BAB I
PENDAHULUAN

2.1 Latar Belakang

Menurut Wahyudiyono (2020), menjelaskan bahwa penggunaan internet untuk kehidupan sehari-hari terus berkembang dengan pesat. Berdasarkan survei yang diadakan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) yang dilaksanakan bulan April 2020, jumlah pengguna internet di Indonesia Sebesar 171,7 juta jiwa atau sekitar 64,8% dari total populasi penduduk Indonesia sebanyak 264 juta jiwa. Pengguna internet tersebut meningkat 10,2% atau 27,9 juta orang yang dibandingkan dengan pengguna internet tahun sebelumnya (APJII 2020). Kenaikan ini disebabkan karena ada pembangunan infrastruktur diberbagai daerah seperti ketersediaan *fiber optic* dan infrastruktur pendukung lainnya yang menopang aktivitas berinternet yang dilakukan oleh 540 anggota APJII. Kontribusi terbesar atas penetrasi internet di Indonesia berasal dari pulau Jawa yaitu 55% dari total keseluruhan populasi. Pengguna internet Indonesia mayoritas adalah masyarakat dengan rentang usia 15-19 tahun, diikuti dengan usia 20-24 tahun, 25-29 tahun dan 30-34 tahun dan yang paling sedikit adalah pengguna dengan usia 5-9 tahun dan 65 tahun ke atas.

Pada dunia digital saat ini, hampir semua orang menggunakan teknologi komputer yang terhubung dengan dunia internet. Dengan kemajuan teknologi internet saat ini kebutuhan serta pekerjaan dapat dengan mudah dikerjakan, semua informasi yang kita butuhkan dapat kita temui dengan internet menggunakan fitur "*Google Search*". Dengan kemajuan internet pula kita dapat berkomunikasi dengan siapapun dari jarak yang jauh sekalipun, atau kita bisa juga membagikan yang diinginkan. Dengan perkembangan teknologi internet yang sangat pesat, ada pula orang yang tidak bertanggung jawab memanfaatkan hal tersebut untuk melakukan sebuah penyerangan untuk bisa masuk dalam sistem komputer sehingga mendapatkan data-data penting dan menjadi sebuah keuntungan bagi orang yang tidak bertanggung jawab. (Muammar, dkk. 2021)

Gollman (dalam Rendra & dkk, 2020) menjelaskan bahwa keamanan suatu komputer merupakan berhubungan dengan pencegahan diri dan deteksi terhadap

tindakan yang mengganggu yang tidak dikenali di sistem komputer. Pada keamanan sistem komputer yang harus dilakukan adalah untuk mempersulit orang lain mengganggu komputer yang sifatnya pribadi, jaringan *local* ataupun jaringan global. Harus dipastikan sistem dapat berjalan dengan baik atau lancar serta kondusif, selain itu program dari aplikasinya masih dapat dipakai tanpa adanya suatu masalah. Melesatnya teknologi, juga dapat menimbulkan kewaspasdaan terhadap serangan siber yang dapat menyerang kapanpun, dimanapun dan dengan media apapun. Sehingga perlu adanya peningkatan keamanan internet, tidak hanya untuk individu, perusahaan swasta, bahkan di pemerintahan.

SMPN 6 Satap Baebunta yang beralamatkan di Baebunta, Kec. Baebunta, Kabupaten Luwu Utara merupakan salah satu sekolah menegah pertama negeri yang sudah memiliki sarana dan prasarana di bidang IT salah satunya fasilitas jaringan internet sebagai salah satu media pendukung informasi yang dimana pengguna jaringan internet dengan media *wireless* yang terbuka terhadap pemakai-pemakainya baik pegawai maupun pengunjung. Penggunaan tersebut bisa dipergunakan dengan benar maupun disalahgunakan oleh pemakainya.

Menurut kepala sekolah SMPN 6 Satap Baebunta Bapak Maikel menjelaskan bahwa masalah yang sering terjadi di yaitu lambatnya jaringan dikarenakan banyaknya pihak pengguna dalam hal ini pegawai maupun pengunjung dalam mengakses jaringan *wireless* internet tanpa adanya pengamanan atau pendeteksian lalu lintas data atau paket-paket yang masuk atau pihak yang tidak bertanggung jawab dapat menganalisa dan berusaha melakukan koneksi melalui aplikasi tertentu. Hal inilah yang mengakibatkan penurunan performa jaringan internet.

Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang terjadi. Sistem yang hanya mendeteksi ini akan di implementasikan dengan menggunakan aplikasi *Intrucsion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* yaitu *Snort* sebagai penindak lanjut terhadap *alert snort* yang dihasilkan. Dengan adanya sebuah keamanan *Intrucsion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* yaitu *Snort* dan sebagai penindak lanjut terhadap *alert snort* yang dihasilkan sehingga peningkatan sistem keamanan jaringan dan komputer akan lebih

meningkat dari sebelumnya seperti adanya serangan ataupun penyalahgunaan jaringan. Perancangan sistem yang akan digunakan untuk merancang suatu sistem yang sebelumnya membutuhkan *tools* dan komponen yang diperlukan untuk membangun sistem tersebut yang nantinya akan bekerja sama untuk mendapatkan hasil yang maksimal.

Berdasarkan pemasalahan di atas maka penulis akan menganalisa keamanan jaringan dengan judul "Analisis Sistem Keamanan Jaringan Dengan Metode IDS dan IPS pada SMPN 6 Satap Baebunta".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka disusun rumusan masalah yang akan dibahas yaitu bagaimana menganalisis sistem keamanan jaringan dengan metode IDS dan IPS pada SMPN 6 Satap Baebunta?

1.3 Tujuan Masalah

Adapun tujuan dari penelitian ini untuk mengetahui hasil analisis keamanan jaringan dengan metode IDS dan IPS pada SMPN 6 Satap Baebunta.

1.4 Manfaat Penelitian

Manfaat yang bisa di dapat dalam penelitian ini adalah sebagai berikut:

1. Manfaat bagi Instansi terkait.

   Diharapkan dengan adanya dengan adanya penelitian ini dapat meningkatkan keamanan jaringan internet bagi SMPN 6 Satap Baebunta.

2. Manfaat bagi Penulis

   Merupakan studi khsus yang baru dalam merangcang sebuah sistem keamanan jaringan yang diperoleh selama duduk di bangku kuliah dan sebagai pembekalan dalam menghadapi dunia kerja.

3. Manfaat bagi Akademik

Diharapkan dari hasil akan memberikan suatu referensi yang berguna dalam perperkembangan dunia akademik khususnya dalam penelitian-penelitian yang akan datang. Dapat pula memberikan sumbangan pemikiran bagi perkembangan teknologi informasi dalam dunia ilmu pengetahuan penulis.

1.5 Batasan Penelitian

1. Penelitian ini hanya di lakukan pada SMPN 6 Satap Baebunta.
2. Penelitian ini menggunakan metode *Intruction Detection System* (IDS) dan *Intrusion Prevention System (IPS)* dalam menganalisis keamanan jaringan pada SMPN 6 Satap Baebunta.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Bagian ini merupakan penjelasan mengenai teori-teori dan beberapa sumber dan menjadi referensi dalam penulisan penulis.

1. Analisis

Menurut Komaruddin dalam (Yuni, dkk .2020), menjelasakan bahwa pengertian analisis adalah kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu. Menurut Harahap dalam (Azwar, 2019), menjelaskan bahwa pengertian analisis adalah memecahkan atau menguraikan sesuatu unit menjadi unit terkecil.

Riadi (2020), mendefinisikan Analisis yaitu proses untuk menentukan kebutuhan yang diperlukan untuk membangun jaringan komputer, sistem *gateway* sekaligus sebagai pemfilter beberapa aplikasi. Analisis dilakukan untuk membuat suatu bentuk rancangan jaringan komputer yang akan digunakan dalam penelitian ini.

Jadi dapat disimpulkan anilisis adalah kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu untuk menentukan kebutuhan yang diperlukan untuk membangun jaringan komputer, sistem *gateway* sekaligus sebagai pemfilter beberapa aplikasi.

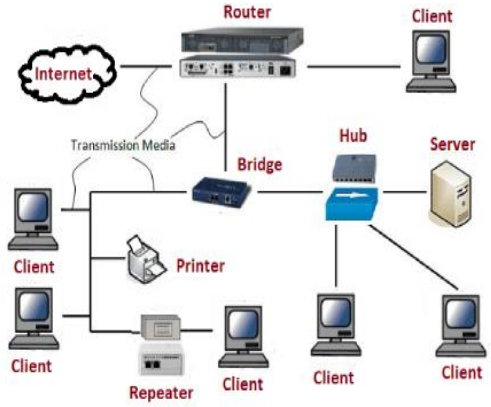
2. Sistem Keamanan Jaringan Komputer

Kemajuan jaringan komputer sekarang ini sudah sangat melekat dengan gaya hidup manusia moderen. Hampir setiap peralatan berbasis komputer memanfaatkan jaringan komputer untuk berkomunikasi data, baik komunikasi dengan *device* yang sama, maupun berbeda. Jaringan komputer adalah cikal bakal munculnya teknologi internet yang saat ini sangat berpengaruh di kehidupan manusia moderen. Pengetahuan tentang jaringan komputer menjadi fondasi

penting untuk mengembangkan teknologi canggih masa depan yang berjalan di atas internet (Mulyanto, dkk., 2022).

Menurut Dasmen & Khudri (dalam Dasmen, dkk., 2022) menjelaskan bahwa jaringan komputer adalah setidaknya dua PC yang terkait satu sama lain dan digunakan untuk berbagi informasi. Sebuah organisasi bekerja dengan perpaduan peralatan dan pengaturan pemrograman untuk membuat kerangka kerja yang dapat bekerja secara konsisten.

Menurut Widya, dkk., (2022), menjelaskan bahwa jaringan atau biasa disebut dengan *network* merupakan sistem pengoperasian yang menghubungkan beberapa perangkat komputer atau perangkat lain yang bisa terkoneksi dengan komputer. Jaringan komputer sendiri terdiri dari beberapa tipe, berbentuk fisikal ada yang berbentuk nirkabel. Jaringan fisikal artinya jaringan yang masih menggunakan benda fisik seperti kabel untuk melakukan koneksi.



Gambar 1. Jaringan Komputer
Sumber: mediaindonesia.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

Keamanan jaringan komputer ini mencakup ke beberapa jaringan komputer, baik swasta maupun negeri, untuk dilakukan pada pekerjaan sehari-hari dalam transaksi dan komunikasi dikalangan bisnis, instansi pemerintahan dana individu. Dari pengamatan pada keamanan maka keamanan jaringan komputer dapat dilihat dari segi bentuknya, yaitu keamanan *hardware* berhubungan pada perangkat keras yang digunakan dalam jaringan komputer (Widya, dkk., 2022).

Menurut Winrou & Risal (2020), menjelaskan bahwa keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk kedalam sistem jaringan komputer. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Langkah-

langkah pencegahan dapat membantu administrator untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat menggangu aktivitas yang sedang terjadi pada sistem jaringan komputer. Ada tiga hal dalam konsep keamanan jaringan, yaitu ingkat bahaya, ancaman dan kerapuhan sistem.

a. Bentuk Ancaman Keamanan Jaringan Komputer

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer penyalahgunaan informasi *Internet of Things*, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer (Zen & Novianti, 2020).

1) Pertama Kesalahan Informasi *Internet of Things*, biasanya dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs *web* dan mengunduh gambar, file, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs *web*, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer.
2) Kedua serangan pada layanan latar belakang, serangan latar belakang berupa penolakan layanan yang disebut adalah bahwa pengguna sengaja menunda atau secara ilegal menunda layanan jaringan dalam proses mengunjungi situs *web* atau mengunduh file seperti biasa, sehingga menyebabkan kerusakan tertentu pada keamanan jaringan komputer.
3) Ketiga kehancuran integritas keamanan jaringan komputer, peretas atau orang lain yang tidak mematuhi kode etik dengan sengaja menggunakan berbagai cara ilegal untuk menghancurkan keamanan jaringan komputer, sehingga memengaruhi integritas keamanan komputer.

4) Keempat memberitahukan informasi komputer, ketika informasi dalam jaringan komputer ditransmisikan secara langsung ke entitas yang tidak sah tanpa izin dari pengguna, maka sudah pasti informasi menjadi rentan.

b. Faktor-Faktor yang Mengancam Kemanan Jaringan Komputer

Ada banyak faktor yang mengancam keamanan jaringan komputer, yang dapat dibagi menjadi faktor subyektif dan faktor obyektif. Untuk menggambarkan faktor-faktor yang mengancam keamanan jaringan komputer agar lebih komprehensif (Zen & Novianti, 2020):

1) Spam dan *Spywere*

Dalam bentuk komunikasi yang biasa, berkirim *email* adalah cara yang lebih umum digunakan. Terutama di semua jenis pekerjaan seringkali, *email* memainkan peran yang sangat penting dalam melakukan pekerjaan. Karena alasan ini, maka banyak penjahat ingin menggunakan *email* untuk mencuri privasi pengguna atau ada tujuan lain. Mereka terutama memaksa pengguna untuk menerima spam dengan memasukkannya ke dalam *email* yang mereka kirimkan.

2) Ancaman dan Serangan *Hacker*

Peretas merujuk pada sekelompok orang dengan kecerdasan dan kemampuan tinggi, yang akrab dengan pengetahuan komputer dan sangat pandai dalam keamanan jaringan komputer.

3) Implantasi

Pengguna komputer takut terhadap virus komputer, karena virus dapat disisipkan ke berbagai jenis aplikasi program, pengguna dengan tidak sengaja akan mengklik virus tersebut, selanjutnya virus dengan cepat menyebar ke seluruh bagian sistem komputer.

4) Pintu Belakang dan Kebocoran Perangkat Lunak Komputer

Tidak ada perangkat lunak di dunia yang sempurna, sehingga banyak peretas suka memilih peranti lunak untuk diserang. Disebut "*backdoor*" berarti programmer meninggalkan pintu untuk di awal perancangan perangkat lunak, sehingga turut "memfasilitasi" operasi masa depan mereka.

5) Bencana Alam

Bencana alam yang dimaksud merujuk pada penyebab yang tidak dapat dikendalikan seperti perubahan kelembaban, suhu, gempa bumi atau gempa bumi

yang menyebabkan tsunami, pemadaman listrik yang tiba-tiba atau kecelakaan asupan air komputer. Penyebab alami ini berada di luar kendali manusia dan tidak bisa sepenuhnya dihindari. Karena itu, jika ingin meningkatkan keamanan jaringan komputer, kita harus melakukannya mulai dari aspek lain.

6) Sistem Serangan Langsung

Dengan perkembangan ilmu pengetahuan dan teknologi, beberapa orang yang akrab dengan komputer langsung menyerang sistem komputer orang lain melalui jaringan komputer yang dimiliki. Jenis kejahatan ini muncul dengan pengembangan bidang komputer. Serangan secara langsung pada sistem ini lebih canggih, bahkan tanpa meninggalkan beberapa jejak

c. Jenis-Jenis Jaringan Komputer

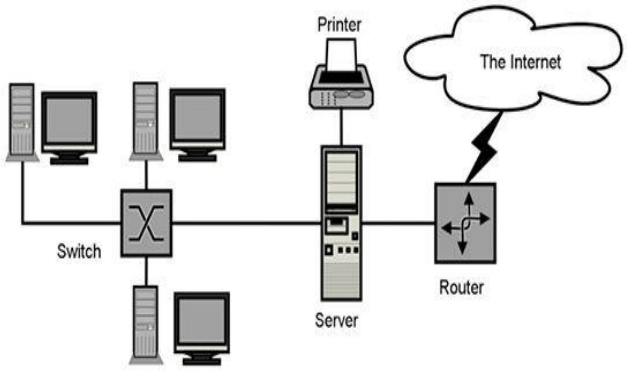
Jenis jaringan komputer terbagi menjadi 4 bagian, pertama: berdasarkan topologi, kedua: berdasarkan area/skala dan ketiga: berdasarkan media penghantar, dan keempat: berdasarkan fungsi (Widya, dkk., 2022):

1) Jaringan Komputer Berdasarkan Jangkauan

Jaringan komputer berdasakan jangkauan terdiri atas tiga yaitu:

a) *Local Area Network*

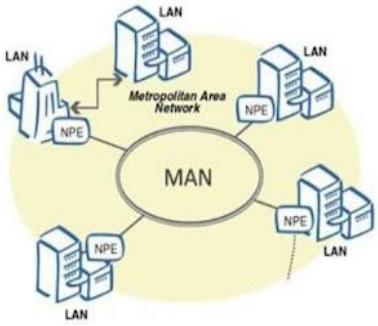
Local Area Network (LAN) merupakan jaringan yang meliputi cakupan wilayah yang kecil, seperti lingkungan kampus, sekolah, atau 1 gedung.



Gambar 2. *Local Area Network* (LAN)
Sumber: jalantikus.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

b) *Metropolitan Area Network*

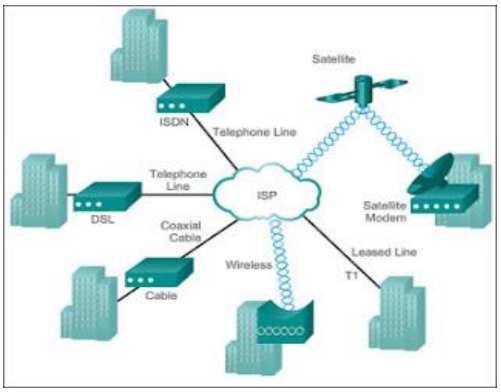
Metropolitan Area Network (MAN) merupakan jaringan yang meliputi cakupan wilayah dalam 1 kota.



Gambar 3. *Metropolitan Area Network* (MAN)
Sumber: www.isky.web.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

c) *Wide Area Network*

Wide Area Network (WAN) merupakan jaringan yang meliputi cakupan wilayah yang luas, seperti antar negara.

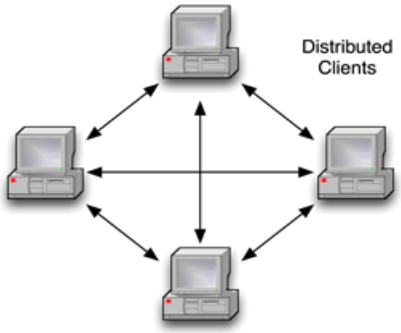


Gambar 4. *Wide Area Network* (WAN)
Sumber: www.isky.web.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

2) Jaringan Komputer Berdasarkan Fungsi

a) *Peer to Peer*

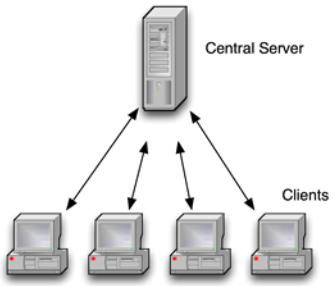
Peer to Peer adalah jaringan komputer dimana setiap komputer dapat bertindak sebagai *server* dan dapat bertindak juga menjadi *client*.



Gambar 5. *Peer to Peer*
Sumber: www.dictio.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

b) *Client Server*

Di dalam model *client/server*, perangkat yang meminta (*request*) informasi atau layanan disebut klien (*client*) dan perangkat yang memberikan layanan pada permintaan tersebut disebut *server*.



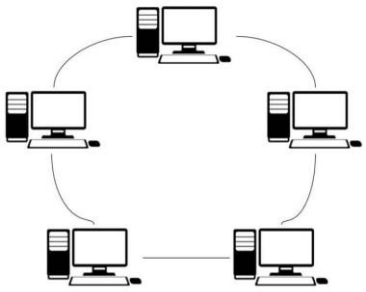
Gambar 6. *Client Server*
Sumber: www.dictio.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

3) Jaringan Komputer Berdasarkan Topologi

Pada jaringan komputer dan komunikasi data dikenal beberapa jenis topologi jaringan. Topologi jaringan merupakan cara perangkat-perangkat pada jaringan komunikasi data saling terhubung satu dengan lainnya. Topologi dasar terdiri dari 4 macam yaitu (Agita, 2022):

a) *Ring*

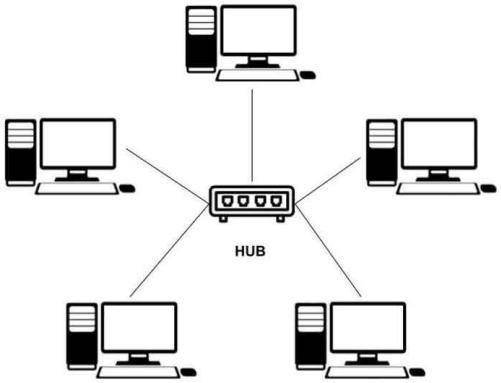
Topologi *Ring* merupakan topologi yang berbentuk cincin dimana setiap node terhubung ke dua node disebelahnya sedemikian rupa sehingga membentuk cincin.



Gambar 7. Topologi *Ring*
Sumber: mediaindonesia.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

b) *Star*

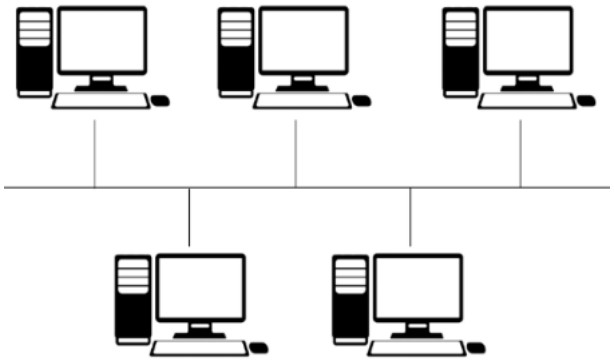
Topologi *Star* merupakan topologi jaringan di mana setiap node terhubung dengan node lainnya menyerupai bentuk bintang. Semua node yang ada terkoneksi ke 1 buah node utama yang terletak di tengah-tengah jaringan.



Gambar 8. Topologi *Star*
Sumber: mediaindonesia.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

c) *Bus*

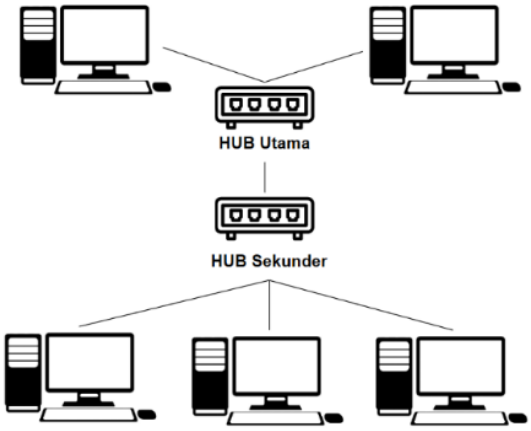
Topologi *Bus* menggunakan kabel utama sebagai pusat lalu lintas jaringan. Semua node pada topologi *bus* terhubung secara serial pada kabel utama tersebut.



Gambar 9. Topologi *Bus*
Sumber: mediaindonesia.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

d) *Tree* (*Hybrid*)

Pada dasarnya topologi *tree* atau *hybrid* merupakan gabungan antara topologi *star* dan topologi *bus*. *Switch* dan *hub* sangat berperan dalam pembentukan topologi ini. Karena topologi ini dapat dibangun dengan menggunakan beberapa *hub/switch* yang saling terhubung satu sama lain untuk membuat *bus*. Dalam pengembangan teknologi jaringan terkini, *bus* banyak dibuat dengan menggunakan *media fibre optic*, sedangkan *switch* dan *hub* digunakan untuk membentuk topologi *star* yang menghubungkan antara *front-end* (komputer *client*) dengan topologi *bus* dan kontrol pusat (*server*).



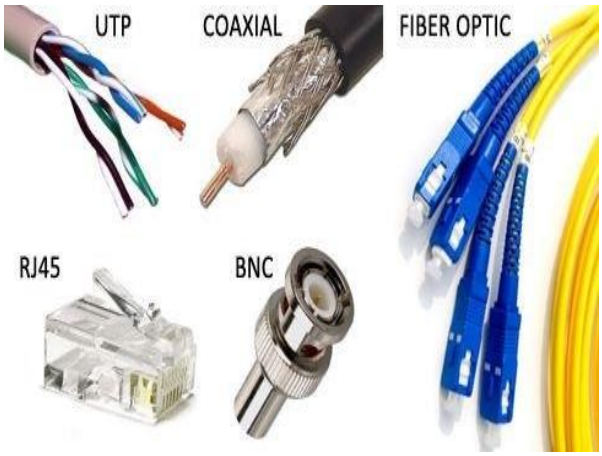
Gambar 10. Topologi *Tree (Hybrid)*
Sumber: mediaindonesia.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

4) Jaringan Komputer Berdasarkan Media Pengantar

Pada jaringan komputer berdasakan media pengantar dikenal beberapa jenis jaringan yang merupakan cara perangkat-perangkat pada jaringan komunikasi data saling terhubung satu dengan lainnya. Berikut ini jaringan komputer berdasarkan media pengantar (Widya, dkk., 2022):

a) *Wire Network*

Wire network adalah jaringan komputer yang menggunakan kabel sebagai media penghantarnya. Kabel yang digunakan untuk membangun jaringan komputer cukup beragam, diantaranya menggunakan kabel *Coaxial*, UTP (*Unshielded Twisted Pair*), STP (*Shielded Twisted Pair*), dan *Fibre Optic*. Pada ujung-ujung kabel, digunakan konektor agar kabel terhubung dengan perangkat jaringan, seperti konektor BNC dan RJ45 (Widya, dkk., 2022).



Gambar 11. *Wire Network*
Sumber: https://netsolution.co.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

b) *Wireless Network*

Wireless network adalah suatu jaringan tanpa kabel dimana media transmisinya menggunakan frekuensi radio (RF) dan infrared (IR), untuk memberi sebuah koneksi jaringan ke seluruh pengguna dalam area disekitarnya. Area jangkauannya dapat berjarak dari ruangan kelas ke seluruh kampus atau dari kantor ke kantor yang lain dan berlainan gedung. Peranti yang umumnya digunakan untuk jaringan *wireless* termasuk di dalamnya adalah PC, Laptop, PDA, telepon seluler, dan lain sebagainya (Widya, dkk., 2022).



Gambar 12. *Wireless Network*
Sumber : https://hendri.staff.uns.ac.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

d. Perangkat Jaringan Komputer

Perangkat jaringan komputer merupakan perangkat jaringan yang memiliki peruntukan yang berbeda antara penyedia, penerima informasi dan perangkat keras yang bertugas mendistribusikan data informasi pada jaringan baik secara *broadcast* maupun terarah sesuai dengan alamat yang terdapat pada data tersebut dan juga perangkat media penyampaian informasi. Berikut ini beberapa perangkat jaringan komputer yaitu (Widya, dkk., 2022):

1) *Router*

Router adalah perangkat jaringan komputer yang menghubungkan dua atau lebih jaringan yang berbeda *network* dan mampu menjalankan *packet-switched*. Fungsi utama *router* yaitu mengelola lalu lintas jaringan dengan memilah dan meneruskan paket data ke alamat IP yang dituju yang ada pada *header packet* data dan memungkinkan beberapa jaringan yang berbeda *network* bisa menggunakan koneksi internet yang sama. Dalam implementasinya *router* diletakkan pada *border* jaringan atau biasa disebut *gateway* yang memisahkan antara jaringan

publik dan jaringan *local* atau pada sub jaringan dalam jaringan lokal (Widya, dkk., 2022).



Gambar 13. *Router*
Sumber : ilmuelektro.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

2) *Switch*

Menurut Spurgeon & Zimmerman dalam (Widya, dkk. 2022), menjelaskan bahwa *switch* merupakan komponen jaringan komputer yang memiliki fungsi menghubungkan beberapa komputer menjadi satu jaringan komunikasi yang sama atau ke banyak segmen jaringan, untuk menerima, memproses dan meneruskan data ke perangkat yang di tuju. *Switch* bekerja pada lapisan *Data-link* dan sama seperti *bridge*.



Gambar 14. *Switch*
Sumber : ilmuelektro.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

3) *Repeater*

Repeater adalah perangkat jaringan yang memperkuat atau meregenerasi sinyal yang masuk. Saat mentransmisikan data melalui media *ethernet* fisik, kualitas sinyal akan menurun seiring waktu dan jarak. Hal ini pada akhirnya akan

menyebabkan penurunan kualitas pada transmisi. *Repeater* akan mencoba menjaga sinyal tetap kuat dan mencegah degradasi hingga paket data mencapai tujuannya (Widya, dkk., 2022).



Gambar 15. *Repeater*
Sumber : ilmuelektro.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

4) *Hub*

Hub adalah perangkat yang dapat digunakan untuk menghubungkan dua komputer atau lebih sehingga dapat membentuk suatu jaringan. Tetapi penggunaan *hub* saat ini jarang digunakan karena fungsinya sama seperti *switch* (Widya, dkk., 2022).



Gambar 16. *Hub*
Sumber : ilmuelektro.id(diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

5) *Bridge*

Bridge merupakan suatu perangkat jaringan yang bisa menjembatani 2 atau lebih arsitektur jaringan yang berbeda karakteristik media transmisi yang

digunakan dan arsitektur yang berbeda sehingga akan membentuk suatu segmen jaringan tersendiri. Seperti menggabungkan antara topologi jaringan yang menggunakan serat optik dan topologi jaringan yang menggunakan kabel UTP ataupun menggunakan topologi nirkabel (Widya, dkk., 2022).



Gambar 17. *Bridge*
Sumber : ilmuelektro.id(diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

6) *Ethernet Card*

Ethernet card merupakan suatu perangkat keras jaringan yang digunakan untuk menghubungkan komputer atau perangkat *end device* dengan jaringan lokal ataupun jaringan internet baik menggunakan media *copper* media, serat optik ataupun menggunakan frekuensi *wireless*. *Ethernet card* memiliki penyebutan yang berbeda-beda tergantung dari media apa yang digunakan untuk mengirimkan data dari sumber ke tujuan. LAN *card* (*Local Area Network Card*) biasanya penyebutan ini digunakan untuk merujuk pada kartu jaringan berbasis *copper* media baik menggunakan UTP atau STP, *Wireless Ethernet card* merupakan kartu jaringan berbasis *wireless*. *Fiber optic Ethernet card* merupakan kartu jaringan berbasis *fiber optic* dan NIC merupakan penyebutan umum kartu jaringan atau *ethernet card* itu sendiri (Widya, dkk., 2022).



Gambar 18. *Ethernet card*
Sumber : ilmuelektro.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

7) Media Transmisi

Media transmisi atau transmision medium merupakan media atau jalur yang digunakan untuk membawa informasi dari pengirim (*sender*) ke penerima (*receiver*). Setiap perangkat jaringan memiliki media transmisi yang berbeda-beda. Informasi yang ditransmisikan dapat berupa sinyal listrik ataupun elektromagnetik (Widya, dkk., 2022).

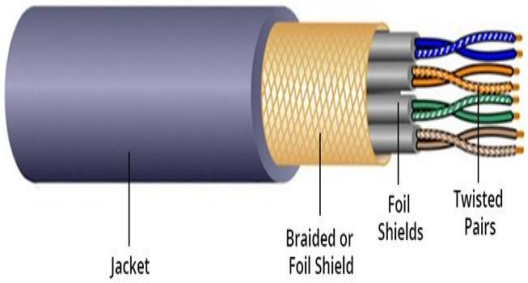
Secara garis besar, media transmisi dapat dibagi menjadi 2 jenis yaitu *Wired* atau *Guided* media dan *Wireless* atau *Unguided* media.

a) *Guided* media/*Wired*

Guided media merupakan jenis media yang memiliki bentuk fisik seperti kabel *twister pair*, kabel serat optik dan kabel *coaxial*. Dikatakan *guided media* karena sinyal listrik atau gelombang dituntun transmisinya melewati media fisik. Ada juga yang menyebutkan *guided* media sebagai *wired* atau *bounded transmission media. Guided* media ini terdiri dari (Widya, dkk., 2022):

(1) *Twisted pair cable*

Pada dasarnya merupakan pasangan kabel tembaga yang di pilin bersama-sama berbentuk spiral dan di bungkus dengan plastik. Kabel *twisted pair* memiliki 2 jenis yaitu *Unshielded Twisted Pair* (UTP) yaitu kabel *twisted* tanpa pelindung interferensi elektromagnetik dan pelindung fisik. *Shielded Twisted Pair* (STP) kabel *twisted* yang memiliki pelindung interferensi elektromagnetik dan pelindung fisik. Kategori kabel ini saat ini yang digunakan dalam jaringan ada 3 jenis yaitu kategori 5, kategori 6 dan kategori 7 (Widya, dkk., 2022).

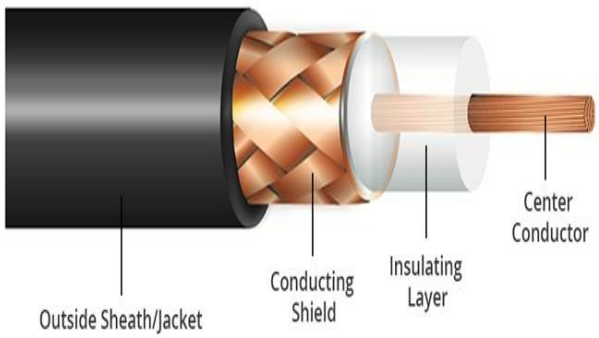


Gambar 19. *Twisted pair cable*
Sumber : www.trivusi.web.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(2) Kabel *coaxial*

Kabel *coaxial* merupakan kabel yang memiliki 2 konduktor, dimana 1 konduktor berada pada rongga luar berbentuk kawat jala dan menyelimuti satu

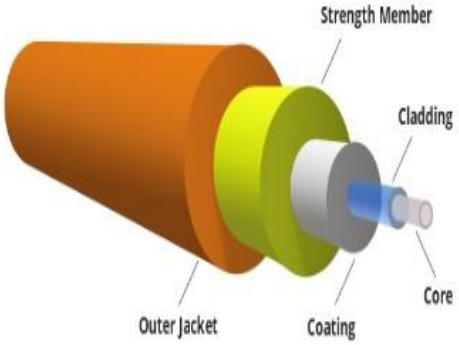
konduktor tunggal berbentuk kabel tembaga yang dipisahkan oleh bahan isolator. Kabel jenis ini sering digunakan untuk mentransmisikan sinyal frekuensi tinggi dalam implementasinya kabel ini digunakan sebagai media transmisi sinyal dari *router* ke antena *wireless outdoor* pada perangkat *router wireless* (Widya, dkk., 2022).



Gambar 20. Kabel *coaxial*
Sumber : www.trivusi.web.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(3) *Fiber Optic Cable*

Fiber Optic Cable merupakan jenis kabel yang terbuat dari serat kaca atau plastik halus yang mampu mentransmisikan sinyal cahaya dari satu tempat ke tempat lainnya. Sumber cahayanya didapatkan dari perangkat *converter* fiber optik *ethernet* yang mengubah sinyal listrik menjadi sinyal cahaya berupa sinar laser. Diameter kabel serat optik sekitar 120 Mikrometer dan keunggulan dari kabel jenis ini adalah jarak jangkauannya yang sangat jauh bisa lebih dari 1 Km. dan tidak terinterferensi oleh gelombang elektromagnetik (Widya, dkk., 2022).



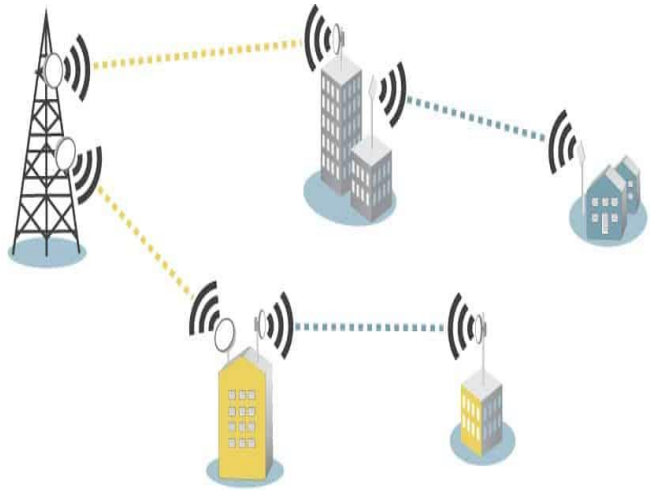
Gambar 21. *Fiber optic cable*
Sumber : www.trivusi.web.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(4) *Unguided Media/Wireless*

Unguided media merupakan media yang menggunakan sistem gelombang elektronik dalam mentransmisikan informasi dari pengirim (*sender*) ke penerima tanpa ada perangkat fisik yang menuntunnya. Istilah lain dari *unguided media* adalah *wireless* dan yang termasuk unguided media antara lain: frekuensi radio, gelombang *microwave*, inframerah dan satelit. *Unguided media* disebut juga dengan *unbounded transmission media* (Widya, dkk., 2022).

(1) Frekuensi Radio

Menurut Widya, dkk., (2022), menjelaskan bahwa frekuensi radio adalah media transmisi yang menggunakan gelombang elektromagnetik dengan kisaran frekuensi diantara 3 kHz hingga 300 Ghz. Frekuensi radio pada umumnya menggunakan antena untuk menyebarkan gelombang elektromagnetiknya seperti antena *omni*, antena *yagi*, antena *sectoral*, antena *grid*, antena *disk* dan lain-lain. Banyak diterapkan pada infrastruktur penyiaran televisi, telepon selular, *metropolitan area network*, penyiaran radio dan lain-lain.



Gambar 22. Frekuensi Radio
Sumber : midteknologi.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(2) Gelombang *Mikro*

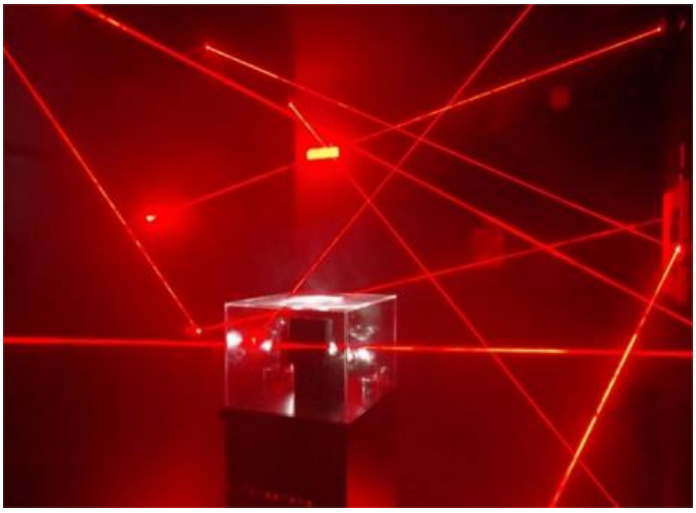
Menurut Widya, dkk., (2022), menjelaskan bahwa gelombang *mikro* adalah media transmisi yang menggunakan gelombang elektromagnetik dengan frekuensi super tinggi (*Super High Frequency*) yaitu frekuensi yang berada di kisaran 3 GHz hingga 30 GHz dengan panjang gelombang sekitar 1 mm hingga 1 m untuk mentransmisikan sinyal dari pengirim ke penerima.



Gambar 23. Gelombang *Mikro*
Sumber : ajeng-rizki.blogspot.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(3) Infra Merah

Menurut Widya, dkk., (2022), menjelaskan bahwa infra merah adalah media transmisi yang menggunakan radiasi elektromagnetik dari panjang gelombang yang lebih panjang dari cahaya tampak tetapi lebih pendek dari radiasi gelombang radio. Infra merah biasanya digunakan pada komunikasi jarak dekat seperti *remote control* pada televisi maupun perangkat elektronika lainnya.



Gambar 24. Infra Merah
Sumber : saintif.com (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

(4) Satelit

Menurut Widya, dkk., (2022), menjelaskan bahwa satelit adalah jenis media transmisi yang menggunakan satelit sebagai penerima sinyal dari stasiun bumi dan memancarnya ke stasiun bumi lainnya. Satelit pada umumnya mengorbit di pada ketinggian 36.000 km dari permukaan bumi. Setiap satelit yang mengorbit akan

beroperasi pada sejumlah band frekuensi yang disebut dengan *channel transponder*. Media transmisi ini sering digunakan untuk siaran televisi, telepon jarak jauh dan jaringan bisnis privat (*Private Business Network*).



Gambar 25. Satelit
Sumber : darilaut.id (diakses pada tanggal 10 Oktober 2024 pukul 20.00 WITA)

3. Arsitektur Internet

Menurut Sritrusta & Rizqi (2020), menjelaskan bahwa internet adalah kumpulan dari jaringan-jaringan komputer yang saling terhubung secara global. Pada dasarnya Internet merupakan WAN, tetapi internet menghubungkan semua komputer di seluruh dunia dan menyediakan layanan publik. Internet dibangun oleh koneksi berbagai jaringan yang dimiliki oleh *Internet Service Provider* (ISPs) sebagai penyedia koneksi internet dengan beragam kecepatan akses bagi para pengguna internet.

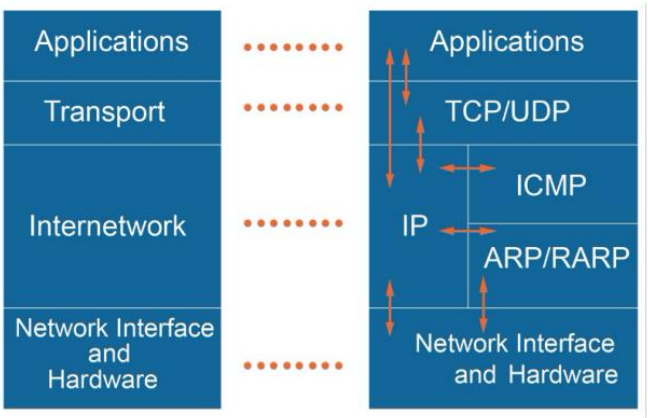
a. Model Arsitektur TCP/IP

Protokol TCP/IP terbentuk dari 2 komponen yaitu *Transmission Control Protocol* (TCP) dan *Internet Protocol* (IP). Tujuan dari TCP/IP adalah untuk membangun suatu koneksi antar jaringan (*network*), dimana biasa disebut *internetwork,* atau *intenet*, yang menyediakan pelayanan komunikasi antar jaringan yang memiliki bentuk fisik yang beragam. Tujuan yang jelas adalah menghubungkan empunya (hosts) pada jaringan yang berbeda, atau mungkin terpisahkan secara geografis pada area yang luas (Sritrusta & Rizqi, 2020).

Aspek lain yang penting dari TCP/IP adalah membentuk suatu standarisasi dalam komunikasi. Tiap-tiap bentuk fisik suatu jaringan memiliki teknologi yang

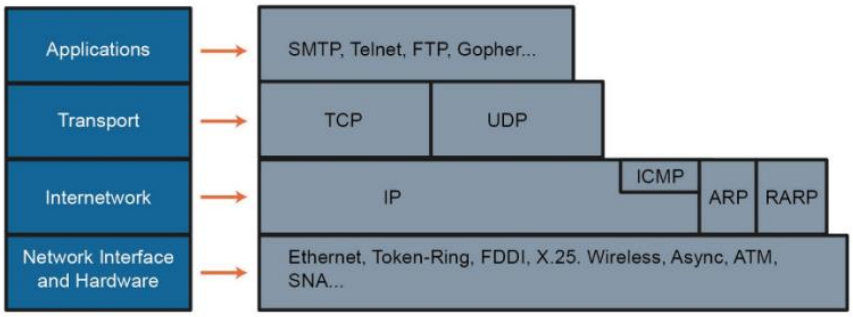
berbedabeda, sehingga diperlukan pemrograman atau fungsi khusus untuk digunakan dalam komunikasi. TCP/IP memberikan fasilitas khusus yang bekerja diatas pemrograman atau fungsi khusus tersebut dari masing-masing fisik jaringan. Sehingga bentuk arsitektur dari fisik jaringan akan tersamarkan dari pengguna dan pembuat aplikasi jaringan. Dengan TCP/IP, pengguna tidak perlu lagi memikirkan bentuk fisik jaringan untuk melakukan sebuah komunikasi (Sritrusta & Rizqi, 2020).

b. Lapisan (*Layer*) pada Protokol TCP/IP



Gambar 26. Protokol TCP/IP
Sumber : Sritrusta & Rizqi (2020)

Seperti pada perangkat lunak, TCP/IP dibentuk dalam beberapa lapisan (*layer*). Dengan dibentuk dalam *layer*, akan mempermudah untuk pengembangan dan pengimplementasian. Antar *layer* dapat berkomunikasi ke atas maupun ke bawah dengan suatu penghubung *interface*. Tiap-tiap layer memiliki fungsi dan kegunaan yang berbeda dan saling mendukung *layer* diatasnya. Pada protokol TCP/IP dibagi menjadi 4 *layer*, tampak pada gambar dibawah. (Sritrusta & Rizqi, 2020)



Gambar 27. Arsitektur TCP/IP
Sumber : Sritrusta & Rizqi (2020)

c. Aplikasi TCP/IP

Level tertinggi pada *layer* TCP/IP adalah aplikasi. Dimana *layer* ini melakukan komunikasi sehingga dapat berinteraksi dengan pengguna. Karakteristik dari protokol aplikasi antara lain (Sritrusta & Rizqi, 2020):

1) Merupakan program aplikasi yang dibuat oleh pengguna, atau aplikasi yang merupakan standar dari produk TCP/IP. Contoh aplikasi yang merupakan produk dari TCP/IP antara lain:

a) TELNET, terminal interaktif untuk mengakses suatu *remote* pada internet.
b) FTP (*File Transfer Protocol*), transfer file berkecepatan tinggi antar *disk*.
c) SMTP (*Simple Mail Transfer Protocol*), sistem bersurat di internet
d) Dll

2) Menggunakan mekanisme TCP atau UDP.
3) Menggunakan model interaksi *client/server*.

d. Standarisari TCP/IP

TCP/IP semakin popular diantara *developer* dan pengguna, karena itu perlu adanya standarisasi. Standarisasi di kelola oleh *Internet Architecture Board* (IAB). IAB mengacu pada *Internet Engineering Task Force* (IETF) untuk membuat standar baru. Dimana standarisasi menggunakan RFC. Untuk Internet Standar Process, menggunakan RFC 2026 *The Internet Standard Process Revision* 3, dimana didalamnya berisi tentang protokol, prosedur, dan konvensi yang digunakan dari oleh internet (Sritrusta & Rizqi, 2020).

4. *Instruction Detection System* (IDS)

Menurut Ariyus dalam (Andriani, 2021), menjelaskan *Intruction Dectection System* (IDS) dapat didefinisikan sebagai *tool*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer, *Intruction Dectection System* (IDS) sebenarnya tidak cocok diberikan pengertian tersebut karena IDS tidak mendeteksi penyusup tetapi hanya mendeteksi aktivitas pada lalu lintas jaringan yang tidak layak terjadi. *Intruction Dectection System* (IDS) secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstal IDS, IDS tidak berdiri sendiri dalam melindungi suatu sistem.

a. Jenis *Intruction Detection System* (IDS)

Ada dua bentuk dasar IDS yang sering digunakan yaitu: NIDS dan HIDS (Winrou & Rissal, 2020):

1) NIDS (*Network based Intrusion Detection System*)

NIDS (*Network based Intrusion Detection System*) merupakan sebuah perangkat lunak yang bekerja secara otomatis untuk memantau suatu paket data yang masuk ke dalam sistem jaringan. Semua paket data yang berjalan pada sistem jaringan, akan dianalisis untuk melihat apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Jika ada kecocokan dengan *rules* yang telah dibuat, maka hasilnya akan dicatat dalam sebuah file.

2) HIDS (*Host Intrusion Detection System*)

HIDS (*Host Intrusion Detection System*) merupakan jenis IDS yang bekerja pada *host* yang individual atau perangkat tertentu pada sistem jaringan komputer secara *real-time*. HIDS akan memantau paket-paket data ketika sedang terjadi penyusupan saja.

b. *Intruction Detection System* (IDS) didasarkan pada beberapa terminologi

Pembagian jenis-jenis IDS yang ada saat sekarang ini disadarkan pada beberapa terminologi, di antaranya (Andriani, 2021):

1) Arsitektur Sistem

a) *Host-Target Co-Location*: IDS dijalankan pada sistem yang akan dilindungi. Kelemahan sistem ini adalah jika penyusup berhasil memperoleh akses ke sistem maka penyusup dapat dengan mudah mencari informasi dari *Client*.

b) *Host-Target Separation*: IDS diletakan pada komputer yang berbeda dengan komputer yang akan dilindungi.

2) Tujuan Sistem

a) Tanggung Jawab adalah kemampuan untuk menghubungkan suatu kegiatan dan bertanggung jawab terhadap semua yang terjadi, diantaranya adalah serangan.

b) *Respons* adalah suatu kemampuan untuk mengendalikan aktivitas yang merugikan dalam suatu sistem komputer.

3) Strategi Pengendalian

a) Terpusat, seluruh kendala pada IDS, baik monitoring, deteksi, dan

pelaporannya dikendalikan secara terpusat.

b) Terdistribusi Parsial, monitoring dan deteksi dikendalikan dari node *local* dengan *hierarki* pelaporan pada satu atau beberapa pusat lokasi.

c) Terdistribusi Total, monitoring dan deteksi menggunakan pendekatan berbasis agen, dimana keputusan respon dibuat pada kode analisis.

4) Waktu

a) *Interval-Based (Batsh Mode).* Informasi dikumpulkan terlebih dahulu, kemudian dievaluasi menurut interval waktu yang telah ditentukan.

b) *Realtime (Continues).* IDS memperoleh data terus menerus dan dapat mengetahui bahwa penyerang sedang terjadi sehingga secara cepat dapat melakukan *respons* terhadap penyerangan.

c. *Intruction Detection System* (IDS) dalam melakukan analisis paket data

Dilihat dari cara kerja dalam menganalisa apakah paket data dianggap sebagai penyusupan atau bukan, IDS dibagi menjadi 2 (Andriani, 2021):

1) *Signature based* atau *Misuse detection*

IDS ini dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS (berisi *signature-singnture* paket serangan). Jika paket data mempunyai pola yang sama dengan (setidaknya) salah satu pola di *database rule* IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut dianggap bukan serangan.

2) *Behavior based* atau *Anomaly based*

IDS ini dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan pada sistem, atau adanya penyimpanan dari kondisi normal, sobagai contoh ada pengguna memori yang secara terus menerus atau ada koneksi *parallel* dari 1 buah IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi-kondisi diatas dianggap kejanggalan yang dianggap yang kemudian oleh IDS jenis *anomaly based* sebagai serangan.

5. *Intrusion Prevention System* (IPS)

Intrusion Prevention System (IPS) adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik.

Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, di saat serangan telah teridentifikasi, IPS menolak akses (*block*) dan mencatat (*loging*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya *firewall* yang melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi traffic di jaringan dan terminal, di mana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat dideteksi sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan local (Ariyus, 2006).

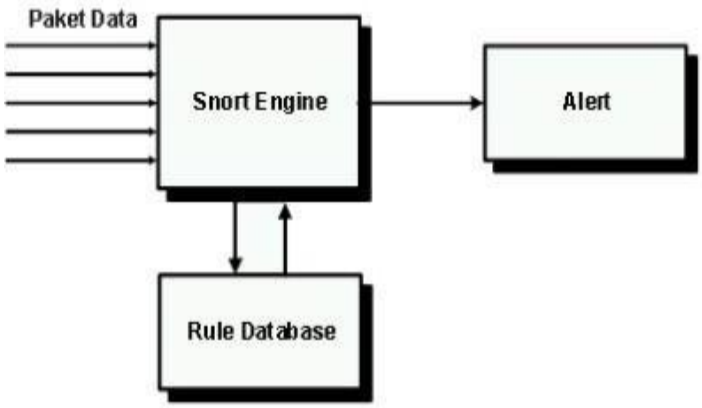
6. *Snort*

Rio & Imam (2021) menjelaskan bahwa *snort* adalah perangkat lunak berbasis IDS yang *open source* dan dapat diimplementasikan sebagai alat pendeteksi intrusi atau serangan pada jaringan komputer. *Snort* dirancang beroperasi dalam *command line* dan diintegrasikan ke beberapa aplikasi pihak ketiga dan sudah mendukung *cross platform* seperti *Linux* dan *Windows*. Kehandalan *snort* sebagai alat pendeteksi intrusi sangat bergantung pada pengaturan jaringan dan *rules* yang di buat dan diintegrasikan pada *host* maupun target serangan yang akan dilindungi. *Rule snort* sangat berdampak pada kehandalan *snort* itu sendiri dalam kemampuanya mengamankan jaringan dari ancaman yang terjadi. *Rules* membuat *snort* mampu mendeteksi serangan dengan mengenali *signature* yang telah di atur untuk fokus bekerja mendeteksi *ip, port,* protokol maupun jenis serangan yang digunakan dengan menutup akses paket data yang berasal dari penyusup dengan *signature* yang telah ditentukan.

Snort merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemindaian, maupun penyerangan. *Snort* merupakan gabungan dari protokol analisis dan pendeteksi penyusupan yang berguna untuk merespon kejadiankejadian yang sedang terjadi pada jaringan komputer secara *real-time*. *Snort* akan merespon kejadian yang terjadi dalam penyerangan *host-host* jaringan . (Winrou & Risal, 2020)

Pemantauan mendasar perlu dilakukan untuk tetap menjaga keamanan data atau jaringan. Salah satu cara untuk membangun sistem keamanan jaringan dengan sederhana dan tidak memerlukan biaya yang mahal adalah dengan menggunakan *Snort*. *Snort* tidak bisa menindaklanjuti serangan yang terdeteksi atau penyalahgunaan jaringan karena sifatnya hanya mendeteksi. Cara kerja *Snort* hampir sama dengan *TcpDump*, tetapi *Snort* hanya berfokus pada *sniffing* paket yang aman. (Natanael & Wiwin, 2021)

Sebagai kelengkapan dari sebuah sistem perangkat lunak. *Snort* IDS mempunyai 3 komponen utama yang saling berhubungan satu sama lain. Komponen utama dari Snort tersebut adalah snort engine, rule snort dan alert. Snort engine merupakan proses yang akan melakukan pembandingan paket data dengan *rule snort* untuk dapat menghasilkan *output* berupa *alert*. Ketiga komponen tersebut bekerja dalam satu siklus yang saling berpengaruh, seperti ditunjukkan pada Gambar 28 tentang komponen *Snort* tersebut adalah sebagai berikut:



Gambar 28. Skema kerja *Snort*
Sumber: Natanael & Wiwin (2021)

Snort memiliki fitur-fitur yang dapat menjaga kemanan sistem jaringan dengan cara memberikan peringatan atau *allert* dan juga meng-*capture* setiap sesi yang sedang berjalan. Dengan adanya fitur ini menjadikan snort merupakan sistem yang mampu mendeteksi adanya ancaman pada sistem jaringan yang sangat berguna pada *user*. *Snort* dapat dioperasikan dengan 3 *mode*, yaitu: (Winrou & Risal, 2020)

a. *Sniffer mode*, pada mode operasi ini *snort* dapat menangkap atau melihat semua paket yang sedang berjalan dalam jaringan dimana *snort* diletakkan. *Snort* juga memiliki kemampuan menampilkan hasil *sniffing* secara *real time*.

b. *Packet logger mode*, pada mode ini *Snort* mencatat setiap paket yang berjalan dan mengubahnya ke dalam bentuk file.
c. *Network intrusion detection mode*, pada mode ini *Snort* berjalan dengan melakukan konfigurasi yang kompleks terlebih dahulu, yaitu menjalankan *Snort* beserta file konfigurasi yang sudah ditentukan (secara *default file snort.conf*)

Baker, dkk., (dalam Andriani, 2021) menjelaskan bahwa *snort* dibagi menjadi beberapa komponen. Komponen-komponen ini yang nantinya akan bekerja sama untuk mendeteksi serangan dan menghasilkan *output* yang diinginkan dari *format detection system*. *Snort* memiliki beberapa komponen utama antara lain:

1) *Packet capture library* komponen ini yang memisahkan paket data yang melalui *Ethernet card* yang selanjutnya akan digunakan oleh *snort*.
2) *Packet Doceder* komponen ini mengambil data *layer* 2 yang dikirim oleh komponen sebelumnya (*Paket Capture Library*). Untuk proses pertama yaitu dengan memisahkan *data link* kemudian *protocol IP*, dan yang terakhir adalah jenis paket TCP dan UDP. Hasil proses ini adalah informasi mengenai protokol yang digunakan selanjutnya.
3) *Preprocessor* selanjutnya dilakukan analisis terhadap paket sebelum diproses oleh komponen berikutnya. Adanya proses analisis yang dilakukan berupa ditandai, dikelompokan atau dihentikan karena paket yang diterima tidak lengkap.
4) *Detection Engine* ini bisa dikatakan sebagai jantung *snort*. Paket yang diterima disini setelah melalui beberapa proses akan dibandingkan dengan *rule* yang ada atau telah ditetapkan sebaliknya. *Rule* disini berisi *signature* yang merupakan kategori serangan.
5) *Output* setelah proses *detection engine* dilakukan maka hasilnya adalah berupa *report* dan *elert*. *Snort* mendukung variasi dari output yang dihasilkan yaitu *teks*, *syslog*, XML, *binary* atau *database*.

2.2 Hasil Penelitian yang Relevan

Dalam melakukan penelitian ini, peneliti juga mempelajari penelitian-penelitian terdahulu yang dapat dijadikan sebagai bahan acuan penelitian serta

perbandingan dengan sistem yang akan dibangun. Adapun penelitian yang terkait antara lain:

1. Winrou Wesley & Rissal (2020). Penelitian yang berjudul Perancangan dan Analisis Keamanan Jaringan Komputer menggunakan *Snort*. Penelitian ini dilakukan di perusahaan PT. Promanufacture Indonesia untuk membantu kinerja perusahaan tersebut. Pengelola jaringan PT. Promanufacture Indonesia selama ini membangun sistem keamanan jaringan dengan menerapkan sistem *firewall* pada tiap unit server di jaringannya. Dibutuhkan keamanan yang dapat menjamin agar dapat meminimalisir ataupun bahkan menghilangkan kerugian yang disebabkan oleh serangan keamanan jaringan tersebut yaitu menggunakan *Snort*.
2. Rio & Imam (2021). Penelitian yang bejudul Sistem Deteksi Penyusup Pada Jaringan Komputer Menggunakan Teknik *Host Based Intrusion Detection System.* Penelitian ini membahas Keterbukaan akses informasi memunculkan berbagai masalah antara lain pemeliharaan validitas dan integritas data sehingga diperlukan suatu sistem keamanan jaringan yang dapat menanggulangi potensi ancaman yang dapat terjadi secara cepat dan akurat dengan memanfaatkan IDS (*intrusion detection system*). Salah satu perangkat IDS yang sering digunakan adalah *Snort* yang bekerja secara *real-time* memonitor dan mendeteksi jaringan yang sedang berlangsung dengan memberikan peringatan dan informasi terhadap potensi ancaman berupa serangan DoS.
3. Hendri, dkk., (2020). Penetilian yang berjudul Analisa Keamanan Jaringan Menggunakan *Network Intrusion Detection and Prevention System*. Penelitian ini membahas masalah serangan yang terjadi dalam jaringan komputer yaitu penyusup dapat melakukan *port scanning*, masuk pada sistem menggunakan *port-port* yang terbuka seperti telnet, ftp dan lainnya. Tujuan dari penelitian ini adalah mengimplementasikan IDPS, mampu mendeteksi dan memblokir adanya serangan dari penyusup.
4. Aminanto, dkk., (2020), penelitiannya yang berjudul "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort* dan *Honeypot Artilery*" IPS (*Intrusion Prevention System*) *Snort* merupakan sistem keamanan *server*

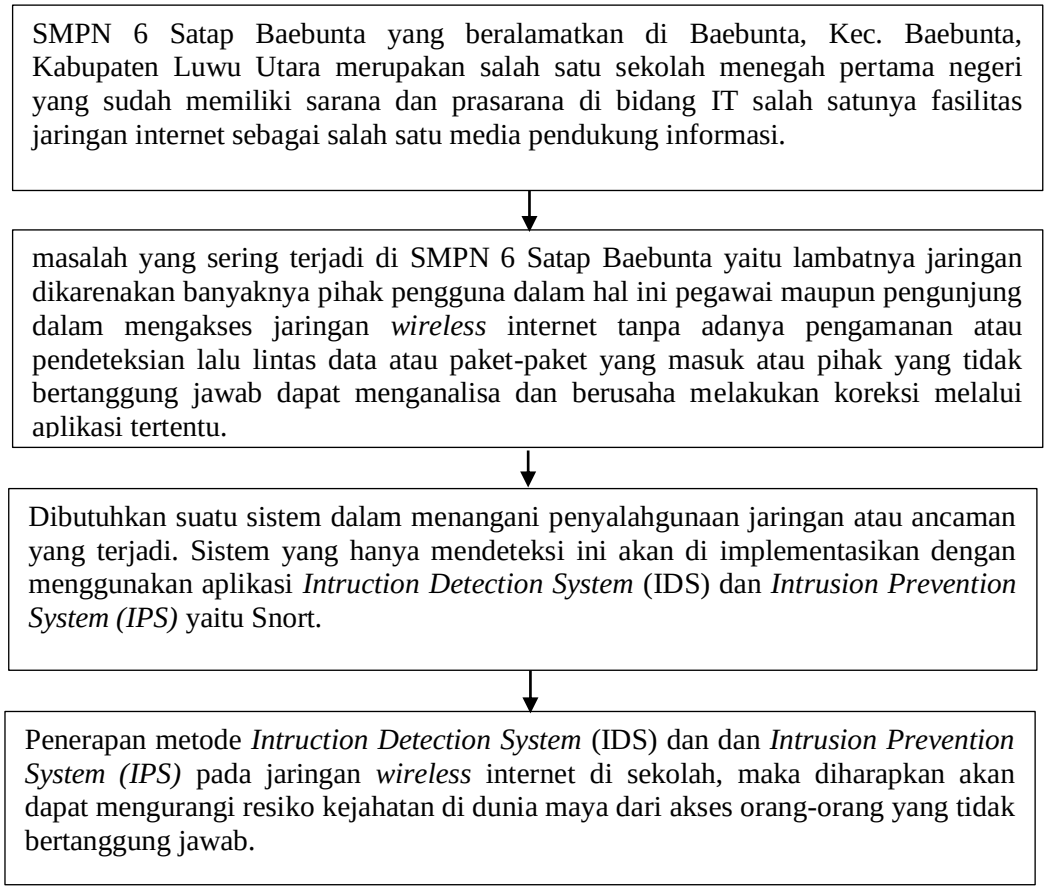
yang dapat mencegah serangan dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS Snort akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Namun dengan hanya menggunakan IPS *Snort* yang hanya dapat memeriksa dan mencatat *allert* serangan yang masuk di rasa kurang untuk mengamankan sebuah server dengan mengkolaborasikan dengan sistem keaman *server* yang lain di rasa dapat membuat kemanan jaringan *server* menjadi lebih baik. Dipilihlah *honeypot artillery* yang berfungsi ketika ada *hacker* mencoba melakukan penetrasi melalui port yang terbuka maka dapat terdeteksi seolah olah Hacker dapat menembus sistem, lalu *honeypot artillery* akan memberikan informasi tentang siapa penyerang dan bagaimana penyerang bisa masuk ke sistem *Snort* IPS untuk kemudian di catat di database yang dapat dilihat di web interface, Allert yang tercatat pada percobaan yang telah dilakukan di database sebanyak 9453 pada protokol TCP sebanyak 9%, UDP sebanyak <1%, dan ICMP sebanyak 91%.

5. Firmansyah, dkk., (2019), berjudul "Mengimplementasikan Sistem Kemanan Jaringan *Intrusion Prevention System* Berbasis *Snort* Pada Arsitektur *Software Defined Network*" *Software Defined Network* (SDN) adalah sebuah arsitektur jaringan yang memisahkan antara control plane dan data plane. SDN bisa juga disebut sebagai sentralisasi jaringan karena keseluruhan jaringan dapat diatur hanya dari satu titik yang disebut *controller* menjadikan SDN memiliki fleksibilitas yang lebih tinggi dibandingkan jaringan konvensional. Dibalik kelebihannya, keamanan masih menjadi perhatian utama di dalam arsitektur ini. IDS akan mendeteksi paket yang dianggap serangan sesuai rules yang sudah ditentukan. Kemudian dari rules tersebut akan diambil data seperti *packet source*, *packet destination* dan *protokol paket* untuk bisa melakukan blokir terhadap serangan. Serangan yang akan disimulasikan bervariasi mulai dari menggunakan banyaknya paket sampai ukuran paket yang dikirim sebagai parameter.
6. Syafriadi, (2020). penelitiannya yang berjudul "Desain Dan Implementasi Sistem Pembelajaran Berbasis *E-Learning* Pada Sekolah Menengah Pertama

Negeri 1 Pakue Tengah". Penelitian ini bertujuan mendesain dan mengimplementasikan sistem pembelajaran berbasis *e-learning* pada Sekolah Menengah Pertama Negeri 1 Pakue Tengah fokus pada materi pembelajaran bahasa Inggris kelas VII (tujuh). Hasil penelitian yang telah dilakukan menunjukkan bahwa dari hasil pengujian program yang telah dilakukan, *e-learning* yang telah dirancang ini bebas dari kesalahan logika yang dapat menyebabkan program tidak berjalan sesuai dengan apa yang diharapkan serta kesimpulan dari Rekapitulasi hasil perhitungan sebelumnya diperoleh hasil *Region* (R) = 23, *Cyclomatic Complexcity* (CC) = 23 dan *Independent Path* (IP) =23, sehingga dapat disimpulkan program ini telah bebas dari kesalahan logika.

2.3 Kerangka Pikir

Kerangka pikir merupakan alur penelitian yang menentukan jalannya penelitian. Adapun yang menjadi kerangka pikir dalam penelitian ini yaitu :



Gambar 29. Kerangka Pikir