BAB II

TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Teknologi nirkabel telah lama digunakan sejak tahun 1997, dimana pada tahun tersebut protokol pertama jaringan nirkabel yakni 802.11 dipublikasikan. Semenjak dipublikasikan, orang-orang mulai melirik teknologi ini dengan berbagai alasan. Alasan yang paling dominan adalah mobilitas. Pengguna teknologi jaringan nirkabel memiliki mobilitas lebih tinggi dibandingkan dengan pengguna kabel karena pada teknologi ini pengguna bisa berpindah tempat dengan leluasa tanpa terputus koneksinya. Selain mobilitas juga ada alasan tentang kemudahan, pada teknologi jaringan nirkabel hanya membutuhkan perangkat penerima sinyal dan pengguna bisa langsung terhubung, berbeda dengan kabel yang membutuhkan media kabel terlebih dahulu untuk melakukan hubungan.

Studi mengenai *Unfied Wireless Network* tidak lepas dari jaringan nirkabel itu sendiri, dimana jaringan nirkabel adalah komponen yang membangun *Unified Wireless Network*. Menurut Nur Mardhiyah (2011) pada penelitiannya yang berjudul "Membangun Jaringan Wireless LAN pada Kantor Kelurahan Bintaro" menyebutkan bahwa pengertian Wireless *Local Area Network* (disingkat Wireless LAN atau WLAN) adalah jaringan komputer yang menggunakan frekuensi radio dan infrared sebagai media transmisi data. Menurut Jim Geier (2004) dalam bukunya "Wireless Networks first-step" mengatakan Wireless LAN sering disebut sebagai jaringan nirkabel atau jaringan wireless. Perancangan dan

implementasi dari jaringan nirkabel juga sudah pernah dilakukan dalam beberapa penelitian sebelumnya seperti berikut:

1. David Pangputra (2001) dalam skripsinya pengembangan sistem teknologi jaringan area lokal tanpa kabel (Wireless LAN) dengan standar IEEE 802.11. Penelitian ini membahas apa itu teknologi jaringan area lokal tanpa kabel dan hal-hal apa saja yang perlu dipersiapkan untuk membuat jaringan area lokal tanpa kabel. Hasil dari penelitian ini adalah karakteristik dari jaringan area lokal tanpa kabel sesuai dengan lapisan fisik yang akan dipakai sehingga estimasi biaya dari pembuatan dan hal-hal lain dapat diketahui sebelum jaringan area lokal tanpa kabel diimplementasikan.
2. Tri Arianto (2009) dalam jurnalnya mengimplementaiskan Wireless *Local Area Network* dalam sebuah jaringan RT/RW net dengan menggunakan Antena Omni 2.4GHz 10dB sebagai medianya. Hasil dari penelitian ini adalah jaringan nirkabel yang diimplementasikan mampu menjangkau ruang-ruang yang sulit dijangkau oleh jaringan kabel.
3. Dina Angela (2010) dalam jurnalnya menganalisis kinerja jaringan Wi-Fi dengan mengambil kasus di gedung sebuah institusi pendidikan. Penelitian dilakukan dengan mengukur penerimaan sinyal yang dilakukan langsung di beberapa titik dalam gedung kampus dan dihitung secara teoritis menggunakan One Slope Model.
4. Nur Mardhiyah (2011) dalam skripsinya membangun jaringan wireless lan pada kantor kelurahan bintaro dengan menggunakan AP wireless

TP-Link TD8817 sebagai mode repeater. Penelitian ini membahas bagaimana membangun jaringan nirkabel di kelurahan bintaro, dimana pada kelurahan bintaro masih banyak tempat yang belum dijangkau oleh access point. Metode yang digunakan dalam penelitian ini adalah NDLC (Network Development *Life Cycle*) dengan mengubah mode access point ke repeater. Hasil dari penelitian ini menyimpulkan bahwa sistem jaringan nirkabel dengan mode repeater yang diimplementasikan telah berhasil dijalankan dengan baik.

5. Agus Hidayatullah (2011) dalam skripsinya perancangan Wireless *Local Area Network* (WLAN) pada Sekolah Tinggi Agama Islam Syekh Manshur (STAISMAN) Pandeglang. Penelitian ini membahas mengenai penerapan dari WLAN untuk menjangkau area-area yang tidak bisa dijangkau oleh jaringan kabel. Metode yang digunakan dalam penelitian ini adalah observasi dimana peneliti langsung mendatangi lokasi / area penelitian. Hasil dari penelitian ini adalah dengan pemanfaatan WLAN dapat digunakan sebagai perluasan dari jaringan kabel yang sudah ada.

Sistem *Unified Wireless Network* bukan sebuah sistem yang baru lahir, melainkan sistem yang sudah ada dan sudah digunakan oleh industri-indsustri di Indonesia dan Mancanegara. Beberapa industri yang sudah beralih ke sistem UWN (*Unified Wireless Network*) adalah:

1. Universitas Hospital Inssbruck

   Universitas Hospital Unssbruck meruapakan universitas dengan konsentrasi dibidang kesehatan di Austria. Sistem UWN digunakan untuk meningkatkan skalabilitas dari jaringan nirkabel, mobilitas dan efisiensi dari staff serta meningkatkan kenyamanan dari pengguna.

2. Sierra Gorda

   Sierra Gorda merupakan industri yang bergerak di sektor tambang bertempat di chili. Sierra Gorda mengalami kesulitan dalam melakukan laporan dari aktifitas dalam pertambangan seperti hasil tambang, laporan harian, dan koordinasi lapangan dikarenakan posisi/lokasi dari Sierra Gorda berada di Gurun. Sistem UWN digunakan untuk mengatasi masalah tersebut dengan cara membuat akses point-to-point jaringan nirkabel. Hasil dari penerapan sistem UWN pada Sierra Gorda, produktifitas dari industri bertambah sekitar 720 jam per orang per bulan, operasional juga tumbuh pesat dan kepuasan konsumen meningkat.

3. PT. Ramayana Lestari Indonesia Tbk

   PT. Ramayana Lestari Indonesia Tbk atau lebih dikenal dengan nama Ramayana, merupakan salah satu dari 20 besar perusahaan kecil di dunia versi Forbes pada oktober 2001. Ramayana menggunakan sistem UWN untuk mengatasi masalah tentang waktu yang diperlukan bagi sebuah sistem POS (Point-of-Sale) untuk melakukan koneksi ke pusat. Dengan menggunakan sistem UWN, Ramayana telah berhasil mengatasi

masalah tersebut dan pendapatan dari Ramayana pun meningkat seiring dengan waktu yang diperlukan untuk terkoneksi lebih cepat.

WLAN memang sudah banyak diterapkan diberbagai tempat, baik itu di institusi pendidikan, pemerintahan, ruang publik hingga komersil. Kemudahan dalam mengimplementasi WLAN menjadi daya tarik tersendiri mengapa pengguna ataupun penyedia lebih condong ke WLAN daripada jaringan kabel. Kekurangan dari penelitian-penelitian sebelumnya berada pada access point yang digunakan masih berupa *stand alone access point* sehingga akan mengurangi keefektifitasan dalam segi pengelolaan jaringan apabila AP yang disebar berjumlah banyak. Untuk mengatasi hal teserbut maka digunakanlah *light weight access point* (LWAP), dengan menggunakan LWAP, LWAP yang disebar diseluruh penjuru akan dengan mudah dikonfigurasi dan dikontrol menggunakan sebuah kontroler.

Didalam penelitian ini digunakan Cisco Virtual Wireless Controller (vWLC) untuk mengatasi masalah-masalah atau kekurangan-kekurangan yang ada dalam desain jariangan eksisting. Dengan menggunakan vWLC pengaturan dari jaringan nirkabel akan lebih efektif dan efisien. Sehingga jaringan akan memiliki skalabilitas tinggi dan mudah untuk diatur.

2.2 Landasan Teori

2.2.1 Standar 802.11

802.11 adalah standar protokol dari IEEE (*Institute of Electrical and Electronics Engineers*) khusus untuk WLAN. Protokol 802.11 mengalami perkembangan-perkembangan seiring berjalannya waktu. Ilmuwan-ilmuwan yang

menciptakan tidak henti-hentinya untuk mengembangkan standar ini untuk mendapatkan hasil yang lebih baik dari sebelumnya.

Dalam perkembangannya, protokol 802.11 mengalami beberapa evolusi. Evolusi dari standar protokol 802.11 dapat dilihat pada Tabel 2.1

Tabel 2.1 Evolusi standar protokol 802.11

Standar	Tahun	Teknologi	Frekuensi	Bandwidth	Data-rate tertinggi
802.11 (Legacy)	1997	DSSS	2.4GHz	20MHz	2Mbps
802.11b	1999	CCK	2.4GHz	20MHz	11Mbps
802.11a	1999	OFDM	5GHz	20MHz	54Mbps
802.11g	2003	OFDM	2,4GHz	20MHz	54Mbps
802.11n	2009	OFDM, MIMO	2,4GHz, 5GHz	20MHz, 40MHz	1x1: 150Mbps 2x2: 300Mbps 3x3: 450Mbps
802.11ac	2012-13	OFDM, MIMO, MU-MIMO	Hanya 5GHz	20MHz, 40MHz, 80MHz & 160MHz	2x2 (80MHz) : 866Mbps 4x4(80MHz): 1733Mbps

Kedepannya protokol 802.11 ini akan terus mengalami perkembangan seiring dengan semakin kompleksnya kebutuhan pengguna dan perkembangan ilmu sains dan teknologi.

2.2.2 *Access Point*

Access Point (AP) adalah perangkat yang digunakan untuk menghubungkan pengguna wirelesss dengan koneksi internal maupun external (internet). Cisco membuat AP sendiri untuk keperluan integrasi dengan perangkat-perangkat lain yang diciptakannya. Dalam operasionalnya AP Cisco memiliki dua mode yang berbeda yaitu:

a. *Stand Alone* AP (*Autonomous* AP)

Stand Alone AP memungkinkan network administrator untuk mengatur dan mengelola AP secara mandiri. Mode ini sama saja dengan mode pada AP di vendor lain pada umumnya.

b. *Light Weight* AP (LAP)

Light Weight AP memungkinkan network administrator untuk mengatur dan mengelola AP secara terpusat. Karena diatur dan dikelola secara terpusat maka dibutuhkan sebuah kontroller sebagai kendali dalam mengoperasionalkan Light Weight AP.

2.2.3 Cisco Virtual Wireless Controller

Cisco Virtual Wireless Controller (vWLC) merupakan produk dari Cisco Systems yang digunakan untuk mengatur dan mengelola AP baik dalam skala kecil maupun besar. vWLC merupakan bagian dari *Unified Wireless Network* yang menyediakan real-time dan komunikasi terpusat antara AP dengan vWLC. vWLC didesain untuk memenuhi kebutuhan jaringan nirkabel dari skala kecil sampai enterprise dengan menawarkan fitur-fitur berikut:

1. Managemen wireless terpusat dan kemampuan mengontrol sampai dengan 200 cabang lokasi.
2. Kemampuan untuk IT Manager dalam mengatur , mengelola dan melakukan troubleshooting sampai dengan 200 AP dan 6000 pengguna melalui FlexConnect.
3. Kemanan Guest Access, kemampuan untuk mendeteksi rogue AP dan in-branch (locally switched) Wi-Fi Voice dan Video.

4. Konektifitas reliable dengan solusi Cisco FlexConnect untuk jaringan cabang.
5. Proteksi dari kemungkinan putusnya jaringan dengan remote controller melalui WAN, dengan ini pengguna jaringan lokal masih bisa mengakses sumber lokal.
6. Integrasi dengan Network Servis Tervirtualisasi seperti *Cisco Prime Infrastructure*, *Cisco Mobility Servive Engine* dan *Cisco Identity Service Engine*.
7. *Pay as you go*, lisensi dibayar berdasarkan kebutuhan.

Deskripsi dari spesifikasi vWLC dapat dilihat pada Table 2.2.

Tabel 2.2 Spesifikasi vWLC

Target Deployment	Small or Midsized Business Branch
Form Factor	Virtual Machine Software
Deployment Mode	
FlexConnect	Yes
Central Mode	-
Mesh	No
FlexConnect+Mesh	Yes
Scale	
Minimum Access Point	5
Maximum Access Point	200
Maximum Client Support	6000
Maximum Number AP Groups	200
Maximum Number Flex Groups	100
Maximum Access Point per Group	100
Max WLANs	512
Max VLANs	512
Interfaces or Network I/O	2vNICS
Feature Support	
Workgroup Bridge	Yes
Link Aggregation Group (LAG)	-
Radio Resource Management (RRM)	Yes
Datagram Transfer Layer Security (DTLS)	Yes

Software Version	8.1.102.0

2.2.4 CAPWAP

CAPWAP atau *Control and Provisioning of Wireless Access Point* adalah standar protokol yang digunakan *Wireless LAN Controller* (WLC) untuk mengatur *Access Point* (AP) atau *Wireless Termination Point* (WTP). CAPWAP berdasarkan dari *Lightweight Access Point Protokol* (LWAPP). CAPWAP diciptakan berdasarkan dari beberapa RFC (*Request For Comment*). Berikut ini RFC dari CAPWAP:

1. RFC 4564 : Mendefinisikan tujuan dari protokol CAPWAP.
2. RFC 5418 : Membahas mengenai analisis ancaman pada IEEE 802.11
3. RFC 5415 : Mendefinisikan spesifikasi dari protokol CAPWAP.

Pada mulanya vWLC menggunakan LWAPP sebagai protokol untuk berkomunikasi antara AP dengan vWLC, mulai dari Software versi 5.2 vWLC menggunakan standar dari IETF (*Internet Engineering Task Force*) CAPWAP. Alasan kenapa vWLC menggunakan CAPWAP adalah:

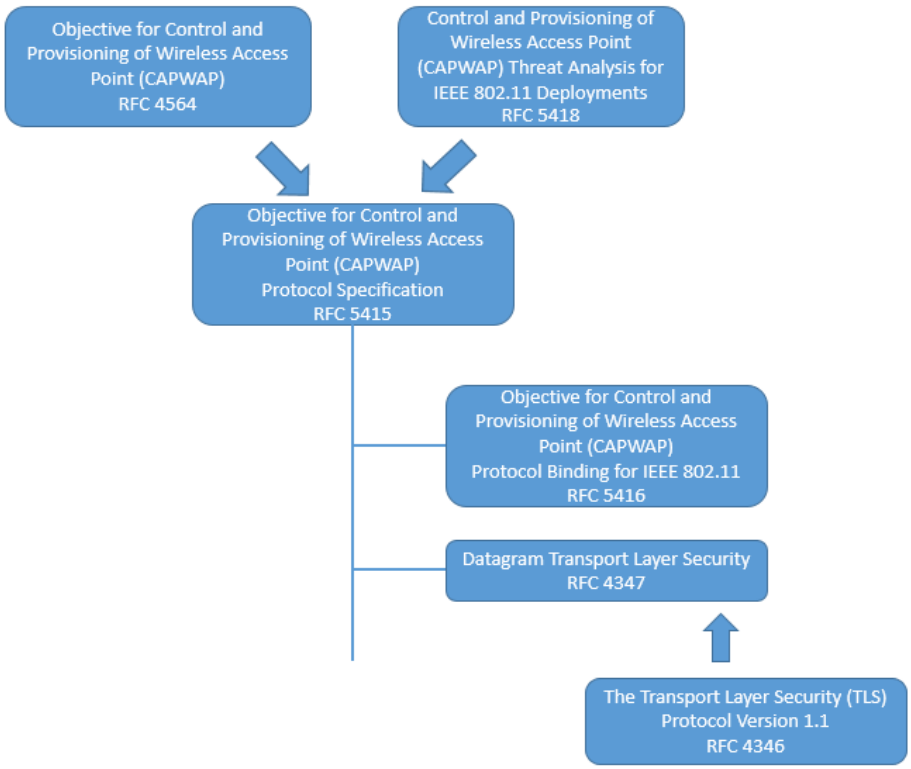
1. Untuk menyediakan upgrade bagi produk cisco yang awalnya menggunakan LWAPP ke generasi baru produk cisco yang menggunakan CAPWAP.
2. Untuk mengatur dan mengontrol RFID Reader dan peralatan yang mirip lainnya.
3. Untuk memungkinkan kontroller berkomunikasi dengan AP pihak ketiga di mendatang.

Protokol CAPWAP ini memungkinkan AP untuk mengetahui alamat IP Address dari Kontroller sebelum memutuskan untuk bergabung dengan controller tersebut.

CAPWAP bekerja pada Layer 3 sehingga deployment pada layer 2 tidak mungkin bisa menggunakan CAPWAP.

Protokol CAPWAP tidak termasuk kedalam teknologi wireless tertentu akan tetapi malah bergantung kepada spesifikasi untuk memperluas teknologi pada teknologi wireless tertentu. Kebergantungan pada spesifikasi pada protokol 802.11 didefinsikan pada RFC 5416.

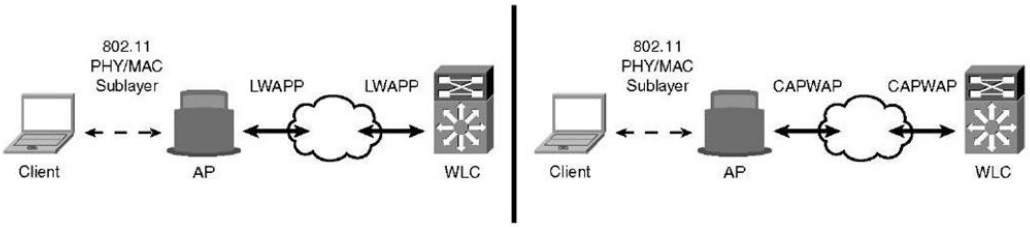
Untuk menjamin keamanan dari protokol CAPWAP digunakanlah DTLS (Datagram Transport Layer Security) yang didefinisikan pada RFC 4347. Sedangkan untuk DTLS sendiri merujuk kepada RFC 4346. Hubungan dari RFC dengan jaringan nirkabel dapat dilihat pada Gambar 2.2.



Gambar 2.2 RFC pada jaringan nirkabel

Sumber: http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/overview-of-capwap-cisco-wireless-lan-controllers/

Pembahasan mengenai CAPWAP tidak bisa terlepas dari LWAPP (*Light Weight Access Point Protocol*) karena LWAPP adalah generasi pertama dari CAPWAP. LWAPP bekerja pada Layer 2 dan Layer 3. Deployment dari CAPWAP dan LWAPP dapat dilihat pada Gambar 2.3.



Gambar 2.3 Layer *Deployment* CAPWAP dan LWAPP
Sumber: http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/overview-of-capwap-cisco-wireless-lan-controllers/

Namun apabila dilihat dari segi keamanan, CAPWAP lebih aman dikarenakan CAPWAP dilengkapi dengan DTLS sedangkan LWAPP tidak. Perbandingan antara CAPWAP dan LWAPP dapat dilihat pada Tabel 2.3.

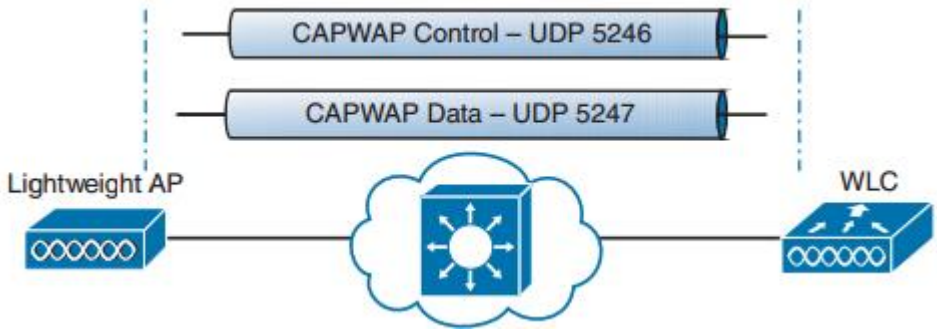
Tabel 2.3 Perbandingan CAPWAP dengan LWAPP

Feature	CAPWAP	LWAPP
L2 Mode Support	No	Yes
Security	AES-CCMP with DTLS Protokol	AES-CCMP
Control plane encryption	Yes	Yes
Data plane encryption	Optional, depending on hardware; 5500s only	No
Fragmentation and reassembly	CAPWAP Fragmentation	IP Fragmentation
MTU discovery	Yes	No
Protokol control ports	5246	12222

Protokol data ports	5247	12223

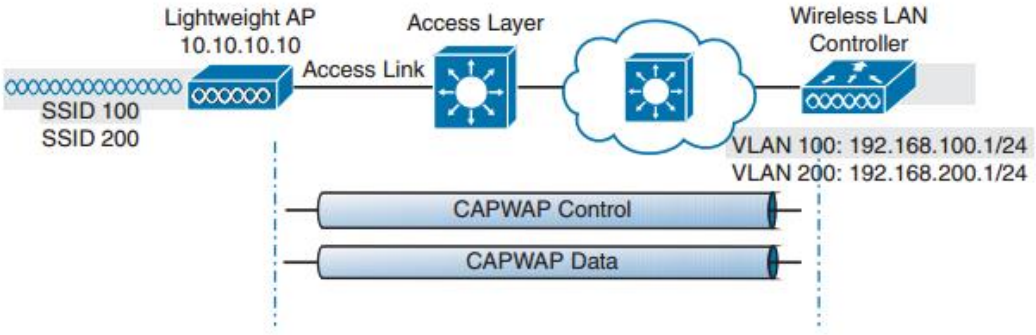
Dengan menggunakan CAPWAP, LAP yang di *deploy* tidak harus berada dalam satu subnet dengan kontroler. Dengan menggunakan CAPWAP Tunneling protokol, AP yang berbeda subnet dengan kontroler dapat berkomunikasi dan mengirimkan data melalui paket IP. Tunneling yang ada didalam CAPWAP adalah sebagai berikut:

- CAPWAP control messages – digunakan oleh vWLC sebaga jalan untuk mengatur LAP dan operasinya. Control messages diautentikasi dan dienkripsi sehinga LAP dengan aman hanya dikontrol oleh vWLC yang di transportasikan menggunaka UDP port 5246.
- CAPWAP data – digunakan untuk arus pertukaran data dari pengguna ke vWLC dan sebaliknya. Paket data ditransporatiskan menggunakan port UDP 5247, namun secara default paket data ini tidak terenkripsi. Ketika data diatur untuk dienkripsi, paket data akan dilindungi menggunakan DTLS. Gambar 2.4 merupakan CAPWAP Tunnel dari LWAP dan WLC.



Gambar 2.4 CAPWAP Tunnel

Simulasi dari paket data yang di tunneling menggunakan CAPWAP dapat dilihat pada Gambar 2.5.



Gambar 2.5 *Traffic* Paket Data CAPWAP

Sumber: Hucaby, David. 2014. CCNA Wireless 640-722 Official Cert Guide. USA: Cisco Press

2.2.5 DHCP Opsi 43

RFC 2132 mendefinisikan dua opsi dhcp yang berelevansi dengan opsi spesifik vendor. Adalah opsi 60 dan opsi 43. DHCP opsi 60 adalah *Vendor Class Identifier* (VCI). VCI adalah sebauh teks *string* unik yang digunakan untuk mengidentifikasi tipe dari alat vendor. Opsi 60 dimasukkan kedalam proses awal DHCP discover yang dibroadcast oleh pengguna untuk mendapatkan sebuah IP address. Opsi 60 digunakan oleh pengguna (client) atau dalam hal ini adalah AP untuk mengidentifikasi dirinya sendiri. Sedangkan DHCP opsi 43 digunakan oleh AP untuk mencari alamat dari vWLC sebelum meregistrasikan dirinya. Supaya AP bisa menemukan alamat dari vWLC maka perlu ditambahkan alamat dari management interface pada vWLC kedalam paket DHCP berdasarkan VCI dari AP. Untuk melakukan hal tersebut, DHCP server harus bisa mengenali VCI dari jenis masing-masing AP dan mendefinisikan informasi spesifik vendor (*Vendor Specific Information* / VSI) darinya.

Pada DHCP server, VSI dimappingkan ke VCI teks string. Ketika DHCP server menemukan VCI yang dikenali pada saat proses DHCP discover dari pengguna, DHCP server mengembalikkan VSI yang dimappingkan pada proses DHCP offer ke pengguna sebagai DHCP Opsi 43. Pada DHCP server, opsi 43 didefinisikan dalam masing-masing pool dari DHCP.

RFC 2132 mendefinisikan DHCP server harus mengembalikan VSI sebagai DHCP opsi 43. RFC 2132 membolehkan vendor untuk mendefinisikan vendor-specific sub-option codes yang ternekapsulasi antara 0-255. Sub-option dimasukkan kedalam paket DHCP offer sebagai blok type-length-value (TLV) didalam opsi 43. Definisi dari sub-option code dan pesan yang berkaitan diserahkan ke masing-masing vendor.

Ketika DHCP server diatur untuk memberikan IP Address dari kontroller sebagai opsi 43 pada Cisco 1000 Series AP, blok sub-option TLV didefinisikan sebagai berikut :

- *Type* – 0x66 (desimal dari 102).
- *Length* – Hitungan dari karakter string ASCII dalam value-field. Length harus termasuk koma jika lebih dari satu kontroler didefinisikan.
- *Value* – string akhir ASCII non-zero yang dipisahkan koma untuk daftar kontroler.

Ketika DHCP server diatur untuk memberikan IP Address dari kontroller sebagai opsi 43 pada AP cisco selain series 1000, blok sub-option TLV didefinisikan sebagai berikut:

- *Type* – 0xf1 (desimal dari 241).

- *Length* – Nomor dari IP Address kontroler * 4.
- *Value* – daftar dari managament interface dari kontroler yang di translasikan ke hexadesimal.

Pengaturan dari opsi 43 berbeda untuk masing-masing vendor penyedia dhcp server seperti Microsoft DHCP server, Linux ISC DHCP server, Lucent QIP DHCP server dan lain-lain.

2.2.6 Freeradius

Sebelum membahas mengenai freeradius, perlu diketahui terlebih dahulu tentang apa itu radius. Radius adalah singkatan dari *Remote Authentication Dial In User Service*, adalah protokol jaringan yang mendefinisikan aturan dan konvensi untuk komunikasi antara perangkat jaringan, untuk autentikasi dan penghitungan pengguna. Radius pada umumnya digunakan oleh ISP (Internet Service Provider), Penyedia jaringan seluler, korporat dan jaringan edukasi. Radius mempunyai tiga fungsi utama yaitu:

- Autentikasi – Mengautentikasi pengguna atau perangkat sebelum memperbolehkannya untuk mengakses / masuk kedalam jaringan.
- Otorisasi – Mengotorisasi pengguna atau perangkat kedalam sebuah servis jaringan.
- Akunting – Menghitung dan mencatat penggunaan dari servis yang dipakai.

Latar belakang diciptakan radius adalah ketika Merit Network sebuah non-profit penyedia jasa internet pada tahun 1991 membutuhkan cara yang efektif untuk mengatur dial-in access ke beberapa *Points-Of-Presence* (POPs) dijaringannya. Pada saat radius diciptakan, Sistem akses jaringan didistribusikan sepanjang area

luas dan dijalankan oleh beberapa organisasi independen. Administrasi pusat menginginkan adanya upaya preventif tentang masalah keamanan dan skalabilitas serta tidak ingin mendistribusikan *username* dan *password*. Mereka ingin server akses yang jauh menghubungi akses server di pusat untuk melakukan otorisasi tentang servis yang akan digunakannya. Akses server pusat nantinya tinggal memberikan jawan sukses atau gagal, selebihnya server akses yang jauh yang memutuskan ke pelanggannya.

Tujuan dari radius adalah membuat suatu lokasi terpusat untuk autentikasi pengguna, dimana pengguna bisa berada dimana saja dapat meminta akses ke jaringan. Untuk alasan simplisitas, efesiensi dan usabilitas, radius diadopsi oleh vendor-vendor penyedia jaringan sampai akhirnya menjadi standar industri dan dijadikan standar pada IETF (Internet Engineering Task Force).

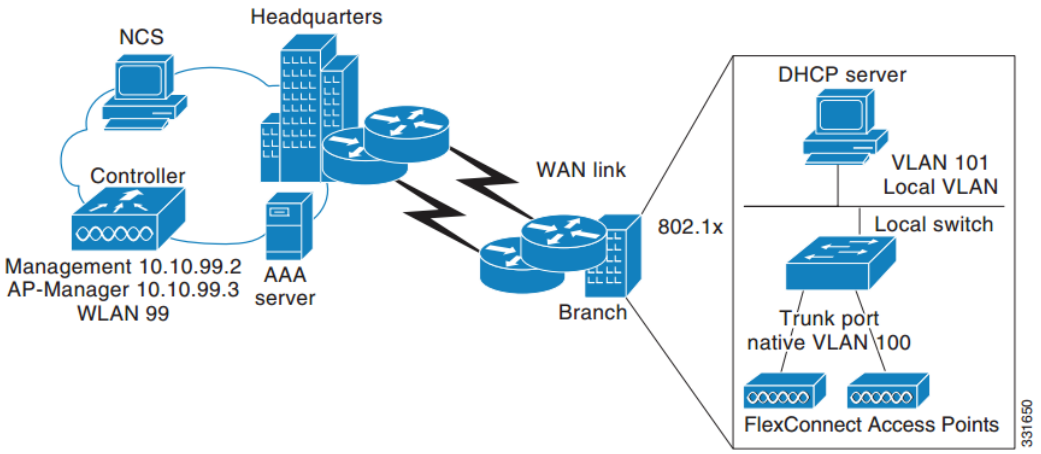
Freeradius adalah open source radius server paling terkenal dan paling banyak dipakai didunia. Freeradius banyak dipakai oleh Tier 1 ISP untuk proses AAA (Authentication, Authorization, and Accounting). Selain dari ISP, freeradius juga banyak dipakai pada institusi akademis dan perusahaan komersil. Freeradius dimulai pada Agustus tahun 1999 oleh Alan DeKok dan Miquel van Smoorenburg. Miquel sebelumnya sudah membuat *software* Cistron Radius Server yang banyak diadopsi ketika Livingston server tidak lagi bekerja. Freeradius dikembangkan dengan menggunakan desain modular untuk mendorong komunitas lain bergabung dalam pengembangnnya.

Software radius server tidak hanya freeradius, namun dibandingkan dengan software lain, freeradius memiliki beberapa kelebihan seperti berikut:

- Fitur yang kaya, banyak jenis-jenis autentikasi yang didukung oleh freeradius. Sebagai contoh freeradius adalah satu-satunya radius server yang mendukung Extensible Authentication Protokol (EAP).
- Modularitas, desain modular yang dipakai freeradius membuatnya mudah untuk dipahami. Modular interface juga memudahkan untuk menambahkan modul atau menghilangkannya. Sebagai contoh ketika modul tertentu tidak dipakai, maka bisa dihilangkan tanpa mempengaruhi performa dari server. Sehingga *resource* dari server semakin *ramping*.
- Skalabilitas, satu server freeradius mampu untuk mentransisikan dirinya dari menghadapi beberapa permintaan dalam beberapa detik sampai ke ribuan permintaan dalam sedetik. Dengan cara merubah konfigurasi standar ke konfigurasi sesuai dengan kebutuhan.

2.2.7 FlexConnect

FlexcConnect (sebelumnya dikenal dengan nama *Hybrid Remote Edge Access Point* atau H-REAP) adalah solusi jaringan nirkabel untuk kantor cabang dan kantor jarak jauh. Flexconnect memungkinkan untuk mengatur dan mengkonfigurasi AP yang berada di cabang dari pusat tanpa perlu memasang kontroler di cabang. Flexconnect AP dapat merubah data pengguna untuk di *switch* secara lokal dan melakukan autentikasi lokal juga apabila koneksi dengan kontroler yang berada di pusat terputus. Gambar 2.6 merupakan *deployment* dari mode FlexConnect.



Gambar 2.6 FlexConnect *Deployment*

Ketika terdapat pengguna yang terhubung dengan FlexConnect AP, AP akan mengirimkan semua pesan autentikasi ke kontroler dan atau men-switch kan paket data pengguna secara lokal (*locally switched*) atau mengirimkannya ke kontroler (*centrally switched*) tergantung dari konfigurasi WLAN. Dengan berbagai macam keamanan dalam WLAN, WLAN dapat berada dalam kondisi dibawah ini tergantung dari konfigurasi dan konektifitas dengan kontroler:

- Autentikasi terpusat (*Central Authentication*), *Central Switching* – dalam kondisi ini kontroler menangani autentikasi dari pengguna dan semua data pengguna di tunnel kan kembali ke kontroler.
- Autentikasi terpusat (*Central Authentication*), *Local Switching* – dalam kondisi ini kontroler menangani autentikasi dari pengguna dan FlexConnect AP men-switchkan secara lokal. Apabila proses autentikasi berhasil, kontroler akan memberi perintah FlexConnect AP untuk memulai proses switch data secara lokal.

- Autentikasi lokal, *Local Switching* – dalam kondisi ini FlexConnect AP menangani proses autentikasi pengguna sekaligus men-switch kan data pengguna secara lokal.

  Autentikasi lokal dianggap cocok dalam kondisi tidak bisa menjaga koneksi dengan kantor cabang dengan minimal bandwidth 128 kbps dan *round-trip-latency* tidak lebih dari 100ms serta *maximum transmission unit* (MTU) tidak kurang dari 500 bytes. Dengan menggunakan autentikasi lokal, maka akan mengurangi kebutuhan latensi di kantor cabang.
- Autentikasi *down*, *switch down* – dalam kondisi ini WLAN memutuskan koneksi yang ada dan berhenti memberikan *beacon* dan *probe request*.
- Autentikasi *down*, *local switching* – dalam kondisi ini WLAN menolak semua permintaan autentikasi namun masih memberikan *beacon* dan *probe request.*

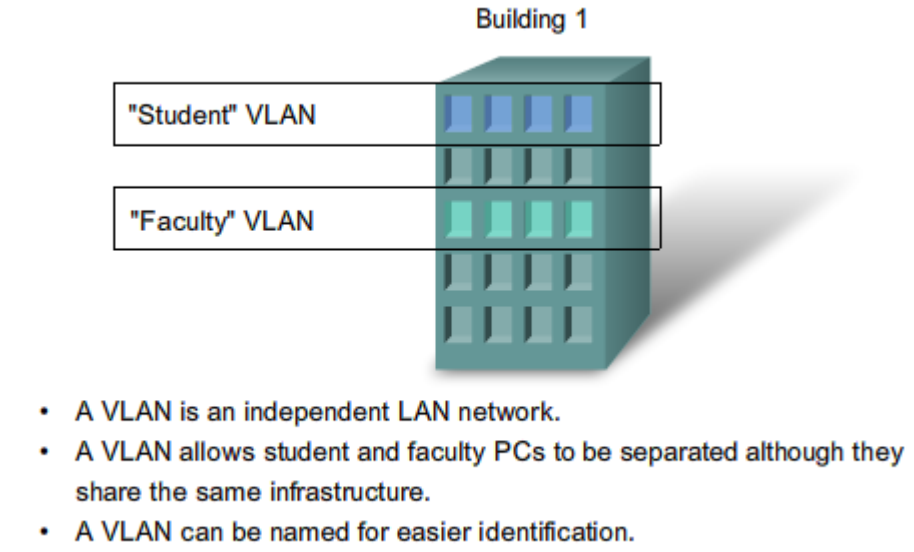
FlexConnect AP dapat berubah menjadi standalone ketika AP mengalami putus koneksi dengan kontroler. Untuk FlexConnect AP yang menggunakan switch-terpusat ketika FlexConnect AP terputus dengan kontroler, maka semua pengguna yang ada akan terputus juga, sedangkan untuk FlexConnect AP yang menggunakan switch-lokal ketika FlexConnect AP terputus dengan kontroler maka pengguna yang ada masih bisa mengakses ke jaringan namun untuk pengguna baru yang akan meminta akses ke jaringan akan ditolak sampai FlexConnect AP terhubung kembali dengan kontroler dan melakukan proses autentikasi terpusat. Ketika FlexConnect AP berubah kedalam mode standalone, hal yang terjadi adalah AP akan mengecek apakah bisa menghubungi default gateway melalui ARP. Jika

tidak maka AP akan terus berusaha untuk menghubungi kontroler. Jika AP gagal dalam menghubungi gateway melalui ARP berikut ini yang akan terjadi :

- AP akan mencoba untuk mencari selama lima kali dan apabila masih belum bisa mendapatkan kontroler, AP akan melakukan pergantian IP (renew DHCP) ke interface ethernet nya.
- Hal diatas akan terjadi selama tiga kali.
- Jika sudah tiga kali namun AP masih belum bisa menemukan kontroler, AP akan kembali ke IP statis dan melakukan reboot.
- *Reboot* dilakukan untuk menghilangkan kemungkinan-kemungkinan dari error yang tidak dikenali pada konfigurasi AP.

2.2.8 VLAN

VLAN adalah sub jaringan logika yang terpisah. VLAN memungkinkan beberapa jaringan IP yang berbeda berada dalam satu switch. Pada umumnya satu switch mampu mengatasi satu jaringan, namun apabila dalam keadaan nyata kebutuhan dari jaringan mungkin lebih dari satu. Sehingga normalnya harus menambahkan switch baru. Hal ini menjadi tidak efisien terutama dalam hal biaya, oleh karena itu digunakan VLAN. Penjelasan mengenai VLAN dapat dilihat pada Gambar 2.7.



Gambar 2.7 Virtual *Local Area Network*

Sumber: http://netacad.com

VLAN menghilangkan batasan bahwa satu switch hanya bisa untuk satu jaringan. Pada teknisnya VLAN juga bisa diberi nama sehingga pengaturan VLAN jadi lebih mudah. Berikut ini adalah keuntungan dari menggunakan VLAN :

- Keamanan – Group yang memiliki data sensitif dapat dipisahkan dengan jaringan lain, sehingga mengurangi celah kebocoran data.
- Pengurangan biaya – Biaya lebih minimalis karena membutuhkan sedikit infrastruktur dan hemat bandwidth.
- Performa lebih tinggi – Membagi Layer 2 jaringan akan membagi juga broadcast layer 2 sehingga performa jaringan menjadi lebih baik.
- Mitigasi broadcast storm – Membagi jaringan ke beberapa VLAN mengurangi jumlah perangkat yang mungkin menyebabkan broadcast storm.

- Efisiensi pengelolaan – Dengan membagi jaringan menggunakan VLAN, admin jaringan menjadi lebih mudah dalam melakukan pemeliharaan jaringan.

VLAN akses dibagi menjadi dua kategori, yaitu normal VLAN dan extended VLAN, perbedaan dari VLAN extended dan VLAN standar (normal) dapat dilihat pada Tabel 2.5.

Tabel 2.5 Perbandingan normal VLAN dan extended VLAN

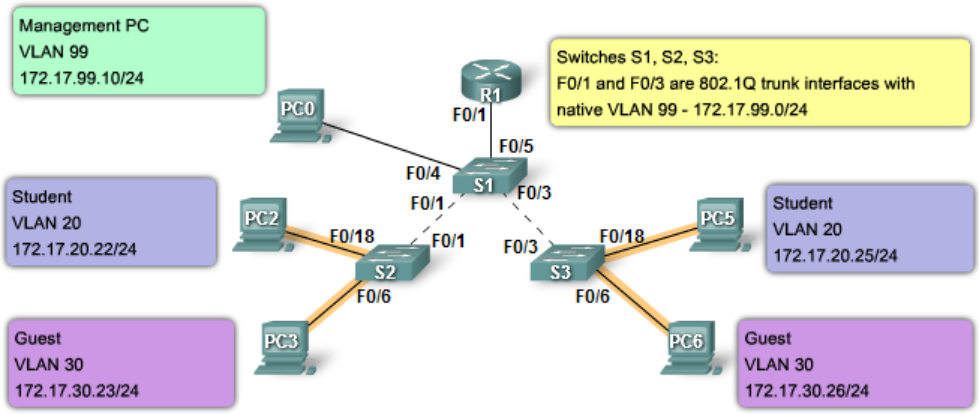
Normal VLAN	Extended VLAN
Digunakan dalam unit bisnis kecil sampai unit enterprise	Memiliki skalabilitas lebih tinggi
Diidentifikasikan dari nomor ID 1 sampai 1005	Diidentifikasikan dari nomor ID 1006 sampai 4094
ID 1002 sampai 1005 dipesan untuk VLAN Token Ring dan FDDI	Mendukung hanya beberapa fitur VLAN dibandingkan dengan normal VLAN
ID 1 dan 1002 sampai 1005 dibuat secara otomatis dan tidak bisa dihapus	Disimpan dalam running configuration file
Konfigurasi disimpan dalam berkas VLAN database dengan nama vlan.dat	VTP tidak mengenali range dari extended VLAN
VTP mengenali VLAN normal	

Dalam dunia jaringan penggunaan VLAN bisa jadi digolongkan berdasarkan fungsi spesifiknya. Seperti:

- Data VLAN – data VLAN adalah VLAN yang konfgurasi hanya untuk membawa trafik yang dihasilkan oleh pengguna.
- Default VLAN – semua port switch pada mulanya menggunakan default VLAN termasuk untuk mengatur switch itu sendiri. Untuk alasan keamanan sangat dianjurkan untuk mengganti management vlan.
- Management VLAN – VLAN yang dikhususkan untuk mengatur dan mengontrol switch.

- *Native* VLAN – *Native* VLAN biasanya didefinisikan pada protokol 802.1Q trunk. Dengan menggunakan native VLAN, VLAN yang diset sebagai native tidak akan ditandai oleh protokol 802.1Q trunk.
- *Voice* VLAN – VLAN yang dibuat khusus untuk jalur VoIP (Voice over IP). Dengan VLAN ini diharapkan kualitas data tidak terganggu walaupun sedang digunakan untuk sambungan suara.

Contoh pengimplementasian VLAN pada jaringan dapat dilihat pada Gambar 2.8.



Gambar 2.8 Implementasi VLAN di jaringan

Sumber: http://netacad.com