

BAB II KAJIAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan Komputer

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

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

2.1.1.1. Manfaat Jaringan Komputer

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

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

2.1.2 Mengetahui Jenis Jaringan Komputer

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

(Wahana Komputer, 2010: 3)

1. Berdasarkan Ruang Lingkup

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

Berdasarkan luas areanya maka jaringan komputer dapat dibedakan menjadi :

a. PAN (*Personal Area Network*)

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

b. LAN (*Local Area Network*)

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

c. MAN (*Metropolitan Area Network*)

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

d. WAN (*Wide Area Network*)

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

2. Berdasarkan Topologi

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

beberapa jenis jaringan yang dikelompokkan berdasarkan topologi, sebagai berikut:

a. Topologi Bus

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

b. Topologi Star

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

c. Topologi Ring

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

3. Berdasarkan Medium Penghantar Jaringan

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

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

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

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

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

4. Berdasarkan Fungsi

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

- a. *Peer to Peer*

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

b. *Client Server*

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

2.1.3 Standar Jaringan Komputer

1. *Internasional Standards Organization (ISO)*

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

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

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

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

3. *American National Standards Institute (ANSI)*

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

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

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

5. *Electronic Industries Associations (EIA)*

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

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

6. *World Wide Web Consortium (W3C)*

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

7. *Open Mobile Alliance (OMA)*

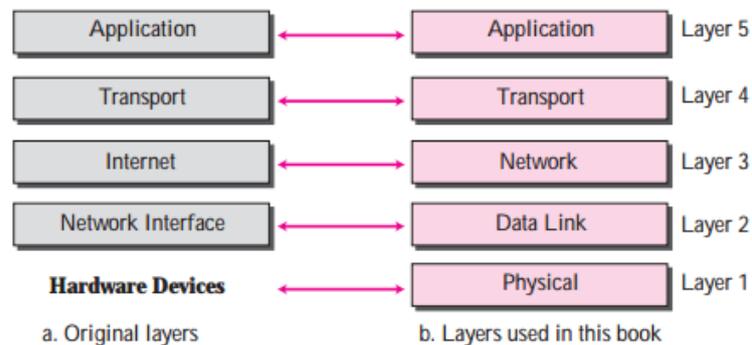
Organisasi standar OMA diciptakan untuk mengumpulkan berbagai forum dalam jaringan komputer dan teknologi nirkabel di bawah naungan satu otoritas tunggal. Misinya adalah untuk menyediakan standar terpadu untuk protokol aplikasi

2.1.4 Arsitiketur Protokol

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

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

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



Gambar 2.1 Lapisan di protokol TCP / IP Protocol

Sumber (Forouzan, 2010:29)

1. *Process/ Application Layer*

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

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

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

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

a. *Flow Control.*

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

b. *Error Detection.*

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

3. *Internet Layer*

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

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

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

4. *Network Access layer / Link Layer*

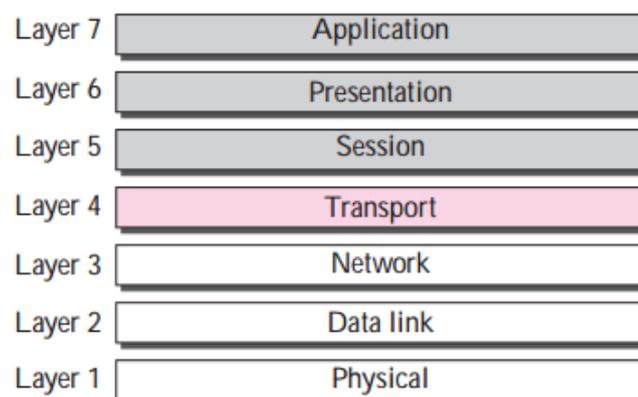
Pada lapisan ini, didefinisikan bagaimana penyaluran data dalam bentuk frame-frame data pada media fisik yang digunakan secara andal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberapa contoh protokol yang digunakan pada lapisan ini adalah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

2.1.5 OSI (*Open Systems Interconnection*) Model

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

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

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



Gambar 2.2 OSI Model

Sumber (Forouzan, 2010:21)

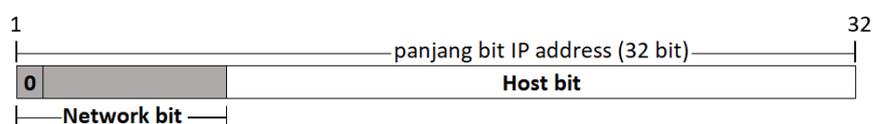
2.1.6 Internet Protocol (IP)

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

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

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

a Kelas A



Gambar 2.3 IP Address Class A

Sumber (Sofana, 2012:263)

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

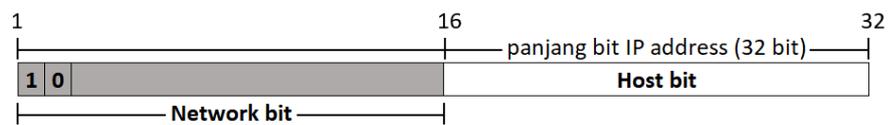
IP address kelas A dapat dituliskan sebagai :

nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

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

b Kelas B

Bagan IP address kelas B sebagai berikut:



Gambar 2.4 IP Address Class B

Sumber (Sofana, 2012:264)

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

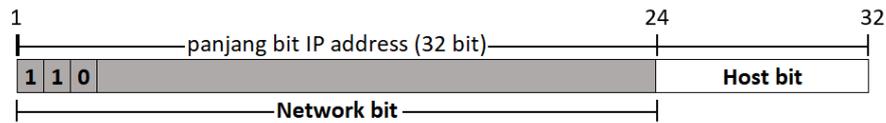
IP address kelas B dapat dituliskan sebagai:

nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

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

c Kelas C

Bagan IP address kelas C sebagai berikut:



Gambar 2.5 IP Address Class C

Sumber (Sofana, 2012:264)

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

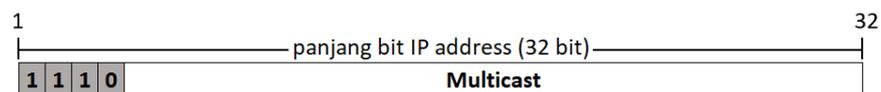
IP *address* kelas C dapat dituliskan sebagai:

nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

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

d Kelas D

Bagan IP *address* kelas D sebagai berikut :



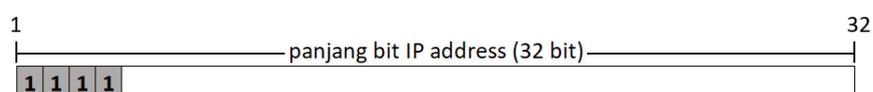
Gambar 2.6 IP Address Class D

Sumber (Sofana, 2012:265)

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

e Kelas E

Bagan IP address kelas DE sebagai berikut:



Gambar 2.7 IP Address Class E

Sumber (Sofana, 2012:265)

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

2.2 Teori Khusus

2.2.1 Keamanan Jaringan

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

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

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

2.2.2.1 Ancaman Terhadap Keamanan

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

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

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

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

2.2.2.2 Aspek-aspek Keamanan Komputer

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

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

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

2.2.2 Monitoring

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

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

2.3 Tools/software/aplikasi/system

2.3.1 Wireshark

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

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

2.3.2 Nagios

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

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

2.3.3 Raspberry

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

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

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

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

2.4 Penelitian Terdahulu

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

Berikut ini adalah jurnal yang pernah dilakukan untuk penelitian:

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

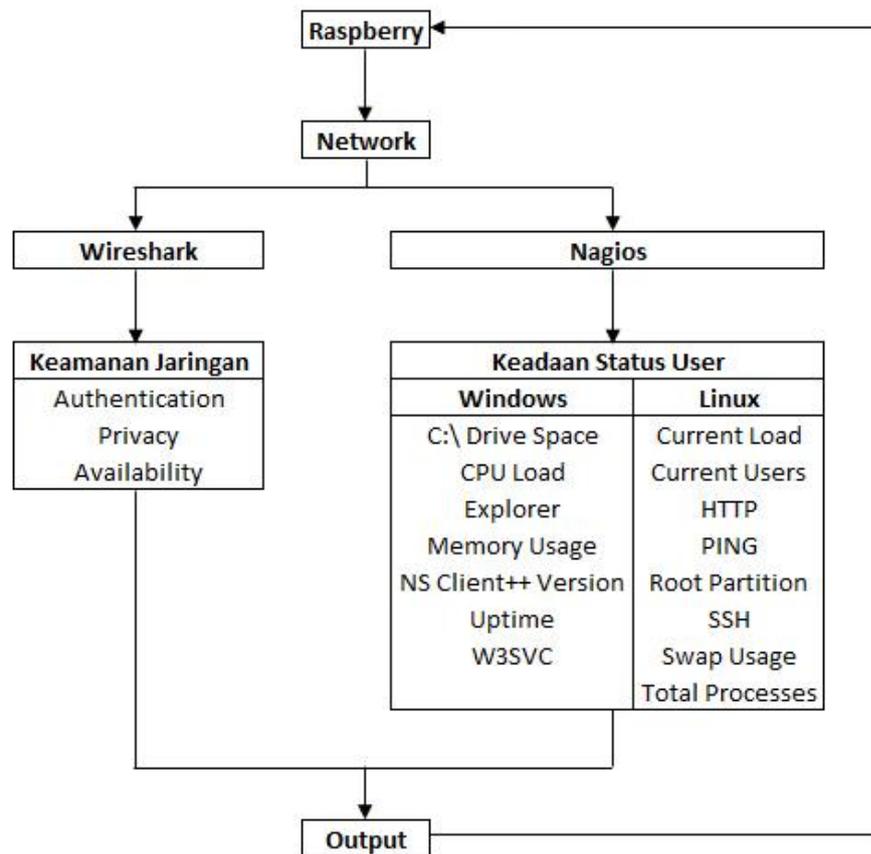
merancang sistem untuk aktivitas ilegal. Hasil pengujian ini berhasil dilakukan lebih mudah dengan bantuan dari *tools* Wireshark dibandingkan aplikasi lain seperti *forensic tools snort* terhadap informasi sumber, tujuan *protocol*, dan waktu *capture*-nya.

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

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

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

2.5 Kerangka Pemikiran



Gambar 2.8. Kerangka Pemikiran

Berikut ini adalah cara kerja kerangka penelitian, sebagai berikut:

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

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