BAB 2
Tinjauan Pustaka

2.1 Teori Yang Berkaitan Dengan Jaringan

Pada bab ini, akan dijelaskan mengenai definisi dari jaringan komputer, selain itu mengenai OSI (*Open Sistem Interconnection*) yang merupakan standarisasi dari jaringan komputer.

2.1.1 Definisi Jaringan Komputer

Jaringan komputer merupakan perpaduan antara teknologi komputer dan teknologi komunikasi. Dimana komputer yang berjumlah banyak dan terletak pada tempat yang terpisah-pisah tetapi dapat saling terhubung dalam melaksanakan tugasnya (Tanembaum, 2003:8). Setiap komputer, *printer*, atau peralatan lainnya yang terhubung dalam jaringan disebut node.

Manfaat dari jaringan komputer menurut (Tanembaum, 2003:8-10) dalam sebuah organisasi yaitu :

1. *Resource Sharing*

   Program, peralatan, dan data dapat digunakan oleh setiap orang yang terhubung dalam jaringan tanpa mementingkan lokasi *resource* dan pemakai.
2. Reliabilitas

   Dengan memiliki sumber alternatif persediaan, misalnya file-file disalin ke beberapa mesin lain sehingga jika satu mesin tidak berfungsi dengan baik (terjadi gangguan) maka salinan di mesin lain dapat digunakan.
3. Menghemat pengeluaran

   Mengganti komputer *mainframe* dengan membangun sistem yang terdiri dari komputer-komputer pribadi (model *client-server*).

Pada awal perkembangannya, jaringan sangat erat dengan media kabel sebagai penghubungnya. Tetapi seiring perkembangan teknologi informasi, penggunaan media nirkabel sudah banyak diterapkan. Selain karena banyaknya *user* yang lebih memilih menggunakan laptop karena mobilitasnya, perkembangan alat komunikasi seperti telepon genggam juga menjadi salah satu pemicu penerapan media nirkabel diberbagai tempat.

Arah transmisi komunikasi data dapat berupa *simplex*, *half-duplex*, dan *full-duplex* (Stallings, 2007:67).

1. *Simplex*

   Transmisi sinyal pada metode *simplex* hanya terjadi satu arah. Hal ini menjadikan satu stasiun sebagai pemancar sedangkan stasiun lainnya sebagai pemerima. Pada metode ini, aliran data hanya dapat terjadi secara satu arah (dari pemancar ke penerima). Stasiun radio merupakan salah satu contohnya.

2. *Half-Duplex*

   Pada metode *half-duplex*, transmisi sinyal dapat terjadi secara dua arah. Kedua stasiun dapat bertindak sebagai pemancar dan penerima tetapi tidak bisa secara bersamaan melainkan bergantian. Sehingga pada metode ini aliran data dapat terjadi secara dua arah bergantian. *Walkie-talkie* merupakan contoh alat yang beroperasi pada metode *half-duplex*.

3. *Full-Duplex*

   Pada metode *full-duplex*, transmisi sinyal terjadi secara dua arah secara bersamaan. Stasiun-stasiun yang menggunakan metode ini bertindak sebagai pemancar dan penerima secara bersamaan. Aliran data pada metode ini terjadi secara dua arah dan bersamaan. Telepon merupakan salah satu contohnya.

2.1.2 Model Referensi

Model-model referensi dalam jaringan terdapat 2 model yang paling sering digunakan, masing-masing adalah model referensi OSI dan model referensi TCP/IP.

2.1.2.1 Model Referensi OSI

Model referensi OSI dikembangkan oleh ISO (*International Organization for Standaritation*) sebagai model dari arsitektur protokol komputer dan rangka awal untuk pengembangan protokol standar (Stalling, 2007:42-43). OSI sendiri merupakan singkatan dari *Open System Interconnection.* Model ini juga sering disebut dengan "model tujuh lapis OSI" (*OSI seven layer model*).

Model OSI membagi fungsi-fungsi dari sebuah protokol menjadi beberapa *layer*. Setiap *layer* mempunyai properti yang menggunakan fungsi *layer* sebelumnya, kemudian mengirim pada *layer* selanjutnya.

1. *Application Layer*

   Application layer merupakan *layer* paling atas dalam model OSI dan *layer* yang paling dekat dengan *user*. Fungsinya antara lain sebagai antarmuka aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini yaitu *HTTP*, *FTP*, *SMTP*, dan *NFS*.

2. *Presentation Layer*

   Berfungsi untuk mentranslasikan data dari *application layer* yang akan dikirim ke dalam format yang dapat dibaca. Enkripsi, dekripsi, translasi, dan kompresi data

juga dilakukan pada layer ini yang bertujuan untuk mengamankan data.

3. *Session Layer*

   Bertugas untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, dan dihancurkan. *Session layer* juga menyediakan *service* kepada *presentation layer*. Dan *layer* ini juga mensinkronisasikan dialog antara dua *host layer representation* dan mengatur pertukaran data.

4. *Transport Layer*

   Transport layer mempunyai tugas untuk membagi data menjadi segmen, menjaga koneksi logika *end-to-end* antar terminal, dan menyediakan layanan yang *reliable*. Layer ini juga membuat tanda (*acknowledgement*) bahwa paket diterima dengan sukses dan mentransmisikan ulang bila ada paket yang hilang.

5. *Network Layer*

   Layer ini bertugas untuk menyediakan koneksi dan pemilihan jalur antar dua sistem. Selain itu layer ini juga berfungsi untuk pendefinisian alamat IP (*Addressing*), membuat *header* dari *frame* yang akan dikirim (*logical protocol*), dan kemudian melakukan *routing* (*network routing*) dengan menggunakan router atau switch *layer-3*.

6. *Data Link Layer*

   Menyediakan link untuk data, memaketkan bit yang diterima menjadi *frame* untuk diangkut melalui media. Pada *layer* ini juga berfungsi untuk *flow control*, pengalamatan perangkat keras (*Media Access Control Address* (*MAC Address*)), dan *error correction*. Spesifikasi IEEE 802 membagi level ini menjadi dua level anak yaitu *Logical Link Control* (LLC) dan *Media Access Control* (MAC).

7. *Physical Layer*

   Layer ini berhubungan langsung dengan *hardware*. *Layer* ini memiliki fungsi untuk mendefinisikan media transmisi, sinkronisasi bit, metode pensinyalan, arsitektur jaringan. Selain itu pada level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio. *Physical layer* bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media.

2.1.2.2 Model Referensi TCP/IP

TCP/IP (*Transmission Control Protocol*) yang secara umum dikenal dengan TCP/IP *protocol suite* merupakan hasil dari pengembangan dan riset protokol yang dilakukan atas jaringan paket seperti ARPANET dan didanai oleh DARPA (*Defence Advanced Research Project Agency*) (Stallings, 2007:34-42). Tujuan utama dari model TCP/IP yaitu mempertahankan jaringan yang ada dari hilangnya perangkat keras *subnet*, dimana komunikasi yang terjadi tidak terputus.

Model TCP/IP memiliki 4 layer, yaitu :

1. *Application Layer*

   Application layer menangani protokol tingkat tinggi yang berhubungan dengan representasi, *encoding* dan *dialog control*. Protokol TCP/IP menggabungkan hal-hal yang berhubungan dengan aplikasi ke dalam satu *layer* dan menjamin data dipaketkan dengan benar sebelum masuk ke *layer* berikutnya.

2. *Transport (host-to-host) Layer*

   Transport layer menyediakan layanan transportasi dari sumber ke tujuan (*host-to-host*). *Transport layer* merupakan koneksi logikal antara *sending host* dan

receiving host. Protokol-protokol yang berfungsi pada layer ini yaitu :

- *Transmission Control Protocol* (TCP)

  TCP mempunyai fungsi untuk memecah suatu blok data besar menjadi segmen yang diberi nomor urut, sehingga penerima dapat menyusun kembali segmen tersebut seperti sebelum pengiriman dilakukan. TCP merupakan jenis protokol yang membuat koneksi *end-to-end* baik secara logikal atau fisikal sebelum mengirim data (*connection oriented*) oleh karenanya TCP lebih *reliable*.

- *User Datagram Protocol* (UDP)

  UDP merupakan protokol yang tidak *reliable* dan *connectionless.* UDP banyak digunakan untuk aplikasi yang kurang peka terhadap gangguan jaringan seperti SNMP (*Simple Network Management Protocol*) dan TFTP (*Trivial File Transfer Protocol*).

3. *Internet Layer*

   Tujuan dari *internet layer* adalah untuk memilihi jalur terbaik untuk mengirimkan paket data dalam jaringan. *Internet Protocol* (IP) merupakan protokol utama yang berfungsi dalam *layer* ini. Beberapa protokol yang berfungsi dalam layer ini adalah :

   - *Internet Protocol*

     IP merupakan protokol yang memberikan alamat untuk peralatan dalam jaringan komputer. Fungsi utama dari IP adalah *connectionless oriented*, pemecahan (*fragmentation*) dan penyatuan (*unification*) paket data, dan meneruskan paket data (*routing*).

   - *Address Resolution Protocol* (ARP)

     ARP merupakan protokol yang melakukan translasi *IP Address* menjadi *MAC Address*. ARP merupakan jenis protokol *broadcast*.

- *Reverse Address Resolution Protocol* (RARP)

  RARP bertugas untuk melakukan translasi *MAC Address* menjadi *IP Address*. *Router* menggunakan protokol RARP untuk mendapatkan *IP Address* dari *MAC address* yang sudah diketahui.

- *Bootstrap Protocol* (BOOTP)

  Protokol ini digunakan untuk proses *boot diskless workstation*. Dengan adanya protokol ini, suatu peralatan dalam jaringan dapat diberikan *IP address* berdasarkan *MAC Address*-nya.

- *Dynamic Host Configuration Protocol* (DHCP)

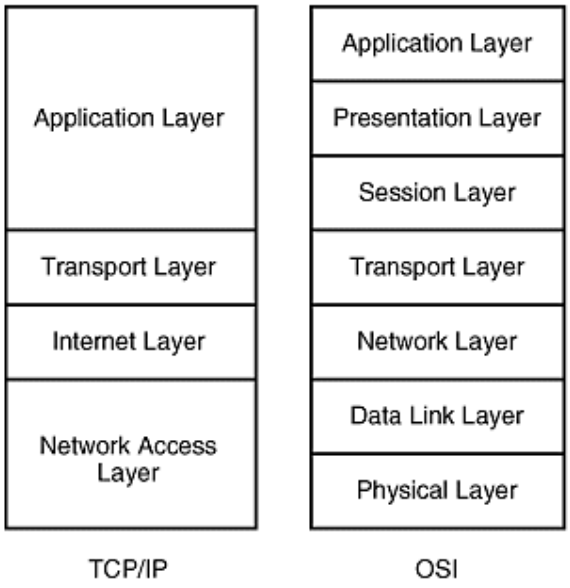
  DHCP dapat memberikan *IP Address* secara otomatis ke suatu *workstation* dalam jaringan yang menggunakan protokol TCP/IP.

- *Internet Control Message Protocol* (ICMP)

  ICMP merupakan protokol yang berguna untuk memberitahukan jika terjadi suatu masalah ketika pengiriman paket data.

4. *Network Access Layer*

   Meliputi pertukaran data antara *end sistem* (*server*, *workstation*, dll) dan jaringan dimana sistem itu terhubung. Komputer pengirim harus mempersiapkan alamat dari komputer tujuan agar jaringan dapat mengirim data pada alamat yang benar.



Gambar 2.1 Perbandingan *layer* OSI dengan TCP/IP

2.2 Teori Yang Terkait Tema Penelitian (Tematik)

Pada bagian ini, akan dijelaskan mengenai definisi dari *wireless* LAN dan tipe enkripsi *wireless* LAN. Selain itu terdapat juga penjelasan mengenai *single sign on* (SSO) serta FreeRadius dan juga CoovaChilli Dan juga sedikit membahas mengenai mikrotik.

2.2.1 Wireless LAN

Sebuah wireless LAN (WLAN) memungkinkan *client* terhubung ke jaringan dengan frekuensi radio melalui udara. WLAN digunakan untuk jaringan lokal. *Wireless LAN* menggunakan standar IEEE 802.11, dimana frekuensi untuk mengirim dan menerima sama sehingga WLAN merupakan komunikasi *half-duplex*. (Teare, 2008:181).

2.2.1.1 Standar WLAN

Semua peralatan *wireless* harus mengikuti standar dari IEEE 802.11. Berikut beberapa standar IEEE 802.11 untuk WLAN :

1. 802.11a: memiliki *transfer rate* 54 Mbps dengan frekuensi 5 GHz, disahkan pada 1999
2. 802.11b: memiliki *transfer rate* 11 Mbps dengan frekuensi 2.4 GHz, disahkan pada 1999
3. 802.11g: memiliki *transfer rate* 54 Mbps dengan frekuensi 2.4 GHz, memiliki *transfer rate* lebih baik dari 802.11b, disahkan pada 2003
4. 802.11n: *High-throughput draft*, rencana pengesahan pada 2007

Tabel 2.1 Standar IEEE 802.11 untuk WLAN

IEEE 802.11 Standard	Rilis	Data Rate	Jarak Indoor	Jarak Outdoor
802.11a	1999	54MB/s	~35m	~120m
802.11b	1999	11MB/s	~38m	~140m
802.11g	2003	54MB/s	~38m	~140m
802.11n	2009	248MB/s	~70m	~250m

2.2.1.2 Pengamanan WLAN

Pengamanan WLAN menurut (Teare, 2008:580) yaitu sebagai berikut :

1. *Authentication*: Memastikan hanya *client* sah yang bisa mengakses jaringan melalui *access point* yang dipercaya.
2. *Encryption*: Memastikan keamanan data yang ditransfer.

3. *Intrusion Detection and Intrusion Protection*: Memonitor, mendeteksi dan mengurangi akses yang tidak terauthorisasi dan serangan ke jaringan.

2.2.1.3 *Access Point*

Access Point adalah *hardware* atau *software* yang berfungsi sebagai titik penghubung untuk *client* sebelum terhubung ke sebuah LAN, AP juga berlaku sebagai penyebar dan penerima sinyal dari WLAN. (Teare, 2008:566).

2.2.1.4 SSID

SSID (*Service Set Identifier*) adalah identitas untuk sebuah WLAN. SSID pada sebuah AP dan *client* harus sama. AP membroadcast SSID, memberitahukan ketersediaan servisnya, *client* yang mengetahui adanya SSID yang spesifik harus memilih untuk melakukan asosiasi dengan SSID yang tersedia. (Teare, 2008:579).

2.2.2 Tipe Enkripsi Wireless LAN

WEP (*Wired Equivalent Privacy*) merupakan protokol enkripsi yang diperkenalkan sebagai standar IEEE 802.11 pertama kali pada 1999. Protokol ini memiliki dasar dari algoritma enkripsi RC4, dengan kunci rahasia 40 bit atau 104 bit dikombinasikan dengan 24 bit *Initialisation Vector* (IV) untuk mengenkripsi teks pesan M dengan *checksum*-nya.

WPA (*WiFi Protected Access*) / *Temporal Key Integrity Protocol* (TKIP) adalah protocol keamanan untuk komunikasi WLAN dan menyediakan kerahasiaan dan integritas. WPA didesain untuk memperbaiki kelemahan dari WEP, yang merupakan protocol sebelumnya, WPA menggunakan dua macam kunci, yaitu 64 bit *message integrity check* (MIC) *key* yang berfungsi untuk mendeteksi

pemalsuan atau pengubahan pesan dan 128 bit *encryption key* yang digunakan untuk enkripsi dan dekripsi paket, keduanya didapat dari sebuah *master key*.

WPA2 merupakan standar akhir dari IEEE 802.11i yang disahkan pada 2004, WPA2 memiliki kemiripan dengan WPA, yang membedakan mereka adalah WPA2 menggunakan *Advanced Encryption Standard* (AES), bukan TKIP seperti WPA. AES merupakan *block cipher*, berbeda dari RC4 yang dipakai di WEP dan WPA yang merupakan *stream cipher*. *Stream cipher* mengeksekusi karakter satu per satu, sedangkan *block cipher* langsung mengoperasikan seluruh blok teks sekaligus, sehingga merupakan alternatif yang lebih aman. (Katz, 2010:1-4).

2.2.3 SSO (*Single Sign On*)

Single Sign On adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Teknologi ini sangat diminati, khususnya dalam jaringan yang sangat besar dan bersifat heterogen (di saat sistem operasi serta aplikasi yang digunakan oleh komputer adalah berasal dari banyak vendor, dan pengguna dimintai untuk mengisi informasi dirinya ke dalam setiap platform yang berbeda tersebut yang hendak diakses oleh pengguna). Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan. (Pangestu, 2010:3).

2.2.4 Remote Authentication Dial-In User Service (RADIUS)

RADIUS pertama kali dibuat oleh Livingston Enterprise, merupakan standar protocol yang berdasar pada model *client-server* yang dijelaskan pada RFC (*Request for Command*) 2865 dan RFC 2866. *RADIUS server* bisa melakukan autentikasi, authorisasi, dan akuntansi

bagi user setelah menerima permintaan dari *client*. Komunikasi antara *client* dan *server* dienkripsi dengan *private key* yang tidak pernah dikirim dari jaringan, dengan kata lain telah ditentukan sebelum jaringan terbentuk (Szilagyi, 2009:1-2).

RADIUS server juga bisa berperan sebagai *proxy server* dimana *RADIUS server* melanjutkan permintaan dari *server* lain dan menerima balasan dan kemudian melanjutkan kembali ke *client.* RADIUS pada standar awalnya menggunakan *User Datagram Protocol* (UDP) *port* 1645 dan 1646 untuk autentikasi dan akuntansi paket-paket yang kemudian diubah menjadi 1812 dan 1813, tapi masih banyak juga yang menggunakan port lama untuk *RADIUS*.

RADIUS memungkinkan variasi mekanisme pengautentikasian. Atribut-atributnya bisa diperluas dengan atribut baru tanpa mempengaruhi implementasi yang telah ada. *RADIUS* memiliki *Extensible Authentication Protocol* (EAP) yang memungkinkan *RADIUS* mendukung lebih banyak protocol autentikasi. *RADIUS* juga telah mendukung IPv6.

2.2.5 CoovaChilli

CoovaChilli, merupakan *open source captive portal* atau *Wireless LAN access point controller.* Digunakan untuk meng-authentikasi user dari sebuah jaringan Wireless LAN. Men-support login berbasis web yang merupakan standard untuk *public hotspot* dewasa ini. *CoovaChilli* juga dapat berfungsi sebagai media autentikasi, authorisasi dan accounting (AAA) yang merupakan framework atau arsitektur kerja dari sebuah *RADIUS server*. (coova.org, 2012).

Chilli men-support dua jenis metode authentikasi, yaitu :

1. *Universal Access Method* (UAM) :

   Dengan UAM, *wireless client* me-request sebuah IP address, dan dialokasikan oleh *Chilli*. Ketika seorang user membuka sebuah web browser, *Chilli* akan menangkap koneksi TCP tersebut dan me-redirect browser tersebut ke authentikasi *web server*. *Webserver*

meminta user untuk melakukan input *username* dan *password*, kemudian password di-enkripsi dan dikirim kembali ke Chilli.

2. *Wireless Protected Access* (WPA) :

   Dengan WPA, metode authentikasi dihandle oleh *access point* dan *subsequently* di *forward* dari *access point* ke *Chilli*. Jika WPA digunakan, maka koneksi yang terjadi antara *access point* dan user di-enkripsi.

2.3 Hasil Penelitian atau Produk Sebelumnya

Sudah banyak orang melakukan penelitian mengenai Single Sign On (SSO). Beberapa orang yang telah melakukan penelitian mengenai Single Sign On (SSO) 10 tahun terakhir yaitu :

- Christopher J. Davenport et al dengan judul "*SYSTEM AND METHOD FOR AUTHENTICATION VIA A SINGLE SIGN ON SERVER*".

  Jurnal ini membahas sistem yang terdiri dari workstation client, server *SSO* diakses oleh klien workstation, dan sejumlah server host dapat diakses oleh workstation klien. Akses oleh workstation client ke server host pertama menyebabkan workstation klien secara otomatis kembali diarahkan ke server *SSO* dan server *SSO* menyebabkan workstation klien untuk meminta sign on dari pengguna jika pengguna belum sign in untuk setiap dari server host. Host server pertama, bukan server *SSO*, mengotentikasi pengguna.

- Harding, P , Johansson, L , Klingenstein, N dengan judul "*DYNAMIC SECURITY ASSERTION MARKUP LANGUAGE: SIMPLIFYING SINGLE SIGN ON*".

  Jurnal ini membahas pertumbuhan dalam penggunaan proses bisnis outsourcing dan platform kolaboratif mendorong permintaan bagi organisasi untuk selektif berbagi informasi identitas mereka

mempertahankan tentang pengguna mereka dengan mitra lain. Protokol yang diterima secara luas seperti *Security Assertion Markup Language (SAML)* dirancang untuk memberikan *Single Sign On (SSO)* dan atribut keamanan lainnya, tetapi meskipun organisasi dapat memperoleh nilai bisnis yang signifikan dengan menggunakan teknik manajemen identitas federasi, mereka terus menghadapi rintangan implementasi besar (seperti ingin skala kurang dari 10 mitra untuk puluhan, ratusan, atau bahkan ribuan dari mereka). Dinamis SAML mengambil keuntungan dari praktik terbaik keamanan dan pertukaran informasi konfigurasi untuk meminimalkan langkah-langkah manual yang saat ini administrator harus melakukan mengkonfigurasi koneksi *SAML* aman. Meskipun mungkin belum untuk sepenuhnya mengotomatisasi keputusan kepercayaan manusia, dinamis *SAML* dapat mengotomatisasi bursa mendasari untuk membuat keputusan ini cepat, sederhana, dan aman.

- Rudy, Riechie, Odi Gunadi dengan judul "INTEGRASI APLIKASI MENGGUNAKAN SINGLE SIGN ON BERBASISKAN *LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL*(*LDAP*) DALAM PORTAL BINUS@CCESS(BEE-PORTAL)".

  Jurnal ini membahas tentang pengimplementasian metode *Single Sign On (SSO)* dengan menggunakan *Central Authentication Service (CAS)* dan *Lightweight Data Access Protocol (LDAP)* di dalam Web Portal Bina Nusantara. Tujuan utama dari pengimplementasian *SSO* ini adalah untuk menggabungkan aplikasi yang ada pada binus-access ke dalam sebuah site sehingga terbentuk integrasi aplikasi, khususnya dalam bentuk web yang biasa disebut dengan Web Portal. Dengan adanya Web Portal yang menggunakan metode *Single Sign On (SSO)* ini, berarti setiap user hanya perlu memiliki satu username, satu password. Dan bila ingin mendapatkan layanan atau fasilitas di Web Portal, user ini hanya perlu login satu kali saja bisa dapat menggunakan semua fasilitas atau layanan aplikasi yang ada di dalam Web Portal tersebut. Hal ini dapat mempermudah user dalam menggunakan aplikasi yang ada. User tidak perlu menghapal banyak account, hanya satu account dan tidak perlu berulang kali login, cukup

dengan sekali login. Hal ini juga dapat mempermudah dalam pengorganisasian data user yang ada, sehingga keamanan data user lebih terjamin, karena menggunakan tempat penyimpanan data user yang terpusat. *CAS* digunakan untuk menangani masalah komunikasi antara aplikasi web yang berbeda, sehingga semua aplikasi dapat diintegrasikan ke dalam sebuah Web Portal. *LDAP* digunakan sebagai sebuah protokol direktori servis, dimana semua data user disimpan di dalam *LDAP*.