ANALISIS KEAMANAN JARINGAN WIRELESS DI KANTOR KECAMATAN SUNGAI BEDUK TERHADAP PAKET SNIFFING

SKRIPSI

Oleh:
Bayu Febriono
120210169

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2019

ANALISIS KEAMANAN JARINGAN WIRELESS DI KANTOR KECAMATAN SUNGAI BEDUK TERHADAP PAKET SNIFFING

SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh:
Bayu Febriono
120210169

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2019

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 6 Februari 2019
Yang membuat pernyataan,

Bayu Febriono
120210169

ANALISIS KEAMANAN JARINGAN WIRELESS DI KANTOR KECAMATAN SUNGAI BEDUK TERHADAP PAKET SNIFFING

Oleh
Bayu Febriono
120210169

SKRIPSI
Untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal seperti tertera di bawah ini

Batam, 6 Februari 2019

Arif Rahman Hakim, S.Kom., M.Kom.
Pembimbing

ABSTRAK

Kantor Kecamatan Sungai Beduk merupakan salah satu bagian dari Instansi Pemerintah yang bertugas dalam melayani kepentingan masyarakat. Penggunaan jaringan internet digunakan untuk kegiatan administrasi maupun pelayanan publik. Kebutuhan akan jaringan komputer semakin bertambah penting, baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, salah satu hal penting dalam mengelola jaringan komputer yaitu kemanan dari jaringan itu sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut. Dengan adanya pemanfaatan internet tersebut, tentu saja diperlukan keamanan jaringan terutama pada jaringan *nirkabel (wireless)* dikarenakan jaringan *wireless* di Kantor Kecamatan Sungai Beduk dapat diakses oleh semua orang. Selain meningkatnya pelayanan oleh masyarakat, hal-hal yang perlu diantisipasi yaitu serangan terhadap fasilitas internet, salah satunya yaitu serangan *packet sniffing* yang bertujuan untuk mendapatkan informasi yang seharusnya bersifat rahasia. Analisa terhadap jaringan *wireless* di Kantor Kecamatan Sungai Beduk dilakukan dengan cara *penetration testing* dengan menggunakan aplikasi *wireshark*. *Penetration testing* ini dilakukan dengan mengakses jaringan *wireless* yang terbuka, kemudian melakukan *monitoring* menggunakan aplikasi *wireshark*, lalu melakukan *capture* pada lalu lintas data yang memungkinkan untuk mendapatkan informasi terhadap pengguna jaringan *wireless* di Kantor Kecamatan Sungai Beduk.

Kata kunci: Keamanan Jaringan, Jaringan *Wireless*, *Penetration Testing, Wireshark, Packet Sniffing*

ABSTRACT

The Sungai Beduk District Office is one part of the Government Agency in charge of serving the interests of the community. The use of internet networks is used for administrative activities and public services. The need for computer networks is increasingly important, both in education, work and in a game, one of the important things in managing a computer network is the security of the network itself, with so much access to the network there will be many opportunities for crimes that occur within the network , for example, the data theft that occurred in the network or the hackers that shut down the network resources. With the use of the internet, of course network security is needed, especially on wireless networks because wireless networks in the Sungai Beduk District Office can be accessed by everyone. In addition to increasing service by the community, things that need to be anticipated are attacks on internet facilities, one of which is packet sniffing attacks that aim to obtain information that should be confidential. Analysis of wireless networks in the Sungai Beduk District Office is done by means of penetration testing using the Wireshark application. Penetration testing is done by accessing the open wireless network, then monitoring using the Wireshark application, then capturing data traffic that allows to obtain information on wireless network users in the Sungai Beduk District Office.

Key Word: Network Security, Wireless Network, Penetration Testing, Wireshark, Packet Sniffing

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah melimpahkan segala rahmat dan karunia-NYA, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam, Andi Maslan, S.Kom., M.SI.
3. Bapak Arif Rahman Hakim, S.Kom., M.Kom. selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Bapak Muhammad Burhan selaku narasumber yang telah rela meluangkan banyak waktunya untuk mendukung penelitian ini
6. Keluarga yang selalu memberikan doa dan motivasi yang baik
7. Novita Dwi Lestari yang telah memberikan motivasi dan meluangkan waktu untuk mendukung penelitian ini.

8. Rekan-rekan mahasiswa/i Universitas Putera Batam yang turut memberikan doa dan dukungannya
9. Mitra kerja yang selalu memberikan masukan yang berguna untuk penelitian ini
10. Serta pihak-pihak lain yang tidak dapat disebutkan satu per satu.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan taufik dan hidayah-Nya, Amin.

Batam, 6 Februari 2019

Penulis

DAFTAR ISI

HALAMAN SAMPUL DEPAN……..i
HALAMAN JUDUL ……ii
HALAMAN PERNYATAAN ……..iii
HALAMAN PENGESAHAN……iv
ABSTRAK v
ABSTRACT..... vi
KATA PENGANTAR vii
DAFTAR ISI..... ix
DAFTAR GAMBAR xi
DAFTAR TABEL..... xii
DAFTAR LAMPIRAN..... xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Penelitian.....1
1.2 Identifikasi Masalah 4
1.3 Pembatasan Masalah.....4
1.4 Perumusan Masalah.....5
1.5 Tujuan Penelitian.....5
1.6 Manfaat Penelitian.....5
BAB II KAJIAN PUSTAKA 6
2.1 Teori Dasar 6
2.1.1 Jaringan Komputer 6
2.1.2 Standar Jaringan Komputer 28
2.1.3 Jenis Jaringan Komputer 31
2.1.4 Model *OSI Layer* 33
2.2 Teori Khusus.....42
2.2.1 Keamanan jaringan.....42
2.2.2. Wireless.....50
2.2.3. Packet Sniffing 55
2.3 *Software* Pendukung.....56
2.3.1. Wireshark 56
2.4 Penelitian Terdahulu.....57
2.5 Kerangka Pemikiran 59
BAB III METODE PENELITIAN.....61
3.1. Desain Penelitian 61
3.2. Analisis Jaringan Lama/yang Sedang Berjalan 64
BAB IV METODE PENELITIAN 74
4.1 Hasil Penelitian.....74
4.2 Pembahasan 82
BAB V KESIMPULAN DAN SARAN.....85
DAFTAR PUSTAKA 87
DAFTAR RIWAYAT HIDUP.....74

SURAT KETERANGAN PENELITIAN 75
LAMPIRAN 76

DAFTAR GAMBAR

Gambar 2.1 Kabel Coaxial 11
Gambar 2.2 Kabel Fiber Optik 16
Gambar 2.3 Ethernet Card 17
Gambar 2.4 Hub/Switch 18
Gambar 2.5 Repeater 19
Gambar 2.6 Router 20
Gambar 2.7 Topologi Bus 22
Gambar 2.8 Topologi Ring 23
Gambar 2.9 Topologi Star 24
Gambar 2.10 Topologi Daisy Chain 26
Gambar 2.11 Topologi Tree 26
Gambar 2.12 Topologi Mesh 27
Gambar 2.13 Topologi Hybird 28
Gambar 2.14 Logo Wireshark 55
Gambar 2.15 Kerangka Pemikiran 59
Gambar 3.1 Desain Penelitian 61
Gambar 3.2 Topologi Jaringan Kecamatan Sungai Beduk 66
Gambar 4.1 Tampilan Setup Wizard 75
Gambar 4.2 Tampilan Agreement Wireshark 75
Gambar 4.3 Tampilan Install Component 76
Gambar 4.4 Tampilan Install WinPcap 76
Gambar 4.5 Tampilan WinPcap License Agreement 77
Gambar 4.6 Tampilan Setup Finish 77
Gambar 4.7 Tampilan Aplikasi Wireshark 78
Gambar 4.8 Tampilan Capture Interface 78
Gambar 4.9 Tampilan Website 79
Gambar 4.10 Tampilan Monitoring 79
Gambar 4.11 Tampilan Command Prompt 80
Gambar 4.12 Tampilan Proses Filter 81
Gambar 4.13 Hasil Capture Packet Sniffing 81

DAFTAR TABEL

Tabel 2.1 *Layer Data Link*.....36
Tabel 2.2 Tabel Penomoran *IEEE*.....37
Tabel 3.1 Tabel Perangkat Keras (*Hardware)* 64
Tabel 3.2 Jadwal Penelitian.....73

DAFTAR LAMPIRAN

LAMPIRAN I FOTO DOKUMENTASI

BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Kota Batam terletak di Provinsi Kepulauan Riau yang terdiri dari 12 Kecamatan dan 64 Kelurahan. Kecamatan Sungai Beduk merupakan salah satu dari 12 Kecamatan tersebut yang wilayahnya terdiri 4 Kelurahan, yaitu Kelurahan Tanjung Piayu, Kelurahan Duriangkang, Kelurahan Mangsang dan Kelurahan Mukakuning. Kantor Kecamatan Sungai Beduk sebagai Organisasi Perangkat Daerah (OPD) dari Pemerintah Kota Batam yang bertugas dalam melayani masyarakat, dimana terdapat 5 Seksi dan 2 Sub Bagian didalam struktur organisasi, yang terdiri dari Seksi Pelayanan Umum, Seksi Ketentraman dan Ketertiban, Seksi Kesejahteraan Rakyat, Seksi Pembangunan dan Pemberdayaan Masyarakat, Seksi Pemerintahan, Sub Bagian Umum Kepegawaian dan Sub Bagian Program Keuangan dan Evaluasi, yang dikepalai oleh Camat yang dibantu oleh Sekretaris Kecamatan. Pelayanan masyarakat di semua Seksi dan Sub Bagian pada Kantor Kecamatan Sungai Beduk bertujuan untuk memaksimalkan pelayanan terhadap masyarakat. Penggunaan jaringan internet digunakan untuk kegiatan administrasi maupun pelayanan publik.

Kebutuhan akan jaringan komputer semakin bertambah penting , baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, salah satu hal penting dalam mengelola jaringan komputer yaitu kemanan dari jaringan itu

sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut, dsb (Sulaiman, 2016).

Untuk terhubung dengan fasilitas internet, Kantor Kecamatan Sungai Beduk menggunakan jenis jaringan kabel dan *nirkabel (wireless)*. Secara teknis operasional, *Wi-Fi* merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat *WLANs (wireless local area network)* (Jamaludin, 2016).

Untuk memaksimalkan kegiatan administrasi dan pelayanan terhadap masyarakat, Kantor Kecamatan Sungai Beduk menggunakan 23 unit *personal computer (PC),* Seksi Pelayanan Umum menggunakan 6 unit, Seksi Ketentraman dan Ketertiban menggunakan 1 unit, Seksi Kesejahteraan Rakyat menggunakan 2 unit, Seksi Pembangunan dan Pemberdayaan Masyarakat menggunakan 3 unit, Seksi Pemerintahan menggunakan 1 unit, Sub Bagian Umum Kepegawaian menggunakan 2 unit dan untuk Sub Bagian Program Keuangan dan Evaluasi menggunakan sejumlah 8 unit. Seluruh perangkat komputer terhubung dengan satu jaringan internet yang menggunakan *topologi star.* Dalam topologi star, semua kabel dihubungkan dari komputer-komputer ke lokasi pusat *(central location)*, dimana semuanya terhubung ke suatu alat yang dinamakan *hub* (Ervina Jeronimo Guterres, JokoTriyono & Kumalasari Nurnawati, 2014).

Penggunakan jaringan *nirkabel* di Kantor Kecamatan Sungai Beduk dapat digunakan baik oleh karyawan kantor maupun masyarakat umum. Dengan adanya

pemanfaatan internet tersebut, tentu saja diperlukan keamanan jaringan terutama pada jaringan *nirkabel (wireless)* dikarenakan jaringan ini dapat diakses oleh semua orang. Selain meningkatnya pelayanan oleh masyarakat, hal-hal yang perlu diantisipasi yaitu serangan terhadap fasilitas internet yang ada. Salah satu potensi penyerangan keamanan jaringan yaitu packet sniffing. Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer,yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan (Adriant dan Mardianto, 2015).

Kantor Kecamatan Sungai Beduk adalah salah satu Organisasi Perangkat Daerah yang bertugas untuk melayani masyarakat. Untuk memaksimalkan tugasnya, tentu saja diperlukan pemanfaatan teknologi informasi khususnya jaringan internet. Kantor Kecamatan Sungai Beduk memiliki jaringan wireless yang dapat digunakan oleh semua orang (*open public*). Susunan jaringan ini terhubung dengan jaringan internet yang sama dengan jaringan yang digunakan oleh seluruh pegawai yang ada di Kantor Kecamatan Sungai Beduk. Dengan kondisi tersebut, hal ini berpotensi terhadap adanya penyerangan kepada jaringan di Kantor Kecamatan Sungai Beduk, khususnya terhadap pegawai setempat.

Dalam penggunaan jaringan internet, banyak terjadinya tindakan pencurian informasi-informasi pengguna seperti *username* dan *password* dari suatu akun atau data-data penting disebabkan oleh karena tidak adanya perlindungan terhadap aspek *confidentiality* dalam suatu jaringan komputer, hal ini tentunya akan berakibat fatal terhadap pengguna jaringan tersebut (Babys, Kusrini, &

Sudarmawan, 2013). Dari latar belakang di atas, dengan ini penulis bermaksud untuk mengambil judul "**ANALISIS KEAMANAN JARINGAN *WIRELESS* DI KANTOR KECAMATAN SUNGAI BEDUK TERHADAP PAKET *SNIFFING***."

1.2 Identifikasi Masalah

Setelah pemaparan latar belakang di atas, maka adapun identifikasi masalah yang dapat disimpulkan, seperti :

1. Penggunaan jaringan wireless di Kantor Kecamatan Sungai Beduk berpotensi terhadap serangan *packet sniffing*.
2. Perlu adanya evaluasi terhadap jaringan di Kantor Kecamatan Sungai Beduk.

1.3 Pembatasan Masalah

Adapun batasan masalah pada penelitian ini mencakup yakni sebagai berikut :

1. Menganalisa kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk.
2. Melakukan pengujian keamanan jaringan di Kantor Kecamatan Sungai Beduk.

3. Pengujian terhadap Packet Sniffing dilakukan dengan menggunakan metode aplikasi Wireshark.

1.4 Perumusan Masalah

Berdasarkan pembatasan masalah tersebut, penulis merumuskan masalah :

1. Bagaimana menganalisa kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing*?
2. Bagaimana mengevaluasi kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing*?

1.5 Tujuan Penelitian

Adapun penelitian ini dilakukan dengan tujuan sebagai berikut :

1. Untuk menganalisa kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing.*
2. Untuk mengevaluasi kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing.*

1.6 Manfaat Penelitian

Secara spesifik, penelitian ini dilakukan dengan harapan mampu memberikan manfaat baik dari aspek teoritis (keilmuan) maupun aspek praktis (guna laksana). Manfaat tersebut antara lain:

1. Aspek teoritis (keilmuan)

Mengembangkan ilmu pengetahuan tentang keamanan jaringan agar dapat diterapkan dalam kehidupan sehari-hari khususnya dalam menganalisa keamanan jaringan terhadap paket *sniffing.*

2. Aspek praktis (guna laksana)

Memberikan bahan pertimbangan untuk meningkatkan keamanan jaringan khususnya wireless di Kantor Kecamatan Sungai Beduk terhadap serangan paket *sniffing.*

BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

Teori dasar menjelaskan definisi dan hal mendasar mengenai jaringan. Secara umum, teori adalah suatu penalaran yang merupakan gabungan dari definisi dan konsep yang disusun secara sistematis (Sudaryono, 2015). Berikut adalah penjelasan tentang jaringan komputer, standard jaringan komputer, jenis jaringan komputer, model *OSI layer,* keamanan jaringan, *wireless* dan *packet sniffing.*

2.1.1 Jaringan Komputer

Menurut Syafrizal (2012: 2), Jaringan komputer adalah himpunan "interkoneksi" antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel *(wireless)*. Bila sebuah komputer dapat membuat komputer lainnya *restart, shutdown,* atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh). Menurut Anjik Sukmaji & Rianto (2013: 2), pada umumnya jaringan komputer adalah komputer ke satu atau beberapa server yang saling berhubungan. Server

yaitu “pelayan” pengiriman data dan/atau penerima data berupa komputer serta berfungsi mengatur pengiriman dan penerimaan data di antara komputer-komputer yang tersambung.

Menurut Hakim (2017: 24) Internet dari kata *Interconnection Networking* dapat diartikan dengan jaringan yang selalu berhubungan, semakin pesat serta banyak muncul beberapa teknologi untuk menggunakan internet. Kita bisa menikmati berbagai macam fasilitas jika ingin mencari informasi tentang sesuatu. Untuk tersambung pengguna harus menggunakan layanan khusus yang disebut *ISP (Internet Service Provider).* Begitu tersambung ke server *ISP*, user bisa mengakses jaringan internet. Permasalahan yang sering terjadi koneksi internet tersendat bahkan terputus, padahal kita sebagai pengguna menginginkan koneksi internet yang lancar.

2.1.1.1 Manfaat Jaringan Komputer

Menurut Anjik Sukmaji & Rianto (2013: 2), jaringan komputer lebih bermanfaat dibandingkan dengan komputer yang sifatnya berdiri sendiri. Jaringan komputer lebih berguna untuk manajemen sumber daya yang lebih efisien, misalnya :

1. Pengguna Komputer yang menggunakan jaringan komputer dapat berbagi *printer* satu sama lain dengan kualitas tinggi, dibanding menggunakan *printer* yang berkualitas rendah pada masing-masing meja kerja. Disamping itu, lisensi perangkat lunak *(software)* pada jaringan komputer lebih murah

jika dibandingkan dengan lisensi komputer yang berdiri sendiri untuk pengguna yang sama jumlahnya.

2. Jaringan komputer berfungsi untuk membantu dalam mempertahankan informasi agar tetap andal dan *update*. Sistem penyimpanan data yang terpusat serta dikelola dengan baik memungkinkan banyak pengguna untuk malakukan akses data dari lokasi yang berbeda dan hak akses yang bisa diatur secara bertingkat.
3. Jaringan komputer mempercepat proses dalam data *data sharing* antara satu komputer dengan komputer lain. Kecepatan *Transfer* data pada komputer yang menggunakan jaringan, lebih efisien dibandingkan dengan sarana *data sharing* lainnya.
4. Jaringan komputer membantu pengguna dalam berkomunikasi dengan lebih efisien. Substansinya adalah menyampaikan pesan secara elektronik seperti penjadwalan, monitoring proyek, konferensi *online*, *groupware,* dan lain sebagainya yang bertujuan membantu tim untuk bekerja lebih efektif.
5. Jaringan komputer juga berperan serta dalam suatu perusahaan untuk melayani pelanggan dengan lebih efisien.

Menurut Syafrizal (2012: 14-15), tujuan/manfaat jaringan komputer bagi *user* dikelompokan menjadi dua, yaitu jaringan umum dan untuk kebutuhan perusahaan.

1. Tujuan/manfaat jaringan komputer bagi perusahaan :
   a. *Resource sharing*, yang berfungsi untuk mendukung semua program, peralatan, khususnya data, agar bisa digunakan oleh seluruh pengguna pada jaringan komputer tanpa dipengaruhi oleh *resource* dan pemakai.
   b. *High reliability* (keandalan tinggi), diperoleh karena sumber daya alternatif yang tersedia. Apabila salah satu mesin mati, maka *file* tetap dapat diakses dari mesin lain yang masih aktif dikarenakan semua file dapat disalin *(back-up)* ke semua mesin. Selain itu, pada penggunaan *CPU* yang lebih dari satu, maka bila salah satu *CPU* tidak bekerja, maka *CPU* lainnya akan mengambil alih tugas *CPU* yang tidak bekerja, walaupun dapat menyebabkan menurunnya kinerja *CPU* tersebut. Kemampuan melanjutkan pekerjaan saat mendapatkan masalah pada perangkat keras adalah suatu hal yang sangat penting.
   c. *Saving money* (menghemat uang), komputer yang berukuran kecil mempunyai resiko harga/kinerja yang lebih baik jika dibanding dengan komputer besar. Komputer *mainframe* kira-kira memiliki kecepatan 10 kali lipat kecepatan komputer pribadi, tetapi memiliki harga *mainframe* yang 10 kali lebih mahal.
2. Tujuan/manfaat jaringan komputer untuk umum :
   a. Mengakses informasi yang berada di tempat yang berbeda (info *e-commerce*, *e-business* atau *e-government*), semuanya *uptodate.*

b. Komunikasi pengguna ke pengguna lainnya (*person-to-person* seperti *chatting, e-mail, video conference,* dan lain sebagainya).

c. Hiburan interaktif (seperti radio *streaming*, *tv on-line*, *download film* atau lagu dan lain sebagainya).

2.1.1.2 Perangkat Keras (Hardware) Jaringan Komputer

Salah satu bagian dari terbentuknya sebuah jaringan komputer yaitu adalah perangkat keras *(hardware).* Menurut Syafrizal (2012: 21-37), media baik *hardware* maupun *software* dibutuhkan dalam membentuk suatu jaringan baik itu bersifat *LAN (Local Area Network)* maupun *WAN (Wide Area Network)*, membutuhkan beberapa media perangkat keras (*hardware)* yang penting didalam membangun suatu jaringan adalah kabel atau perangkat *ethernet card*, *Wi-Fi*, *repeater*, *hub* atau *switch*, *bridge*, atau *router*, dan lain lain.

1. Kabel

Dalam penggunaan kabel, sebelumnya harus lulus uji kelayakan sebelum nantinya akan dipasarkan dan digunakan. Ada beberapa jenis kabel yang sering digunakan dan menjadi standar dalam jaringan komputer yang penggunaannya untuk komunikasi data. Oleh karena itu dibuatlah pengenalan tipe kabel dikarenakan setiap kabel mempunyai kemampuan dan spesifikasi yang berbeda.. Ada dua jenis kabel yang dikenal secara umum dan sering dipakai untuk *LAN*, yaitu *STP (shielded twisted pair) coaxial* dan *twisted pair (UTP unshielded twisted pair)*.

Gambar 2.1 Kabel Coaxial
(Sumber: http://abi-blog.com/wp-content/uploads/2015/11/Kabel-Coaxial.png)

a. Coaxial Cable

Ada dua jenis tipe kabel *koaksial* yang dipergunakan untuk membuat jaringan komputer, yaitu:

1. *Thick coax* (ukuran diameter yang lumayan besar)
2. *Thin coax* (ukuran diameter yang lebih kecil).

Berikut penjelasan tentang kedua kabel di atas :

1) *Thick coaxial cable* (kabel *koaksial* ”gemuk”)

Spesifikasi kabel *coaxial* jenis ini mengacu pada standar *IEEE 802.3 10BASE5*, kabel jenis ini disebut dengan standard *ethernet* atau *thick ethernet*, atau hanya disingkat *ThickNet*, atau bahkan hanya disebut sebagai *yellow cable* karena berwarna kuning. Kabel ini mempunyai diameter rata-rata 12mm, kabel *Coaxial (RG-6)* ini jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

a) Setiap ujung harus *diterminasi* dengan *terminator* 50 ohm (dianjurkan menggunakan *terminator* yang sudah dirakit, tidak

menggunakan satu buah *resistor* 50 ohm 1 watt, dikarenakan *resistor* mempunyai disipasi tegangan yang lumayan lebar).

b) Maksimal 3 segment dengan aperalatan terhubung *(attached devices)* atau berupa *populated segments.*

c) Setiap kartu jaringan mempunyai pemancar *tambahan (external transceiver).*

d) Setiap segmen maksimum berisi 100 perangkat jaringan , termasuk dalam hal ini *repeaters.*

e) Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).

f) Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter).

g) Setiap segment harus diberi *ground.*

h) Jarak maksimum antara tap atau pencabang dari kabel utama ke perangkat *(device)* adalah 16 feet (sekitar 5 meter).

i) Jarak minimum antara tap adalah 8 feet (sekitar 2,5 meter).

2) *Thin coaxial cable* (kabel koaksial ”kurus”)

Kabel *coaxial* jenis ini tidak memerlukan *output* daya yang besar dan banyak dipergunakan di kalangan radio amatir. Pada jenis ini, yang banyak digunakan adalah *RG8* atau *RG-59* dengan *impedansi* 75 ohm. Tetapi untuk perangkat jaringan, kabel *coaxial* yang digunakan yaitu *(RG-58)* yang telah memenuhi standarisasi *IEEE 802.3 IOBASE2*,

yang berdiameter rata-rata berkisar 5 mm dan biasanya berwarna hitam dan setiap perangkat *(device)* terhubung dengan *BNC T-conn*ector. Kabel ini juga dikenal dengan sebutan *thin Ethernet* atau *leinNet.* Contoh dari kabel jenis ini yaitu *RG-58 A / U* atau *C /U*, jika diimplementasikan dengan *T-connector* dan *terminator* pada sebuah jaringan, harus mengikuti aturan sebagai berikut:

a) Setiap ujung kabel diberi *terminator* 50-ohm.

b) Panjang maksimal kabel adalah 606.8 feet (185 meter) per segment.

c) Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan *(devices)*.

d) Kartu jaringan cukup menggunakan *transceiver* yang *onboard*, tidak perlu tambahan *transceiver*, kecuali untuk *repeater*.

e) Maksimum ada 3 segment terhubung satu sama lain *(populated segment).*

f) Setiap segment sebaiknya dilengkapi 1 *ground.*

g) Panjang minimum antar *T-Connector* adalah 1,5 feet (0.5 meter).

h) Maksimum panjang kabel dalam satu segment adalah 1,818 feet (555 meter).

i) Maksimum setiap segment memiliki 30 perangkat terkoneksi.

b. *Twisted Pair Cable*

Ethernet dapat juga menggunakan jenis kabel lain selain dari kabel koaksial, yakni kabel *UTP (Unshielded Twisted Pair)* dan *Shielded Twisted Pair (STP)*. Kabel *UTP* atau *STP* yang terdiri dari 4 pasang kabel yang terpilin adalah yang paling sering digunakan. Dari 8 buah kabel, hanya 4 buah saja yang digunakan untuk mengirim dan menerima data (*Ethernet)*. Perangkat-perangkat lainnya yang berhubungan dengan penggunaan untuk jenis kabel ini yaitu HUB dan konektor *RJ-45*.

Pemasangan kabel UTP yang sering digunakan pada jaringan lokal terdiri dari dua jenis, ditambah satu jenis pemasangan khusus untuk cisco router, yakni :

1. Pemasangan lurus *(Straight Through Cable)*
2. Pemasangan menyilang *(Cross Over Cable)*
3. Pemasangan rol/melingkar *(Roll Over Cable)*

Berikut akan dijelaskan tentang ketiga kabel di atas :

1) Pemasangan lurus *(Straight Through Cable)*

Penghubungan beberapa unit komputer melalui alat *HUB/Switch* biasanya menggunakan kabel jenis ini, dan berfungsi sebagai *konsentrator* maupun *repeater*. Penggunaan kabel UTP model *straight through* pada jaringan lokal biasanya akan membentuk *topologi star* (bintang) atau *tree* (pohon) dengan *HUB/switch* sebagai pusatnya. Jika sebuaha *HUB/swi*tch tidak berfungsi , maka

seluruh komputer yang terhubung dengan *HUB* tersebut tidak dapat saling berhubungan. Pada masing-masing komputer, kecepatan dari *Ethernet card* yanga digunakan harus disesuaikan dengan penggunaan. Karena perbedaan kecepatan pada *HUB* dan *NIC* berarti kedua perangkat tersebut tidak dapat saling berkomunikasi secara maksimal.

2) Pemasangan menyilang *(Cross Over Cable)*

Penggunaan kabel menyilang ini digunakan untuk komunikasi antara komputer (langsung tanpa *HUB*), berbeda dengan pemasangan kabel lurus *(straight through)*, atau dapat juga digunakan untuka *meng-cascade HUB* jika diperlukan. Untuk saat ini tidak hanya dapat menggunakan kabel lurus, ada beberapa jenis *HUB* yang dapat *di-cascade* tanpa harus menggunakan kabel menyilang *(cross over)*,

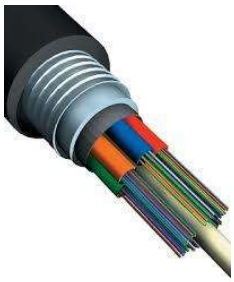
3) Pemasangan rol/melingkar *(Roll Over Cable)*

Ada satu cara lain pemasangan kabel *UTP* yang digunakan untuk menghubungkan sebuah terminal dan modem ke Cisco Router seri 2500 Access Server pada sistem *CISCO*, cara ini disebut dengan *Roll-Over*. Kabel *Roll-Over* tersebut sebelumnya terkoneksi dengan *DB-25 Adapter*. Anda dapat mengenali sebuah kabel *roll-over* dengan melihat kedua ujungan kabel. Warna kabel akan berbalik pada sisi kabel di ujung yang lain, dari sisi yang

satu. Misalnya kabel putih *orange* yang berada pada pin 1 ujung kabel A akan berada pada pin 8 ujung kabel B.

c. *Fiber Optic Cable*

Kabel yang memiliki inti serat kaca sering menggunakan saluran *BACKBONE* sebagai saluran dalam menyalurkan sinyal antar terminal karena kehandalannya yang tinggi dibandingkan dengan kabel *UTP* atau *coaxial cable*. Kabel ini tidak terpengaruh oleh cuaca dan panas.



Gambar 2.2 Kabel Fiber Optik
(Sumber: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQc_lXqWAiuztBhGIpa9pMzrSWvsC_H8lyxWhdptTtuqamrv6KW)

2. *Ethernet Card (Kartu Jaringan Ethernet) / Network Adapter*

Setiap *node* dalam suatu jaringan menerim setiap transmisi data yang dikirima oleh suatu *node* yang lain merupakan cara kerja *Ethernet Card* berdasarkan *broadcast network*, di mana setiap *Ethernet card* mempunyai alamat sepanjang 48 *bit* yang dikenal sebagai *Ethernet address (MAC Address)*. Alamat tersebut dikenal dengan sebutan *Media Access Control (MAC)* atau lebih dikenal dengan istilah *hardware address,* alamat tersebut telah ditanam ke dalam setiap rangkaian kartu jaringan *(NIC)* 24 bit atau 3

byte awal merupakan kode yang telah ditentukan oleh *IEEE*. Kartu jaringan *Ethernet* biasanya dibeli secara terpisah dengan komputer, kecuali *network adapter* yang sudah *onboard*. Komputer *Macintosh* juga sudah mengikutkan kartu jaringan *ethernet* di dalamnya. Kartu jaringan *ethernet model l0 Base* umumnya telah menyediakan *port* koneksi untuk kabel *coaxial* ataupun kabel *twisted pair*. Konektor *BNC* didesain untuk kabel *coaxial*, bila didesain untuk kabel *twisted pair* maka akan punya *port konektor RJ-45*. Beberapa kartu jaringan *ethernet* dikoneksikan dengan coaxial, twisted pair, ataupun dengan kabel *fiber optic* dan ada juga yang menggunakan konektor *AUI*.

Gambar 2.3 Ethernet Card
(Sumber : https://images-na.ssl-images-amazon.com/images/I/41rhUON-GgL.jpg)

3. *Hub dun Switch* (Konsentrator)

Sebuah perangkat yang menyatukan kabel-kabel *network* dari tiap *workstation*, *server* atau perangkat lain merupakan disebut dengan *konsentrator (Hub atau switch)*. Pada topologi bintang, kabela *twisted pair*

datang dari sebuah *workstation* masuk ke dalam *hub* atau *switch*. Sejumlah komputer terhubung dengan *Hub* dan *switch* yang memiliki banyak lubang untuk *port RJ-45,* yang dapat dipasang konektor *RJ-45*. Beberapa jenis hub mampu dipasang hingga 4 susun atau bertingkat *(stackable)*, dan biasanya memiliki jumlah lubang sebanyak 4 buah, 8 buah, 16 buah, hingga 24 buah. Sebagai *konsentrator* yang jika dibandingkan dengan *hub, switch* memiliki kemampuan lebih baik dalam melakukan manajemen *trafic* data. Saat ini telah terdapat banyak tipe *switch* yang *managible* dan dapat mengatur *traffic data* serta dapat diberi *IP Address*.

Gambar 2.4 Hub/Switch
(Sumber : http://www.fiberopticshare.com/wp-content/uploads/2017/09/hub-picture.jpg)

4. Repeater

Memperkuat sinyal dengan cara menerima sinyal dari suatu segmen kabel *LAN* lalu memancarkan kembali dengan kekuatan yang sama dengan sinyal asli pada segmen kabel yang lain merupakan fungsi utama *repeater*. Dengan cara ini jarak antara kabel dapat diperjauh. Penggunaan *repeater* antara dua segmen atau

lebih segmen kabel *LAN* mengharuskan penggunaan protokol *physical laye*r yang sama antara segmen-segmen kebel tersebut, misalnya *repeater* dapat menghubungkan dua buah segmen kabel *Ethernet 10BASE2*.

Gambar 2.5 Repeater
(Sumber : http://www.schoolpouringrights.com/wp-content/uploads/2018/02/Repeater-765x510.jpg)

5. Bridge

bridge memiliki fungsi yang sama dengan *repeater,* yang membedakan adalah tingkat *fleksibel bridge* lebih cerdas daripada *repeater*. Jaringan yang menggunakan metode transmisi yang berbeda, dapat dihubungkan dengan *Bridg*e. Misalnya *bridge* dapat menghubungkan Ethernet baseband dengan *Ethernet broadband.* Dengan mengimplementasikan mekanisme *frame filtering, Bridge* mampu memisahkan sebagian dari trafik. Bridge menggunakan Mekanisme yang umum disebut sebagai *store* and *forward*. Walaupun demikian, *broadcast traffic* yang dibangkitkan dalam *LAN* tidak dapat difilter oleh *bridge*. Terkadang pertumbuhan *network* sangat cepat sehingga diperlukan jembatan untuk keperluan itu. Kebanyakan *bridges* dapat mengetahui masing-masing alamat dari tiap~tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di

sebelahnya pula. Diibaratkan bahwa *bridges*ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi *network* tetap dapat berjalan dengan baik dan teratur. *Bridges* juga dapat digunakan untuk mengkoneksikan *network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula. B*ridges* dapat mengetahui alamat masing-masing komputer di masing-masing sisi jaringan.

6. Router

Router memiliki tugas yang sama dengan *bridge*. Sebuah *router* bertugas untuk mengirimkan data/informasi yang berasal dari satu jaringan menuju jaringan lain yang berbeda. Meskipun dapat dikatan tidak lebih pintar jika dibandingkan dengan *bridge*, namun pengembangannya dewasa ini sudah mulai mencapai bahkan melampaui batas tuntutan teknologi yang diharapkan.

Gambar 2.6 Router
(Sumber : https://images-na.ssl-images-amazon.com/images/I/51o7VZ6KCML._SL1350_.jpg)

2.1.1.3 Topologi Jaringan

Menurut Syafrizal (2012: 39-44), topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antar komputer dalam *Local Area Network* yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, *Ethernet card*, dan perangkat pendukung lainnya.

Ada beberapa jenis topologi yang terdapat pada hubungan komputer pada jaringan lokal area, seperti :

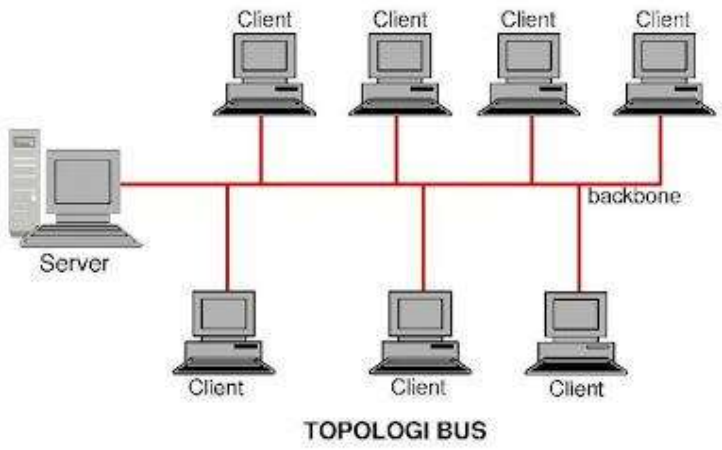
1. Topologi Bus

Topologi ini merupakan bentangan satu kabel yang kedua ujungnya ditutup, di mana di sepanjang kabel terdapat node-node. Signal dalam kabel dengan topologi ini dilewati satu arah sehingga memungkinkan sebuah *collision* terjadi. Adapun keuntungannya adalah sebagai berikut :

a. Murah, karena tidak memakai banyak media dan kabel yang dipakai banyak tersedia di pasaran.
b. Setiap komputer dapat saling berhubungan secara langsung.

Adapun kerugiannya adalah sebagai berikut :

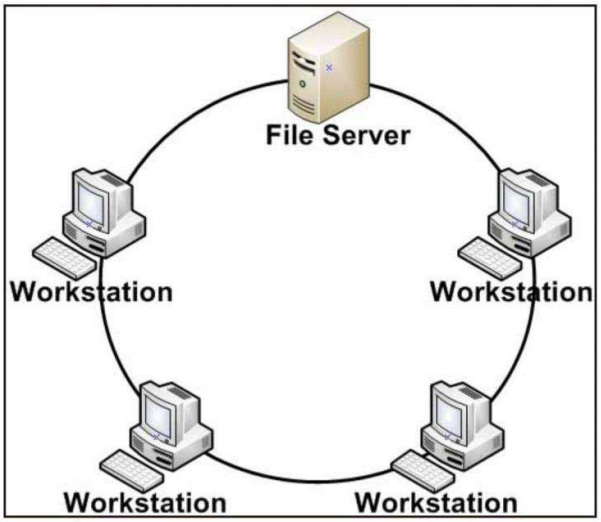
a. Sering terjadi *hang/crass talk*, yaitu bila lebih dari satu pasang memakai jalur di waktu yang sama, harus bergantian atau ditambah relay.



Gambar 2.7 **Topolgi Bus**
(Sumber : Syafrizal, 2012)

2. Topologi Ring

Topologi jaringan yang berupa lingkaran tertutup yang berisi node-node. Signal mengalir dalam dua arah sehingga dapat menghindarkan terjadinya *collision* sehingga memungkinkan terjadinya pergerakan data yang sangat cepat. Semua komputer saling tersambung membentuk lingkaran (seperti bus tetapi ujung-ujung bus disambung).



Gambar 2.8 Topologi Ring
(Sumber : Syafrizal, 2012)

Data yang dikirim diberi *address* tujuan sehingga dapat menuju komputer yang dituju. Tiap stasiun (komputer) dapat diberi *repeater (transceiver*) yang berfungsi sebagai:

a. *Listen State*

   Tiap bit dikiiim kembaii dengan mengalami delay waktu

b. *Transmit State*

   Bila *bit* yang berasal dari paket lebih besar dari *ring* maka *repeater* akan mengembalikan ke pengirim. Bila terdapat beberapa paket dalam *rin*g, *repeater* yang tengah memancarkan, menerima *bit* dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.

c. *Bypass State*

   Berfungsi untuk menghilangkan delay waktu dari stasiun yang tidak aktif.

Keuntungan :

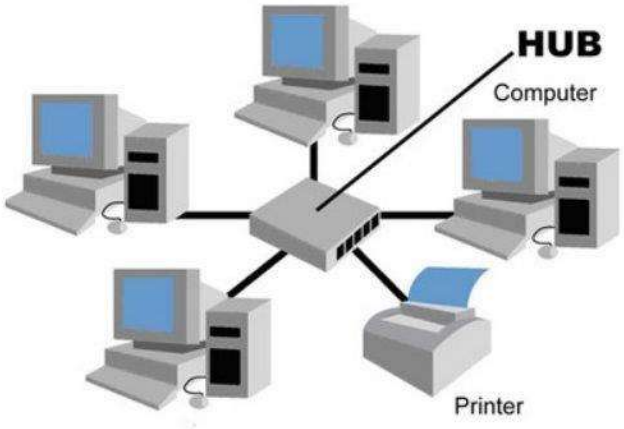
1. Kegagalan koneksi akibat gangguan media dapat diatasi lewat jalur lain yang masih terhubung.
2. Penggunaan sambungan *point to point* membuat *transmission error* dapat diperkecil.

Kerugian:

1. Data yang dikirim, bila vmelalui banyak komputer, transfer data menjadi lambat.

3. *Topologi Star*

Karakteristik dari topologi jaringan ini adalah *node (station)* berkomunikasi langsung dengan *station* lain melalui *central node (hub/switch), traffic* data mengalir dari *node* ke *central node* dan diteruskan ke *node (station)* tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak akan terputus.



Gambar 2.9 Topologi Star
(Sumber : Syafrizal, 2012)

Keuntungan:

a. Akses ke *station* lain *(client atau server*) cepat.

b. Dapat menerima *workstation* baru selama *port* di *centralnode(hub/switch)* tersedia.

c. *Hub/switch* bertindak sebagai *konsentrator.*

d. *Hub/switch* dapat disusun seri (bertingkat) untuk menambah jumlah *station* yang terkoneksi di jaringan.

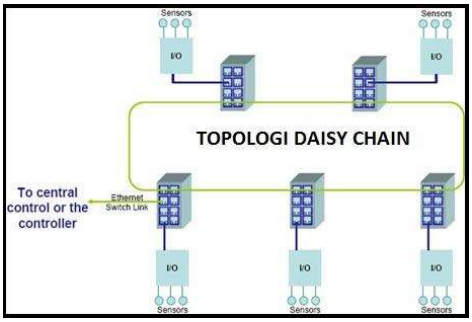
e. *User* dapat lebih banyak dibanding topologi *bus* maupun *ring*.

Kerugian:

a. Bila *traffic* data cukup tinggi dan terjadi *collision*, maka semua komunikasi akan ditunda, dan koneksi akan dilanjutkan dengan cara *random*, apabila *hub/switch* mendeteksi tidak ada jalur yang sedang dipergunakan oleh *nod*e lain.

4. *Topologi Daisy-Chain (linear)*

Topologi ini merupakan peralihan dari *topologi Bus* dan *topologi Ring*, di mana tiap simpul terhubung langsung ke dua simpul lain melalui segmen kabel, tetapi segmen membentuk saluran, bukan lingkaran utuh. Antar komputer seperti terhubung secara seri.



Gambar 2.10 Topologi Daisy Chain
(Sumber : Syafrizal, 2012)

Keuntungan :

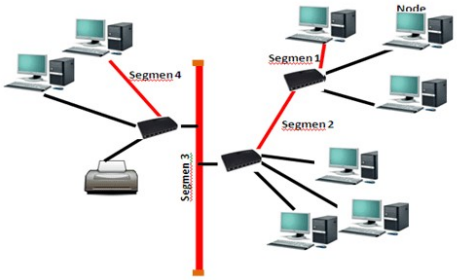
a. Instalasi dan pemeliharaannya murah.

Kerugian:

a. Kurang andal (tidak sesuai dengan kemajuan zaman)

5. *Topologi Tree/Hierarchical*

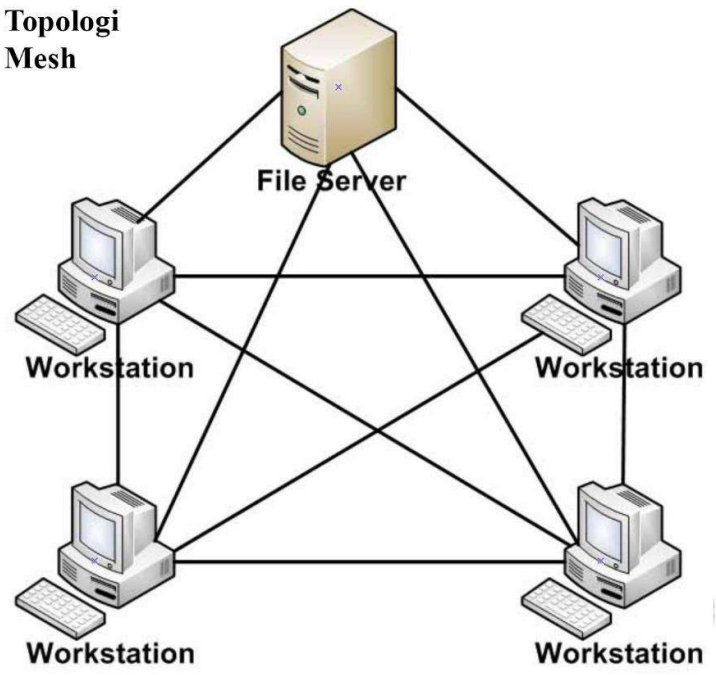
Tidak semua stasiun mempunyai kedudukan yang sama. Stasiun yang kedudukannya lebih tinggi menguasai stasiun di bawahnya, sehingga jaringan sangat tergantung pada stasiun yang kedudukannya lebih tinggi *(hierachical topology)*, dan kedudukan stasiun yang sama disebut *peer topology.*



Gambar 2.11 Topologi Tree
(Sumber : Syafrizal, 2012)

6. *Topologi Mesh dun Full Connected*

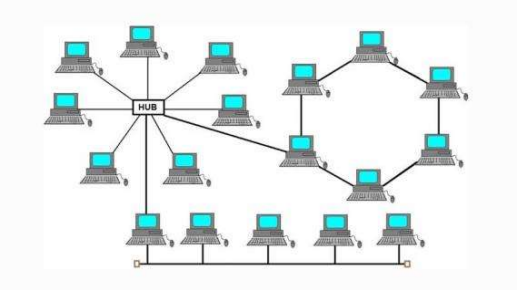
Topologi jaringan ini menerapkan hubungan antarsentral secara penuh. Jumlah saluran yang harus disediakan untuk membentuk jaringan *Mesh* adalah jumlah sentral dikurangi 1 (n-l, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Di samping kurang ekonomis juga relatif mahal dalam pengoperasiannya.Topologi mesh ini merupakan teknologi khusus *(ad hock)* yang tidak dapat dibuat dengan pengkabelan, karena sistemnya yang rumit, namun dengan teknologi *wireless* topologi ini sangat memungkinkan untuk diwujudkan (karena dapat dipastikan tidak akan ada kabel yang berantakan).



Gambar 2.12 Topologi Mesh
(Sumber : Syafrizal, 2012)

Biasanya untuk memperkuat sinyal transmisi data yang dikirimkan, di tengah-tengah (area) antarkomputer yang kosong ditempatkan perangkat radio *(air point)* yang berfungsi seperti *repeater* untuk memperkuat sinyal sekaligus untuk mengatur arah komunikasi data yang terjadi.

7. ***Topologi Hybrid***



Gambar 2.13 Topologi Hybird
(Sumber : Syafrizal, 2012)

Topologi ini merupakan topologi gabungan dari beberapa topologi yang ada, yang bisa memadukan kinerja dari beberapa topologi yang berbeda, baik berbeda sistem maupun berbeda media transmisinya.

2.1.2 Standar Jaringan Komputer

Dalam sebuah jaringan komputer, terdapat sebuah standar aturan atau biasa disebut dengan protokol. Protokol ini merupakan standard dari sebuah jaringan yang harus dipenuhi baik itu dari pengirim ataupun penerima dalam melakukan aktivitas jaringan komputer.

(Maslan & Wangdra, 2012), *Protocol* adalah sebuah aturan atau metoda bagaimana komunikasi data dilakukan di antara beberapa komputer didalam

sebuah jaringan, aturan termasuk didalamnya petunjuk yang berlaku bagi cara-acra atau metode akses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan *transfer* data. Banyak *protocol* komunikasi komputer telah dikembangkan untuk membentuk jaringan komputer. Kompetisi antar perusahaan seperti DEC, IBM dan lain-lain mengeluarkan berbagai standar jaringan komputer. Terdapat 3 *protocol* umum yang yang paling sering digunakan yaitu *Ethernet*, *Local Talk* dan *Token Ring.*

1. *Ethernet*

Protocol Ethernet merupakan *protocol* yang paling banyak digunakan, *protocol* ini menggunakan metode akses yang disebut CSMA/CD (*Carrier Sense Multi Acces / Collision Detection).*

2. *Local Talk*

Local Talk adalah sebuah *protocol network* yang dikembangkan oleh *Apple Computer*, Inc, untuk mesin-mesin komputer Macintos. Metode yang digunakan oleh *Local Talk* CSMA/CD (*Carrier Sense Multi Acces / Collision Detection).* Hampir sama dengan CSMA/CD.

3. *Token Ring*

Protocol Tokendi kembangkan oleh IBM pada pertengahan tahun 1980. Metode aksesnya melalui lewatnya sebuah token dalam lingkaran seperti cincin. Dalam token komputer-komputer dihungkan satu dengan yang lainnya seperti sebuah cincin.

(Wardoyo, Ryadi, & Fahrizal, 2014), Pesatnya perkembangan media telekomunikasi dan informasi di berbagai bidang selaras dengan tingginya tingkat aktivitas dan kebutuhan manusia akan informasi dalam kehidupan sehari-hari, ditambah lagi dengan semakin gencarnya teknologi-teknologi yang mendukung hal tersebut. Diantara teknologi dan media komunikasi yang terus berkembang sampai saat ini adalah internet, *website*, *smartphone*, *tablet pc*, yang kesemuanya berbasis IP (Internet Protokol).

Internet Assigned Numbers Authority (IANA), sebuah lembaga resmi internasional pengelola alamat IP merilis data bahwa jumlah alamat tersisa dari IPv4 pada tahun 2011 kurang lebih hanya tersisa 10 persen dari kapasitas awal atau sekitar 400 juta alamat saja. Jumlah ini tidak memadai untuk mengantisipasi perkembangan pengguna internet saat ini yang amat luar biasa ditambah lagi dengan adanya perkembangan teknologi telekomunikasi masa datang yang berbasis IP. IPv6 merupakan protokol internet baru yang dikembangkan untuk mengantisipasi protokol IPv4 yang sebentar lagi penuh. IPv4 (Internet Protokol versi 4) merupakan protokol yang paling banyak digunakan dari pertama kali internet diperkenalkan ke seluruh dunia, IPv4 berbasis 32-bit (232 atau sekitar 4,294 x 109) sudah membantu setiap pengguna internet di selurug dunia selama lebih dari 20 tahun terakhir dan diperkirakan tidak akan mampu menampung banyaknya kebutuhan akan pengalamatan internet. Bayangkan, penduduk dunia saat ini adalah 6,5 Milyar, jika nantinya masing-masing punya satu komputer, 1 Laptop (mobile), 1 PDA, 2 Handphone (GSM & CDMA). Lalu setiap perangkat

butuh 1 IP address untuk bisa *connected each other*. Secara otomatis hal tersebut tidak mungkin untuk dilakukan.

2.1.2.1 TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam suatu jaringan. Prinsip pembagian lapisan pada TCP/IP menjadi protokol komunikasi data yang fleksibel dan dapat diterapkan dengan mudah di setiap jenis komputer dan antar-muka jaringan. Oleh karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu.

2.1.3 Jenis Jaringan Komputer

Menurut Syarifal (2012: 16-17), secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu :

1. *Local Area Network (LAN)*

   Sebuah *LAN* adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar *node* tidak lebih jauh dari sekitar 200 m.

2. *Metropolitan Area Network (MAN)*

Sebuah *MAN* biasanya meliputi area yang lebih besar dari *LAN*, misalnya antargedung dalam suatu daerah (wilayah seperti propinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar. Sebagai contoh, jaringan beberapa kantor cabang sebuah bank di dalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.

3. *Wide Area Network (WAN)*

Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media *wireless*, sarana satelit, ataupun kabel serat *optic*, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antarkota dalam suatu wilayah, tetapi mulai menjangkau area/ wilayah otoritas negara lain. Sebagai contoh, jaringan komputer kantor *City Bank* yang ada di Indonesia ataupun yang ada di negara lain, yang saling berhubungan, jaringan *ATM Master Card, Visa Card* atau *Cirrus* yang tersebar di seluruh dunia, dan lain-lain. Biasanya *WAN* lebih rumit dan sangat kompleks bila dibandingkan *LAN* maupun *MAN*. Menggunakan banyak sarana untuk menghubungkan antara *LAN* dan *WAN* ke dalam komunikasi global seperti internet, meski demikian antara *LAN, MAN* dan *WAN* tidak banyak berbeda dalam beberapa hal. Hanya lingkup areanya saja yang berbeda satu dengan yang lain.

2.1.4 Model *OSI Layer*

Menurut Anjik Sukmaji & Rianto (2013: 14), *OSI* memberikan pandangan yang "abstrak" dari arsitektur jaringan yang dibagi dalam 7 lapisan. Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh *International Standard Organization (ISO)* sebagai langkah awal menuju standarisasi protokol internasional yang digunakan pada berbagai layer. Model ini disebut *OSI Reference Model*, karena model ini ditujukan untuk interkoneksi *Open System*. *Open System* diartikan sebagai suatu sistem yang terbuka untuk berkomunikasi dengan sistem-sistem lain yang berbeda arsitektur maupun Sistem Operasi. Prinsip-prinsip yang digunakan bagi ketujuh layer tersebut adalah:

1. Sebuah *layer* harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2. Setiap *layer* harus memiliki fungsi tertentu.
3. Fungsi *layer* di bawah adalah mendukung fungsi *layer* di atasnya.
4. Fungsi setiap *layer* harus dipilih dengan teliti sesuai dengan ketentuan standar protokol internasional.
5. Batas-batas setiap *layer* diusahakan untuk meminimalkan aliran informasi yang melewati antarmuka.
6. Jumlah layer harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu *layer* di luar keperluannya. Akan tetapi jumlah *layer* juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.

Menurut Syafrizal (2012: 76-77), ketujuh lapisan model referensi OSI dapat dibagi kedalam dua kategori, yaitu lapisan atas dan lapisan bawah.

1. Lapisan Atas

   Lapisan atas dari model *OSI* berurusan dengan persoalan aplikasi dan pada umunya diimplementasikan hanya pada *software*. Lapisan tertinggi (lapisan aplikasi) adalah lapisan penutup sebelum kepengguna *(user)*. *User* berinteraksi langsung dengan lapisan aplikasi ini.

2. Lapisan Bawah

   Lapisan bawah dari model *OSI* mengendalikan persoalan *transport* data. Lapisan fisik dan lapisan data link diimplementasikan kedalam *hardware* dan *software*. Lapisan-lapisan bawah yang lain pada umunya hanya diimplementasikan dalam *software*. Lapisan terbawah, yaitu lapisan fisik, adalah lapisan penutup bagi media jaringan fisik (misalnya jaringan kabel), dan sebagai penanggung jawab bagi penempatan informasi pada media jaringan.

Menurut Anjik Sukmaji & Rianto (2013: 16-24), *OSI* memberikan pandangan yang "*abstract*" dari arsitektur jaringan yang dibagi dalam 7 lapisan. Lapisan tersebut antara lain adalah sebagai berikut :

1. Layer-1 (Physical Layer)

   Physical layer atau lapisan fisik melakukan fungsi pengiriman dan penerimaan *bit stream* dalam medium fisik. Dalam lapisan ini kita akan mengetahui spesifikasi *mekanikal* dan *elektrikal* dari media transmisi serta

antarmukanya. Hal-hal penting yang dapat dibahas lebih jauh dalam lapisan fisik ini adalah :

1. Karakteristik fisik dari media dan antar muka.
2. Representasi bit-bit.

   Dalam hal ini lapisan fisik harus mampu menerjemahkan bit 0 atau 1, termasuk pengkodean dan bagaimana mengganti sinyal 0 ke 1 atau sebaliknya.

c. *Dara rate* (laju data).

d. Sinkronisasi bit.

e. *Line configuration* (konfigurasi saluran). Misalnya : *point-to-point* atau *point-to-multipoint configuration*.

f. Topologi fisik. Misalnya : *mesh topology, star topology, ring topology,* atau *bus topology*.

g. Mode transmisi. Misalnya : *half-duplex mode, full-duplex (simplex) mode.*

2. Layer-2 (Data Link)

Pada *layer-2 (data link layer)* komunikasi data dilakukan dengan menggunakan identitas berupa alamat simpul fisik yang disebut sebagai alamat *hardware* atau *hardware address*. Proses komunikasi antara komputer atau simpul jaringan hanya mungkin terjadi, bila kedua belah pihak mengetahui identitas masing-masing melalui alamat fisik *(physical address)*. Bentuk topologi yang digunakan ditentukan oleh *protocol data*

link. Sebagai contoh adalah *BUS* untuk teknologi *Ethernet, RING* untuk teknologi *tokenring* ataupun teknologi *FDDI*. Selain ketiga bentuk topologi tersebut pada komunikasi serial terdapat topologi *point-to-point* atau *point-to-multipoint* pada jaringan yang menggunakan teknologi *frame relay*.

Penanganan keslahan komunikasi yang terjadi pada lapisan *data link* menggunakan pendeteksian *error* dan menginformasikan kepada lapisan di atasnya, bahwa terjadi kesalahan transmisi. Kendali kesalahan yang bisa dilakukan pada lapisan ini hanya mendeteksi dan tidka melakukan perbaikan kesalahan *(error correction)*. *Data link* akan mengubah *BYTES (1 byte = 8 bit)* yang diterima dari lapisan fisik menjadi satuan data yang disebut dengan *FRAME. FRAME* =terdiri dari *FRAME-HEADER* (identitas yang menjelaskan *frame*) dan *DATA*. Selain *FRAME-HEADER*, informasi lain yang ditambahkan adalah *FCS (Frame Check Sequence)*, penjabarannya adalah sebagai berikut :

Tabel 2.1 *Layer Data Link*

Frame-Header	**DATA**	**Frame Check Sequence**

(Sumber : Syafrizal, 2012)

Frame-Header berisi informasi yang dibutuhkan oleh *protocol data link*. Secara umum, informasi yang terdapat dalam *frame header* :

a. *Hardware Address (MAC Address)* pengirim.

b. *Hardware Address (MAC Address)* penerima.

c. *Flag.*

d. *Control Bits.*

Teknologi ethernet, token ring, dan FDDI menggunakan *48 bit Media Access Control (MAC)* sebagai *hardware address*. Dari *48 bit* ini, *24 bit* awal ditentukan oleh standar internasional (IEEE) dan *24 bit* sisanya adalah perusahaan pembuat kartu jaringan *(Network Interface Card)*. Sebagian penomoran yang diberikan IEEE diantaranya adalah :

Tabel 2.2 Tabel Penomoran *IEEE*

Vendor NIC	Nomor MAC (24 bit awal)
Cisco System	00 00 0C
3Com Corporation	00 20 AF
Hewlett-Packard Company	08 00 09
Apple Computer	08 00 07

(Sumber : Syafrizal, 2012)

Pada teknologi WAN, frame relay menggunakan DLCI (Data Link Control Identifier), ATM menggunakan *VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier)*, dan *X25* menggunakan *X.21* sebagai *hardware address.*

Tugas utama lapisan *data link* dalam proses komunikasi data adalah :

a. *Framing* : membagi *bit stream* yang diterima dari lapisan *network* menjadi unit-unit data yang disebut *frame*.
b. *Physical addressing* : definisi identitas pengirim dan/atau penerima yang ditambahkan dalam *header.*
c. *Flow control* : melakukan tindakan untuk membuat stabil laju *bit rate* atau laju *bit stream* berlebih atau berkurang.
d. *Error control* : penambahan mekanisme deteksi dan *retransmisi frame-frame* yang gagal terkirim.

e. *Communication control* : menentukan *device* yang harus dikendalikan pada saat tertentu jika ada dua koneksi yang sama.

3. Layer-3 (Network Layer)

Pada lapisan ini terjadi proses pendefinisian alamat logis *(logical addressing)*, kemudian mengombinasikan *multiple data link* menjadi satu *network*. Lapisan *network* bertanggung jawab untuk membawa paket dari satu simpul ke simpul lainnya dengan mengacu pada *logical address*. Fungsi lain adalah sebagai *packet forwarder* (penerus). Lapisan *network* sebagai *packet forwarder* megnantarkan paket dari sumber *(source)* ke tujuan *(destination)* yang disebut dengan istilah *routing.*

Ada dua tugas pokok lapisan *network* yaitu :

a. *Logical addressing* : pengalamatan secara logis yang ditambahkan pada *header* lapisan *network*. Pada jaringan *TCP/IP* pengalamatan logis ini popular dengan sebutan *IP address.*

b. *Routing* : hubungan antar jaringan yang membentuk *internetwork* membutuhkan metode jalur alamat agar paket dapat ditransfer dai satu *device* yang berasal dari jaringan satu menuju *device* lain pada jaringan yang lain. Fungsi *routing* didukung oleh *routing protocol* yang bertujuan mencari jalan terbaik menuju tujuan dan tukar-menukar informasi tentang topologi jaringan dengan *router* lainnya. *Protocol routing* ini misalnya *Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP).*

8. La*yer-4 (Transport Layer)*

Lapisan *transport* bertanggung jawab terhadap pengiriman *source-to-destination (end-to-end)* yang dapat dijelaskan sebagai berikut:

a. Sevice-port addressing.

Suatu komputer sering menjalankan berbagai macam program aplikasi ataupun *services* berlainan pada waktu bersamaan. Karena itu, lapisan *transport* ini tidak hanya menangani pengiriman *source-to-destination* dari komputer satu ke komputer yang lain, namun lebih spesifik kepada *delivery* jenis *message* untuk aplikasi yang berlainan. Dengan demikian, setiap *message* yang berlainan aplikasi harus memiliki alamat tersendiri yang disebut *service point address* atau yang lebih umum disebut *port address (port 80 = www, port 25 = SMTP).*

b. *Segmentation* dan *reassembly*.

Sebuah *message* dibagi dalam segmen-segmen yang terkirim. Setiap segmen memiliki *sequence number*. *Sequence number* berguna bagi lapisan *transport* untuk merakit *(reassembly)* segmen-segmen yang terpecah menjadi *message* yang utuh.

c. *Connection control*.

Pada lapisan *transport* terdapat dua kondisi yakni *connectionless* atau connection-oriented. Fungsi dari *connection control*adalah mengendalikan kondisi tersebut.

d. *Flow control*.

Seperti halnya lapisan *data link*, lapisan *transport* bertanggung jawab untuk melakukan kontrol aliran *(flow control)*. Bedanya dengan *flow control* di lapisan *data link* adalah dilakukan untuk *end-to-end.*

e. *Error control*.

Fungsi tugas ini sama dengan tugas *error control* di lapisan *data link*, namun berorientasi *end-to-end.*

Dalam jaringan berbasis *TCP/IP* protokol yang terdapat pada lapisan ini adalah *Transmission Control Protocol (TCP*) dan *User Datagram Protocol (UDP).*

9. *Layer-5 (Session Layer)*

Lapisan sesi membuka, merawat, mengendalikan dan melakukan terminasi hubungan antarsimpul. Lapisan aplikasi dan presentasi melakukan *request* dan menunggu *response* yang dikoordinasikan oleh lapisan di atasnya misalnya :

a. *RPG (remote Procedure Call)* : Protokol yang mengeksekusi program pada komputer *remote* dan memberikan nilai balik kepada komputer *local* sebagai hasil eksekusi tersebut.

b. *Netbios API* : *Session layer application programming interface*.

c. NFS (Network File System)

d. SQL (Structured Query Language)

10. *Layer-6 (Presentation Layer)*

    Berfungsi untuk mentranslasikan data yang akan ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. *Protocol* yang berada dalam level ini adalah perangkat lunak *redirector (redirector software)*, seperti layanan *workstation* (dalam *windows NT*) dan juga *network shell (Virtual Network Computing(VNC))* atau *Remote Desktop Protocol (RDP)*. Lapisan presentasi melakukan *coding* dan konversi data misalnya format data untuk *image* dan *sound(JPG, MPEG, TIFF, WAV,* dan lain-lain), konversi EBCDIC-ASCII, presentasi *Big Endian* dan *Little Endian*, Kompresi, dan Enkripsi.

11. *Layer-7 (Application Layer)*

    Aplikasi adalah layanan/*service* yang mengimplementasikan komunikasi antar simpul. *Application layer* berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan mengatur bagaimana aplikasi dapat mengakses jaringan dan membuat pesan-pesan kesalahan. Beberapa hal yang dilakukan oleh lapisan aplikasi mengidentifikasi mitra komunikasi, aplikasi transfer datam *resource, availability* dan lapisan aplikasi terkait dengan aplikasi *end-user.*

    Protokol-protokol pada lapisan aplikasi di antaranya :

    a. *File Transfer Protocol (FTP)* : Protokol standar untuk transfer file komputer antar mesin dalam sebuag *internetwork.*

b. *Simple Mail Transfer Protocol (SMTP)* : merupakan salah satu *protocol* yang umum digunakan untuk pengiriman surat elektronik di internet. Protokol ini digunakan untuk mengirimkan data dari komputer pengirim ke server surat elektronik penerima yang didukung oleh *POP3* dan *IMAP*.

c. *Hypertext Transfer Protocol (HTTP)* : protokol yang dipergunakan untuk transfer dokumen dalam *World Wide Web (WWW)*. Protokol ini adalah protokol ringan, tidak berstatus dan generik yang dapat digunakan berbagai macam tipe dokumen.

2.2 Teori Khusus

Adapun teori khusus yang akan dijabarkan pada sub bab ini terfokus kepada keamanan jaringan, *wireless*, dan *packet sniffing.*

2.2.1 Keamanan jaringan

Menurut Indrajit (2014: 82-83), Informasia merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap infomasi (kamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi

yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi. Infomasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk baik dokumen berbasis kertas hingga berkas elektronik. Apapun bentuk maupun cara penyimpanannya, harus selalu ada upaya dan untuk melindungi keamanannya sebaik mungkin. Keamanan yang dimaksud harus memperhatikan sejumlah aspek, yaitu:

1. Kerahasiaan memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya.
2. Integritas melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif.
3. Ketersediaan memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang djmaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

2.2.1.1 Aspek-Aspek Keamanan Komputer

Menurut Anjik Sukmaji & Rianto (2013: 159-163), Garfinkel mengemukakan bahwa keamanan komputer *(computer security)* melingkupi empat aspek, yaitu *privacy, integrity, authentication,* dan *availability*. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation*.

1. Privacy/Confidentiality

Inti utama aspek *privacy* atau *confidentiality* adalaha usaha untuk menjaga informasi dari orang yang tidak berhak mengakses *Privacy* lebih ke arah data-data yang sifatnya privat, sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu. Contoh hal yang berhubungan dengan *privacy* adalah *e-mail* seorang pemakaia *(user)* tidak boleh dibaca oleh administrator. Contoha *confidential information* adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, *social security number*, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya.

2. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya *virus, trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja "ditangkap" *(intercept)* di tengah jalan,

diubah isinya *(altered,a tampered, modified),* kemudian diteruskan ke alamat yang dituju. Penggunaan *enkripsi* dan *digital signature*, misalnya, adapat mengatasi masalah ini. Salah satu contoh kasus *trojan horse* adalah distribusi paket program *TCP Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses *TCP/IP*) yang dimodifikasi oleh orang yang tidak bertanggung jawab.

3. Authentication

Authentication berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang dihubungia adalaha *server* yang asli. Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan *digital signature*. *Watermarking* juga dapat digunakan untuk menjag "*intelectual property*", yaitu dengan menandai dokumen atau hasil karya dengana "tanda tangan" pembuat. Masalah kedua biasanya berhubungan dengan *access control*, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwaa memang dia adalaha pengguna yang sah.

4. Availabilily

Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika adibutuhkan. Sistem informasi yang di serang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan

adalah serangan yang sering disebut dengan "*denial of service attack" (DOS attack)*, di mana *server* dikirimia permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang di luar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang, crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirimi *e mail* bertubi-rubia dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses *e-mailnya*. Bayangkan apabila mendapat kiriman 5000 *e-mail* seriap hari dan hak diambil *(download)* dengan menggunakan koneksi *dial-up*, pasti akan berpikiran untuk ganti *e-mail address*. Serangan terhadap *availability* dalam bentuk *DOS attack* merupakan yang paling populer.

5. Access Control

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasiflkasi data*(public, private, confidential, top secret)* dan *user (guest. Admin, top manager*. dan lain sebagainya). Mekanisme authentification, *privacy*, dan *access control* seringkali dilakukan dengan menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain seperti kartu atau *biometrics*.

6. Non-repudiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan *e-mail* untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan *e-mail*

tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan *digital signature, certificates*, dan teknologi *kriptografl* secara umum dapat menjaga aspek ini. Akan tetapi, hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal.

2.2.1.2 Security Attack

Menurut Anjik Sukmaji & Rianto (2013: 163-165)*, Security attack*atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer, yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings, ada beberapa kemungkinan serangan (attack):

1. Interruption : Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availability)* dari sistem. Contoh serangan adalah *"denial of service attack".*
2. *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretapping)*.
3. *Modification* : Pihak yang tidak berwenang tidak saja berhasil mengakses, tetapi dapat juga mengubah *(tamper)* aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website.*
4. Fabrication : Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti *e-mail* palsu ke dalam jaringan komputer.

Berikut adalah beberapa jenis serangan yang pernah dijumpai pada keamanan jaringan komputer :

a. Denial of Service Attack

"Denial of Service (DoS) attack" merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya *(denial of service)* atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnya pun dapat beragam. Sistem yang diserang dapat menjadi *hang, crash*, tidak berfungsi atau menurunkan kinerjanya.

Serangan *denial of service* berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan *DoS* tidak ada yang dicuri. Akan tetapi, serangan *DoS* dapat mengakibatkan kerugian Finansial. Sebagai contoh, apabila sistem yang diserang merupakan server yang menangani transaksi *"commerce"*, maka apabila *server* tersebut tidak berfungsi, transaksi tidak dapat dilangsungkan. Bayangkan apabila sebuah bank diserang oleh bank saingan dengan melumpuhkan *outlet ATM (Anjungan Tunai Mandiri, Automatic Teller Machine)* yang dimiliki oleh bank tersebut. Atau sebuah *credit cardmerchant server* yang diserang sehingga tidak dapat menerima pembayaran melalui *credit card.*

Selain itu, serangan *DoS* sering digunakan sebagai bagian dari serangan lainnya. Misalnya, dalam serangan *IPspoofing* (seolah serangan datang dari

tempat lain dengan nomor *IP* milik orang lain), seringkali *DoS* digunakan untuk membungkam *server* yang akan di*spoo£*.

b. Ping-o-death

Ping-o-death sebenarnya adalah eksploitasi program *ping* dengan memberikan *packet* yang ukurannya besar ke sistem yang dituju. Berapa sistem *UNIX* ternyata menjadi *hang* ketika diserang dengan cara ini. Program *ping* umum terdapat di berbagai sistem operasi, meskipun umumnya program *ping* tersebut mengirimkan paket dengan ukuran kecil dan tidak memiliki fasilitas untuk mengubah besamya paket. Salah satu implementasi program *ping* yang dapat digunakan untuk mengubah ukuran paket adalah program *ping* yang ada di sistem *Windows 95.*

c. Ping broadcast (smurf)

Salah satu mekanisme serangan yang baru-baru ini mulai marak digunakan adalah menggunakan *ping* ke alamat *broadcast*, ini yang sering disebut dengan *smurf*. Seluruh komputer *(device*) yang berada di alamat *broadcast* tersebut akan menjawab. Jika sebuah sistem memiliki banyak komputer *(device)* dan *ping broadcast* ini dilakukan terus-menerus. jaringan dapat dipenuhi oleh respon-respon dari *device-device* tersebut, akibatnya jaringan menjadi lambat. *Smurf attack* biasanya dilakukan dengan menggunakan *IP spoofing*, yaitu mengubah nomor *IP* dari datangnya *request*. Dengan menggunakan *IP spoofing*, respon dari *ping*dialamatkan ke komputer yang *IP* nya *di-spoof*, akibatnya komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosan

penggunaan *(bandwidth)* jaringan yang menghubungkan komputer tersebut. Dapat dibayangkan apabila komputer yang di-*spoof* tersebut memiliki hubungan yang berkecepatan rendah dan *ping* diarahkan ke sistem yang memiliki banyak *host.* Hal ini dapat mengakibatkan *DoS attack*.

2.2.2. Wireless

Menurut Priyambodo & Heriadi (2015: 1-5), Komunikasi tanpa kabel/nirkabel (wireless? tclah menjadi kebutuhan dasar atau gaya hidup baru masyarakat informasi. LAN nirkabel yang lcbih dikenal dengan jaringan Wi-Fi menjadi teknologi alternatif dan rclatif lcbih mudah untuk diimplementasikan di lingkungan kexja (SOHO/Small Office Home Office), seperti di perkantoran, laboratorium komputer, dan sebagainya. Instalasi perangkat jaringan Wi-Fi lebih Hcksibcl karena tidak membutuhkan penghubung kabcl antar komputer. Tidak seperti halnya Ethernet LAN (Local Area thwork)/jaringan konvcnsional yang mcnggunakan jenis kabel koaksial dan kabel UTP (Unshiclded Twisted Pair) sebagai media transfer. Komputer dcngan Wi-Fi Device dapat saling tcrhubung yang hanya membutuhkan ruang atau space dengan syarat jarak jangkauan dibatasi kckuatan pancaran sinyal radio dari masingmasing komputer.

2.2.2.1.Teknologi Jaringan Wi-Fi

Wi-Fi atau *Wireles Fidelity* adalah satu standar *Wireless Networking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan. Teknologi *Wi-Fi* memiliki standar, yang ditetapkan oleh sebuah institusi internasional yang bernama *Institute of Electrical and Electronic Engineers (IEEE*), yang secara umum sebagai berikut:

1. Standar *IEEE 802.11a* yaitu *Wi-Fi* dengan frekuensi 5 Ghz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 300 m
2. Standar *IEEE 802.11b* yaitu *Wi-Fi* dengan frekuensi 2,4 Ghz yang memiliki kecepatan 11 Mbps dan jangkauan jaringan 100 m
3. Standar *IEEE 802.11g* yaitu *Wi-Fi* dengan frekuensi 2,4 GHz yang memilild kecepatan 54 Mbps dan jangkauan jaringan 300 m

Teknologi Wi-Fi yang akan diimplementasikan adalah standar *IEEE 802.11g* karena Standar tersebut lebih cepat untuk proses transfer data dengan jangkauan jaringan yang lebih jauh serta dukungan vendor (perusahaan pembuat *hardware*). Perangkat tersebut berada di frekuensi 2,4 GHz atau disebut sebagai pita frekuensi *ISM (Industrial, Scientific, and Medical)* yang juga digunakan oleh peralatan lain, seperti *microwave open, cordless phone,* dan *bluetooth.*

2.2.2.2.Tipe Jaringan *Wi-Fi*

Seperti halnya *Ethemet-LAN* (jaringan dengan kabel), jaringan *Wi-Fi* juga dikonfigurasikan ke dalam dua jenis jaringan:

1. Jaringan *peer to peer/Ad Hoc Wireless LAN*

   Komputer dapat saling berhubungan berdasarkan nama *SSID (Service Set Identifier*). SSID adalah nama identitas komputer yang memiliki komponen nirkabel.

2. Jaringan *Server Based/Wireless Infrastructure*

   Sistem Infrastruktur membutuhkan sebuah komponen khusus yang berfungsi sebagai Access Point.

2.2.2.3.Komponen Utama Jaringan Wi-Fi

Terdapat empat komponen utama untuk membangun jaringan *Wi-Fi* :

1. *Access Point*

   Komponen yang berfungsi menerima dan mengirimkan data dari *adapter wireless. Access Point* mengonversi sinyal frekuensi radio menjadi sinyal digital atau sebaliknya. Komponen tersebut bertindak layaknya sebuah *hub/switch* pada jaringan *ethernet*. Satu *Access Point* secara teori mampu menampung beberapa sampai ratusan klien. Walaupun demikian, *Access point* direkomendasikan dapat menampung maksimal 40-an klien.

2. *Wireless-LAN Device*

   Komponen yang dipasangkan di *Mobile/Desktop PC.*

3. *Mobile/Desktop PC*

   Komponen akses untuk klien, *mobile PC* pada umumnya sudah terpasang *port PCMCIA (Personal Computer Memory Card International Association),* sedangkan *Desktop PC* harus ditambahkan *PCI (Peripheral Componen Interconnect) Card,* serta *USB (Universal Serial Bus) Adapter*.

4. *Ethernet LAN*

   Jaringan kabel yang sudah ada (bila perlu)

2.2.2.4 Keamanan Jaringan Wireless

Pancaran sinyal yang ditransmisikan pada jaringan *Wi-Fi* menggunakan frekuensi secara bebas sehingga dapat ditangkap oleh komputer lain sesama *user Wi-Fi*. Untuk mencegah user yang tidak berhak masuk ke dalam jaringan, ditambahkan sistem pengamanan, misalnya *WEP (Wired Equivalent Privacy).* Jadi, *user* tertentu yang telah memiliki otorisasi saja yang dapat menggunakan sumber daya jaringan *Wi-Fi.*

Keamanan jaringan Wi-Fi secara umum terdiri dari NonSecure dan *Share Key (Secure).*

1. Non Secure/Open

   Komputer yang memiliki Wi-Fi dapat menangkap transmisi pancaran dari sebuah Wi-Fi dan langsung dapat masuk ke dalam jaringan tersebut.

2. Share Key

   Untuk dapat masuk ke jaringan Wi-Fi diperlukan kunci atau password, contohnya sebuah network yang manggunakan WEP.

Selain pengamanan yang telah dituliskan di atas, masih terdapat cara lain agar jaringan *Wi-Fi* dapat berjalan dengan baik dan aman, antara lain:

1. Membeli *access point* dengan fasilitas *password* bagi *administrator*-nya sehingga *user* dapat dengan mudah mengacak-acak jaringan.
2. Selain menggunakan *WEP*, dapat ditambahkan *WPA (Wi-Fi Protected Access).*
3. Membatasi akses dengan mendaftarkan *MAC Address* dari komputer lain yang berhak mengakses jaringan.

2.2.2.5 Keunggulan dan Kelemahan Jaringan Wi-Fi

Keunggulan jaringan *Wi-Fi:*

1. Biaya pemeliharaan murah.
2. Infrastruktur berdimensi kecil.
3. Pembangunannya cepat, mudah dan murah untuk direlokasi.
4. Mendukung portabilitas.

Kelemahan jaringan *Wi-Fi:*

1. Biaya peralatan mahal.
2. *Delay* yang sangat besar.
3. Kesulitan karena masalah propagasi radio Mudah untuk terinterferensi.
4. Kapasitas jaringan kecil karena ketcrbatasan spektrum (pita frekuensi yang tidak dapat diperlebar).
5. Keamanan/kerahasiaan data kurang terjamin

2.2.3. Packet Sniffing

Sniffing merupakan jenis serangan terhadap jaringan komputer yang melakukan pengendusan dengan cara memonitor dan menangkap semua lalu lintas jaringan paket data yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Seseorang dapat mengetahui informasi seperti username dan password yang lewat pada jaringan komputer. Sedangkan dampak positif sniffing, seorang admin dapat menganalisa paket-paket data yang lewat padajaringan untuk keperluan optimasi jaringan, seperti dengan melakukan penganalisaan paket data, dapat diketahui dapat membahayakan performa jaringan atau tidak, dan dapat mengetahui adanya penyusup atau tidak. Bahaya yang mengancam dari proses sniffing yaitu hilangnya sifat *privacy dan confidentiality* seperti tercurinya informasi penting dan rahasia seperti *username* dan *password* (Parmo, 2014).

2.3 *Software* Pendukung

Software pendukung merupakan beberapa perangkat lunak yang digunakan untuk melakukan analisa dan *penetration testing* dalam penelitian ini. Perangkat lunak yang dibutuhkan adalah *Wireshark*.

2.3.1. Wireshark

Wireshark adalah *tool* yang ditujukan untuk penganalisaan paket data jaringan (Kurniawan, 2012). *Wireshark* disebut juga Network *packet analyzer* yang berfungsi menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi dipaket tersebut sedetail mungkin.

Sebenarnya *network packet analyzer* sebagai alat untuk memeriksa apa yang sebenarnya terjadi di dalam jaringan baik kabel maupun *wireless.* Dengan adanya *wireshark* ini semua sangat dimudahkan dalam hal memonitoring dan menganalisa paket yang lewat di jaringan. Ada beberapa contoh penggunaan W*ireshark :*

1. Admin sebuah jaringan menggunakan untuk *troubleshooting* masalah di jaringan.
2. Admin menggunakan *Wireshark* untuk mengamankan jaringannya.

Beberapa fitur kelebihan *Wireshark*, diantaranya :

1. Berjalan pada sistem operasi *Linux* dan *Window*s.
2. Menangkap paket (*Capturing Packet)* langsung dari *network interface*.

3. Mampu menampilkan hasil tangkapan dengan detail.
4. Dapat melakukan pemfilteran paket.
5. Hasil tangkapan dapat di save, di import dan di export.

2.4 Penelitian Terdahulu

Untuk mendukung teori yang berkaitan dengan penelitian, peneliti mencantumkan beberapa penelitian terdahulu di bidang keamanan jaringan.

Sulaiman & Krianto (2016), Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. Memiliki kelemahan disisi admin jaringan yang kesulitan untuk mendaftarkan mac address yang akan diizinkan menggunakan jaringan tersebut. Sticky port security sangat efisien digunakan karena kemampuannya yang dapat mempelajari secara dynamic mac-address yang akan didaftarkan.

Jamaludin (2016), Teknik Keamanan Jaringan Wireless LAN Pada Warnet Salsabila *Computer* Net. Tingkat keamanan pada wireless LAN lebih tinggi dibanding dengan jaringan kabel LAN biasa di mana secara fisik adalah aman sementara jaringan wireless LAN tidak hanya bisa dibatasi oleh dinding di dalam gedung namun jaringan wireless bisa menembus dinding pembatas gedung. Untuk penanganan keamanan jaringan wireless di Salsabila Net menggunakan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK dan mengimplementasikan fasilitas MAC Address.

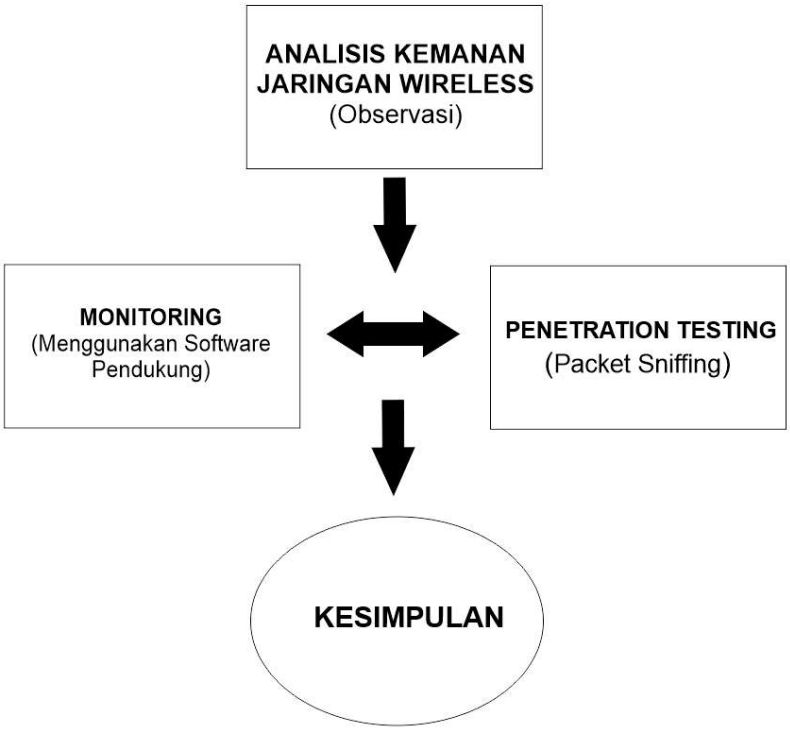
Guterres et al.(2014), Perancangan Dan Pengembangan Jaringan Vlan Pada Dili Institute of Technologi (Dit) Timor Leste Menggunakan Packet Tracer. Pada Rancangan yang di lakukan dengan Packet Tracert belum sempurna karena belum bisa di uji coba pengiriman data secara bersamaan dalam satu kali pengiriman. Adanya Router dari protocol Dot1q jaringan yang di rancang dapat saling berkomunikasi antar VLAN karena mempunyai koneksi Inter-VLAN.Kemampuan untuk membagi VLAN sesuai Departement yang ada di Dili Institute Of Tecnhology dan di samping itu memberikan hak akses VLAN berdasarkan hak akses yang telah ditentukan.Memudahkan dalam pengontrolan dan pembagian hak akses kepada seluruh anggota VLAN. Beberapa

Adriant & Mardianto (2015), Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan. Dengan menggunakan Wireshark penyadapan atau pengendusan data dan informasi dapat dilakukan pada paket yang lewat di jaringan yang mengakibatkan tercurinya informasi penting dan rahasia seperti username dan password. Dari percobaan diatas, Sniffing merupakan suatu yang cukup sulit untuk dicegah. Untuk sekarang ini sudah ada beberapa cara penangguhan sniffing seperti menggunakan enkripsi pada data rahasia (username, password), HTTPS (Hypertext Transport Protocol Secure) pada protokol jaringan lapisan aplikasi. Saran lebih ditujukan pada asas kehati-hatian ketika melakukan aktifitas seperti mengakses halaman web email, e-banking, social media, pada jaringan internet yang belum dikenal seperti warnet, kantor, kafe.

Babys et al. (2013), Analisis Aspek Keamanan Informasi Jaringan Komputer (Studi Kasus : STIMIK Kupang). Untuk mengamankan atau menjaga kerahasiaan informasi pengguna pada jaringan local area network yang menggunakan kabel sebagai media transmisi dari tidakan eksploitasi terhadap celah keamanan pada port yang yang terbuka disetiap client/host yang dilakukan melalui internal jaringan dapat dilakukan dengan beberapa hal, diantaranya adalah dengan menginstal personal firewall di setiap client/host untuk melindungi port-port yang terbuka. Dalam penelitian ini menunjukan bahwa McAfee 8.8 mampu melindungi port-port yang terbuka dari tindakan eksploitasi, dan dengan melakukan segmentasi pada jaringan menggunakan VLAN dengan menggunakan metode ACL untuk membatasi hak akses tiap user dalam jaringan dan port security untuk mengamankan port-port pada switch.

2.5 Kerangka Pemikiran

Kerangka pemikiran memuat pemikiran terhadap alur yang dipahami sebagai acuan dalam pemecahan masalah yang diteliti secara logis dan sistematis. Kerangka berfikir yang baik akan menjelaskan secara teoritis pertautan antar variabel yang diteliti (Sugiyono, 2014: 60). Berikut ini adalah kerangka pemikiran yang mendasari penelitian ini.



Gambar 2.32 Kerangka Pemikiran
(Sumber : Data Penelitian 2019)

Dalam penelitian ini, peneliti melakukan observasi langsung terhadap jaringan wireless di Kantor Kecamatan Sungai Beduk. Setelah melakukan observasi dan mendapatkan data yang dibutuhkan, lalu peneliti melakukan monitoring menggunakan *wireshark,* untuk kemudian dilakukan uji penetrasi terhadap keamanan jaringan wireless di Kantor Kecamatan Sungai Beduk. Hasil uji penetrasi kemudia n akan dijadikan sebagai hipotesis pada penelitian ini.

BAB III
METODE PENELITIAN

Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Data yang telah diperoleh dari penelitian dapat digunakan untuk memahami, memecahkan dan mengantisipasi suatu masalah (Sugiyono, 2014: 2-3).

3.1. Desain Penelitian

Menurut Sarwono (2016: 27) desain penelitian merupakan alat yang akan menentukan berhasil atau tidaknya suatu penelitian yang sedang dilakukan. Desain penelitian yang baik akan mendukung jalanny penelitian dengan baik pula. Desain penelitian berfungsi sebagai penuntun bagi peneliti yang akan menentukan arah berlangsungnya proses penelitian secara benar dan tepat sesuai dengana tujuan yang ditetapkan. Desain penelitian yang benar adalah desain yang terhindar dari sumber potensial kesalahan dalam proses penelitian secara keseluruhan seperti kesalahan dalam perencanaan, pengumpulan data, melakukan analisis data, dan kesalahan dalam pelaporan hasil penelitian. Tanpa desain penelitian yang benar, peneliti tidak mempunyai pedoman arah penelitian yang jelas sehingga penelitian tidak dapat dilakukan dengan baik (Sarwono, 2016: 79).

Penelitian ini menggunakan desain penelitian dengan beberapa tahap proses penelitian seperti yang terlihat pada gambar di bawah ini.

Gambar 3.1 Desain Penelitian
(Sumber : Data Penelitian 2019)

Berikut ini adalah penjelasan dari desain penelitian yang ada pada gambar di atas:

1. Identifikasi permasalahan

Penelitian dimulai dengan melakukan identifikasi permasalahan yang berkaitan dengan topik penelitian, agar peneliti mendapatkan apa yang menjadi masalah untuk dipecahkan.

2. Perumusan masalah

Pada tahap ini, peneliti merumuskan masalah yang telah didapat secara lebih spesifik agar masalah tersebut dapat dijawab dengan baik melalui penelitian.

3. Menentukan tujuan penelitian

Peneliti menentukan tujuan penelitian yaitu untuk menganalisa kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing* dan untuk mengevaluasi kemanan jaringan wireless di Kantor Kecamatan Sungai Beduk terhadap paket *sniffing*.

4. Mencari dan mempelajari literatur

Untuk mendukung penelitian, peneliti mencari dan mempelajari beberapa sumber pengetahuan berupa buku teori, jurnal penelitian, dan sumber pustaka otentik lainnya yang berkaitan dengan penelitian, diantaranya yaitu system keamanan jaringan, jaringan *wireless*, packet *sniffing*, dan lain sebagainya.

5. Menganalisa jaringan yang sedang digunakan

Setelah data-data yang berkaitan dengan analisis keamanan jaringan wireless didapatkan, baik melalui studi literatur maupun observasidi Kantor Kecamatan Sungai Beduk, peneliti menganalisa kondisi jaringan yang sedang digunakan, kemudian dari datayang sudah didapat,akan dilakukan *penetration testin*g guna menganalisa kemanan jaringan di Kantor Kecamatan Sungai Beduk.

6. Menganalisa kemanan jaringan wirelessdengan melakukan *penetration testing*

Berdasarkan kondisi keamanan jaringan yang sedang digunakan, penulis kemudian melakukan penetration testing menggunakan *software wireshark* dimana *penetration testing* merupakan tindakan yang membahayakan data karena peneliti melakukan pengujian bersifat aktif dalam melakukan serangan *packet sniffing* untuk mencari kelemahan dari sistem tersebut.

7. Menarik kesimpulan

Tahapanan terakhir pada penelitian ini adalah menyimpulkan hasil penelitian yang didapat setelah melakukan penetration testing. Dalam tahap ini, peneliti juga memberikan saran yang penting untuk membantu dalam memecahkan permasalahan yang ada.

3.2. Analisis Jaringan Lama/yang Sedang Berjalan

Pada bagian ini, peneliti akan menjelaskan sistem jaringan yang sedang berjalan, termasuk diantaranya: topologi jaringan, detail *hardware* jaringan yang sedang dipakai, detail *software* yang sedang dipakai (*Operating System* dan aplikasi), *Policy*/Kebijakan bidang jaringan yang sedang berjalan, SOP tentang Jaringan yang sedang diterapkan, Tata kelola jaringan yang sedang berjalan, dan lain sebagainya yang dianggap perlu.

3.2.1 Analisis Hardware Jaringan

Analisis perangkat keras *(hardware)* merupakan proses analisis yang lebih menekankan kepada aspek pemanfaatan perangkat keras yang selama ini telah dimiliki oleh Kantor Kecamatan Sungai Beduk. Setelah dilakukan analisis terhadap perangkat keras yang dimiliki oleh Kecamatan Sungai Beduk,perangkat keras/hardware yang digunakan adalahPC/Laptop, Modem Router, dan Switch. Kecamatan Sungai Beduk memiliki seperangkat komputer sebagai berikut :

Tabel 3.1 Tabel Perangkat Keras (*Hardware)*

No	Perangkat Keras	Lokasi Perangkat
1	PC	Ruang Pelayanan Umum
2	PC	Ruang Pelayanan Umum
3	PC	Ruang Pelayanan Umum
4	PC	Ruang Pelayanan Umum
5	PC	Ruang Pelayanan Umum
6	PC	Ruang Pelayanan Umum
7	PC	Ka.Subag Umum & Kepegawaian
8	PC	Ka.Subag Umum & Kepegawaian
9	PC	Ka. Trantib
10	PC	Ka.Kesejahteraan Rakyat
11	PC	Ka.Kesejahteraan Rakyat
12	PC	Ka.PPM
13	PC	Ka.Pemerintahan
14	Laptop	Klinik PIK
15	PC	Ruang Sekcam
16	PC	Ka.Subag Program dan Keuangan
17	PC	Ka.Subag Program dan Keuangan
18	PC	Ka.Subag Program dan Keuangan
19	PC	Ka.Subag Program dan Keuangan
20	PC	Ka.Subag Program dan Keuangan
21	Laptop	Ka.Subag Program dan Keuangan
22	Laptop	Ka.Subag Program dan Keuangan
23	Laptop	Ka.Subag Program dan Keuangan

(Sumber : Data Penelitian 2019)

3.2.2 Analisis Software / Perangkat Lunak

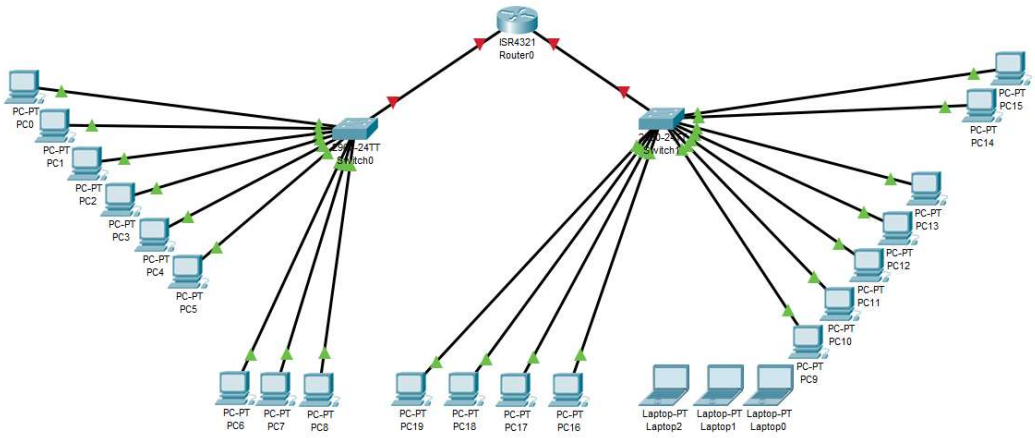
Perangkat lunak adalah komponen dalam pengolahan data yang berupa perangkat lunak. Berdasarkan hasil analisis peneliti, perangkat lunak yangdigunakan di Kantor Kecamatan Sungai Beduk saat ini menggunakan perangkat lunak yang umum seperti berikut :

1. Sistem Operasi yang digunakan :
   a. *Windows 10.1 Home Edition*
   b. *Windows 7 Proffesional*
2. Aplikasi Pendukung : *Microsoft Office 2013*

3.2.3 Topologi Jaringan

Berdasarkan dari hasil observasi langsung oleh peneliti, sistem jaringan internet di Kecamatan Sungai Beduk menggunakan *Topologi Star*. Menurut Syafrizal (2012), karakteristik dari topologi jaringan ini adalah *node (station)* berkomunikasi langsung dengan *station* lain melalui *central node (hub/switch), traffic* data mengalir dari *node* ke *central node* dan diteruskan ke *node (station)* tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak akan terputus.

Berikut adalah gambaran mengenai topologi yang sedang digunakan di Kantor Kecamatan Sungai Beduk :



Gambar 3.1 Topologi Star
(Sumber : Data Penelitian 2019)

3.2.4 SOP Jaringan

3.2.4.1 Penjelasan Singkat Penggunaan

1. Ruang Lingkup

Ruang lingkup SOP ini mencakup beberapa rangkaian kerja, yaitu lingkup instalasi dan pemasangan akses jaringan pada jaringan *LAN* yang meliputi : penyediaan dan persiapan kabel *UTP* beserta kebutuhan panjang kabel *UTP*, proses *crimping konektor RJ-45*, instalasi konektor kabel *UTP* pada *switch, face plate dan PC/ laptop*, *setting* konfigurasi pada *switch/core switch/access point* dengan penerapan segmentasi *VLAN*, penerapan seting *IP address/subnet mask/gateway/proxy, testing kabel* dan akses *node* menuju *ga*teway. Pelaporan

hasil pekerjaan disimpan pada dokumentasi instalasi akses jaringan *LAN*. SOP ini hanya berlaku di lingkungan instansi Kecamatan Sungai Beduk.

2. Tujuan

Tujuan penyusunan SOP adalah untuk memberikan pedoman bagi pelaksanaan kegiatan dalam hal pemasangan/ instalasi akses jaringan pada jaringan *LAN*. Dengan diterbitkannya SOP ini, kegiatan instalasi akses jaringan *LAN* diharapkan dapat dilaksanakan oleh pengguna secara jelas, efektif, efisien, dan terukur. Pencapaian tujuan SOP sangat ditentukan oleh kualitas tim teknis IT dalam menguasai sistem dan konfigurasi jaringan baik bersifat *hardware, software* maupun konsep-konsep dalam TI. Selain itu, juga harus memperhatikan urutan rangkaian instruksi kegiatan yang telah ditetapkan.

3. Ringkasan

Ringkasan Penjelasan singkat penggunaan SOP Penanganan Akses Jaringan Pada Jaringan Internet sebagai berikut :

a. Instansi Kecamatan Sungai Beduk meminta pemasangan layanan akses jaringan *LAN* kepada pihak ketiga atau penyedia layanan menggunakan *email*/ telepon/surat.
b. Pihak Ketiga menginstruksikan teknisi jaringan untuk melakukan survei lokasi dan mencatat semua kebutuhan material supportnya.
c. Teknisi pihak ketiga atau penyedia jaringan melakukan survei lokasi dan mencatat estimasi kebutuhan material instalasi jaringan.

d. Teknisi pihak ketiga atau penyedia jaringan melaporkan hasil survei lokasi dan kebutuhan material instalasi jaringan kepada koordinator jaringan.

e. Instansi Kecamatan Sungai Beduk menerima laporan hasil survei dari teknisi jaringan serta mereview kebutuhan material perangkat apakah sudah tersedia atau tidak.

f. Jika "Ya", Kecamatan Sungai Beduk menginstruksikan pihak ketiga atau penyedia untuk melaksanakan instalasi akses jaringan *LAN*.

g. Teknisi pihak ketiga atau penyedia jaringan mencatat semua hasil pekerjaannya dan melaporkannya kepada Kecamatan Sungai Beduk bahwa instalasi akses jaringan *LAN* sudah selasai.

4. Istilah dan Definisi

Batasan atau definisi yang definitif tentang teknologi informasi dan konsep jaringan komputer perlu ditetapkan agar tidak terjadi kesalahan penafsiran dan interpretasi.

a. *Switch* : Adalah suatu perangkat keras yang di gunakan pada *layer data-link* yang memungkinkan terjadinya *Hub Router Firewall Core Switch NIC VLAN Access Point* distribusi *packet* data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan di banyak *layer* sehingga packet data dapat langsung sarnpai ke tujuan.

b. *Hub* : adalah perangkat jaringan yang sederhana dan tidak mengatur alur jalannya data di jaringan sehingga setiap *packet* data yang melewatinya

akan dikirim *(broadcast)* ke semua *port* yang ada hingga *packet* data tersebut sarnpai ke tujuan.

c. *Router* : Adalah perangkat jaringan yang menghubungkan antar dua atau lebih jaringan/ *network* untuk meneruskan data dari satu jaringan ke jaringan lainnya.

d. *Firewall* : adalah adalah suatu mekanisme sehingga suatu *client* dari luar dilarang/dibolehkan mengakses ke dalam jaringan (atau *client* yang berada di dalam dilarang/dibolehkan mengakses keluar jaringan) berdasarkan aturan-aturan yang ditetapkan.

e. *Core Switch* : adalah perangkat *switch Layer* 3 yang memiliki kemampuan untuk melakukan routing dan *VLAN management.*

f. *NIC* : adalah sebuah *Network Interface Car*d yang merupakan perangkat yang memungkinkan komputer untuk bergabung bersama dalam *LAN*, atau jaringan area lokal. Fungsi *NIC* adalah sebagai penghubung bagi komputer untuk mengirim dan menerima data pada *LAN.*

g. *VLAN* : adalah merupakan pendekatan *switching* yang sangat membantu kinerja dari jaringan karena bisa memperkecil *broadcast* domain, melakukan segmentasi pada *layer* 3 serta dapat melakukan pengalamatan IP dalam *subnetting.*

h. *Access Point* : adalah sebuah perangkat jaringan yang berisi sebuah *transceiver* dan antena untuk transmisi dan menerima sinyal ke dan dari *clients remote.*

i. *Wifi* : adalah standar *IEEE 802. llx* dengan menggunakan LAN WLAN Kabel *UTP teknologi wireless/ nirkabel* yang mampu menyediakan akses internet dengan *bandwidth* yang bisa mencapai 11 *Mbps.*

j. *TIK* : adalah teknologi yang menyertai proses komunikasi untuk menyampaikan informasi.

k. *LAN* : adalah jaringan kornputer dimana jaringannya hanya mencakup wilayah kecil dan berbasis pada teknologi *IEEE 802.3 ethernet* yang lebih sering menggunakan perangkat *switch* serta mempunyai kecepatan transfer data 10, 100, atau 1000 *Mbit/s* atau *Giga Ethernet*.

l. *WLAN* : adalah merupakan *Local Area Network (LAN)* yang menggunakan teknologi *Wireless* (tanpa kabel / nirkabel).

m. Kabel *UTP* : adalah kabel yang biasa digunakan untuk membuat jaringan atau *network* kornputer berupa kabel yang didalamnya berisi empat (4) pasang kabel yang yang setiap pasangnya adalah kernbar dengan ujung konektor *RJ-45.*

n. Kabel *FO* :adalah sebuah kabel yang terbuat dari serat kaca dengan teknologi canggih dan mempunyai kecepatan transfer data yang lebih cepat daripada kabel biasa, biasanya *fiber optic* digunakan pada jaringan *backbone.*

o. *Intranet* : adalah sebuah jaringan kornputer berbasis protokol *TCP/IP* seperti internet hanya saja digunakan dalam internal perusahaan atau kantor.

p. *Internet* : adalah sistem global dari seluruh jaringan kornputer yang saling terhubung menggunakan standar *Internet Protocol Suite (TCP/IP)* untuk melayani miliaran pengguna di seluruh dunia.

q. *Crimping Tool* : adalah alat untuk memasang kabel *UTP* ke konektor *RJ-45 / RJ-11* tergantung kebutuhan dengan fungsi yang bisa memotong kabel, mengupas dan lain sebagainya.

r. *Connector RJ-45* : adalah konektor kabel *Ethernet* yang biasa digunakan dalam topologi jaringan kornputer *LAN* maupun jaringan komputer tipe lainnya.

s. Kabel Tester : adalah alat untuk memeriksa kesempurnaan pemasangan kabel konektor *LAN (RJ45)* dimana fungsinya agar bisa mengetahui kabel *LAN* yang ingin kita pakai itu sudah sempurna atau tidak.

3.3 Lokasi dan jadwal Penelitian

3.4.1. Lokasi

Pelaksanaan Penelitian ini dilakukan di Kantor Kecamatan Sungai Beduk, dengan mempertimbangkan hal-hal sebagai berikut :

1. Ketersediaan data pendukung
2. Kemudahan dalam mendapatkan data
3. Efisiensi waktu dan biaya

3.4.2. Jadwal Penelitian

Setiap rancangan penelitian perlu dilengkapi dengan jadwal kegiatan yang akan dilaksanakan yang berisi jadwal kegiatan apa saja yang akan dilakukan selama penelitian (Sugiyono, 2014: 286). Berikut akan ditampilkan jadwal penelitian selama penelitian berlangsung :

Tabel 3.2 Jadwal Penelitian

No	Kegiatan	Tahun 2018/2019															
		Okt 2018				Nov 2018				Des 2018				Jan 2019			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan Judul Penelitian																
2	Penyusunan Bab I																
3	Penyusunan Bab II																
4	Penyusunan Bab III																
5	Penyusunan Bab IV																
6	Penyusunan Bab V, Daftar Pustaka, Lampiran																

(Sumber : Data Penelitian 2019)