BAB II

LANDASAN TEORI

2.1. Definisi Wireless Distribution System

Pada standart IEEE 802.11 terminologi dari *distribution system* adalah sistem yang saling terhubung dinamakan *Basic Service Set* (BSS). BSS lebih baik jika dibandingkan dengan "*Cell*" yang dikendalikan oleh akses poin tunggal. Sehingga *Distribution System* menghubungkan antar *cell* yang bertujuan untuk membangun jaringan luas sebagai dasar pemikiran dan memungkinkan pengguna perangkat *mobile* dapat berpindah-pindah serta tetap terhubung ke sumber jaringan yang tersedia.

Satu aspek penting dari WDS (skema ini berbeda dengan koneksi *wireless* antar AP sebelumnya yang digunakan oleh instansi untuk pemasangan di luar ruangan) sebenarnya adalah *single* laptop *card* pada AP dapat mengasumsikan peran ganda pada waktu yang sama. Hal ini dapat "mengendalikan" *cell* (seperti pada jaringan kabel yang menghubungkan antar AP), dan seperti infrastruktur yang menghubungkan klien secara *wireless*, serta dapat mempertahankan hingga enam koneksi *wireless* yang berbeda ke AP lainnya. Sehingga memungkinkan operasional (frekuensi) kanal harus sesuai dengan *cell* yang dikendalikan oleh AP dan untuk *wireless link* ke AP yang lain (ORINOCO Technical Bulletin, 2002).

2.2. Cara Kerja WDS (pengalamatan)

Perangkat *local area network* (LAN) (termasuk perangkat wireless LAN) berkomunikasi antar perangkat menggunakan alamat MAC (alamat *hardware* yang unik diberikan oleh pabrik disetiap perangkatnya). Sehingga setiap *wireless*

personal computer (PC) *card* memiliki alamat MAC yang digunakan oleh sistem untuk mengirimkan data *frame*. Jika perangkat LAN mengirimkan data, maka akan menambahkan alamat MAC-nya sendiri untuk menunjukkan kepada penerima darimana *frame* berasal. Secara singkatnya semua *frame* data yang dikirimkan melalui LAN diberi header berisi alamat MAC sumber dan tujuan. Jika data *frame* dikirimkan maka hanya memerlukan dua alamat MAC tersebut. Ketika data *frame* yang tidak terhubung ke segmen LAN yang sama ditransmisikan di antara ujung ke ujung LAN, maka perangkat penghubung diperlukan untuk menghubungkan frame dari satu segmen ke segmen yang lain. Akses poin adalah perangkat yang juga dikenal sebagai *bridge*, yang memiliki kemampuan untuk menyampaikan lalu lintas dari satu segmen ke segmen yang lain. Ia melakukan tugas ini dengan menggunakan "*table bridge*", di mana alamat MAC disimpan.

Lalulintas antar perangkat LAN nirkabel yang sesuai dengan standar IEEE 802.11 membutuhkan 4 alamat MAC bukan 2. Ketika perangkat nirkabel saling terhubung ke AP maka akan selalu di arahkan ke lalulintas tersebut ke AP dengan menggunakan alamat MAC yang terdapat pada PC *card* pada AP sebagai alamat tujuan langsung. Alamat MAC dari stasiun akhir yang terdapat pada *frame* yang akan dikirimkan termasuk dengan *header frame*, sehingga PC *card* pada AP dapat mengetahui kemana frame tersebut dikirimkan. Pada akhirnya stasiun pengirim menggunakan alamat MAC sendiri di dalam frame sebagai alamat sumber. Sehingga total mempunyai tiga alamat yang digunakan (ORINOCO Technical Bulletin, 2002).

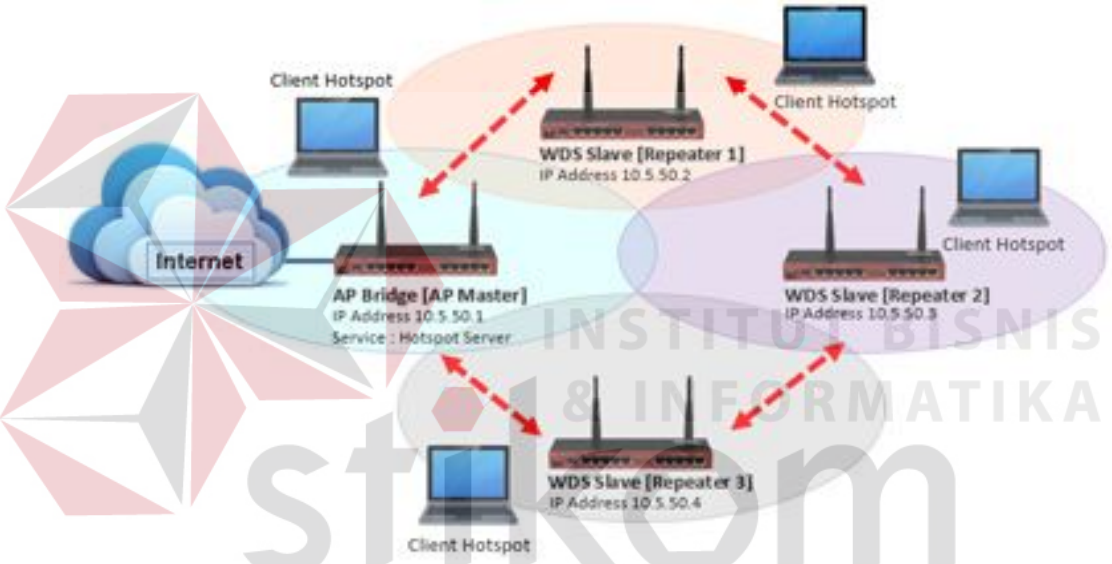
Ketika jalur WDS diaktifkan diantara dua AP, maka terdapat empat alamat

yang tersedia pada *header* MAC yang digunakan antara lain:

- Alamat MAC dari pengirim,
- Alamat MAC dari tujuan akhir,
- Alamat MAC dari PC *card* pada AP, dan
- Alamat MAC dari PC *card* penerima pada AP yang berbeda.

2.3. Komponen WDS

Komponen dan struktur dari WDS dapat dilihat pada Gambar 2.1



Sumber : https://www.mikrotik.co.id

Gambar 2.1 Struktur komponen WDS

Berikut adalah komponen dari WDS.

- **WDS *Master***

  Merupakan AP yang mengaktifkan WDS dan bertugas untuk menghubungkan jaringan dengan *server* (Yoga, 2005).

- **WDS *Slave***

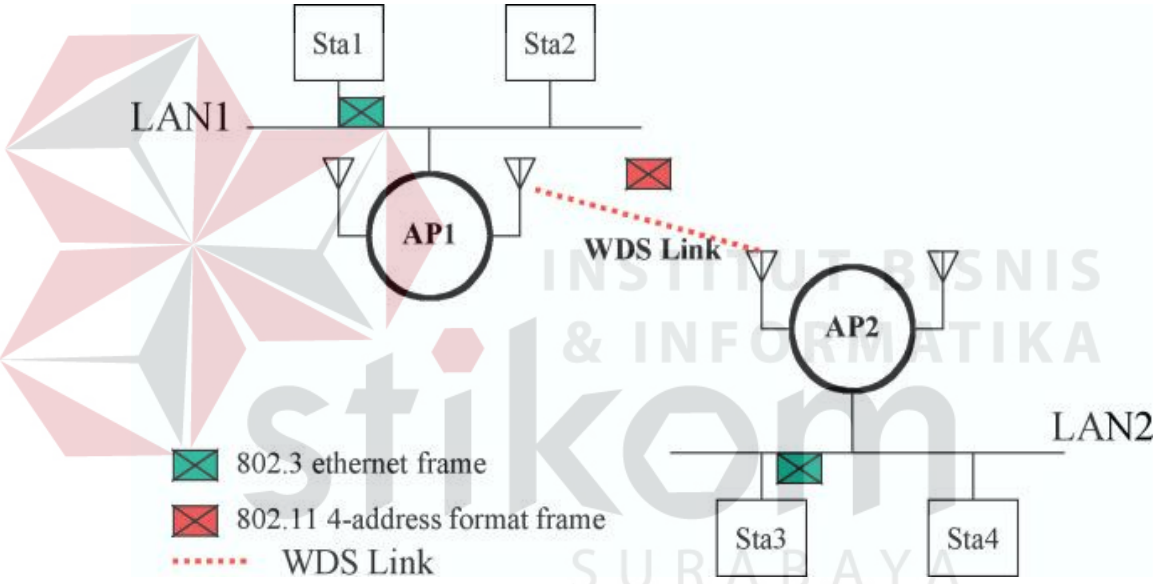
  Mode WDS slave ini berfungsi sebagai pemancar atau AP sekaligus

penerima (*station*) atau disebut sebagai *repeater* (Yoga, 2005).

2.4. Jenis WDS

WDS mempunyai 2 tipe konfigurasi antara lain WDS bridging dan WDS repeater. WDS bridging penghubung antara client ke AP menggunakan kabel sebagai penghubungnya namun penghubung antar AP menggunakan jalur WDS. WDS repeater penghubung antara client ke AP dan AP ke AP semua tidak menggunakan kabel. Berikut adalah penjelasan tentang kedua tipe WDS:

2.4.1. *Bridging* WDS



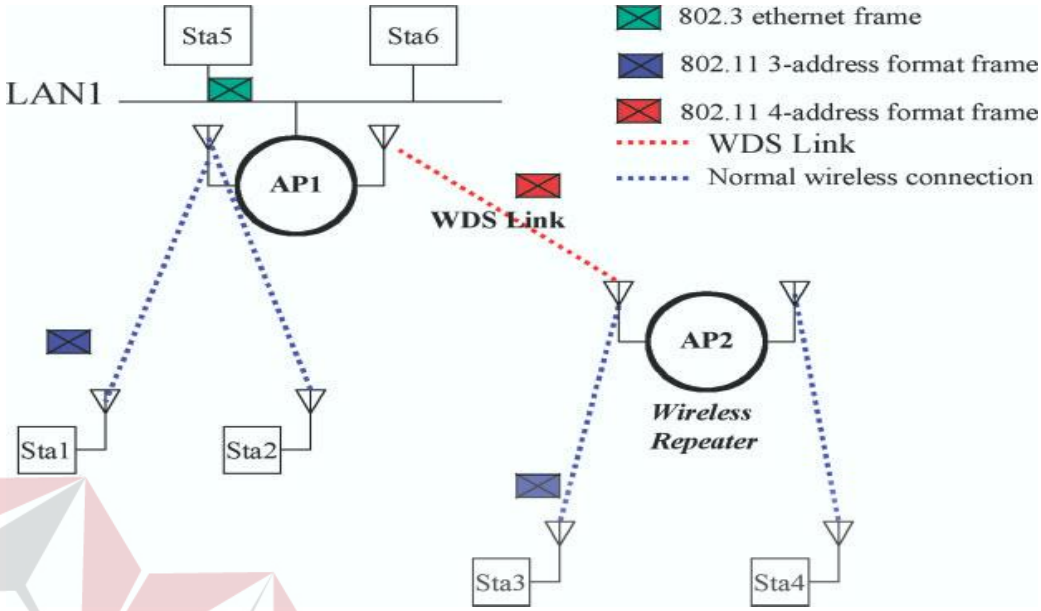
Gambar 2.2 WDS *Bridge*

WDS pada Gambar 2.2 diatas disebut konfigurasi "*wireless bridge*", karena memungkinkan untuk mengakses dua LAN di *link layer*. Pada Gambar 2.2 diatas AP bertingkah seperti *brige* pada umumnya yang meneruskan paket antar WDS *link* (*link* yang terhubung antar AP) dan port *Ethernet*. Seperti *bridge* pada umumnya, AP mempelajari alamat MAC hingga 64 *wireless* dan atau total 128 perangkat jaringan menggunakan kabel dan nirkabel, yang terhubung ke masing-masing port *Ethernet* untuk membatasi data yang akan diteruskan. Hanya data

yang ditunjukkan untuk stasiun yang berada pada *link Ethernet*, data *multicast* atau data dengan tujuan yang tidak diketahui perlu di teruskan ke AP yang lain melalui *link* WDS.

Sebagai contoh *frame* 802.3 *Ethernet* dikirimkan melalui kabel dari stasiun 1 (Sta1) ke Sta3 pada gambar 2.2, *frame* membutuhkan translasi ketika *frame* melanjutkan melalui WDS *link* antara AP1 dan AP2. Ketika AP1 menerima *frame* 802.3, *frame* tersebut akan di tranlasikan ke standar IEEE 802.11 dengan *frame* format empat alamat sebelum dikirimkan ke WDS *link*. Pada format empat alamat, alamat MAC AP2 dan MAC Sta3 semuanya dimasukkan ke dalam *header frame* 802.11, dan data *frame* sama seperti *frame Ethernet* pada umumnya. Berdasarkan informasi format *frame* empat alamat, AP2 akan membangun ulang *frame Ethernet* 802.3 ketika *frame* diteruskan ke LAN2. Jika algoritma keamanan yang dikonfigurasi pada perangkat AP, maka akan dienkripsi dan didekripsi format *frame* empat alamat tersebut sebelum *frame* tersebut diteruskan. Dari sudut pandang Sta3, fungsi *bridging* merupakan transparan, *frame* yang diterima sama seperti jika Sta1 dan Sta3 pada LAN yang sama (Packard, 2004).

2.4.2. *Repeater* WDS



Gambar 2.3 WDS *Repeater*

Pada Gambar 2.3, AP2 digunakan untuk memperluas jangkauan infrastruktur *wireless* dengan meneruskan lalulintas antara yang menghubungkan antara stasiun *wireless* dan *repeater* yang lain atau AP yang terhubung dengan kabel LAN. Perlu diperhatikan bahwa dalam mode ini lalu lintas *Ethernet* lokal tidak diteruskan. Lalu lintas antara Sta3 dan Sta4 tidak meneruskan WDS *link*, maupun lalu lintas antara Sta5 dan Sta6. Seperti mode *wireless bridge*, perangkat AP beroperasi pada mode *wireless repeater* membutuhkan untuk translasi kedalam format *frame* yang berbeda ketika *frame* tersebut dilanjutkan diantara koneksi nirkabel dan WDS *link*, format *frame* empat alamat 802.11 yang digunakan oleh *link* yang terhubung ke stasiun *wireless*, selama format *frame* empat alamat 802.11 digunakan pada WDS *link* yang terhubung pada AP yang lain. Algoritma enkripsi atau dekripsi yang juga diminta jika AP dikonfigurasi agar aman.

Kantor yang terhubung dengan AP *wireless* 11a/b/g dapat berfungsi sebagai

wireless repeater atau *wireless bridge* jika WDS *link*yang dikonfigurasi antar AP yang terhubung secara tepat. Sebuah WDS *link* menetapkan sepasang alamat MAC antar AP yang terhubung. Untuk membuat WDS *link* diantara dua kantor yang terhubung dengan AP *wireless* 11a/b/g, mencantumkan alamat MAC AP yang lain pada masing-masing AP melalui daftar WDS.

Sebagai tambahan, pastikan semua konfigurasi AP WDS bekerja dalam kanal radio yang sama. Semenjak WDS *link* dapat beroperasi pada kanal radio 2,4 GHZ atau 5,4 GHZ, tidak disarankan menggunakan pemilihan kanal secara otomatis (Packard, 2004).

2.5. Quality of Service

Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan kapasitas jaringan, mengatasi *packet loss, delay* dan *throughput* (Langi, 2011). Sedangkan menurut Rahayu, (2013) kualitas layanan atau QoS adalah kemampuan sebuah jaringan untuk menyediakan layanan yang lebih baik bagi trafik. QoS merupakan sebuah sistem arsitektur *end-to-end* dan bukan merupakan sebuah *feature* yang dimiliki oleh jaringan. QoS suatu *network* merujuk ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi.

QoS dirancang untuk membantu pengguna menjadi lebih produktif dengan memastikan bahwa pengguna mendapatkan kinerja yang handal dari aplikasi – aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda – beda. QoS merupakan suatu tantangan yang besar dalam jaringan berbasis IP dan internet secara keseluruhan (Langi, 2011)

QoS dapat dilihat dari tingkat kecepatan dan keandalan dalam mengelola penyampaian data dalam suatu informasi dengan jenis beban yang beragam. Terdapat beberapa parameter yang digunakan untuk mengukur tingkat kecepatan dan keandalan satu jaringan, diantaranya *latency* (*delay*), *packet loss* dan *troughput.*

2.6. Parameter – parameter *Quality of Service*

QoS mempunyai beberapa parameter namun berikut adalah parameter – parameter yang digunakan:

2.6.1. Delay

Delay merupakan akumulasi berbagai waktu tunda dari ujung ke ujung pada jaringan. Waktu tunda mempengaruhi waktu tempuh paket untuk mencapai tujuan (Langi, 2011).

2.6.2. Packet Loss

Paket hilang (*packet loss*) merupakan penyebab utama pelemahan audio dan video pada multimedia *streaming*. Paket hilang dapat disebabkan oleh pembuangan paket di jaringan (*network loss*) atau pembuangan paket di *gateway/terminal* sampai kedatangan terakhir (*late loss*). *Network loss* secara normal disebabkan kemacetan (*router buffer overflow*), perubahan rute secara seketika, kegagalan *link*, dan *lossy link* seperti saluran *wireless*. Kemacetan atau kongesti pada jaringan merupakan penyebab utama dari paket hilang (Langi, 2011).

2.6.3. Throughput

Throughput merupakan *rate* (kecepatan) transfer data efektif, yang diukur dalam *bit per second* (bps). *Throughput* merupakan jumlah total kedatangan paket

yang sukses yang diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut (Langi, 2011).

2.7. Definisi alamat *Internet Protocol*

Alamat *internet protocol* (IP) terdiri atas 32 bit angka, pada umumnya ditulis dalam notasi *dotted-decimal*. "*Decimal*" merupakan istilah yang berasal dari setiap *byte* (8 bit) pada 32 bit alamat IP yang di konversi kedalam desimal. Dari keempat angka desimal yang dihasilkan tertulis didalam urutan, dengan "*dots*," atau titik yang memisahkannya dinamakan *dotted-decimal*. Setiap angka decimal pada alamat IP disebut *octet*. Istilah *octet* digunakan secara umum bukan *byte*. Ukuran angka desimal disetiap oktetnya berkisar antara 0 hingga 255. (Odom, 2004).

2.7.1. Jenis Alamat

Pada tulisan memorandum yang ditulis oleh insinyur dan ilmuan komputer tentang metode, perilaku, penelitian, atau inovasi yang berlaku untuk kinerja internet dan sistem yang tersambung ke internet (RFC 790) mendefinisikan protokol IP, termasuk beberapa perbedaan kelas dari sebuah jaringan. IP didefinisikan kedalam tiga bagian kelas jaringan yang berbeda yaitu A, B, dan C, yang digunakan oleh *host*.

2.7.2. Kelas IPv4

Setiap jaringan kelas A, B, dan C mempunyai perbedaan ukuran sebagai identifikasi jaringan :

1. **Kelas A** adalah alamat jaringan yang mempunyai panjang 1 *byte* untuk jaringan. 3 *bytes* sisanya untuk bagian *host*.
2. **Kelas B** adalah alamat jaringan yang mempunyai panjang 2 *bytes* untuk

jaringan. 2 *bytes* sisanya untuk bagian *host*.

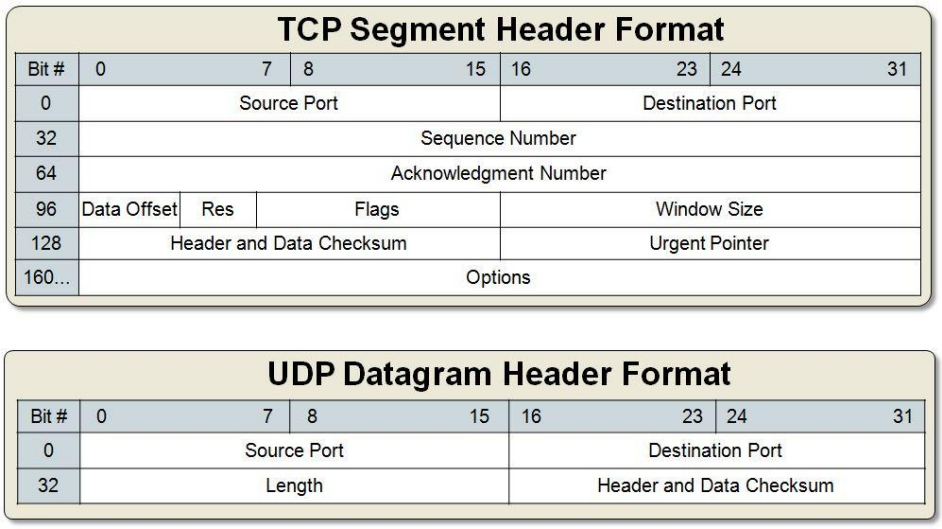
3. **Kelas C** adalah alamat jaringan yang mempunyai panjang 3 *bytes* untuk jaringan. 1 *bytes* sisanya untuk bagian *host*.

2.8. *User Datagram Protocol* (UDP)

UDP menyediakan layanan aplikasi untuk saling bertukar pesan. Tidak seperti TCP, UDP merupakan *connectionless*, *no reliability*, *no windowing*, dan tanpa melakukan penataan kembali data yang diterima. Akan tetapi UDP memberikan beberapa fungsi dari TCP, seperti pengiriman data, segmentasi, dan *multiplexing* yang menggunakan angka *port*, dan juga melakukan dengan *byte* lebih sedikit dari yang disediakan dan sedikit pemrosesan.

Multiplexing pada UDP akan menggunakan angka *port* untuk identitas sama seperti pada TCP. Satu – satunya perbedaan dalam soket UDP bahwa, sebagai gantinya menunjuk seperti halnya protokol *transport* pada TCP, UDP adalah protokol *transport*. Suatu aplikasi dapat membuka identitas angka *port* pada *host* yang sama namun menggunakan TCP dalam satu kasus dan disisi lain menggunakan UDP itu jarang terjadi, tapi hal tersebut tentunya diperbolehkan. Jika suatu layanan tertentu mendukung *transport* UDP atau TCP, akan menggunakan nilai *port* yang sama angka port TCP dan UDP.

Data transfer UDP berbeda dengan data transfer pada TCP bahwa tidak ada penataan kembali. Penggunaan aplikasi UDP mentoleransi terjadinya kehilangan data, atau mempunyai suatu mekanisme untuk mendapatkan kembali data yang hilang.



TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Sumber : https://microchip.wdfiles.com

Gambar 2.4 *Header* TCP dan UDP.

Pada Gambar 2.4 menunjukkan format *header* dari TCP dan UDP. Perhatikan kedua *source port* dan *destination port* pada *header* TCP dan UDP, pada UDP tidak ada *sequence number* dan *acknowledgement*. UDP tidak membutuhkan bagian tersebut karena hal tersebut membuatnya tidak adanya penomoran data untuk *acknowledgements* atau *sequencing*.

UDP mempunyai beberapa keunggulan dibandingkan TCP dengan tidak adanya *acknowledgement* dan *sequence*. Keuntungan yang paling jelas dari UDP adalah memiliki lebih sedikit *byte* dari yang disediakan. Tidak jelas seperti sebenarnya UDP tidak perlu menunggu *acknowledgement* atau menahan data di memori hingga setelah *acknowledgment*. Dengan demikian aplikasi UDP tidak diperlambat dengan proses *acknowledgement*, dan memorinya terbebas sehingga lebih cepat (Odom, 2004).

2.9. Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup

berbagai fitur yang dibuat untuk IP *network* dan jaringan *wireless*, cocok digunakan oleh ISP dan *provider hotspot*. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun (Sinaga, 2013).

2.9.1. *Router* Mikrotik

Router Mikrotik mempunyai produk *routerboard* yang kecil dan diperuntukkan untuk di dalam rumah. Memiliki 4 buah *port ethernet* 10/100, dengan prosesor baru Atheros 400MHz.

Gambar 2.5 Router Mikrotik 941 *haplite*

2.10. Layanan RTSP dan RTP

Real time transmission protocol (RTP) merupakan protokol standar internet untuk pengiriman data *real time*, termasuk audio dan video. Protokol ini dapat digunakan untuk media *on demand* dan juga layanan interaktif seperti telepon internet. RTP telah dikembangkan oleh *Internet Engineering Task Force* (IETF) dan digunakan secara luas. Sebenarnya standar RTP mendefinisikan sepasang protokol yaitu RTP dan *real time transport control protocol* (RTCP).

RTP digunakan untuk pertukaran data multimedia, selama RTCP mengontrol sebagian dan digunakan secara periodik termasuk mengontrol *feedback* informasi mengenai kualitas transmisi yang berhubungan dengan data flow. RTP berjalan diatas protokol UDP/IP namun upaya yang dilakukan membuatnya menjadi *transport independence* sehingga hal tersebut seharusnya digunakan diatas protokol lain. RTP yang berhubungan dengan RTCP menggunakan *port transport layer* secara berturut – turut, ketika digunakan pada UDP.

Internet merupakan sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi. Tujuannya agar setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan. Ada beberapa layanan untuk media pengiriman seperti *real time streaming protocol* (RTSP).

Seperti yang telah dideskripsikan oleh RFC 2326, pada *layer* aplikasi protokol RTSP memungkinkan untuk mengontrol melalui data yang dikirimkan dengan *real time* dari sebuah IP. Termasuk seperti mengontrol *pausing playback*, memposisikan *playback*, mempercepat atau mengembalikan *playback*. RTSP bukan bertipe mengirimkan media secara terus – menerus, meskipun demikian RTSP menyisipkan media *streaming* secara terus - menerus dengan sebisa mungkin mengendalikan *streaming*.

RTSP adalah protokol presentasi multimedia antar *client* dan *server*. Sehingga tidak ada *notion* pada koneksi RTSP. Sebagai gantinya, server mengelola identifikasian sesi label. Pada sesi RTSP protokol *transport* tidak terikat. Selama sesi RTSP terjadi, RTSP *client* akan membuka dan menutup agar koneksi pada *transport reliable* untuk *request* RTSP kepada *server*. Hal tersebut

mungkin sebagai alternatifnya menggunakan protokol transport *connectionless* seperti UDP.

RTSP didesain untuk bekerja dengan protokol tingkat dasar seperti *real time protocol* (RTP) atau *resource reservation protocol* (RSVP) untuk memberikan servis *streaming* secara komplit pada internet. Hal tersebut berarti untuk memilih kanal pengiriman (seperti UDP, *multicast* UDP dan TCP), dan mekanisme pengiriman berdasarkan RTP. Pesan RTSP dikirimkan melalui pita media *streaming*. RTSP bekerja untuk *multicast* audien yang besar seperti halnya *single viewer unicast* (Durresi, 2005).

2.11. Network Monitoring

Monitoring jaringan dibutuhkan untuk melakukan pengawasan pada jaringan yang dilakukan, agar jaringan tersebut selalu terkontrol dan apabila terputus dapat diketahui langsung oleh *user*. Pada tugas akhir ini *software* yang digunakan untuk *monitoring* jaringan yaitu Wireshark.

2.11.1. Wireshark

Wireshark merupakan salah satu *tool monitoring* jaringan yang berfungsi untuk mengawasi lalu lintas pada jaringan komputer dan dapat menganalisa keseluruhan jaringan *computer* (Cahyaningtyas, 2013). Logo wireshark dapat dilihat pada Gambar 2.6

Sumber: http://www.wireshark.org

Gambar 2.6 Logo Wireshark

Wireshark dapat melihat dan meyimpan informasi mengenai paket keluar dan

masuk dalam jaringan yang terkirim dan diterima.

2.11.2. Tujuan dan Manfaat Wireshark

Manfaat dari *software* Wireshark, sebagai berikut :

- Menangkap informasi yang dikirim dan diterima,
- Mengetahui aktivitas dalam jaringan komputer,
- Mengetahui dan menganalisa kinerja jaringan computer,
- Mengamati keamanan jaringan komputer (Cahyaningtyas, 2013).