 GB DVDRW *Keyboard* dan *Mousepad*
7	LFC-Rendy	*Processor* Intel i5 2.2 GHz LCD *Monitor* 14” *Harddisk* 500 GB *Memory* 4 GB DVDRW *Keyboard* dan *Mousepad*

3.2.4 Analisis Topologi Lama/ yang sedang berjalan

Topologi yang sedang berjalan di PT.LFC Teknologi Indonesia menggunakan topologi *Star* yang bentuk susunan topologinya sebagai berikut:

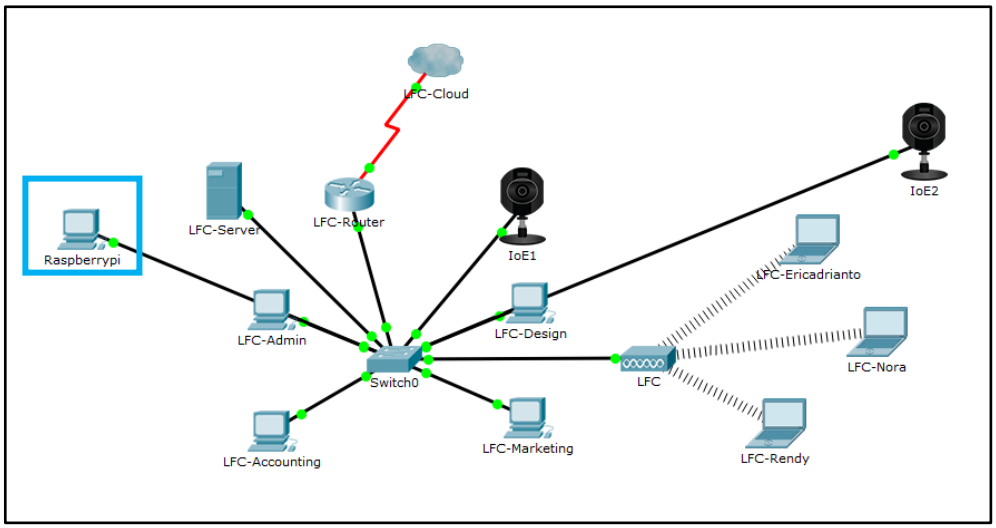


Gambar 3.2 Desain Topologi Lama (Sumber: Penelitian 2018)

Topologi yang telah dibangun di dalam PT.LFC Teknologi Indonesia menggunakan jaringan *LAN* dan memiliki sebuah *switch* dan *router* yang berfungsi untuk mengatur dan mengendalikan keseluruhan sistem fungsi jaringan dan juga bertindak sebagai penguat aliran data. *IP Address* yang digunakan Class C dengan *network* 192.168.100.0/24. Sistem komunikasi antar pengguna menggunakan *client-server*

3.3 Rancangan Jaringan yang Dibangun/Diusulkan

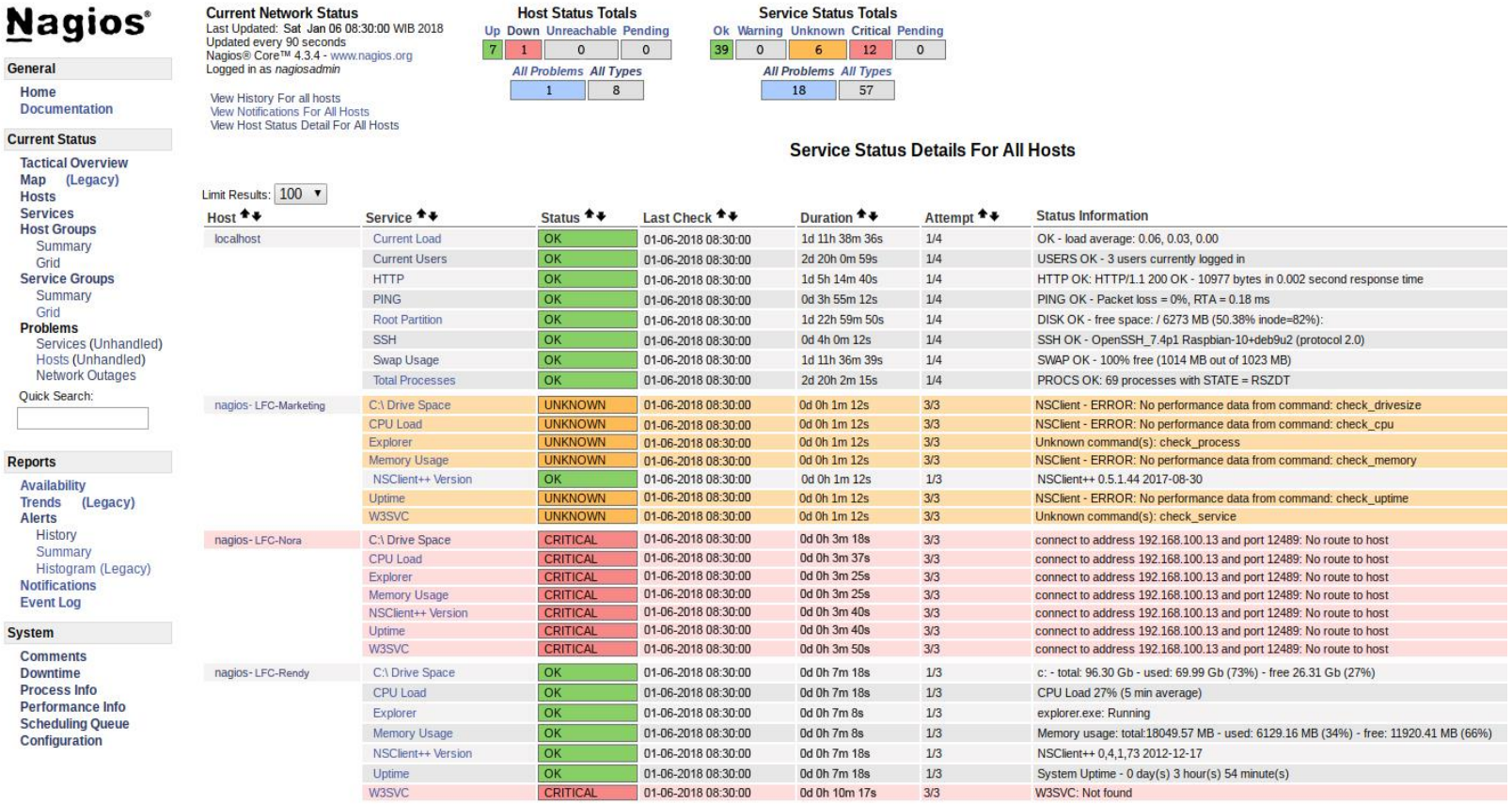
Jaringan yang akan dibangun tidak beda jauh dengan desain topologi lama hanya menambahkan *raspberry pi*, berikut desain topologi yang akan dibangun.



Gambar 3.3 Desain Topologi Baru (Sumber: Penelitian 2018)

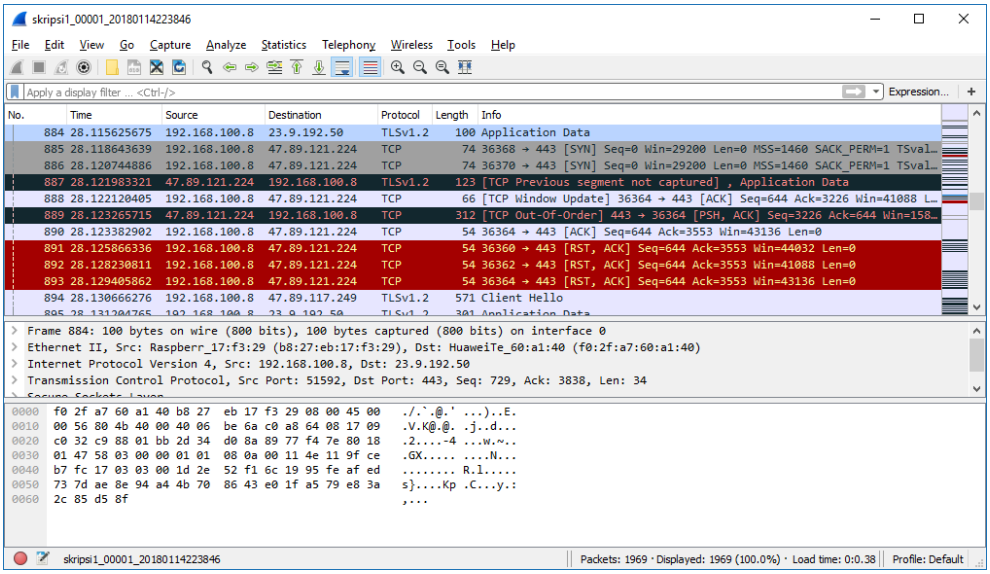
Raspberry pi yang akan di pasangkan di dalam jaringan telah di instal sistem operasi *raspbian* yang sudah berbasis *GUI* (*Graphical User Interface*) dan dalam *raspberry* yang dipakai telah di install aplikasi *Wireshark* dan *Nagios* yang berfungsi untuk menganalisis jaringan dan me-*monitoring* jaringan kemudian memberikan hasil analisis dalam bentuk *log* yang akan diperiksa oleh peneliti lihat apa saja masalah yang ditemukan.

Masalah *monitoring* juga bisa dilihat secara manual dalam *browser* dapat dilihat pada Gambar 3.4. Dapat kita lihat sini semua *service* berwarna merah dikarenakan client tidak terkoneksi dalam jaringan perusahaan sehingga *raspberry* tidak dapat me-*monitoring service* yang ada dalam *pc client* yang sedang berjalan.



Gambar 3.4 Contoh *Monitoring* Dengan Nagios (Sumber Penelitian 2018)

Masalah keamanan jaringan juga bisa dilihat pada Gambar 3.5. Dimana ada terjadinya *TCP RST* and *Bad TCP*. Dimana *TCP* RST terjadi pada saat adanya komunikasi atau gangguan luar pada saat pengiriman data dan Bad TCP dapat disebut juga dengan *loss* terjadi ketika satu atau beberapa paket data yang melintasi jaringan komputer gagal mencapai tujuannya.



Gambar 3.5 Contoh Paket *Wireshark* (Sumber: Penelitian 2018)

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi Penelitian

Penelitian dilakukan di PT. LFC Teknologi Indonesia dan penelitian ini dilakukan untuk mengetahui hasil kinerja jaringan sesudah dan sebelum implementasi *raspberry portable* sebagai pengukuran keamanan jaringan dan *network monitoring*.

3.4.2 Jadwal Penelitian

Jadwal penelitian ini dilakukan selama 5 bulan yang dimulai dari Bulan Sep 2017 – Januari 2018, dengan kegiatan studi kepustakaan, penentuan topik, penentuan judul, pengajuan bab I, pengajuan bab II, pengajuan bab III, penelitian lapangan, pembuatan laporan, pemeriksaan laporan, dan persentase penelitian.

Tabel 3.1 Jadwal Penelitian

(Sumber Penelitian 2018)

No	Kegiatan	Sep 2017				Okt 2017				Nov 2017				Dec 2017				Jan 2018				Feb 2018			
1	Studi Kepustakaan																								
2	Penentuan Topik																								
3	Penentuan Judul																								
4	Pengajuan Bab I																								
5	Pengajuan Bab II																								
6	Pengajuan Bab III																								
7	Penelitian Lapangan																								
8	Pembuatan Laporan																								
9	Pemeriksaan Laporan																								
10	Pengumpulan Penelitian																								