

IMPLEMENTASI ARSITEKTUR FIREWALL SEBAGAI SISTEM KEAMANAN JARINGAN WIFI 802.11AX ARUBA SOFTWARE-DEFINED WAN (SD-WAN)

Muhajir Syamsu¹, Widodo² (*)

¹ITB Ahmad Dahlan, Jakarta

²ITB Ahmad Dahlan, Jakarta

Abstract

The concept of WLAN technology continues to evolve so as to be able to keep up with the increasing number of user densities, schemes with density Access Point (AP) and User Stations (STA), IEEE 802.11 creates an IEEE 802.11ax (TGax) to develop a set of physical layer specifications (PHY) and Media Access New Control (MAC). IEEE 802.11ax is called a high efficiency WLAN (HE). currently in the concept of its application in the implementation of the firewall architecture on the 802.11ax WIFI network security system. This study aims to determine the concept of an 802.11ax Wifi network security system architecture developed by Aruba with the latest Access Point system that is able to support the latest Wi-Fi standards and is a wireless Access Point product that may be the first to get Wi-Fi Alliance (WFA) certification in Indonesia. the field of the latest WPA3 and Enhanced Open security system standards, and can provide much stronger encryption services and have simpler IoT security configuration settings. This research uses the literature method where the researcher collects data - information data related to the subject of the research conducted by the researcher. As well as using the data analysis technique used is using content analysis in the form of written documentation and organizing data into categories, describing it into units, what is meant by data analysis techniques. The results of this study

Kata Kunci: Firewall, Wifi 802.11ax, WLAN, IEEE 802.11ax, IoT

Juli - Desember 2022, Vol 3 (2) : hlm 141-157
©2022 Institut Teknologi dan Bisnis Ahmad Dahlan.
All rights reserved.

(*) Korespondensi: muhajirsyamsu77@gmail.com (Muhajir Syamsu), widodoprata8392@gmail.com (Widodo)

PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini berkembang dengan pesatnya, yang disebabkan munculnya jaringan internet, sehingga bisa diakses dengan hampir semua perangkat jaringan komputer namun tentu harus terkoneksi dengan jaringan internet sebagai media dalam mengakses informasi, pertukaran data dan proses komunikasi yang bisa dilakukan dimanapun, kapanpun dan tidak mengenal waktu prosesnya. Sejalan dengan perkembangan teknologi jaringan komputer tersebut, tentu akan memberikan dampak pada keterhubungi pada semua sistem yang dijalankan, mulai dari LAN, MAN, WAN yang semua jalur akses memanfaatkan jaringan internet tentu akan membuka sebuah celah lubang keamanan (*security hole*) dan akan mendapatkan sebuah masalah yang besar, jika hal tersebut tidak ditangani secara serius maka pengguna yang seharusnya dalam hal ini seorang *hacker* dan *intruder* (penyusup) yang tidak mendapatkan hak akses pada sistem yang kita rancangan akan mudahnya melakukan pengrusakkan, pencurian data artinya dengan mudahnya melakukan sebuah kejahatan dalam istilah dunia *cyber* yang dikenal dengan *Cyber Crime*, seperti *sniffing*, *spoofing*, *DoS attack*, dan sejenisnya yang dapat dikategorikan sebagai kejahatan dalam dunia maya. Menurut (Gregory, 2015) menggemukan *cyber crime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengeksploitasi komputer lain yang terhubung dengan internet. Begitupun juga yang dikatakan (Widodo, 2011) pengertian *cyber crime* adalah semua kegiatan individu atau kelompok yang memakai jaringan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan.

Menurut (Golose, 2006) modus kejahatan *cyber crime* dibagi kedalam beberapa bentuk berdasarkan bentuk sesuai modus operasinya seperti berikut: (1). *Unauthorized Access to Computer System and Service*, merupakan kejahatan yang dilakukan dengan memasuki atau menyusupke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. (2). *Illegal Contents/Illegal Contents* adalah kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dandapat dianggap melanggar hukum atau mengganggu ketertiban umum. (3). *Data Forgery Data Forgery* adalah kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. (4). *Cyber Espionage* adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network sistem) pihak sasaran. (5). *Cyber Sabotage and Extortion* merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. (6). *Offense against Intellectual Property* merupakan kejahatan yang ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, (7). *Infringements of Privacy* merupakan kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. (8). *Cracking*

merupakan kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses.. (9). Carding merupakan kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

Keberadaan *Wireless Communications* (nirkabel) yang telah menghubungkan koneksi miliaran pengguna atau *user* ke jaringan Internet yang kini dapat mengambil banyak manfaat dari sisi digital ataupun dari sisi ekonomi, bahkan keberadaan nirkabel telah menjadi sebuah ketergantungan diberbagai sektor kehidupan, mulai dari pengguna jejaring sosial, pelaku perekonomian, pelaku perbankan, jasa transportasi hingga berbagai layanan – layanan dalam kebutuhan sehari – hari seperti, pembayaran ataupun belanja. Kelebihan yang kita dapatkan dari komunikasi nirkabel adalah segi mobilitas, fleksibilitas, dan dari segi kemudahan penggunaannya. Kini jaringan nirkabel telah menjadi sebuah teknologi yang bisa dipasangkan ke perangkat – perangkat seperti: *Cellular Phone (smartphone)*, *Radio Transceiver*, *Remote Sensing*, *Remote Control*, *Radio Receiver*, *TV*, *GPS (Global Positioning System)*, *Wireless Modem*, *Microwave*, atau *Satellite* yang bisa memungkinkan sebuah akses ke sumber informasi melalui Internet, dimana konsep sistem komunikasi jaringan nirkabel ini menggunakan Gelombang Elektromagnetik, seperti: *Radio Frequency (RF)*, *WiFi*, *Bluetooth*, *RFID*, *Inframerah (IR)*, *Microwave*, atau jenis gelombang lainnya sebagai pengganti kabel untuk mengirimkan sinyal, data dan informasi. Kini jaringan nirkabel terus berkembang sejalan dengan jaringan komunikasi nirkabel, seperti *5G*, *Artificial Intelligence (AI)* atau kecerdasan buatan), dan *Internet of Things (IoT)*.

WIFI adalah adalah salah satu standar wireless networking tanpa kabel, dan hanya beberapa perangkat yang sesuai yang dapat terhubung dan terkoneksi dengan jaringan. *Institute of Electrical and Electronic Enginneers (IEEE)* adalah sebuah institusi yang menetapkan standar dari teknologi wifi (Priyambodo, 2005). Berikut adalah beberapa standar jaringan wireless berdasarkan standar yang dikeluarkan oleh IEEE: (1). 802.11a. Peraturan ini dikeluarkan pada bulan Oktober 1999. Standar wireless network dengan maksimum data transfer rate 54 Mbps dan bekerja pada frekuensi 5 GHz. Metodetransmisi yang digunakan adalah *Orthogonal Frequency Division Multiplexing (OFDM)*, yang mengizinkan penggunaan transmisi data secara parallel didalam sub-frekuensi (resisten terhadap interferensi dengan gelombang lain). Range maksimal untuk indoorhanya sekitar 15 meter/ \pm 50 ft. Sedangkan outdoor \pm 100 ft/30 meter. Standar 802.11a tidak kompatibel dengan 802.11b,g. (2). 802.11b. Peraturan yang keluar ke publik pada tahun 2000 adalah standar *wireless network* dengan kemampuan maksimum data transfer rate 5.5 Mbps dan 11 Mbps bekerja pada frekuensi 2,4 GHz. Dikenal juga dengan IEEE 802.11 HR. Pada implementasi di lapangan,kecepatan maksimum yang dapat dicapai sekitar 5.9 Mbps pada protokol TCP, dan 7.1Mbps pada protokol UDP. Metode transmisi yang digunakannya adalah DSSS. Memiliki range area yang lebih panjang ~150 feet atau 45

meter (indoor) dan ~300 feet/90 meter(outdoor). (3). 802.11g, Peraturan yang dikeluarkan ke publik pada bulan Juni 2003 dapat mencapai kecepatan hingga 54 Mbps pada pita frekuensi 2,4 GHz, sama seperti halnya IEEE 802.11 biasa dan IEEE 802.11b. Dengan standar wireless network yang hampir sama dengan 802.11b tetapi metode transmisi yang digunakan adalah OFDM (sama dengan 802.11a). Range area ~150 feet/45 meter untuk indoor dan ~300 feet/90 meter untuk outdoor. (4). 802.11n, peraturan yang dikeluarkan pada tanggal 11 September 2009. Secara teoritis, dapat mencapai kecepatan 600 Mbps. Tetapi, setelah pengujian yang dilakukan oleh pihak *Wi-Fi Alliance*, kecepatan maksimum yang diperoleh sebesar 450 Mbps. Bekerja pada frekuensi 2,4 GHz dan 5 GHz. Sama seperti teknologi MIMO (*multiple-input multiple-output*), 802.11n bekerja dengan cara mengutilisasi banyak komponen pemancar dan penerima sinyal sehingga transmisi data dapat dilakukan paralel untuk meningkatkan nilai *throughput* (50-144 Mbps). Range maksimal untuk indoor 70 meter sedangkan outdoor bisa mencapai 250 meter. Wi-Fi 802.11n ini akan diaplikasikan di device router dan adapter. Kini telah banyak jasa perusahaan yang bergerak dibidang IT menawarkan jasa untuk melakukan kontrak dalam keamanan jaringan yang digunakan pada sebuah perangkat jaringan berbasis nirkabel. Sebagai salah satu perusahaan Hewlett Packard Enterprise yaitu Aruba memperkenalkan seri baru dari produk Access Point nirkabel 802.11ax (Wi-Fi 6) IoT (AP) dan Access Switch pelengkapannya, bersama dengan inovasi di bidang keamanan, manajemen daya cerdas, dan otomatisasi, dimana produk ini didukung oleh AI (kecerdasan buatan) yaitu sebuah layanan jaminan menghadirkan kinerja, keandalan dan kesederhanaan yang sangat dibutuhkan oleh badan instansi atau organisasi sebagai layanan digital yang sangat baik kepada *user* atau penggunanya. Tujuan dari penelitian ini adalah mengetahui konsep sebuah arsitektur sistem keamanan jaringan Wifi 802.11ax yang dikembangkan oleh Aruba dengan sistem *Access Point* terbaru yang mampu mendukung standar Wi-Fi terkini dan merupakan produk *Access Point* nirkabel yang mungkin pertama mendapatkan sertifikasi *Wi-Fi Alliance (WFA)* di bidang standar sistem keamanan *WPA3* dan *Enhanced Open* terbaru, dan dapat menyediakan layanan enkripsi jauh lebih kuat dan mempunyai *setting* konfigurasi keamanan IoT yang lebih sederhana.

METODE

Metode yang digunakan dalam penelitian ini yaitu menggunakan metode *literature* dimana peneliti melakukan pengumpulan data – data informasi yang berhubungan dengan pokok pembahasan yang dilakukan peneliti. Menurut (Danial, Warsiah. 2009:80), Studi *literature* adalah merupakan penelitian yang dilakukan oleh peneliti dengan mengumpulkan sejumlah buku buku, majalah yang berkaitan dengan masalah dan tujuan penelitian. Pendekatan penelitian secara kualitatif dimana dengan pendekatan penelitian pada analisa konsep obyek yang alamiah adalah obyek yang berkembang apa adanya, tidak dimanipulasi oleh peneliti dan kehadiran peneliti tidak begitu mempengaruhi dinamika pada obyek tersebut (Sugiyono, 2010: 15). Objek penelitian dalam hal ini yaitu, pada implementasi arsitektur *firewall* yang diterapkan oleh Aruba *software-defined WAN (SD-WAN)*, dengan sumber data yang akan diolah secara natural. Peneliti berperan aktif dalam memuat rencana penelitian,

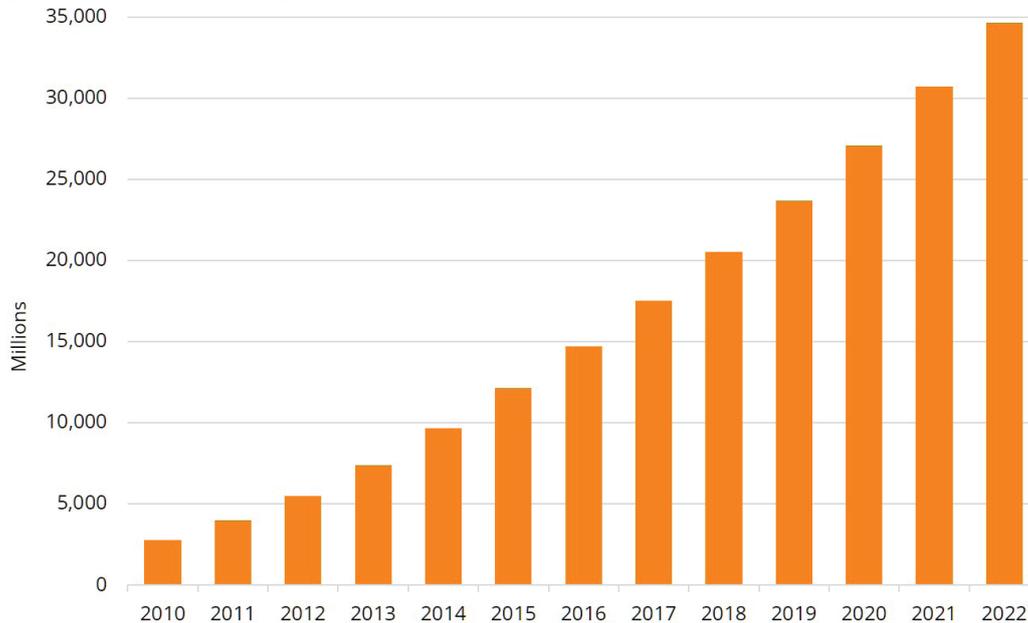
proses, dan pelaksanaan penelitian, serta menjadi faktor penentu dari keseluruhan proses dan hasil penelitian. Teknik pengumpulan data, penjelasan – penjelasan dari nara sumber serta literatur – literatur dengan data yang alamiah serta mendeskripsikan semua implementasi arsitektur *firewall* yang diterapkan oleh Aruba *software-defined WAN (SD-WAN)*. Teknik pengumpulan data dengan Studi kepustakaan adalah teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan, merupakan langkah yang penting dimana setelah seorang peneliti menetapkan topik penelitian, langkah selanjutnya adalah melakukan kajian yang berkaitan dengan teori yang berkaitan dengan topik penelitian. Dalam pencarian teori, peneliti akan mengumpulkan informasi sebanyak-banyaknya dari kepustakaan yang berhubungan. Sumber-sumber kepustakaan dapat diperoleh dari: buku, jurnal, majalah, hasil-hasil penelitian (tesis dan disertasi), dan sumber-sumber lainnya yang sesuai (internet, koran dll) menurut Nazir (1998 : 112). Teknik analisis data yang digunakan pada penelitian ini adalah menggunakan analisis isi berupa dokumentasi yang berbentuk tulisan dan mengorganisasikan data ke dalam bentuk kategori, menjabarkan ke dalam unit-unit, yang dimaksud dengan teknik analisis data Sugiyono (2010: 335), adalah proses mencari data, menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan dokumentasi, dengan cara mengorganisasikan data ke dalam kategori, menjabarkan ke dalam unit-unit, melakukan sintesis, menyusun ke dalam pola memilih mana yang penting dan yang akan dipelajari, dan membuat kesimpulan sehingga mudah dipahami oleh peneliti maupun orang lain.

HASIL DAN PEMBAHASAN

802.11ax sebuah teknologi baru di dunia Wi-Fi. Wi-Fi, sebuah teknologi nirkabel yang memiliki sebuah impact sangat besar dalam keseharian kita dalam mengakses data. Ketika suatu teknologi semakin besar dampaknya di pasar maka perkembangannya juga akan semakin cepat. Begitu pula dengan Wi-Fi, mungkin belum lama ini kita baru mendengar teknologi Wi-Fi baru yang dirilis oleh IEEE (Institute of Electrical and Electronics Engineers), yaitu sebuah badan riset yang tugasnya melakukan publikasi dan standarisasi terhadap banyak hal di dunia Electrical dan Electronics, dimana badan riset ini sebelumnya merilis standar 802.11ac kemudian dikembangkan lagi ke standar 802.11ax. Wi-Fi alliance sebagai lembaga sertifikasi perangkat bersinyal Wi-Fi membuka datanya dimana sampai tahun 2018 sudah ada sekitar 21 milyar perangkat ber-Wi-Fi di dunia dan diperkirakan akan mendekati 35 milyar di akhir tahun 2022.

802.11ac atau 802.11ax adalah kode dua group riset yang berbeda tetapi memiliki kerja yang berkesinambungan. Di 802.11ac kita tahu bahwa data rate akses Wi-Fi dikembangkan sedemikian rupa dari yang teknologi sebelumnya, 802.11n, mampu mencapai 600 Mbps menjadi 1.7 Gbps di 802.11ac. Sebuah lompatan data rate yang sangat signifikan untuk penggunaan wireless. Sejak lama salah satu fokus utama riset Wi-Fi banyak berpusat pada peningkatan data rate untuk mengejar keteringgalannya dari kabel gigabit Ethernet atau multi-gigabit ethernet, tetapi di

802.11ax konsep riset ini sedikit dirubah karena 1.7Gbps untuk user access dianggap sudah sangatlah mencukupi. Group riset 802.11ax mencoba melihat sisi lain dari pengembangan ini dimana masih banyak faktor lain dari Wi-Fi yang bisa dikembangkan untuk membuat akses nirkabel menjadi jauh lebih baik lagi walau memang di 802.11ax data rate memiliki peningkatan tetapi tidak se-drastis peningkatan dari teknologi 802.11n ke 802.11ac.



Source: Wi-Fi Alliance, ABI Riset, January 2018
 Gambar 1 - Jumlah perangkat nirkabel yang beredar dipasaran

Walau masih belum dirilis secara final, standar 802.11ax tinggal menunggu penyempurnaan dan revisi dan rencananya akan segera dirilis final di November 2019 walau sudah mulai ada beberapa vendor mulai ‘curi start’ membuat perangkat 802.11ax menggunakan hasil riset sementara. Melihat kondisi lapangan secara real dan bagaimana data digunakan secara real adalah dasar 802.11ax. Berkaca pada riset sebelumnya dimana data rate ditingkatkan setinggi-tingginya tetapi secara aktual belum tentu bisa digunakan secara maksimal, kali ini akan lebih berfokus pada keadaan yang sebenarnya di lapangan dan bagaimana agar dapat dikembangkan kembali secara keseluruhan kualitas penggunaan data dimana bukan hanya meningkatkan data rate setinggi-tingginya tetapi pada level sinyal menengah pun dapat memiliki kualitas data yang lebih baik.

Berlawanan dengan 802.11ac dimana hanya berfokus ke pengembangan frekuensi 5 GHz, sementara 802.11ax akan kembali mengembangkan frekuensi 2.4 GHz dengan pertimbangan banyaknya perangkat IoT yang beredar di pasaran dan penggunaan WiFi di rumah masih banyak membutuhkan 2.4GHz. Sebagian besar dari perangkat IoT adalah perangkat yang hanya beroperasi di frekuensi 2.4 GHz karena tidak seperti smartphone atau komputer dan laptop yang membutuhkan bandwidth dan data rate yang tinggi, perangkat IoT tidak membutuhkan bandwidth dan data rate tinggi tetapi kebutuhannya lebih kepada coverage yang lebih luas dimana dalam teori gelombang, frekuensi lebih rendah memiliki panjang gelombang yang lebih. 802.11ax akan meng-efisien-kan penggunaan data di frekuensi 2.4 GHz terutama pada komunikasi dengan data rate rendah. Di saat yang sama, perangkat IoT seperti sensor yang battery-sensitive nya juga akan diuntungkan. Ada beberapa fitur utama di

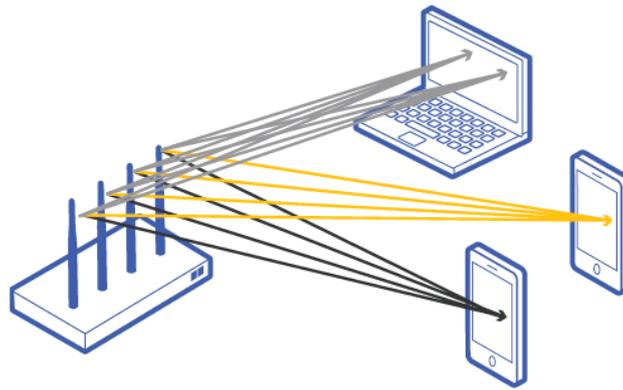
802.11ax yang di highlight yang benar-benar baru dan sebagian lagi bawaan dari teknologi sebelumnya yang disempurnakan. Dikutip dari berbagai sumber, beberapa fitur utama yang akan dijabarkan, antara lain :

1. Konsistensi pengiriman data dalam data-rate yang tinggi
2. Optimasi pengiriman data sehingga data-rate rendah masih dapat beroperasi dengan baik.
3. Optimasi high-density deployment dimana jumlah user per meter sangat besar dengan memanfaatkan OFDMA, Multi-user MIMO, dan spatial re-use.
4. Optimasi power dengan Target Wake Time (TWT) terutama untuk device yang sensitive dengan power seperti perangkat IoT.

802.11n (2008)	802.11ac (2012)
<ul style="list-style-type: none"> • 2.4 and 5 GHz supported • Wider channels (40MHz) • Better modulation (64-QAM) • Additional streams (up to 4) • Beam forming (explicit and implicit) • Backwards compability with 11a/b/g 	<ul style="list-style-type: none"> • 5 GHz only • Even wider channels (80, 160 MHz) • Better modulation (256-QAM) • Additional streams (up to 8) • Beam forming (explicit) • MU-MIMO • Backwards compability with 11a/b/g
802.11ax (2018)	Goals of the 802.11ax project
<ul style="list-style-type: none"> • 2.4 and 5 GHz supported • OFDMA uplink and downlink • Extends and generalizes OFDM • Introduces the concept of Resource Units (RU's) • Better modulation (1024-QAM) • Uplink MU-MIMO • Spatial re-use (BSS color) • Backwards compability with 11a/b/g 	<ul style="list-style-type: none"> • Enhance operation in 2.4 & 5 GHz bands (802.11 ac was only 5 GHz) • Increase average throughput per station by at least 4x in a dense deployment scenario (802.11ac specified aggregate throughput without a specific scenario) • For outdoor and indoor networks • Scenarios include wireless corporate office, outdoor hotspot, dense residential apartments, stadiums • Maintain or improve power efficiency of clients devices

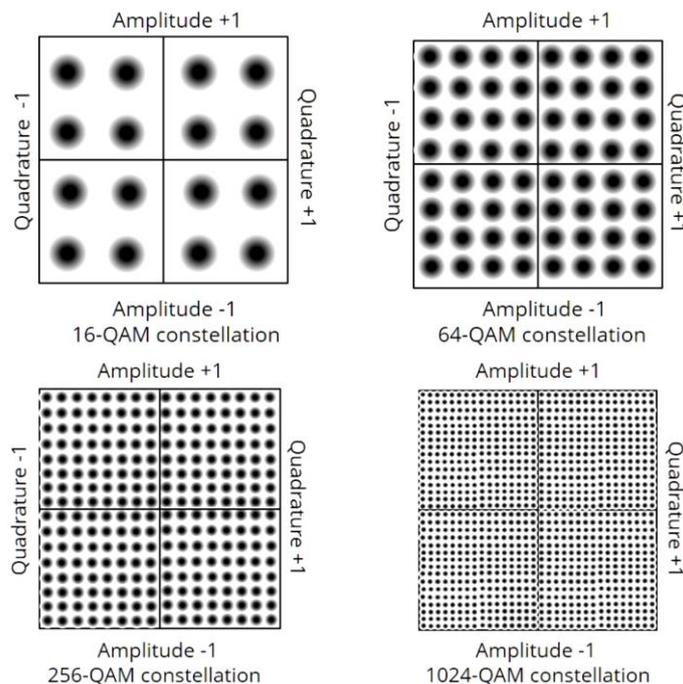
Sumber: Aruba whitepaper on 802.11ax
 Gambar 2 - progress standarisasi WiFi sejak 802.11n

Downlink MU-MIMO (Multi-User Multi-Input Multi-Output) adalah teknologi existing yang sudah ada di 802.11ac tetapi 802.11ax meng-extend fitur ini untuk uplink-nya dimana access point dapat berkoordinasi untuk melakukan transmisi data secara bersamaan ke beberapa user.



Source: Aerohive Poster on 802.11ax
Gambar 3 - Multi-User MIMO

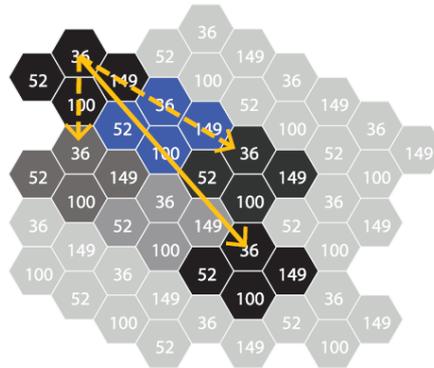
Quadrature Amplitude Modulation (QAM) adalah sebuah teknik modulasi data digital yang umum digunakan. 802.11ax meningkatkan kapasitas QAM memperoleh modulasi data dari 256 di 802.11ac menjadi 1024 di 802.11ax sehingga menimbulkan efek meningkatnya data-rate di kualitas sinyal dengan SNR (Signal-to-Noise Ratio) yang tinggi.



Source: Aruba Whitepaper on 802.11ax
Gambar 4 - Modulasi 1024-QAM

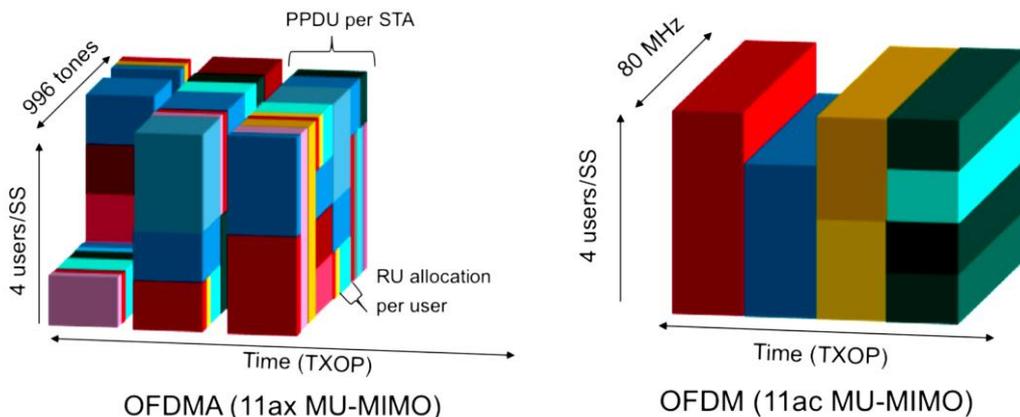
Satu hal yang akan sering didengar untuk teknologi baru di 802.11ax yaitu BSS coloring atau pewarnaan BSS. BSS atau Basic Service Set adalah kode sinyal yang digunakan per access point dalam men-transmit data seperti yang kita tahu data-data ini ditransmit dalam sebuah frekuensi tertentu yang disebut channel. Color atau pewarnaan ini seperti pengelompokan channel-channel yang tidak overlapping dan selanjutnya digunakan untuk pengaturan penggunaan kembali channel-channel ini. BSS coloring ini mengatur client untuk menyetop penerimaan data dan masuk ke sleep mode sesaat ketika client ini menyadari data tersebut bukan data 'penting'.

Teknologi ini bertujuan untuk mengatur pengiriman data dimana akan ada lebih banyak data yang dapat ditransmisikan secara bersamaan dengan mengatur jalur transmisi sehingga mengurangi efek saling tunggu menunggu antar device.



Source: Aruba Basic Service Set on 802.11ax
Gambar 5 - BSS coloring

Dari banyak pengembangan untuk outdoor WiFi, yang terpenting adalah terjadinya repeated data transmission untuk menurunkan data loss dan 802.11ax memperbesar GI (Guard Interval). GI yang lebih kecil dapat memperbesar bandwidth sedangkan GI yang lebih lebar dapat meningkatkan resitensi terhadap interferensi. GI adalah rentang frekuensi yang ada sebagai pengaman antar channel frekuensi yang berbeda. Transmit Beamforming adalah teknologi yang dibawa dari 802.11ac dimana access point dapat memiliki banyak antenna transmit yang dapat diatur arahnya untuk meningkatkan kekuatan sinyal, jarak, dan data rate-nya.



Source: Cisco Whitepaper on 802.11ax
Gambar 6 - OFDM vs OFDMA

Single-user operation. Dengan penggunaan OFDMA, transmisi dibundle bersamaan sehingga mengurangi jumlah transmit yang diperlukan untuk pengiriman sebuah data sehingga dapat meningkatkan efisiensi



Source: Wi-Fi Alliance, ABI Riset, January 2018
 Gambar 7 - Jumlah perangkat nirkabel yang beredar dipasaran

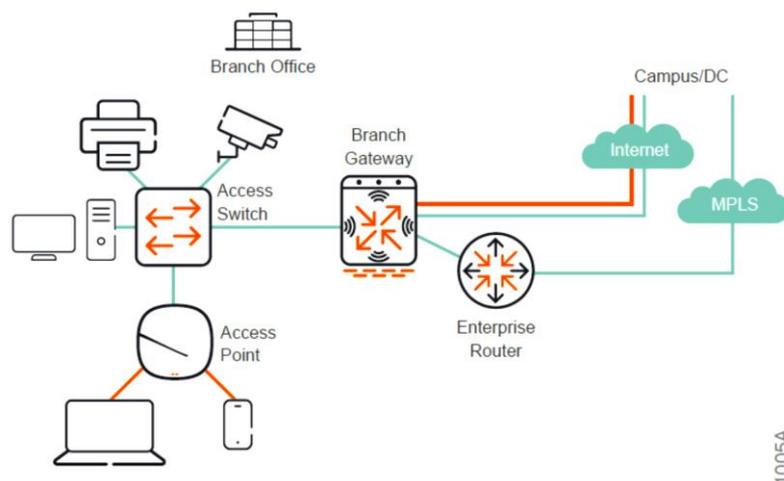
Power save mode yang sudah dimiliki oleh WiFi, sekarang memiliki kemampuan interval sleep yang lebih tinggi dan wake time yang dapat dijadwalkan. Perangkat IoT juga dapat memanfaatkan lebar pita channel 20 MHz only sehingga manajemen dapat menjadi lebih simple dimana chipset yang lebih sederhana dapat compatible dan digunakan dengan lebih umum. Power save menjadi salah satu goal utama dalam pengembangan 802.11ax dimana ada target untuk peningkatan performa sampai dengan 4x lipat dengan power yang sama. Power save memang sudah ada di 802.11 tetapi di 802.11ax dikenalkan sebuah metode baru yang bernama TWT (Target Wait Time) dimana ada semacam penjadwalan antara AP dan client untuk kapan melakukan sleep dan wake-time dimana kegiatan ini dapat dilakukan secara tidak bersamaan dengan client lain sehingga efisiensi transmisi data lebih maksimal. Perangkat IoT yang biasanya bekerja secara terjadwal dan menyala terus menerus 24/7 sangat membutuhkan fitur ini untuk efisiensi kerja baik bagi perangkat IoT itu sendiri dan juga perangkat lain agar transaksi data dapat lebih dioptimisasi.

Downlink dan Uplink OFDMA. Untuk membicarakan hal ini, pertama kita perlu membahas apa itu OFDMA, OFDMA atau Orthogonal frequency-division multiple access adalah sebuah metode modulasi data komunikasi yang merupakan pengembangan dari metode lama OFDM yang sudah sangat umum dipakai dan menambahkan fitur Multi User di dalamnya sehingga menjadi beberapa user dengan data rate yang lebih rendah dapat berkomunikasi secara bersamaan. Dengan fitur ini, sebuah transmisi data dapat di split dalam sebuah frekuensi channel tetapi transmisi yang di-split berbeda ini dapat ditujukan untuk client yang berbeda menggunakan grouping subcarriers (subcarriers semacam media pembawa data dalam Wireless LAN). Uplink OFDMA (data dari client ke access point) mirip seperti downlink OFDMA (data dari access point ke client) tetapi dalam keadaan ini beberapa client melakukan transmit data secara bersamaan ke access point dalam group subcarriers yang berbeda tetapi dalam sebuah channel yang sama.

Perangkat yang semakin beragam, itulah salah satu trend di WiFi saat ini dan faktor ini menjadi salah satu yang dipertimbangkan dalam pengembangan 802.11ax dimana untuk mendukung IoT di 802.11ax WiFi dikembangkan kearah untuk mendukung hal tersebut. Beberapa hal dari 802.11ax yang akan sangat berguna bagi perangkat IoT:

- Waktu sleep time yang lebih efisien dimana penjadwalan sleep-wake melalui penjadwalan, bukan periodik sederhana.
- BSS coloring membantu spatial re-user terjadi sehingga penggunaan data lebih optimal dan interferensi berkurang yang akhirnya menyebabkan data yang di transmit pada SNR rendah dapat menjadi lebih efisien.
- OFDMA mengatur transmisi downlink dan uplink yang lebih efisien.
- Pengembangan kembali frekuensi 2.4GHz.
- Banyak hal lain dari 802.11ax yang mendukung kerja sinyal bukan hanya untuk IoT tapi kerja WiFi secara keseluruhan baik di frekuensi 2.4 GHz dan 5 GHz.

Aruba Software-Defined WAN (SD-WAN) adalah sebuah teknologi untuk membangun jaringan WAN atau jaringan koneksi antar kantor pusat dan kantor cabang secara cloud yang dapat men-simplifikasi operasional kantor cabang dan melakukan optimisasi terhadap manajemen jaringan WAN. Teknologi ini sangat ideal untuk perusahaan yang sedang mengembangkan teknologi IT digitalnya dimana Aruba SD-WAN yang di-manage secara sentral dapat memprovide simplifikasi operasional dan visibilitas serta kontrol terhadap semua cabang. Kantor-kantor cabang dan model bisnis yang terdistribusi di seluruh Indonesia dengan banyaknya kantor cabang yang tersebar adalah model yang sangat cocok menggunakan teknologi ini. Traditional Branch, salah satu tantangan terbesar untuk branch saat ini adalah begitu berkembangnya teknologi perangkat mobile, IoT, kebutuhan bandwidth, dan ekspektasi tinggi untuk penggunaan jaringan. Bersamaan, pendanaan untuk branch-pun mulai dituntut untuk bergeser dari CAPEX menjadi OPEX. Penggunaan aplikasi cloud seperti office 365 biasanya akan menjadi jawaban untuk mensimplifikasi persiapan hardware yang dibutuhkan ketika sebuah cabang baru dibuka. Design jaringan yang tradisional dengan sebuah central hub sudah tidak cocok lagi untuk digunakan. Traditional branch biasanya identik dengan cost yang tinggi bagi IT karena kebutuhan investasi mulai dari router, bandwidth internet tinggi, service ISP, server, dan lain-lain dan biasanya membutuhkan waktu yang panjang untuk di implementasikan.



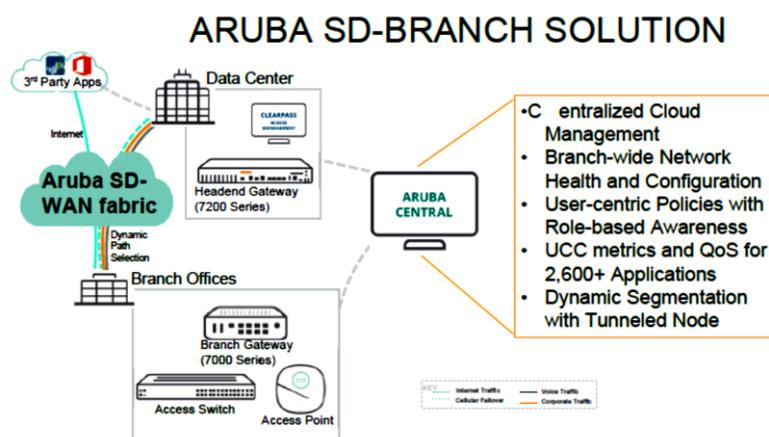
Gambar 8 – SD-WAN yang Diintegrasikan dengan Existing Design.



Gambar 9 – Konsolidasi Berbagai Perangkat Branch Menjadi Satu

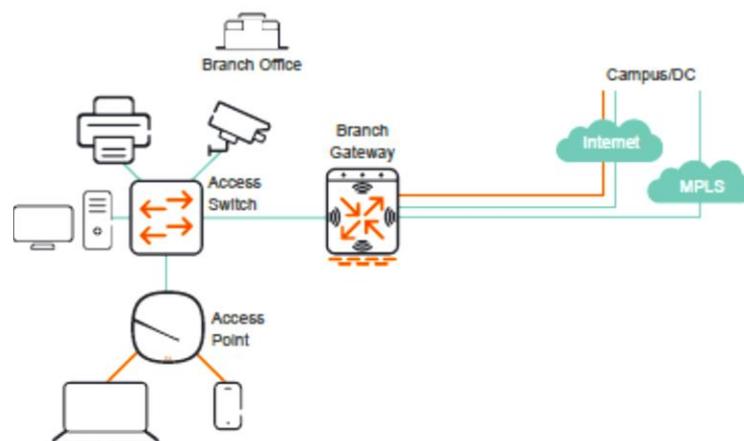
Ketika kita berbicara aturan atau policy dan keamanan maka akan lebih kompleks lagi ketika ada keharusan untuk menyeragamkan hal ini di seluruh branch. Software-defined Branch (SD-Branch/SD-WAN). Dari branch atau cabang bergaya tradisional, bertransisi ke model SD atau Software-defined. SD ini berkembang dari istilah SDN (Software Defined Network) yang menggunakan cloud untuk network management dan efisiensi SDN dikembangkan oleh Aruba menjadi SD-WAN yang merupakan solusi jaringan WAN berorientasi terhadap SD. Dengan solusi ini diharapkan dapat mengatasi beberapa hal seperti :

- Penggunaan SD-WAN untuk menggunakan internet sebagai pengganti MPLS(Multiprotocol Label Switching sebagai Teknologi penyampaian paket pada jaringan backbone berkecepatan tinggi)
- Simplifikasi di sisi LAN cabang dengan menggunakan rule dari pusat sehingga cabang dapat mengurangi perangkat yang terlalu kompleks seperti VLAN, ACLs, dedicated server, dan lain-lain.
- Cara setup yang sangat mudah di sisi branch sehingga tim non-IT juga dapat melakukannya. Cukup menggunakan aplikasi di smartphone untuk men-setup network di branch.
- Setup SD-WAN sangat mudah, beberapa hal yang perlu diperhatikan adalah:
- Cloud Management – Cloud management menggunakan Aruba Central adalah pusat konfigurasi dan management untuk SD-WAN. Aruba Central ini juga bisa digunakan untuk memanage AP, switch, dan perangkat Aruba lainnya. Konfigurasi SD-WAN VPN di Aruba central dapat dilakukan secara otomatis dan dari sini kita bisa mendapatkan gambaran topologi yang ada.



Gambar 10 – Topologi Arsitektur SD-WAN Menggunakan Aruba SD-Branch

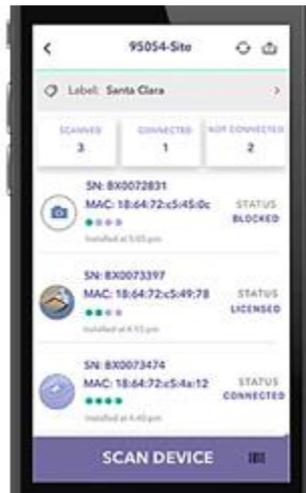
- Branch Gateway – Merupakan sebuah perangkat seperti router berupa hardware. Perangkat ini me- utilisasi controller Aruba seri 7000 yang dengan license dapat mengaktifkan fitur branch gateway di controller. Dalam setiap deployment cukup menaruh perangkat ini di gateway cabang dan ketika terkonfigurasi, perangkat ini melakukan tunnel ke pusat dan meneruskan semua rule yang terkonfigurasi. Beberapa fitur yang dapat diterapkan adalah stateful firewall, web content classification, hybrid WAN connectivity, IPsec VPN, QoS, dan WAN path monitoring and selection.
- Branch WLAN/LAN – Perangkat ini sifatnya opsional, jika membutuhkan akses WLAN atau WiFi maka cukup dengan mendeploy access point Aruba atau switch jika butuh LAN atau wired maka rule yang sama dengan pusat dapat di-enforce ke perangkat-perangkat ini.
- Headened Gateway – Perangkat ini posisinya mirip seperti branch gateway tetapi bedanya perangkat ini yang menjadi sentral semua headened branch dan di posisikan di kantor pusat dengan menggunakan Aruba controller seri 7200. Perangkat ini yang akan menjadi pusat rule dan VPN concentrator menggunakan VPN IPsec.



Gambar 11 – SD-WAN Topology di sisi Cabang

Simplisitas dan otomatisasi, dua hal yang merupakan faktor utama dalam penentuan penggunaan SD-WAN adalah Simplisitas dan Otomatisasi. Kedua hal ini dapat sangat berguna untuk perusahaan yang baru berkembang atau perusahaan yang mempunyai resource IT yang minim. Cabang baru yang menggunakan SD-WAN dapat di setup bahkan oleh orang non-IT sehingga tim IT tidak perlu selalu meluangkan waktu men-setup semua perangkat di cabang dan semua rule dari pusat dapat langsung digunakan secara otomatis dengan topologi SD-WAN tanpa perlu men-setup perangkat jaringan secara lengkap di cabang tetapi hanya dengan menggunakan SD-WAN maka semua rule dapat di-apply secara virtual dari pusat. Dengan teknologi cloud dari Aruba Central, semua perangkat mulai dari kantor pusat hingga cabang dapat di-manage dari internet dengan cloud secara aman. Aruba central menawarkan manajemen dan visibilitas cloud yang simple, aman, dan cost-effective untuk Aruba Instant APs, Switch, dan Branch Gateways untuk perusahaan multi-site. Analytic

service yang unggul dan kesehatan konektifitas, juga guest access membantu IT untuk memberikan solusi cloud branch yang efisien.



Gambar 12 – Konfigurasi Branch Baru dengan Menggunakan ZTP (Zero Touch Provisioning) via Mobile Device

Keamanan selalu menjadi faktor pemikiran ketika penggunaan cloud. Aruba SD-WAN sudah menerapkan berbagai security untuk menjamin keamanan operasional. Koneksi dengan menggunakan VPN digunakan komunikasi antar perangkat ataupun untuk client device. VPN antar perangkat digunakan untuk mengamankan komunikasi antara kantor pusat dan cabang sedangkan VPN ke client digunakan untuk mengamankan komunikasi extranet yaitu koneksi karyawan yang ingin terhubung ke jaringan kantor walau sedang berada diluar kantor. VPN ke client ini dapat terkoneksi langsung baik ke kantor pusat maupun ke cabang. Segmentasi secara dinamis dapat diterapkan karena switch Aruba dapat terintegrasi ke branch gateway dan rule dari branch gateway dapat ditunnel ke switch. Aruba branch gateway memiliki fitur PEF (Policy Enforcement Firewall) yang berupa kumpulan rule stateful firewall untuk secara ketat mengontrol akses data setiap user dan device. Lebih jauh lagi, fitur PEF dapat digunakan untuk mengontrol sampai ke level aplikasi untuk melihat dan membatasi akses suatu aplikasi. Menariknya fitur ini dapat diterapkan secara role-based yang artinya setiap user akan diperlakukan secara dinamis sesuai dengan role-nya bukan secara statis untuk semua user yang ada. Aruba Branch gateway juga menggunakan fitur Web-root Machine Learning Classification Technology yang artinya setiap website dapat diklasifikasi sesuai dengan kontennya. Rating dari setiap website tersebut di monitor dan akses dibatasi sesuai dengan rating konten setiap website yang kemudian dapat memblokir konten yang tidak diinginkan seperti spam, exploits, botnets, phishing, proxies, dan mobile threats. Informasi geolocation dapat digunakan untuk pemblokiran akses secara negara tujuan dari sebuah data. Aruba SD-Branch juga dapat diintegrasikan dengan layanan Cloud Security seperti Palo Alto Networks GlobalProtect atau Zscaler. Hal ini memungkinkan company yang memiliki layanan cloud security untuk memiliki rule firewall yang sama di semua lokasinya. Policy Role-based adalah sebuah perangkat Aruba lainnya, Aruba SD-Branch powerful dengan menggunakan pengaturan role policy role-based dimana setiap user dan perangkat yang terkoneksi mengalami tahap pengecekan berbagai macam rule untuk memasangkannya dengan sebuah role

tertentu dimana di dalam role ini terdapat berbagai role security untuk mengatur alur data.

Untuk pengaturan role yang lebih dinamis dan kompleks, SD-Branch dapat diintegrasikan dengan Aruba Clearpass Policy Manager, sebuah mesin Network Access Control yang mampu memproses rule yang jauh lebih rumit untuk menentukan role sebuah user atau device. Fitur application fingerprinting di Aruba Branch gateway dapat mengidentifikasi sekitar 2600 aplikasi dan menerapkan rule yang berbeda-beda terhadap aplikasi tersebut. Hal ini dapat memastikan aplikasi yang memang digunakan untuk bekerja memperoleh prioritas data yang lebih tinggi. Policy-based dapat diterapkan ke rule routing dimana role tertentu dapat di route secara berbeda. Contohnya role guest untuk ke internet dapat di route menggunakan local internet dan tidak dibawa secara VPN ke kantor pusat.

KESIMPULAN

WiFi di tahun-tahun kedepannya terlihat sangat menjanjikan dengan begitu cepatnya perkembangan baik di sisi pasar maupun teknologi. Dalam beberapa tahun kedepan, IoT akan berkembang dengan cepat dan membutuhkan koneksi low power dan low data-rate dengan jarak yang jauh dimana 802.11ax akan sangat membantu ketika protocol lain seperti 802.11ah masih belum dapat diadaptasi dengan baik. 802.11ax pertama me rilis draft pada September 2017, di update pada Mei 2018, dan rencananya akan merilis final version dan mendapat final approval pada November 2019 dan sudah dikembangkan ditahun 2020 dan sampai saat ini. Seperti biasanya dalam berbagai update WiFi sebelumnya, jangan khawatir dalam hal kompatibilitas, WiFi selalu men-support ke belakang dimana device 802.11ax akan tetap dapat terhubung ke access point yang lebih lama dan juga access point 802.11ax dapat men support client yang lebih lama. Jadi rencana kan lah upgrade ketika memang memungkinkan. Aruba SD-Branch dapat menjadi solusi untuk berbagai issue yang dialami perusahaan di sisi cabang terutama di perusahaan yang memiliki banyak cabang yang tersebar di seluruh Indonesia. Komponen branch gateway yang menjadi solusi Aruba-Branch dapat menggabungkan fungsi-fungsi dari berbagai perangkat seperti firewall, WAN Router, server DPI (Deep Packet Inspection), dan WAN Optimization ke dalam sebuah perangkat dengan tujuan meminimalisir perangkat yang perlu di-deploy dan di-maintain di cabang. Kedepannya model bisnis seperti ini yang me-utilisasi Cloud akan semakin banyak penggunanya karena banyaknya keuntungan yang bisa didapat baik dari sisi pengurangan cost dalam pembangunan infrastruktur cabang maupun simplisitas operasional IT. Sistem manajemen yang tersentral juga memungkinkan monitoring dan pengaturan dari satu titik. Concern untuk masalah keamanan juga dapat dihindari dengan pengamanan komunikasi data menggunakan VPN IPSec antar cabang dan pengaturan policy role-based untuk memastikan keamanan data yang ditransaksikan oleh tiap user.

DAFTAR PUSTAKA

- Tanenbaum , AS, 1996, “*Computer Networks*”, Prentise Hall
- Ardiansyah , Dian, 2003, “Teknologi jaringan komputer”.
- Prihanto , Harry, 2003, “Membangun Jaringan Komputer : Mengenal Hardware dan Topologi Jaringan”.
- Purbo, Onno W, 1992, “Jaringan Komputer Menggunakan Protokol TCP/IP”, *Department of Electrical and Computer Engineering University of Waterloo*.
- Riyana Rahadjeng, I., & Puspitasari, R. 2018. Analisis Jaringan *Local Area Network (LAN)*.
- T. S. Rappaport, *Wireless Communications: Principles and Practice, 1st ed.*New York: *ieee*, 1996
- W. Stallings, *Komunikasi & Jaringan Nirkabel*, 2nd ed. Jakarta: Erlangga: 2007
- Hantoro, Gunadi Dwi. 2009. *WIFI (Wireless LAN) Jaringan Komputer Tanpa Kabel*. Bandung: Penerbit Informatika Haykin.
- Simon. 2005. *Modern Wireless Communication*. London: PearsonPrentice-Hall
- Lee, William C.Y. 2006. *Wireless & Cellular Telecommunications, Third Edition*. Boston: Mcgraw-Hill.
- Andini, Sarah Setya. Rahardjo, Teguh Budi. & Nugraha, Eko. IEEE 802.11g. Jurusan Teknik Elektro FT UGM. Yogyakarta: 2009.
- Azhar, Mariza. Priambodo, Gotama Edo. IEEE 802.11g. Jurusan Teknik Elektro FTUGM. Yogyakarta: 2009
- T. Huschka. Sept. 1994. *Ray Tracing Models for Indoor Environments and theirComputational Complexity, in IEEE 5th International Symposium on Personal,Indoor, and Mobile Radio Communications (PIMRC)*. pp. 486-490.
- E. Khorov , A. Kiryanov , A. Lyakhov , *IEEE 802.11ax: How to Build High Efficiency WLANs, in: 2015 International Conference on Engineering and Telecommunica- tion (EnT), IEEE, 2015*, pp. 14 – 19 .
- B. Bellalta , *IEEE 802.11ax: high-efficiency WLANs, IEEE Wireless Commun.* 23 (1) (2016) 38 – 46 .
- B. Bellalta , L. Bononi , R. Bruno , A. Kessler, *Next generation IEEE 802.11 wireless local area networks: current status, future directions and open challenges, Comput. Commun.* 75 (2016) 1 –2 5 .
- M.S. Afaqui , E. Garcia-Villegas , E. Lopez-Aguilera, *IEEE 802.11ax: challenges and requirements for future high efficiency WiFi, IEEE Wireless Commun.* 24 (3) (2017) 130 –1 37 .
- Sukris Sutiayatno. *Metodologi Penelitian (Penelitian Teknologi Informasi, Penelitian Kuantitatif Dan Kualitatif, Penelitian Eksperimen, Penelitian Research & Development Dan Penelitian Tindakan)*. Yogyakarta: Penerbit K-Media, 2017.
- Samsu. *Metode Penelitian: Teori Dan Aplikasi Penelitian Kualitatif, Kuantitatif, Mixed Methods, Serta Research and Development*. Vol. Cetakan 1. Jambi: Pusaka, 2017.

- Zainal A. Hasibuan. Metodologi Penelitian Pada Bidang Ilmu Komputer dan teknologi Informasi; Konsep, Teknik, Dan Aplikasi. Fasilkom Universitas Indonesia, 2007.
- Sugiyono. Metode Penelitian Kuantitatif, Kualitatif dan R & D. Bandung: Alfabeta: 2014.
- M. Nasir. Metode Penelitian. Bogor : Penerbit Ghalia Indonesia. 2005.
- Ricky Efraim Lie. Aruba Networks. (2018). 802.11ax whitepaper. Cisco Systems. IEEE 802.11ax: The Sixth Generation of Wi-Fi. IEEE. 2018
- Ricky Efraim Lie. P802.11axTM/D2.0 Draft Standard for Information Technology. Wi-Fi Alliance. (Nov 2017). Marketing Requirements Document for Interoperability Testing of Wi-Fi ax. 2017