

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat sekarang ini begitu pesat, dengan perkembangan tersebut banyak bermunculan aplikasi-aplikasi yang mendukung kemajuan teknologi informasi di dunia internet. Disamping kemudahan dalam mengakses internet, kini telah berkembang salah satu teknologi jaringan yaitu jaringan komputer. Jaringan sendiri memiliki fungsi sebagai pemancar yang dimana apabila ada salah satu *user* terhubung pada jaringan tersebut maka akan terhubung keinternet. Jaringan memiliki sebuah keamanan yang penting untuk menjamin kenyamanan bagi pengguna maupun seorang administrator. Apabila jaringan ini tidak memiliki sebuah penerapan untuk mengurangi ancaman keamanan jaringan tersebut, maka ancaman dari luar akan terjadi dan mengganggu kenyamanan pengguna jaringan tersebut. Ancaman ini bisa berupa pelumpuhan jaringan, pencurian data, bahkan serangan-serangan yang dilakukan oleh pihak yang tidak berkepentingan untuk mencari celah pada sistem keamanan jaringan dan mencari kelemahan pada sistem keamanan yang digunakan. Prama, (2018)

Saskara, Indrawan, & Putra (2019) menyatakan bahwa Jaringan komputer adalah koneksi antara dua atau lebih komputer yang berdiri sendiri yang dihubungkan oleh media transmisi kabel atau nirkabel. *Autonomous* adalah ketika komputer tidak memiliki kontrol penuh atas komputer lain. Ini dapat menyebabkan komputer mati dan perlu di nyalah kembali, kehilangan *file*, atau kerusakan sistem. Teknologi informasi berubah dan berkembang sangat pesat dan secara umum sudah banyak digunakan pada zaman modern saat ini, peranan teknologi didalam kehidupan tidak dapat dihindari terutama dalam dunia kerja, bisnis, serta pendidikan. Salah satu fasilitas teknologi saat ini memanfaatkan sebuah *smartphone* menjadi sebuah *Access Point* (AP) agar dapat terhubung ke *internet*, dengan memanfaatkan sebuah teknik *sharing* koneksi yaitu *tethering* dalam sebuah jaringan *Wireless Local Area Network* (Wlan) dan mejadikan udara sebagai media penyaluran informasi pada jaringan tersebut (Kurniawan dan Sari, 2018).

Kebutuhan akan jaringan komputer menjadi semakin penting dalam pendidikan, pekerjaan dan hiburan. Salah satu hal penting dalam mengelola jaringan komputer adalah keamanan jaringan, akses *internet* yang tinggi dapat menyebabkan kejahatan pada jaringan. Misalnya, pencurian data terjadi di jaringan atau beberapa peretas menonaktifkan sumber daya jaringan. Ada banyak teknik yang bisa digunakan untuk mengurangi tingkat kejahatan dalam jaringan salah satunya yaitu menggunakan keamanan *switch port* yang artinya *user* yang ingin masuk ke layanan jaringan harus melalui akses jaringan *port* yang disediakan oleh *switch* (Sulaiman, 2018).

RADIUS adalah protokol keamanan komputer yang digunakan untuk mengotentikasi, mengotorisasi, dan mendaftarkan akun pengguna untuk akses jaringan secara terpusat. *Server* otentikasi adalah perangkat keamanan dalam jaringan komputer yang melakukan otentikasi untuk memproses permintaan otentikasi dari pengguna layanan jaringan. *Server otentikasi* ini mengimplementasikan model AAA (otentikasi, otorisasi, dan akuntansi). Otentikasi adalah proses verifikasi identitas pengguna akhir saat mengakses jaringan. RADIUS memiliki format paket yang digunakan untuk mengirim data (Saskara, dkk, 2019)

Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut sehingga dapat membuka peluang bagi para hacker untuk meretas dan merusak jaringan yang dibangun tersebut. Untuk meminimalisir terjadinya penyalahgunaan jaringan oleh para hacker, maka perlu adanya peningkatan keamanan jaringan yang akan dibangun. Dalam penelitian ini telah dilakukan penelitian untuk mengembangkan keamanan jaringan komputer dengan cara memanfaatkan RADIUS Server untuk Optimalisasi Jaringan Wlan menggunakan Mikrotik Router.

Kantor Desa Taripa adalah salah satu Kantor Desa yang berada di Kecamatan Angkona yang bergerak dalam bidang pelayanan Masyarakat desa. Letak kantor berada di Kecamatan Angkona, Kabupaten Luwu Timur, Sulawesi Selatan. Masalah yang ada pada Kantor Desa Taripa adalah banyaknya pengguna

jaringan yang bukan pegawai Kantor dapat mengakses Jaringan yang dapat menyebabkan lambatnya Jaringan saat digunakan. Penelitian ini akan dirancang bangun RADIUS server memanfaatkan Mikrotik Router Board yang dapat memberikan media *authentication user*. Hal ini akan memberikan suatu *login user* yang hanya akan dimiliki oleh pegawai kantor untuk dapat mengakses jaringan Wireless yang ada di kantor agar dapat terkoneksi ke jaringan internet. Jumlah user yang dapat menggunakan jaringan adalah sebanyak 11 user yang mana 6 user login menggunakan komputer dan 5 menggunakan android. Penggunaan *authentication user*, diharapkan agar masyarakat yang berada di sekitar kantor tidak dapat mengakses jaringan Wireless hanya user yang mempunyai *login user* dan *password* yang dapat mengakses jaringan wireless pada Kantor Desa. Sistem ini nantinya diharapkan membantu pegawai kantor agar tidak merasakan lambatnya akses internet dan juga *over limit user*. Kantor Desa Taripa saat ini akan menerapkan penggunaan media mikrotik sebagai pintu utama sistem keamanan tambahan pada jaringan yang ada di lokasi penelitian. Penggunaan mikrotik diterapkan untuk mengatasi permasalahan yang dihadapi pada lokasi penelitian, dimana dengan diterapkannya mikrotik dapat diberlakukan penggunaan *password* yang berbeda untuk setiap user atau pengguna, sehingga setiap pengguna yang akan menggunakan jaringan internet akan memiliki *password* yang berbeda dengan pengguna lainnya, sehingga jaringan tidak mudah diakses oleh orang yang tidak diberikan izin dalam menggunakan jaringan internet.

Kantor Desa Taripa memiliki 5 unit PC, 1 pc admin, dan 5 android yang terhubung ke jaringan yang digunakan untuk akses kegiatan kantor sehari-hari. Pegawai lapangan yang tinggal di *basecamp* juga memanfaatkan jaringan tersebut untuk aktivitas sehari-hari menggunakan hp android. Kecepatan *download* 10 mbps dan kecepatan *upload* 7 mbps. Model jaringan topologi bus, menggunakan wireless dan switch sebagai penghubung beberapa perangkat komputer yang ada agar dapat melakukan pertukaran paket serta meneruskan data ke perangkat tujuan. Sistem yang sedang berjalan pada Kantor Desa Taripa adalah sebuah sistem jaringan Wireless dalam proses pengiriman data dan komunikasi. Pengguna dengan mudah terhubung ke jaringan wireless hanya dengan *login password* yang disediakan oleh vendor dan termasuk dalam jenis keamanan standar untuk menjaga keamanan

jaringan. Kelemahan dari jaringan *wireless* adalah kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Akibat dari kurangnya keamanan jaringan yang ada yang menyebabkan lambatnya jaringan yang digunakan untuk mengakses internet akibat banyaknya pengguna yang menggunakan jaringan tersebut maka dibuatlah pemanfaatan RADIUS Server untuk optimalisasi keamanan jaringan Wlan menggunakan Mikrotik Router.

Berdasarkan permasalahan di atas maka penulis tertarik untuk melakukan penelitian dengan judul “Pemanfaatan RADIUS Server Untuk Optimalisasi Keamanan Jaringan Wlan pada Kantor Desa Taripa Menggunakan Mikrotik Router”.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas dapat ditarik rumusan masalah yaitu Bagaimana Pemanfaatan RADIUS server untuk optimalisasi keamanan jaringan pada Kantor Desa Taripa menggunakan Mikrotik Router?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah untuk memanfaatkan RADIUS server dalam optimalisasi keamanan jaringan pada Kantor Desa Taripa menggunakan Mikrotik Router”.

1.4 Manfaat Penelitian

Manfaat penelitian ini antara lain adalah:

1. Bagi Penulis

Meningkatkan wawasan dan kompetensi di dalam memahami tentang membangun dan menganalisis jaringan komputer yang nantinya penulis buat. Selain itu merupakan syarat untuk melakukan penyusunan tugas akhir pada Program Studi Teknik Informatika di Universitas Cokroaminoto Palopo.

2. Bagi Instansi Kantor Desa Taripa

Dapat memberikan solusi dalam masalah keamanan jaringan yang di hadapi selama ini.

3. Bagi Akademik

Sebagai sumber informasi dan referensi dalam pengembangan penelitian dan perkembangan dunia akademik khususnya dalam penelitian-penelitian yang akan

datang dan menumbuhkan budaya meneliti terjadi inovasi pembelajaran, dapat pula memberikan sumbangan pemikiran bagi perkembangan teknologi informasi dalam dunia ilmu pengetahuan.

1.5 Batasan penelitian

Batas penelitian ini dilakukan agar penelitian dapat terarah dengan baik sesuai tujuan penelitian dengan adanya keterbatasan waktu pengerjaan maka perlu adanya batasan penelitian. Batasan penelitian ini, yaitu:

1. Membuat sistem *RADIUS server* untuk optimalisasi keamanan jaringan pada Kantor Desa Taripa
2. *Monitoring user* yang sedang aktif pada Kantor Desa Taripa

BAB II

TINJAUAN PUSTAKA

2.1 Kajian Teori

1. Pengertian Pemanfaatan

Menurut Poerwadarminto, (2020) Pemanfaatan adalah suatu kegiatan, proses, cara atau perbuatan menjadikan suatu yang ada menjadi bermanfaat. Istilah pemanfaatan berasal dari kata dasar manfaat yang berarti faedah, yang mendapat imbuhan pe-an yang berarti proses atau perbuatan memanfaatkan. Jadi Pemanfaatan adalah merupakan proses atau cara perbuatan yang dapat bermanfaat. Menurut *Kamus Besar Bahasa Indonesia*, (2018) Pemanfaatan berasal dari kata dasar manfaat yang artinya guna, faedah. Kemudian mendapatkan himbauan pe-an yang berarti proses, cara, perbuatan, pemanfaatan. Dengan demikian pemanfaatan dapat diartikan suatu cara atau proses dalam memanfaatkan suatu benda atau objek.

Berdasarkan definisi diatas maka dapat disimpulkan bahwa dengan demikian pemanfaatan yaitu suatu perolehan atau pemakaian hal-hal yang berguna baik dipergunakan secara langsung maupun tidak langsung agar dapat bermanfaat.

2. Pengertian RADIUS (*Remote Authentication Dial-In User Service*)

RADIUS adalah protokol keamanan jaringan komputer yang digunakan untuk melakukan autentikasi, otorisasi dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. Server *autentikasi* merupakan perangkat keamanan pada suatu jaringan komputer yang menerapkan proses autentikasi untuk melayani permintaan autentikasi dari pengguna layanan jaringan. Server autentikasi ini menerapkan model AAA (*authentication*, *authorization*, dan *accounting*). *Authentication* adalah proses pengesahan identitas pengguna (*end-user*) dalam mengakses jaringan. *Accounting* adalah proses komputasi yang dilakukan oleh sistem dengan pencatatan sumber daya yang telah dipakai oleh pengguna jaringan komputer nirkabel, *usermanager* merupakan fitur radius server yang ada dalam mikrotik (Saskara, dkk, 2019). RADIUS server menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan pengguna. Pada saat computer client akan menghubungkan diri dengan jaringan maka server RADIUS akan meminta identitas pengguna (username dan password) untuk

kemudian dicocokkan dengan data yang ada dalam database server RADIUS untuk kemudian ditentukan apakah pengguna diijinkan untuk menggunakan layanan dalam jaringan komputer (Ardian, 2019)

Berdasarkan definisi diatas dapat disimpulkan bahwa RADIUS Server adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS kini telah diimplementasikan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi selain dial-up seperti halnya VPN (Virtual Private Networking), access point nirkabel, switch Ethernet, dan perangkat lainnya.

3. Pengertian Optimalisasi

Menurut Octavianus (2020) Kata Optimalisasi berasal dari kata dasar optimal, yang berarti tertinggi, terbaik, paling menguntungkan. Bentuk kata kerja dari kata optimal adalah mengoptimalkan yang berarti "menjadikan paling baik, menjadikan paling tinggi," dan pengoptimalan yang berarti "proses, cara, perbuatan mengoptimalkan. Berdasarkan pengertian-pengertian kata optimal di atas, maka pengertian kata optimalisasi dalam tulisan ini berarti proses, cara, menjadikan sesuatu lebih baik atau terbaik, tertinggi, dan atau paling menguntungkan.

4. Keamanan Jaringan

Menurut Fauzan & Purwanto (2021) mengatakan keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Diperlukannya langkah langkah untuk pencegahan dan membantu menghentikan penyusup atau pengguna tidak sah untuk mengakses sistem jaringan komputer dan setiap bagiannya. Keamanan jaringan adalah proses mencegah dan mengidentifikasi penggunaan yang tidak benar dan aktivitas jaringan komputer. Keamanan jaringan juga bertujuan untuk mengantisipasi ancaman dan risiko logis atau fisik yang secara langsung dan tidak langsung mengintervensi. (Masum, 2018).

Berdasarkan definisi keamanan jaringan di atas dapat kita simpulkan bahwa keamanan jaringan dapat dicapai dengan metode keamanan jaringan yang tidak hanya melindungi jaringan, tetapi juga melindungi sistem baik dari dalam maupun luar jaringan, yang dapat mengintervensi jika terjadi serangan pada jaringan.

Dengan pengawasan yang lebih teliti resiko tersebut dapat dikurangi, namun *network security* biasanya bertentangan dengan *network access*, dimana bila *network access* semakin mudah, maka *network security* semakin rawan begitu pula sebaliknya.

Kurniawan dan Sari (2018) mengelompokan prinsip keamanan jaringan sering disebut dengan segitiga CIA (*Confidentiality, Integrity, Availability*) Mydza:

- a. *Confidentiality* (Kerahasiaan): menjaga infrastruktur jaringan agar tidak dapat diakses oleh pihak yang tidak berhak untuk mengaksesnya.
- b. *Integrity* (*Integritas*): menjaga data agar tetap asli dan tidak dimodifikasi selama proses pengiriman dari sumber ke tujuan (penerima).
- c. *Availability* (Ketersediaan): *user* yang mempunyai hak akses (*authorized user*) diberi akses tepat waktu dan tidak terkendala apapun.

5. Keamanan Jaringan Wireless

Keamanan jaringan nirkabel memiliki banyak faktor yang menentukan tingkat keamanan jaringan dari penyerang (*attacker*), ancaman (*threats*), potensi kelemahan (*potential vulnerabilities*), aset yang beresiko (*asset at risk*), perlindungan yang ada (*existing safeguard*) dan perlindungan tambahan (*additional control*). Mekanisme keamanan jaringan nirkabel penting untuk menjaga kerahasiaan data. *Enkripsi* mekanisme keamanan adalah proses mengenkripsi pesan untuk menyembunyikan isinya. Algoritma *cipher modern* yang menggunakan kunci *enkripsi* tidak dapat mendekripsi hasil *enkripsi* tanpa kunci tersebut., Rumalutur (dalam Eko Agus Darmadi, 2018). Jaringan wireless memiliki lebih banyak kelemahan dibanding dengan jaringan kabel (*wired*). Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor (Rumalutur, 2019).

Berdasarkan definisi di atas maka dapat di simpulkan bahwa Keamanan jaringan *wireless* adalah suatu sistem untuk mencegah dan mengidentifikasi

penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan /Keamanan jaringan komputer/ adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Kurniawan dan Sari, (2018) menyatakan bahwa Keamanan jaringan yang ada pada *wireless* antara lain:

a. *Service Set Identifier (SSID)*

Merupakan keamanan rendah yang ada pada suatu sistem jaringan, SSID merupakan nama suatu jaringan.

b. *MAC Filtering*

MAC filtering memfilter jaringan diatas standar 802.11b untuk mengamankan jaringan dan berbentuk bilangan *hexadeciml* 12 digit.

c. *Wi-Fi Protected Access (WPA dan WPA2)*

WPA merupakan sebuah sistem keamanan jaringan yang ada pada jaringan *Wireless*, WPA berbentuk *key* yang dienkripsi yang di-set terlebih dahulu oleh admin.

6. *Wireless (Nirkabel)*

Saskara, dkk, (2019) menyatakan bahwa *wireless* merupakan sebuah teknologi yang dapat digunakan untuk menghubungkan 2 buah piranti yang berupa komputer, laptop maupun *mobile phonet* tanpa menggunakan kabel untuk bertukar data maupun informasi. Salah satu perangkat umum yang digunakan berkomunikasi dalam jaringan lokal nirkabel (*Wireless Local Area Network/WLAN*) adalah *Wireless Fidelity (WiFi)* berdasarkan spesifikasi IEEE 802.11. Har tersebut merupakan standar yang umum digunakan pada komunikasi nirkabel secara internasional. Menurut Nasrullah & Riadi (2018) *Wireless* merupakan salah satu terobosan baru yang memberikan kemudahan dalam pertukaran data antar pengguna dalam satu Jaringan yang memungkinkan pengguna dapat saling berkomunikasi.

Berdasarkan definisi diatas maka dapat disimpulkan bahwa *Wireless* merupakan suatu Jaringan yang berguna untuk menghubungkan 2 pengguna tanpa perlu menggunakan kabel untuk berkomunikasi maupun bertukar data.

a. WLAN (*Wireless Local Area Network*)

Wireless Local Area Network didefinisikan oleh Saskara, dkk. (2019) merupakan sistem komunikasi dengan cakupan yang kecil atau biasa dikenal dengan *Local Area Network* yang sifatnya fleksibel dimana pengirim dan penerima datanya melalui media udara dengan menggunakan teknologi frekuensi radio. Sehingga perangkat dapat bergerak dengan mudah dikarenakan tidak terikat dengan kabel. WLAN sendiri dapat digolongkan menjadi 2 kategori utama yaitu :

1) *Wireless LAN* modus *Ad-Hoc*

Model jaringan modus *ad-hoc*, adalah jaringan antara satu perangkat dengan perangkat yang lain tanpa melalui proses konfigurasi tertentu selama signal dari pemancar dapat diterima dengan baik oleh perangkat- perangkat penerima.

2) *Wireless LAN* modus *Infrastuktur*

Model jaringan dalam bentuk infrastruktur adalah model yang menyediakan *konektivitas* antar perangkat yang terhubung ke WLAN. Perangkat perantara berupa titik akses yang terhubung ke jaringan komputer kabel hal ini diperlukan sebelum mengirim sinyal ke perangkat penerima. Ketersediaan layanan merupakan masalah yang menjadi perhatian dan perdebatan di kalangan praktisi. Oleh karena itu, disebutkan bahwa jaringan komputer aman ketika:

a) *Privacy* dan *Confidentiality*

Sebagai mekanisme yang digunakan untuk melindungi informasi dari pengguna jaringan yang tidak sah, *confidentiality* dengan tujuan maksud informasi diberikan dan hanya dapat digunakan untuk tujuan itu.

b) *Integrity*

Aspek yang lebih mengutamakan akses informasi dengan ditujukannya untuk pengguna tertentu, di mana integritas dari informasi tersebut masih terjaga.

c) *Authentication*

Aspek ini memprioritaskan *efisiensi* akses pengguna ke data, informasi, atau layanan organisasi.

d) *Availability*

Aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.

e) *Access Control*

Aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

f) *Non Repudiation*

Aspek yang berkaitan dengan pencatatan pengguna dengan bertujuan untuk menghindari penyalahgunaan layanan *internet*, data maupun informasi yang tersedia.

7. *MikroTik Router*

Yohaness dan Haeruddin (2020) menyatakan bahwa *MikroTik Router* awal mulanya diciptakan dari sebuah sistem operasi perangkat lunak yang berbasiskan untuk konfigurasi jaringan komputer. Seiring berkembangnya zaman, *MikroTik* mulai menciptakan perangkat keras jaringan seperti salah satunya *router* yang berisikan sistem operasinya sendiri yaitu *MikroTik*. *Mikrotik Router* memiliki banyak fungsi dan keunggulan dari pada kompetitor-kompetitor lainnya seperti *Cisco*. Keunggulannya salah satunya adalah dapat melakukan konfigurasi koneksi ke *internet* secara mudah dalam aspek pengelolaannya dan lebih terpusat. Selain itu *MikroTik Router* juga memiliki fitur pembagian *bandwidth*, konfigurasi *Firewall* NAT dan masih banyak lainnya. Keunggulannya dari sisi *resource* juga banyak, seperti biayanya dan kemudahan penggunaan *interface MikroTik* itu sendiri. Mikrotik merupakan sistem operasi router, yang di-rilease dengan nama mikrotik routerOs yang mampu diinstall pada komputer biasa, tidak seperti sistem operasi router lainnya yang hanya bisa diinstall pada hardware tertentu. Mikrotik memiliki fitur yang sangat lengkap diantaranya : Firewall dan Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Manajemen Bandwidth, Konfigurasi Keamanan dan masih banyak fitur lainnya. Jadi Mikrotik RouterOs difungsikan untuk membagi-bagi koneksi Internet ke beberapa komputer pengguna user (Riadi, 2019).

Berdasarkan defenisi diatas maka dapat disimpulkan bahwa *Mikrotik Router* adalah sistem yang didesain khusus untuk memudahkan berbagai keperluan *computer network*. Contohnya, merancang dan membangun sebuah sistem *computer network* untuk skala besar maupun kecil.

8. Konsep Jaringan Komputer

a. Pengertian Jaringan Komputer

Menurut Saskara, dkk, (2019) Jaringan komputer adalah himpunan interkoneksi antara dua komputer *autonomous* atau lebih yang terhubung. Untuk menghubungkan dua buah komputer *autonomous* diperlukan beberapa perangkat yang menjadi perantara dari kedua komputer tersebut seperti *switch*, *router*, *akses point*, dan juga media perantara untuk mengirimkan data antar dua buah komputer tersebut dapat menggunakan kabel maupun tanpa menggunakan kabel atau dikenal dengan istilahnya adalah *wireless* (nirkabel). Jenis kabel yang biasa digunakan untuk perantara dua buah komputer adalah kabel *Unshielded Twisted Pair*. Novrianda (2020) mendefenisikan jaringan komputer adalah kumpulan komputer *independen* yang saling terhubung antara satu sama lain. Secara umum, jaringan komputer dapat digambarkan sebagai kumpulan komputer yang saling terhubung antar perangkat jaringan komputer sebagai media perantara.

Berdasarkan definisi di atas maka dapat di simpulkan bahwa jaringan Computer merupakan dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer sederhana yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data.

b. Klasifikasi Jaringan Komputer

Yuliandoko (2018) jaringan komputer dikelompokkan menjadi beberapa bentuk sebagai berikut:

1) PAN (*Personal Area Network*)

Merupakan jaringan komunikasi antara satu perangkat dengan perangkat lainnya, hanya beberapa meter jauhnya.

Contoh penggunaan jaringan PAN:

- a) Menghubungkan ponsel ke laptop melalui *bluetooth*.
- b) Menghubungkan *headset* ke laptop melalui *bluetooth*.
- c) Menghubungkan *mouse* ke laptop melalui *bluetooth*.

Kelebihan jaringan PAN :

- a) Control pada PAN dilakukan dengan *autoritas* atau memiliki wewenang hak.
- b) Dapat di gunakan untuk diri sendiri.

Kekurangan jaringan PAN:

- a) Jangkauan jaringan PAN hanya beberapa meter.



Gambar 1. Jaringan PAN
Sumber: Yuliandoko, (2018)

2) LAN (*Local Area Network*)

Merupakan jangkauan jaringan yang mencakup area yang sangat kecil, dengan jarak radius maximal LAN adalah 10 km.

Contoh penggunaan jaringan LAN:

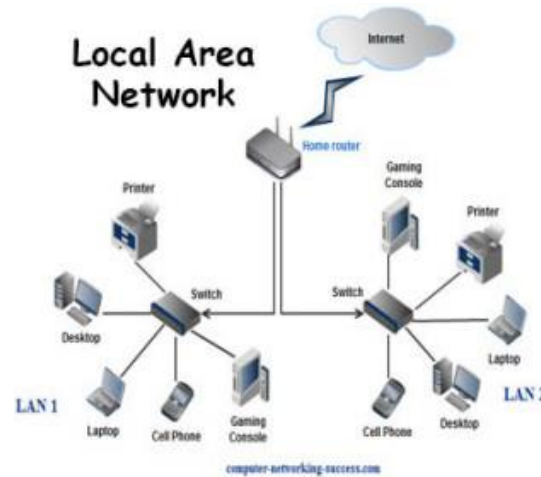
- a) Komputer yang terhubung disekolahan.
- b) Komputer yang terhubung diwarnet.
- c) Hubungan komputer antar rumah.

Kelebihan jaringan LAN:

- a) Mengiriman data dengan cepat antar komputer
- b) IP hanya sampai di *switch* kemudian *router* yang menghubungkan dengan IP publik.
- c) Kegiatan kualitas paling efisien dan lebih efektif.
- d) Tidak memerlukan jaringan *internet* untuk terhubung dari komputer satu dengan lainnya yang dapat menghemat biaya.

Kekurangan jaringan LAN:

- a) Cakupan yang sempit sempit.
- b) Rentan terkena virus bila salah satu PC yang terhubung terinfeksi.
- c) Kecepatan *internet* lambat akibat PC yang meningkat



Gambar 2. Jaringan LAN
Sumber: Yuliandoko, (2018)

3) MAN (*Metropolitan Area Network*)

Merupakan jaringan yang memiliki area jangkauan yang cukup besar yang berhubungan dengan daerah/kota dalam kisaran 10-50 km.

Contoh penggunaan jaringan MAN:

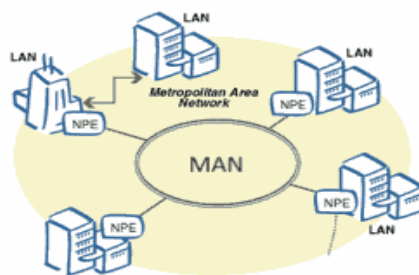
- Jaringan bank.
- Koneksi antar komputer internal.
- Hubungkan kantor cabang lokal dengan kantor pusat.

Manfaat jaringan MAN:

- Jaringan yang relatif besar membuat komunikasi menjadi lebih mudah dan efisien.
- Dukungan bisnis atau hubungan antar instansi atau organisasi kantor.

Kekurangan jaringan MAN:

- Biaya operasional yang relatif tinggi.
- Biaya perawatan juga sangat tinggi.
- Sering menjadi sasaran para *cracker* untuk keuntungan pribadi.



Gambar 3. Jaringan MAN
Sumber: Yuliandoko, (2018)

4) WAN (Wide Area Network)

Merupakan jaringan yang sangat luas mencakup negara dan benua.

Contoh penggunaan jaringan WAN:

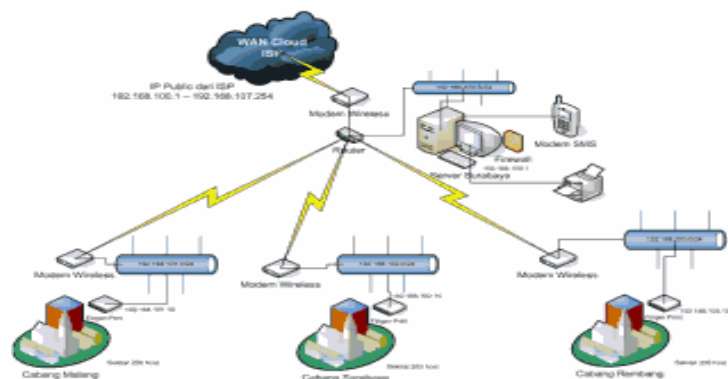
- Jaringan yang dimiliki bank berskala nasional.
- Tv kabel internasional.
- Jaringan pendidikan tinggi nasional.

Kelebihan jaringan WAN:

- Mencakup dan memiliki akses ke area geografis yang luas.
- Perangkat lunak dan sumber daya dapat dibagi (*shared*) dengan *workstation* yang terhubung.
- Share* (berbagi) informasi/file dalam area yang lebih luas.

Kekurangan jaringan WAN:

- Biaya untuk harga operasional mahal dan umumnya lambat.
- Membutuhkan keamanan (*firewall*) yang baik untuk membatasi pengguna dari luar yang ingin masuk dan dapat mengganggu jaringan ini.
- Tidak dapat memenuhi kebutuhan informasi lokal atau kepentingan.
- Rentan ancaman dari luar.



Gambar 4. Jaringan WAN
Sumber: Yuliandoko, (2018)

5) Wireless

Jaringan nirkabel menggunakan udara sebagai media transmisi untuk mentransmisikan gelombang elektromagnetik.

Contoh penggunaan jaringan *Wireless*:

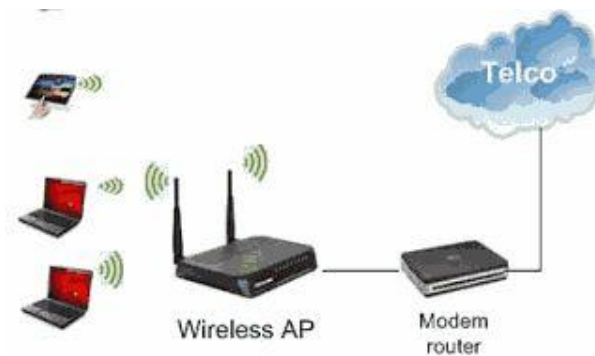
- Penggunaan *remote tv*.
- Penggunaan *remote ac*.
- Telepon selular.

Kelebihan jaringan *Wireless*:

- a) Biaya harga pemeliharaan murah.
- b) Proses membangun jaringan yang cepat.
- c) Jaringan yang lebih mudah dikembangkan.
- d) Jaringan yang lebih mudah dan murah untuk direlokasi.
- e) Jenis infrastruktur yang berdimensi kecil.

Kekurangan jaringan *Wireless*:

- a) Kecepatan sinyal akan dipengaruhi oleh provokasi udara.
- b) Harga Biaya peralatan mahal.
- c) Keamanan data yang rentan.
- d) Delay yang sangat besar.
- e) Produk dari produsen yang berbeda kadang-kadang tidak kompatibel.



Gambar 5. Jaringan *Wireless*
Sumber: Yuliandoko, (2018)

9. Metode Otentikasi Pada RADIUS

Darmadi (2018) menyatakan bahwa RADIUS ini mendukung berbagai mekanisme protokol untuk mentransfer data khusus pengguna yang sensitif ke dan dari server otentikasi. Dua metode yang paling umum adalah PAP (*Password Authentication Protocol*) dan CHAP (*Challenge Handshake Authentication Protocol*). RADIUS dapat menggunakan properti dan metode yang dikembangkan oleh vendor, termasuk dukungan untuk *Windows NT*, *Windows 2000*, dan sistem operasi jaringan lain yang banyak digunakan, dan fitur khusus layanan direktori. Berikut akan dibahas lebih rinci dua metode yang paling umum:

- a. *Password Authentication Protocol (PAP)*

Atribut User-Password adalah sinyal paket permintaan ke server radius yang menggunakan protokol PAP transaksi. Server RADIUS masuk kemudian melalui proses verifikasi dan koneksi diizinkan.

b. *Challenge-Handshake Authentication Protocol (CHAP)*

Menurut El-Gendy (2019) CHAP adalah skema otentikasi yang digunakan oleh *Point to Point Protocol (PPP server)* untuk memvalidasi identitas klien jarak jauh. *Challenge Handshake Authentication Protocol*, atau CHAP, adalah salah satu dari dua protokol otentikasi yang didukung oleh PPP. CHAP bekerja dengan *Link Control Protocol (LCP)* untuk mengotentikasi koneksi setelah *fase* pembentukan tautan. CHAP terus menerus memeriksa kembali validitas *host* penghubung untuk melindungi terhadap akses yang tidak sah. Paket CHAP menggunakan sistem tantangan, yang berarti bahwa *autentikator* mengirimkan paket tantangan secara terus menerus hingga sistem penghubung merespon dengan paket yang berisi respons.

10. Profil Desa Taripa

Desa merupakan salah satu unsur kewilayahan terkecil di dalam Negara Kesatuan Republik Indonesia. Walaupun demikian, Desa mempunyai peran strategis dalam pencapaian sasaran pembangunan. Hal ini dikarenakan pada tingkat Desa secara faktual aktifitas Pemerintahan berjalan dan sebagian besar penduduk Indonesia masih terkonsentrasi saat ini. Sudah selayaknya di tingkat Desa menjadi pusat aktifitas Pemerintahan, Pembangunan dan Pemberdayaan Masyarakat, termasuk juga penyusunan data dasar dalam mendukung berbagai aktifitas tersebut. Kantor Desa Taripa adalah salah satu Kantor Desa yang berada di Kecamatan Angkona yang bergerak dalam bidang pelayanan Masyarakat desa. Letak kantor berada di Kecamatan Angkona, Kabupaten Luwu Timur, Sulawesi Selatan.

2.2 Hasil Penelitian yang Relevan

Penelitian ini mengacu pada beberapa penelitian yang sudah ada, guna sebagai referensi dalam penelitian yang dilalui.

1. Novrianda (2019) dengan judul “Rancang Bangun Keamanan Jaringan *Wireless* Pada STIPER SRIWIGAMA Palembang Dengan RADIUS *Server*”. Server RADIUS terintegrasi ketika anda membangun *server* RADIUS dengan melakukan beberapa langkah dari konfigurasi Mikrotik RB951, konfigurasi *firewall* NAT, konfigurasi *access point* hingga konfigurasi *hotspot*. Pengaturan DNS yang mengarah ke www.stipersriwigama.com melalui prosedur pengaturan titik akses, sehingga anda dapat masuk dan menambahkan pengguna di jendela pembuatan pengguna *creat hotspot localhost*. Hasil dari penelitian ini, tidak hanya mengurangi lalu lintas pengguna dengan membatasi akses ke STIPER Sriwigama Palembang oleh pengguna yang tidak berkepentingan, tetapi keamanan data STIPER Sriwigama Palembang lebih aman karena pengguna tidak dapat terhubung ke jaringan.
2. Mentang, Alicia A. E. Sinsuw, ST., MT., Xaverius B. N. Najoan, ST., MT (2018) dengan judul “Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan *Wireless Intrusion Detection System*” tujuannya adalah untuk menjelaskan proses yang terjadi saat menguji koneksi antara aplikasi dan sensor, menganalisis serangan, serta mendeteksi dan mengelola serangan yang telah dilakukan. Hasil penelitian jaringan komputer hanya dapat dipantau melalui mesin dan komputer bertindak sebagai sensor pada jaringan dan IDS dapat diterapkan untuk melihat anacam yang muncul.
3. Sujadi dan Burhanuddin (2018) dengan judul “Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode Ipsec Vpn (Studi Kasus: Pt.Agrabudi Komunika)” Bertujuan Untuk merancang arsitektur jaringan, artinya satu atau lebih komputer dapat dihubungkan ke komputer lain sehingga dapat saling berkomunikasi dan bertukar data atau mengamankan data dalam perjalanan. IPSec VPN memastikan bahwa data yang ditransmisikan sepenuhnya dienkripsi, sehingga transmisi data dapat dengan mudah dikirim tanpa gangguan oleh pihak ketiga. Hasilnya adalah arus jaringan PT.Agrabudi Komunika menggunakan topologi *star*. Topologi jaringan ini banyak digunakan

di berbagai tempat karena dapat dengan mudah menambah, menghapus atau mendeteksi kegagalan pada jaringan yang ada.

Adapun persamaan dalam penelitian yang saya gunakan dengan ketiga penelitian yang relevan yaitu sama-sama fokus pada sistem keamanan jaringan dengan tujuan mengamankan Jaringan Komputer. Perbedaan dari penelitian yang saya lakukan dengan ketiga penelitian yang relevan yaitu judul penelitian, Aplikasi yang digunakan dan perbedaan tempat penelitian.

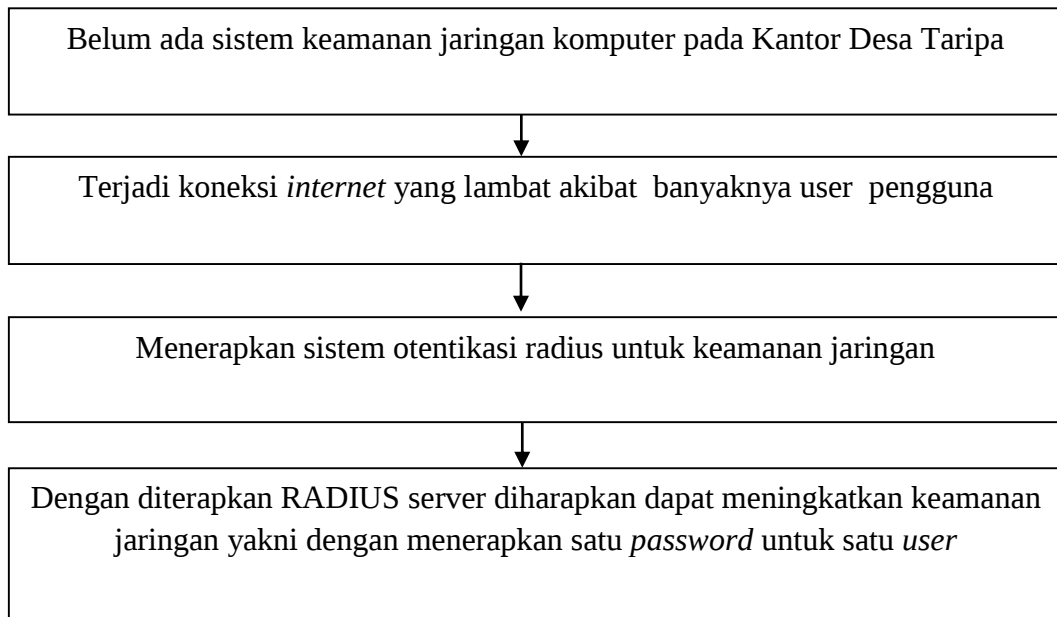
2.3 Kerangka Pikir

Untuk lebih memperjelas permasalahan yang disajikan, maka berikut akan ditunjukkan kerangka pikir seperti pada gambar 6.

Kantor Desa Taripa merupakan sebuah Kantor yang bergerak dalam bidang pelayanan Masyarakat. Kegiatan aktifitas kantor telah dilakukan dengan menggunakan sebuah komputer dan akses jaringan *internet*, dengan hal ini diharapkan proses kerja serta pengarsipan dokumen-dokumen menjadi lebih aman dan pekerjaan cepat dilaksanakan. Sistem keamanan yang masih belum ada membuat masyarakat yang tinggal di lingkungan kantor dengan mudah mengakses jaringan hal ini dapat membahayakan keamanan data Kantor Desa.

Melihat kondisi seperti itu, diperlukan sebuah sistem keamanan jaringan komputer yang dapat menjaga keamanan jaringan komputer yang digunakan di Kantor Desa Taripa. Atas pertimbangan hal tersebut penulis merasa perlu merancang sistem keamanan jaringan komputer di Kantor Desa Taripa sehingga pegawai kantor tidak merasakan akses *internet* yang lambat akibat banyaknya *user* yang mengakses jaringan serta keamanan data-data bisa lebih terjaga.

Pemanfaatan keamanan jaringan komputer diharapkan dapat memberikan salah satu alternatif masukan pemecahan masalah untuk mengatasi kelemahan-kelemahan yang terjadi guna memperbaiki kinerja yang mampu memberikan akses *internet* yang lebih cepat dan aman serta penyimpanan data-data yang lebih terjaga.



Gambar 6. Kerangka Pikir