BAB 2

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Penelitian yang dilakukan oleh Bayu Muji Nugroho (2022) mengenai *"Analisis dan Simulasi Perancangan Wireless Distribution System (WDS) Menggunakan Router Mikrotik pada SMAN 1 Kerumutan"*. Dimana didalamnya membahas tentang analisis penerapan sistem WDS pada koneksi *wireless hotspot* secara optimal dan memperluas jangkauan jaringan *wireless* dan melakukan *management bandwidth* menggunakan *simple queue* dengan router Mikrotik Rb951Ui-2HnD. Pada studi kasus lokasi *client* di SMAN 1 Kerumutan.

Penelitian yang dilakukan oleh Jago Pamungkas (2018) dengan judul *"Implementasi Teknologi WDS (Wireless Distributin System) Menggunakan Router Mikrotik RB951Ui2HnD Pada Indekost Biru 3 Lantai"* yang di dalamnya membahas mengenai penerapan *wireless* menggunakan teknologi WDS dengan melakukan pengujian QOS (*Quality of Service*). Penyebaran sinyal *wireless* tidak merata dilakukan pemetaan sinyal *wireless* menggunakan *software EkahauHeatmapper* dan dengan menggunakan *routing* OSPF untuk koneksi antar router Mikrotik. Studi kasus lokasi *client* di Indekost Biru 3 Lantai.

Penelitian yang dilakukan oleh Kobro Anggoro (2017) mengenai *"Analisis Wireless Distribution System (WDS) dengan 4 buah RB951Ui-2HnD"* yang membahas mengenai analisis jaringan *wireless* menggunakan metode QOS

(*Quality of Service*) pada jaringan *dial up* modem Mifi Smartfren Andromax M2P yang diterapkan pada *client* yang memiliki masalah pada jaringan *wireless* ditempatnya, dikarenakan medan yang padat dan terlalu luas. Dimana dalam pelaksanaannya dilakukan sebuah pemetaan sinyal pada *access point*. Studi kasus lokasi penelitian di lapangan desa Kepurun.

Penelitian yang dilakukan oleh Lutfi Fadthorik (2019) dengan judul *"Analisis Internal Wireless Hotspot Area dengan Sistem Roaming menggunakan Mikrotik di SMK Ma'arif Ponjong Gunungkidul"* yang didalamnya membahas mengenai perancangan pemetaan penyebaran sinyal *access point* menggunakan dua buah *WLAN indoor* (TP-Link WR840N). Dimana dalam penelitian dilakukan integrasi *access point* dengan menggunakan sistem *internal wireless roaming* untuk mempermudah *client* dalam menggunakan dan menghindari terjadinya *segmentasi IP* dan mengotomatisasikan pengalokasian alamat IP tanpa harus melakukan konfigurasi ulang. Studi kasus lokasi penelitian di SMK Ma'arif Ponjong Gunungkidul.

Penelitian yang dilakukan oleh Serphian David Setiawan (2014) mengenai *"Implementasi dan Analisis Wireless Distribution Systems (WDS) Mengguanakan Mikrotik Studi Internet Service Provider Cobralink"*. Dimana didalamnya membahas tentang analisis penerapan teknologi WDS pada koneksi *wireless hotspot* untuk mengetahui kelebihan dan kekurangan dengan cara membandingkan dengan *repeater* mode WDS dan tanpa menggunakan mode WDS menggunakan *access point*. Dari penelitian tersebut dapat disimpulkan bahwa penerapan WDS memiliki keuntungan mempermudah pada saat berpindah-pindah karena tidak

mengalami koneksi terputus. Selain itu keuntungan yang kedua adalah bisa membangun infrastruktur *wireless* tanpa harus membangun *backbone* kabel jaringan sebagai interkoneksi antar *bridge*. Sedangkan dari segi performa penggunaan WDS dengan tanpa WDS dapat disimpulkan sistem tanpa WDS performanya lebih baik dibandingkan performa dengan menggunakan WDS, hal ini dikarenakan *throughput* efektif maksimum akan terbagi dua setelah transmisi pertama (*hop*) dibuat. Pada studi kasus lokasi *client* area hotspot gedung Kost *Eksklusif Internet Service Provider* Cobralink.

Penelitian yang akan dilakukan oleh Irvan Firmansyah (2022) dengan judul *"Analisis dan Perancangan Wireless Hotspot Area dengan Sistem Roaming WDS Menggunakan Mikrotik (Studi kasus : PT Global Prima Utama)"* yang didalamnya akan membahas mengenai analisis performa jaringan WDS yang dimana ketika pengguna melakukan pindah lokasi dari satu ruangan ke ruangan lainnya tidak mengalami putus koneksi atau kehilangan sinyal *wireless* dengan menggunakan parameter pengujian yaitu *throughput*, *delay, packet loss* dan *jitter* dengan *software Jperf-2.0.2*. Dalam pengujian ini akan dilakukan pada 2 topologi yang berbeda yaitu topologi sebelum menggunakan WDS dan sesudah menggunakan WDS, dan kemudian hasil pengujian sistem tersebut akan dibandingkan. Studi kasus lokasi penelitian di PT Global Prima Utama.

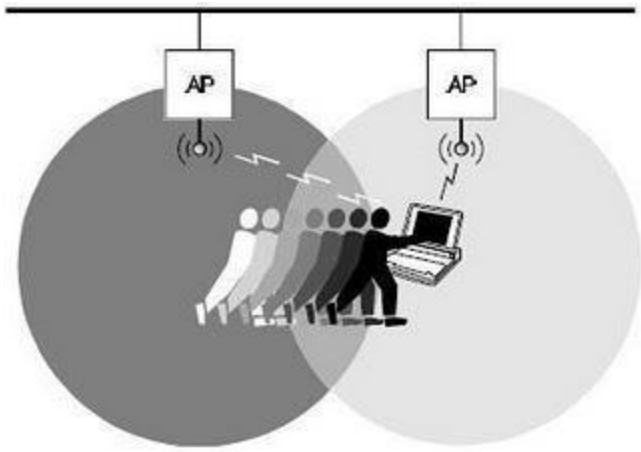
Tabel 2.1 Tinjauan Pustaka

No	Pengarang	Judul Penelitian	Objek	Metode/Teknologi
1	Bayu Muji Nugroho (2022)	Analisis dan Simulasi Perancangan *Wireless Distribution System* (WDS) Menggunakan Router Mikrotik pada SMAN 1 Kerumutan	SMAN 1 Kerumutan	WDS *Repeater*, RB951Ui-2HnD, *Simple Queue*
2	Jago Pamungkas (2018)	Implementasi Teknologi WDS (*Wireless Distribution System*) Menggunakan Router Mikrotik RB951Ui-2HnD Pada Indekost Biru 3 Lantai	Indekost Biru 3 Lantai	WDS *Repeater*, Mikrotik RB951Ui-2HnD, *Routing* OSPF
3	Kobro Anggoro (2017)	Analisis *Wireless Distribution System* (WDS) dengan 4 buah RB951Ui-2HnD	Lapangan Sepakbola Desa Kepurun	WDS *Repeater*, Metode *Quality of Service* (QOS), RB951Ui-2HnD
4	Lutfi Fadthorik (2019)	Analisis *Internal Wireless Hotspot Area* dengan *Sistem Roaming* Menggunakan Mikrotik di SMK Ma'arif Ponjong Gunungkidul	SMK Ma'arif Ponjong Gunungkidul	*Wireless Roaming*, Metode PPDIOO, *Wireless* TL-WR840N
5	Setiawan Serphian David (2014)	Implementasi dan Analisis *Wireless Distribution System* (WDS) Menggunakan Mikrotik Studi Kasus *Internet Service Provider* Cobralink	Internet Service Provider CobraLink	WDS *Mesh*, Rb 750, *Access Point*
6	Irvan Firmansyah (2022)	Analisis dan Perancangan *Wireless Hotspot Area* dengan *Sistem Roaming* WDS Menggunakan Mikrotik (Studi kasus : PT Global Prima Utama)	PT. Global Prima Utama	*Wireless Roaming*, Metode PPDIOO, Mikrotik *wireless* Rb 433

2.2 Dasar Teori

2.2.1 *Wireless Roaming*

Wireless roaming adalah keadaan dimana suatu *mobile station* dapat berpindah dari satu AP ke AP yang lain, dan masih dalam subnet yang sama tanpa harus melakukan koneksi ulang ke AP. *Mobile station* dapat menemukan AP yang memiliki sinyal terbaik, kemudian memutuskan kapan untuk berpindah ke AP yang lain. Semua proses tersebut membutuhkan waktu dalam pemilihan AP terbaik maupun konfigurasi *IP address*. *Wireless roaming* dapat membantu *mobile station* untuk mendapatkan alamat IP yang baru tanpa mempengaruhi koneksi. Pemindaian dan pengambilan keputusan adalah bagian dari proses *roaming* yang memungkinkan *mobile station* menemukan AP baru pada saluran yang cocok ketika pengguna berpindah tempat. Ketika ini terjadi, maka *client* harus mengasosiasikan dengan AP baru.



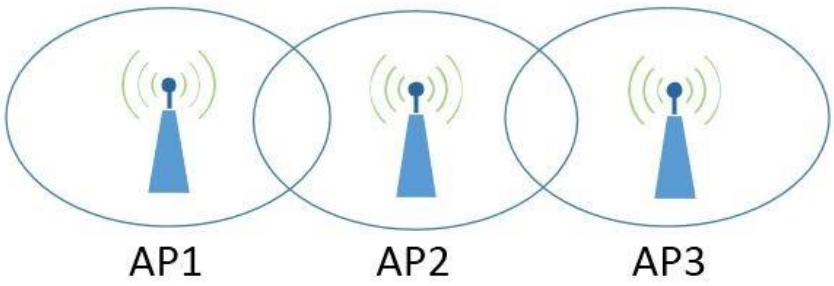
Gambar 2.1 *Wireless Roaming*

Pada Gambar 2.1 terlihat proses perpindahan dari satu AP ke AP yang lain untuk mengambil *service* dari AP tersebut. Dalam jaringan *wireless, roaming* antara dua jaringan terdiri dari *internal roaming* dan *external roaming*. *Internal roaming* terjadi jika *mobile station* berpindah ke jaringan lain melalui satu AP ke AP yang lain tetapi masih dalam satu *home network*. Sedangkan *external roaming* terjadi jika *mobile station* sudah berpindah antar *provider* jaringan yang digunakan.

2.2.2 *Wireless Distribution System (WDS)*

Wireless Distribution System adalah metode atau teknik menghubungkan (*interconnection*) antara satu AP dengan AP lain dengan menggunakan media *wireless* dalam suatu *Wireless Local Area Network (WLAN)*. Dengan WDS ini, area kerja (*coverage*) dari WLAN dapat diperluas tanpa menghubungkan AP dengan sistem *backbone* kabel.

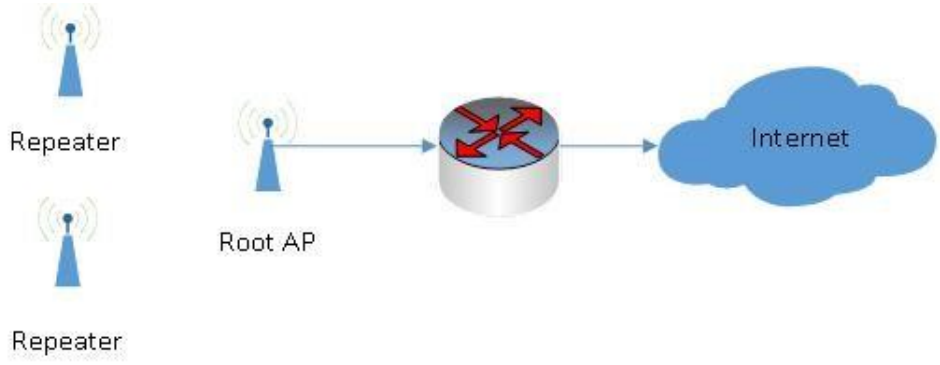
Dengan kata lain, WDS adalah metode untuk menghubungkan beberapa AP dalam suatu WLAN tanpa menghubungkan AP-AP tersebut ke dalam sistem kabel. Ilustrasi dasar dari WDS ini dapat dilihat pada Gambar 2.2 berikut ini.



Gambar 2.2 Tiga *Access Point* yang Tidak Terhubung ke *Backbone* Kabel

Dari gambar diatas, terlihat bahwa *coverage* dari jaringan WLAN dapat diperluas dengan menggunakan 3 unit AP. Ketiga AP tersebut harus dapat berkerja sama satu sama lain melalui koneksi *wireless*. Dapat diperhatikan bahwa ketiga AP tersebut tidak terhubung ke dalam sistem jaringan kabel, ketiganya tidak menggunakan media kabel untuk terhubung satu sama lain.

Untuk dapat membangun WDS setidaknya dibutuhkan 2 unit AP atau lebih untuk dapat bekerja sama satu sama lain melalui koneksi *wireless* dan melakukan distribusi *wireless*, beberapa AP tersebut dikonfigurasikan dengan parameter *ssid* dan *frequency* yang sama. Dengan demikian maka beberapa AP tersebut akan terlihat sebagai salah satu kesatuan jaringan atau lebih tepatnya lagi dikenal sebagai satu *broadcast domain*. Ini berarti antara satu AP dengan AP lainnya harus bisa berkomunikasi dengan baik. Kondisi seperti ini sama seperti ketika membangun jaringan kabel dengan menggunakan beberapa hub ataupun switch. Masing-masing AP tidak menggunakan kabel untuk dapat saling terhubung, hanya menggunakan interface *wireless* saja.



Gambar 2.3 Jaringan *Wlan* dengan 1 *Root AP* dan 2 *Repeater*

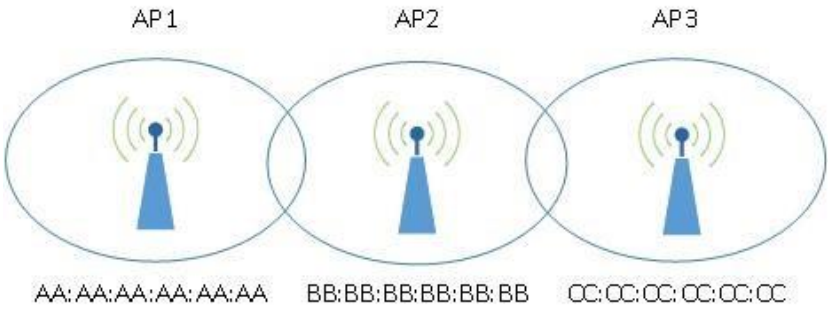
Penerapan pada jaringan yang akan digunakan untuk mengakses internet, umumnya dilakukan menggunakan minimal 1 (satu) AP yang terhubung ke sistem kabel, AP ini disebut sebagai Root AP. Dari Root AP ini akses *wireless* akan didistribusikan ke beberapa AP yang akan menjadi *repeater* AP, tentunya distribusi ini dilakukan dengan menggunakan media *wireless*.

2.2.2.1 *Static* WDS dan *Dynamic* WDS

Pada saat akan membangun jaringan *wireless* dengan teknik WDS, maka akan dihadapkan pada 2 (dua) pilihan:

1. *Static* WDS, pada teknik ini *administrator* jaringan harus memperkenalkan secara manual AP-AP yang akan masuk ke dalam jaringan WDS. Dilakukan dengan memasukkan *MAC Address* dari AP tetangga (*neighbour*).
2. *Dynamic* WDS, pada teknik ini sebuah AP akan mencari sendiri AP tetangga yang akan masuk ke dalam jaringan WDS yang dibangun. Sebuah AP akan mencari sendiri pasangannya berdasarkan kesamaan *SSID*.

Baik *Static* WDS ataupun *Dynamic* WDS memiliki kelebihan dan kekurangan masing-masing. Seperti gambar berikut yang yang terdiri dari 3 (tiga) *AP*. Dengan contoh topologi sederhana ini bisa didapatkan sedikit gambaran mengenai kelebihan dan kekurangan kedua teknik WDS tersebut.



Gambar 2.4 Jaringan dengan 3 *Access Point*

Ketiga AP yang terhubung dengan teknik WDS, untuk WDS *static* pada saat melakukan konfigurasi WDS pada AP-1, harus memasukkan *MAC Address* BB-BB-BB-BB-BB-BB secara manual.

Ini akan membuat AP-1 mengenal AP-2 sebagai pasangannya dalam urusan WDS. Sedangkan pada saat melakukan konfigurasi WDS pada AP-2 yang berada ditengah-tengah jaringan, harus memasukkan *MAC Address* AA-AA-AA-AA-AA-AA dan CC-CC-CC-CC-CC-CC.

Hal ini akan membuat AP-2 mengenal keberadaan AP-1 dan AP-3 sebagai pasangan WDS-nya. Sedangkan pada saat melakukan konfigurasi WDS pada AP-3, harus memasaukkan *MAC Address* BB-BB-BB-BB-BB-BB. Ini akan membuat AP-3 bisa mengenal keberadaan AP-2 yang menjadi pasangan WDS-nya.

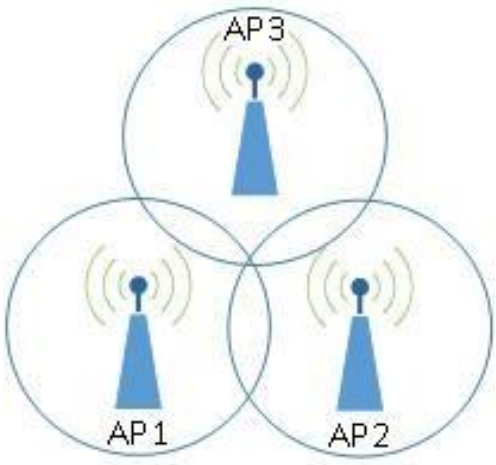
Konfigurasi *Static* WDS terlihat sedikit rumit, karena harus melakukan identifikasi *MAC Address* dari satu AP ke AP yang lain. Setelah mengetahui *MAC Address* masing-masing AP, maka harus memasukkan *MAC Address* pada masing-masing AP sesuai desain WDS. Untuk 2 (dua) AP untuk membangun koneksi WDS, harus mengisi *MAC Address* dari keduanya.

Dibalik rumitnya konfigurasi *static*, ada keuntungan yang bisa diambil. Dengan memasukkan secara manual *MAC Address* dari masing-masing, dapat menjaga dan mengawasi koneksi WDS yang terjadi antara satu AP dengan AP yang lain.

Dynamic WDS, dengan melaukan konfigurasi *dynamic* WDS pada setiap AP yang disertai dengan *SSID* yang sama, maka baik AP-1, AP-2 maupun AP-3 akan otomatis membangun koneksi WDS satu sama lain. Sehingga ketiga AP

tersebut akan langsung bisa berkomunikasi dan bekerjasama. Konfigurasi d*ynamic* WDS tidak memerlukan pendataan *MAC Address* secara detail, sehingga tidak akan membingungkan. Namun jika tidak diawasi dengan baik, maka *dynamic* WDS rentan terhadap koneksi WDS yang tidak diinginkan.

Pada Gambar 2.4, terlihat bahwa desain jaringan tersebut hanya menginginkan AP-3 terhubung ke AP-2. Namun jika yang dilakukan adalah konfigurasi *dynamic* WDS, akan ditemukan kondisi dimana AP-3 dapat membangun hubungan WDS dengan AP-1. Ini bisa terjadi jika tiba-tiba AP-3 mendapatkan signal *wireless* dari AP-1, yang mungkin saja disebabkan signal AP-1 yang terlalu kuat atau pun posisi AP-3 yang kurang tepat, seperti pada Gambar 2.5.



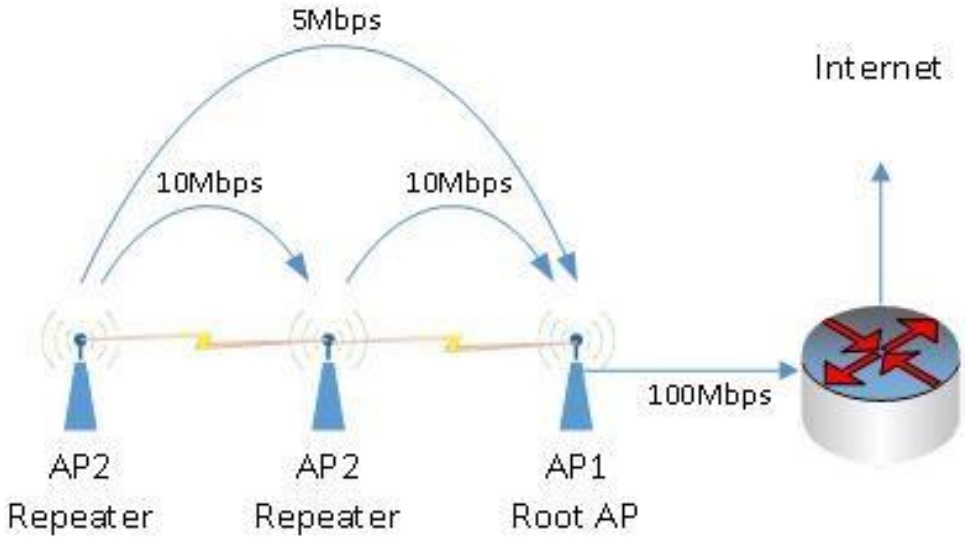
Gambar 2.5 AP-3 Membuat Koneksi dengan AP-1

Terlihat dengan *dynamic* WDS maka link WDS bisa saja tercipta tanpa diketahui oleh adminitrator jaringan. Link atau koneksi WDS seperti yang terjadi pada gambar di atas juga membawa potensi terjadinya *loop* yang pada akhirnya dapat melumpuhkan keseluruhan jaringan *wireless*. Sehingga pada saat akan menggunakan *dynamic* WDS, pengawasan terhadap link WDS harus ditingkatkan.

Peningkatan pengawasan pada jaringan *dynamic* WDS dapat dilakukan oleh setiap *access point*. Router Mikrotik yang bertugas sebagai *access point* sudah dilengkapi dengan fitur *connect list* yang bisa melakukan *filter* atau pembatasan terhadap *access point* yang dapat terhubung melalui link WDS.

2.2.2.2 *Bandwidth* pada WDS

Persoalan lain dalam membangun adalah masalah *bandwidth* yang akan didapatkan oleh *client wireless*. Dalam jaringan *wireless* yang mengandalkan WDS akan terjadi penurunan *bandwidth* yang terkadang cukup mengganggu dan harus menjadi perhatian khusus pada saat melakukan desain awal. Semakin panjang link WDS yang tercipta maka akan semakin menurun alokasi *bandwidth* yang didapatkan sebuah AP yang letaknya jauh dari Root AP. Ilustrasi berikut memperlihatkan jaringan WDS dengan 3 (tiga) AP.

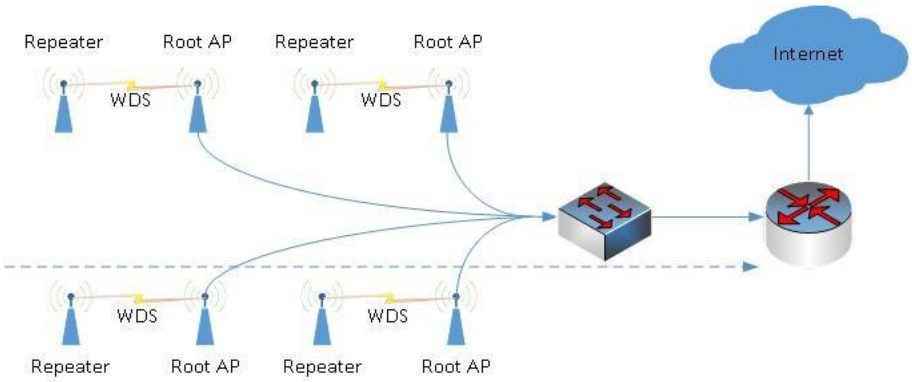


Gambar 2.6 Jaringan WDS dengan 3 AP

Dari gambar diatas, terlihat bahwa AP-1 merupakan Root AP karena terhubung pada sistem kabel. AP-1 akan bisa menggunakan alokasi *bandwidth* secara maksimal, mengingat koneksi AP-1 menggunakan media kabel yang terhubung langsung ke Router GW. AP-1 bisa mendapatkan alokasi *bandwidth* 100 MBps ke Router GW. Hubungan antara AP-1 dengan AP-2 dilakukan dengan media *wireless*, sehingga alokasi *bandwidth* yang didapatkan oleh AP-2 terhadap Router GW tidak akan sebesar alokasi *bandwidth* AP-1 terhadap Router GW. Pada gambar tersebut, AP-2 hanya mendapatkan alokasi *bandwidth* 14 MBps terhadap Router GW. AP-3 menggantungkan koneksi ke Router GW melalui AP-2. Jika AP-2 hanya mendapatkan alokasi *bandwidth* 14 Mbps, maka alokasi yang didapatkan AP-3 akan jauh dibawah nilai 14 Mbps. Pada gambar AP-3 hanya mendapatkan alokasi *bandwidth* sebesar 7 Mbps jika diukur terhadap AP-1.

Semakin jauh atau semakin panjang link WDS yang dibangun maka penurunan *bandwidth* akan terus terjadi. Sehingga bisa diambil kesimpulan bahwa dibalik kemudahan membangun jaringan *wireless* dengan WDS, terdapat kekurangan pada sisi alokasi *bandwidth*. Pada kondisi ini dituntut untuk menjaga keseimbangan antara kemudahan dan kehandalan jaringan. Kedua hal ini harus menjadi perhatian pada saat membangun jaringan *wireless* dengan WDS.

Sebagai contoh desain, jika harus membangun jaringan dengan banyak AP, namun akan tetap menggunakan teknik WDS, maka harus berkompromi untuk tetap menghadirkan beberapa Root AP seperti pada gambar berikut ini.



Gambar 2.7 Jaringan WDS dengan Banyak AP

2.2.3 PPDIOO

PPDIOO adalah singkatan dari *Prepare*, *Plan*, *Design*, *Implement*, *Operate*, dan *Optimize*. PPDIOO adalah metodologi Cisco yang mendefinisikan terus menerus siklus hidup layanan yang dibutuhkan untuk jaringan (Hermawan, 2014). Tahapan PPDIOO sebagai berikut:

2.2.3.1 Persiapan (*Prepare*)

Melibatkan menerapkan persyaratan organisasi, mengembangkan strategi jaringan dan mengusulkan arsitektur tingkat tinggi konseptual mengidentifikasi teknologi terbaik yang dapat mendukung arsitektur. Tahap mempersiapkan dapat membangun pembenaran keuangan untuk strategi jaringan dengan menilai kasus bisnis untuk arsitektur yang diusulkan.

2.2.3.2 Rencana (*Plan*)

Melibatkan identifikasi kebutuhan jaringan awal berdasarkan tujuan, fasilitas, kebutuhan pengguna, dan sebagainya. Rencana fase melibatkan karakteristik situs dan menilai jaringan yang ada dan melakukan analisis gap untuk menentukan apakah infrastruktur sistem yang ada, situs dan lingkungan operasional dapat mendukung sistem yang diusulkan. Sebuah rencana proyek berguna untuk membantu pengelola tugas, tanggung jawab, tonggak penting dan sumber daya yang diperlukan untuk menerapkan perubahan ke jaringan. Rencana proyek harus menyesuaikan dengan ruang lingkup, biaya dan parameter sumber yang diterapkan dalam persyaratan bisnis asli.

2.2.3.3 Desain (*Design*)

Persyaratan awal yang diturunkan dalam tahapan perencanaan mendorong kegiatan spesialis desain jaringan. Spesifikasi desain jaringan adalah desain rinci komprehensif yang memenuhi bisnis saat ini dan persyaratan teknis dan menggabungkan spesifikasi untuk mendukung ketersediaan, keandalan, keamanan, skalabilitas dan kinerja. Spesifikasi desain adalah dasar untuk melaksanakan kegiatan.

2.2.3.4 Pelaksanaan (*Implement*)

Jaringan yang dibangun atau komponen tambahan dimasukkan sesuai dengan spesifikasi desain, dengan tujuan mengintegrasikan perangkat tanpa mengganggu jaringan yang ada atau membuat titik kerentanan.

2.2.3.5 Mengoperasikan (*Operate*)

Operasi adalah tujuan akhir dari kesesuaian desain. Tahapan operasional melibatkan menjaga kesehatan jaringan melalui operasi sehari-hari, termasuk menjaga ketersediaan tinggi dan mengurangi biaya. Deteksi kesalahan, koreksi dan pemantauan kinerja yang terjadi dalam operasi sehari-hari memberikan data awal untuk tahapan optimasi.

2.2.3.6 Pengoptimalan (*Optimalize*)

Melibatkan manajemen proaktif jaringan. Tujuan dari manajemen proaktif adalah untuk mengidentifikasi dan menyelesaikan masalah sebelum mereka mempengaruhi organisasi. Deteksi kesalahan reaktif dan koreksi (pemecahan

masalah) yang dibutuhkan ketika manajemen proaktif tidak dapat memprediksi dan mengurangi kegagalan. Dalam proses PPDIOO, tahapan optimalisasi dapat meminta desain ulang jaringan jika terlalu banyakm masalah jaringan dan kesalahan timbul, jika kinerja tidak memnuhi harapan, atau jika aplikasi baru diidentifikasi untuk mendukung kebutuhan organisasi dan teknis.

2.2.4 Standar Jaringan Nirkabel

Karena jaringan nirkabel menggunakan frekuensi radio, di Amerika jaringan nirkabel diatur oleh hukum yang sama dengan yang digunakan untuk menangani radio AM/FM. *The Federal Communications Commission* (FCC) mengatur penggunaan perangkat jaringan nirkabel. Dipasar jaringan nirkabel sekarang ini ada beberapa standar operasional yang diterima dan diurus atau dipelihara oleh *Institut Of Electrical and Electronic Engineer* (IEEE) (Pangera, 2008).

Standar ini diciptakan oleh kelompok yang mewakili banyak organisasi yang berbeda, termasuk organisasi akademis, bisnis, militer dan pemerintahan. Karena standar yang terpasang permanen oleh IEEE dapat berdampak waktu bertahun-tahun untuk diciptakan dan mendapat persetujuan (Pangera, 2008). Berikut daftar standar yang diterapkan saat ini :

2.2.4.1 IEEE 802.11

Standar jaringan nirkabel asli yang menetapkan kecepatan transfer data yang paling lambat pada RF dan teknologi transmisi yang *light-based*. Standar ini disahkan oleh IEEE di 1997 (pangera, 2008).

2.2.4.2 IEEE 802.11b

Menguraikan kecepatan transfer data yang sedikit lebih cepat dan lingkup yang lebih terbatas tentang teknologi transmisi. Standar ini juga dipromosikan secara luas dengan nama *Wi-Fi*™ oleh *Wi-Fi Allience*. Standar ini telah disahkan oleh IEEE di 1999 sebagai pengembangan dari standar IEEE 802.11 yang asli (Pangera, 2008).

2.2.4.3 IEEE 802.11 a

Menguraikan kecepatan transfer data yang sedikit lebih cepat dibandingkan IEEE 802.11b, menggunakan frekuensi 5GHz UNII. Standar ini telah disahkan oleh IEEE di 1999 sebagai pengembangan dari standar 802.11 yang asli.

2.2.4.4 IEEE 802.11g

Melanjutkan hasil kerja unit 802.11b, unit kerja yang lain yaitu 802.11g membuat spesifikasi baru yang kompatible dengan 802.11b. Spesifikasi yang diselesaikan tahun 2003 ini mampu mengalirkan data dengan kecepatan yang sama dengan 802.11a yaitu 54Mbps. Kedua spesifikasi ini yang paling banyak ditemukan di pasaran saat ini.

2.2.4.5 IEEE 802.11n

IEEE 802.11n didasarkan pada standar 802,11 sebelumnya dengan menambahkan *multiple-inputmultiple-output* (MIMO) dan 40MHz ke lapisan saluran fisik (PHY), dan *frame agregasi* ke *MAC layer*. MIMO adalah teknologi yang menggunakan beberapa antena untuk menyelesaikan informasi lebih lanjut

secara koheren dari pada menggunakan satu antena. Dua manfaat penting MIMO adalah menyediakan keragaman antenna dan spasial *multiplexing* untuk 802.11n.

2.2.5 *IP Address* dan *Subnetting*

IP Address merupakan deretan bilangan biner di antara 32 bit hingga 128 bit yang dipakai sebagai media untuk mengidentifikasi untuk setiap perangkat komputer yang terhubung pada jaringan. Bilangan biner 32 bit dipakai untuk setiap *IP Address* versi 4 atau Ipv4, sedangkan bilangan biner 128 bit digunakan untuk setiap *IP Address* versi 6 atau Ipv6.

IP Address dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Perbedaan tiap kelas adalah pada ukuran dan jumlahnya.

Tabel 2.2 *Class IP Address*

Kelas	Range IP Address	Jumlah Host	Jumlah Network
A	0.0.0.0–127.255.255.255	16,777,216	128
B	128.0.0.0-191.255.255.255	1,048,576	16.384
C	192.0.0.0–223.255.255.255	65,536	2.097.152
D	224.0.0.0–239.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan
E	240.0.0.0–255.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan

Subnetting adalah proses memecah jaringan atau *network* menjadi beberapa *sub network* atau dalam pengertian lain menjadikan *host* sebagai *subnet*.

Subnet mask ada dua bentuk notasi *subnet*, notasi standar dan CIDR (*Classless Internet Domain Routing*). Dalam standar *subnet mask* notasi empat oktet nilai numerik digunakan sebagai dengan alamat dasar, misalnya

255.255.255.0. CIDR (*Classless Internet Domain Routing*) adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, B, C, D, E.

Tabel 2.3 Nilai CIDR

Subnet Mask	Nilai CIDR
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19

Subnet Mask	Nilai CIDR
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

2.2.6 *Router*

Router merupakan sebuah sistem yang digunakan untuk menghubungkan dan mengatur lalu lintas data antara dua atau lebih jaringan yang memiliki *subnet* berbeda. *Router* terdapat dilapisan *layer* 3 dalam sistem *OSI Layer* sehingga mempunyai kemampuan *routing* atau pengalamatan paket data baik data secara *static* maupun *dynamic*. *Router* bekerja dengan melihat alamat tujuan dan alamat asal dari paket data yang melewatinya serta memutuskan rute mana yang harus digunakan oleh paket data tersebut untuk dapat sampai tujuan.

2.2.7 *Access Point*

Access Point (titik akses), disingkat AP merupakan piranti LAN nirkabel urutan kedua terpenting setelah kartu PC nirkabel yang sering dijumpai sebagai seorang administrator LAN nirkabel. Sebagaimana diisyaratkan oleh namanya , AP memberikan titik akses terhadap suatu jaringan kepada *client*. AP ini berupa piranti *half-duplex* yang dilengkapi dengan intelegensi yang setara dengan intelegensi yang setara dengan intelegensi pada *ethernet switch* yang canggih (Pangera, 2008).

2.2.8 *Repeater*

Semakin besar sebuah jaringan computer akan memerlukan jarak jangkauan yang lelbih besar dibandingkan jarak standar yang biasa didukung oleh kabel. Maka dibutuhkan sebuah *repeater*.

Repeater berfungsi untuk memperpanjang atau memperkuat jangkauan maksimum kabel jaringan. *Repeater* akan mengambil sinyal yang diterimanya dari komputer lalu me-regenerasi sinyal tersebut sehingga integritassinya tetap terjaga walaupun jarak yang ditempuh cukup jauh.

Repeater memiliki kemampuan untuk mengarahkan *traffic* di jaringan atau menentukan rute yang ditempuh oleh data. *Repeater* hanya berfungsi untuk memperpanjang atau memperkuat sinyal saja dalam jaringan komputer.

2.2.9 *Mikrotik*

Mikrotik adalah sebuah merek dari perangkat jaringan, pada awalnya m*ikrotik* hanyalah sebuah perangkat lunak atau *software* yang diinstall dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam

perkembangannya saat ini menjadi sebuah *device* atau perangkat jaringan yang handal dan harga yang terjangkau, serta banyak digunakan pada level perusahaan jasa internet (ISP) (Athailah, 2013).

2.2.9.1 Sejarah *Mikrotik*

Mikrotik adalah sebuah perusahaan yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang Amerika yang berimigrasi ke Latvia. Di Latvia ia berjumpa dengan Arnis seorang sarjana fisika dan mekanik sekitar tahun 1995. Tahun 1996 John Trully dan Arnis mulai me-*routing* dunia (Visi Mikrotik adalah me-*routing* seluruh dunia). Mulai dengan *system* linux dan MS DOS yang dikombinasikan dengan teknologi *wireless* LAN (VLAN-LAN) Aeronet berkecepatan 2 Mbps di Molcava, tenaga Latvia, baru kemudian melayani lima pelanggannya di Latvia (Nugroho, 2013).

2.2.9.2 Fitur *Mikrotik* yang Digunakan

2.2.9.2.1 *Firewall*

Firewall berfungsi menjaga keamanan jaringan dari ancaman pihak lain yang tidak berwenang. merubah, merusak, atau menyebarkan data-data penting perusahaan merupakan contoh ancaman yang harus dicegah (Athailah, 2013).

Firewall beroperasi menggunakan aturan tertentu, aturan inilah yang menentukan kondisi ekspresi yang memberitahu router tentang apa yang harus dilakukan router terhadap paket *IP address* yang melewatinya. Setiap aturan disusun atas kondisi dan aksi yang akan dilakukan. Ketika paket IP lewat, *firewall*

akan mencocokkannya dengan kondisi yang telah dibuat kemudian menentukan aksi apa yang akan dilakukan router sesuai dengan kondisi tersebut (Athailah, 2013).

2.2.9.2.2 *Network Address Translation* (NAT)

Network Address Translation (NAT) adalah suatu fungsi *firewall* yang sebenarnya bertugas melakukan perubahan *IP Address* pengirim dari paket data. NAT ini umumnya dijalankan pada router-router yang menjadi batas antara jaringan lokal dan jaringan internet. Secara teknis NAT ini akan mengubah paket data yang berasal dari komputer user seolah-olah berasal dari router (Athailah, 2013).

2.2.9.2.3 DHCP

Dynamic Host Configuration Protocol (DHCP) adalah protocol jaringan yang memungkinkan sebuah perangkat jaringan membagi konfigurasi *IP address* kepada komputer-komputer user yang membutuhkan. Konfigurasi *IP address* ini meliputi *IP Address* itu sendiri, *subnet mask*, *default gateway*,dan DNS Server Sedangkan komputer yang menerima konfigurasi dari server ini dinamakan DHCP *Client* (Athailah, 2013).

2.2.9.2.4 *Hotspot*

Dengan fitur ini, kitadapat mengkonfigurasi jaringan *wireless* yang hanya bisa digunakan dengan *username* dan *password* tertentu. Kita juga dapat melakukan manajemen terhadap user-user tertentu. Misalnya mengkonfigurasi durasi total user

dalam menggunakan *hotspot* kita selama berapa jam. Kita juga dapat membatasi besar data yang di *download* dan *upload* oleh user tertentu (Towidjojo, 2012).

2.2.9.2.5 *Wireless Distribution System* (WDS)

Pradip K. Das (2005) telah dibuat akses jaringan WDS (*Wireless distribution system*) seperti yang telah didefinisikan IEEE 802.11. Penggunaan WDS memungkinkan untuk menghubungkan *access point* satu dengan *access point* yang lain. Tujuan dari penerapan WDS adalah untuk memperluas area jangkauan suatu jaringan sehingga bisa mencakup tempat yang tidak bisa dijangkau jaringan kabel. *Distribution System* menghubungkan suatu sel untuk membangun jaringan yang luas yang memungkinkan pengguna bisa berpindah dari *access point* satu ke *access point* lain namun tetap terhubung pada sumber daya jaringan yang tersedia.

2.2.10 *Quality of Service (QoS)*

QoS merupakan standarisasi kualitas service jaringan yang ke user (Ferguson & Huston, 1998). Parameter QoS antara lain adalah *throughput*, *delay*, *packet loss*, *jitter*, dan *bandwidth*.

2.2.10.1 *Throughput*

Throughput adalah *bandwidth* aktual yang terukur pada satuan ukuran waktu tertentu dalam mentransmisikan berkas. Berbeda dengan *bandwidth* walaupun satuannya sama *bit per second*(bps), tetapi *throughput* lebih menggambarkan *bandwidth* yang sebenarnya pada suatu waktu dan pada kondisi jaringan tertentu yang digunakan untuk mengunduh file dengan ukuran tertentu (Darmawan dkk, 2012).

2.2.10.2 *Delay*

Delay merupakan waktu yang dibutuhkan sebuah paket dikirimkan dari suatu komputer ke komputer yang lain yang dituju. *Delay* dalam sebuah proses transmisi paket Dalam sebuah proses transmisi paket dalam sebuah jaringan komputer disebabkan karena adanya antrian yang panjang, atau mengambil *route* lain untuk menghindari kemacetan pada *routing*. Untuk mencari *delay* pada suatu jaringan komputer menggunakan perintah *ping* yang merupakan salah satu perintah yang dimiliki oleh *command prompt system operasi Windows*, dimana *time* pada hasil perintah *ping* menunjukkan *delay* pada *packet* yang dikirimkan (Darmawan dkk, 2012).

Tabel 2.4 Kategori *Delay*

Kategori	Packet Loss
Sangat Bagus	<150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	>450 ms

(Sumber : TIPHON)

2.2.10.3 *Packet Loss*

Packet loss adalah persentase paket yang hilang selama mentransmisikan data. Hal ini disebabkan oleh tabel 2.5 seperti penurunan *signal* dalam media jaringan, kesalahan perangkat keras jaringan, atau juga radiasi dari lingkungan sekitarnya (Darmawan dkk, 2012).

Pada beberapa *network transfer protocol* seperti TCP (*Transmissions Control Protocol*) yang bersifat *connection oriented*, menyediakan pengiriman

kembali (*retransmission*) atau pengiriman secara otomatis (*resends*) packet yang hilang selama proses transmisi walau segmen telah tidak diakui. Walaupun TCP memiliki kelebihan tersebut, jika TCP melakukan *retransmitting* atau *resends*, *throughput* jaringan semakin menurun. Berbeda halnya dengan protocol UDP (*User Datagram Protocol*) yang bersifat *connection-less*, tidak menyediakan *retransmission* maupun *resends* jika terjadi kehilangan paket (Darmawan dkk, 2012).

Koneksi jaringan yang bagus adalah jaringan yang memiliki *packets loss* minimum bahkan akan lebih baik jika tidak ada *packet loss*. Secara umum terdapat empat kategori penurunan performa jaringan versi TIPHON (*Telecomunication and Internet Protocol Hamonization Over Network*) yaitu sebagai berikut :

Tabel 2.5 Kategori *Packet Loss*

Kategori	Packet Loss
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Jelek	25%

(Sumber : TIPHON)

2.2.10.4 *Jitter*

Jitter adalah variasi dari *delay* atau selisih antara *delay* pertama dengan *delay* selanjutnya. Jika variasi *delay* dalam transmisi terlalu lebar, maka akan mempengaruhi kualitas data yang ditransmisikan. Jumlah toleransi *jitter* dalam jaringan dipengaruhi oleh kedalaman dari *buffer jitter* dalam peralatan jaringan.

Jika *buffer jitter* tersedia lebih banyak, maka jaringan dapat mereduksi efek dari *jitter* (Darmawan dkk, 2012).

Jitter merupakan variasi *delay* antar paket yang terjadi juga pada jaringan berbasis IP. Variasi beban trafik dan besarrnya tubrukan antar paket (*congestion*) yang ada dalam jaringan akan sangat mempengaruhi besar nilai *jitter*. Beban trafik yang makin besar dan kemungkinan *congestion* semakin besar akan menyebabkan nilai QoS (*Quality of Services*) semakin turun (Wibowo, 2014).

Kategori *jitter* versi TIPHON (*Telecomunication and Internet Protocol Hamonization Over Network*) mengelompokkan menjadi empat kategori penurunan kinerja jaringan berdasarkan nilai *jitter* seperti tabel berikut :

Tabel 2.6 Kategori *Jitter*

Kategori	Peak Jitter
Sangat Bagus	0 ms
Bagus	0 s/d 75 ms
Sedang	76 s/d 125 ms
Jelek	125 s/d 225 ms

(Sumber : TIPHON)

2.2.11 *Software Jperf-2.0.2*

Software Jperf adalah perangkat lunak yang dapat digunakan untuk mengukur performansi jaringan berbasis GUI. Parameter jaringan yang dapat diukur antara lain yaitu *throughput*, *delay*. Perangkat lunak lain yang mempunyai fungsi yang sama yaitu *iperf*, namun *iperf* tidak mudah untuk digunakan untuk pemula disebabkan penggunaan yang menggunakan *command line*. Perangkat

lunak ini digunakan untuk *inject traffic* sehingga bisa digunakan untuk layanan MPLS, VPN IP dan lainnya.

Kualitas dari suatu jaringan dapat diukur dengan ketentuan sebagai berikut:

1. *Throughput* dapat diukur dengan tes *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).
2. *Delay* (waktu tunda) dapat diukur dengan tes UDP.

Dalam pengoperasiannya, *jperf* menggunakan metode *client-server*. *Jperf* merupakan *software* berbasis java yang powerful untuk mengukur *reliability* dari sebuah koneksi jaringan. *Jperf* merupakan pengembangan dari *iperf*. *Jperf* bekerja dengan mengirim paket datagram sebesar 1270 byte dan hasilnya dapat dilihat dalam bentuk grafik dan teks, dimana *jperf* menggunakan port 5001 yang merupakan port default dari *software jperf* dan juga merupakan port kosong atau port yang tidak digunakan oleh media yang lain.