IlmuKomputer.Com

Protokol 802.11 pada Wireshark

Arsyad Dwiyankuntoko

11ipa3.arsyad@gmail.com http://arsyaddwiyankuntoko.blogspot.com

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pendahuluan

Wireless network merupakan salah satu metode dalam pembangunan jaringan komputer yang praktis karena dalam implementasinya tidak menggunakan kabel untuk komunikasi datanya melainkan menggunakan media udara. hal itu bisa terjadi karena pada tiap-tiap device yang digunakan tersebut terdapat antena yang mengirim dan menerima sinyal radio yang dikirim. Jadi data-data yang akan dikirim dari suatu device akan diubah terlebih dahulu menjadi sinyal radio dan baru setelah itu dikirim ke device tujuan. Dan setelah diterima oleh device tujuan, sinyal radio tersebut diubah kembali menjadi data-data yang ditampilkan.

Sinyal radio sendiri sebenarnya merupakan gelombang elektromagnetik yang terlepas ke udara. Dan seperti yang telah diketahui, terdapat aturan-aturan dalam penggunaan gelombang elektromagnetik tersebut sebagai media untuk pengiriman data. Terdapat parameter-parameter yang perlu diperhatikan dalam penggunaanya seperti daya yang digunakan, frekuensi, channel, dll karena apabila tidak ada protokol atau aturan tertentu yang mengatur penggunaan gelombang radio tersebut akan terjadi tabrakan antar gelombang yang dapat menyebabkan hilangnya data. Protokol yang mengatur gelombang radio tersebut adalah protokol 802.11. pada tulisan ini akan dicoba capturing protocol tersebut menggunakan wireshark agar dapat diketahui parameter apa

Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com



saja yang ada didalamnya.

Jenis-Jenis Protokol 802.11

Seperti yang telah dijelaskan sebelumnya bahwa protokol 802.11 ini merupakan protokol yang mengatur gelombang radio yang digunakan data sebagai medium pengiriman. Oleh sebab itu, Protokol 802.11 ini pada model OSI terdapat pada layer fisik hingga layer LLC (Logical Link Control). Berikut merupakan gambar yang menunjukkan perbandingan layer-layer pada protocol 802 dengan model OSI



Sumber Gambar: http://budi.insan.co.id/courses/ec7010/dikmenjur/hari-report.doc

Protokol 802.11 sendiri selalu berkembang dari waktu ke waktu, berikut merupakan jenis-jenis protokol 802.11 yang ada :

802.11b

Digunakan mulai akhir tahun 1999 dengan menggunakan frekuensi 2,4 Ghz. Maksimum bandwidth yang bisa dicapai adalah 11Mbps (Megabit per second). Pada koneksi ini, modulasi yang digunakan adalah DSSS (Direct Sequence Spread Spectrum). Kanal yang tidak overlapping berjumlah 3, yaitu kanal 1, kanal 6 dan kanal 11. Protokol ini kompatibel dengan tipe 802.11g jika tipe 802.11g beroperasi pada mode mixed.

802.11a

Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com

IlmuKomputer.Com

Ikatlah limu dengan menuliskannya

Digunakan mulai akhir 2001 dengan menggunakan frekuensi 5Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps sementara modulasi sinyal yang digunakan adalah OFDM (Orthogonal Frequency Division Multiplexing). Kanal yang tidak overlapping berjumlah 12 (bisa lebih). T ipe ini tidak kompatibel denga tipe b maupun g.

802.11g

Digunakan mulai pertengahan tahun 2003 dengan menggunakan frekuensi 2,4Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps. Modulasi yang dighunakan adalah OFDM. Kanal yang tidak overlapping berjumlah 3 buah. Protokol ini kompatibel dengan tipe b namun hasilnya mengikuti tipe b.

802.11a/g

Tipe protokol ini mulai diperkenalkan pertengahan 2003 dengan menggunakan frekuensi 2,4 Ghz dan 5Ghz. Maksimum bandwidth yang bisa dicapai sebesar 54Mbps dengan menggunakan modulasi sinyal OFDM. Kanal yang tidak overlapping berjumlah 16 buah. Bila beroperasi pada modus a, maka protokol ini tidak kompatibel dengan tipe b dan g. Namun, jika beroperasi pada modus g, koneksinya akan kompatibel dengan tipe b.

CAPTURING Protokol 802.11 dengan Wireshark

Berdasarkan Wiki.Wireshark.org, untuk bisa melakukan capture protokol 802.11 menggunakan wireshark harus mengaktifkan dulu fasilitas "monitor mode" pada wireshark. Padahal tidak semua OS support dengan fasilitas ini. OS windows yang sering digunakan juga termasuk OS yang tidak support untuk fasilitas "monitor mode" ini. Monitor mode ini hanya support pada wireshark 1.4 (atau versi selanjutnya) yang menggunakan OS BSD, Linux, dan Mac OS X system yang terdapat libpcap 1.0 (atau versi selanjutnya) didalamnya. Atau bisa juga dengan menggunakan AirPcap. AirPcap merupakan sebuah device tambahan berbentuk seperti USB yang digunakan untuk melakukan capture protokol 802.11 pada OS windows. Device ini merupakan buatan dari riverbed, berikut gambarnya

IImuKomputer.Com



Oleh karena itu, diperlukan cara lain untuk melakukan capture protokol 802.11 ini, salah satunya adalah dengan menggunakan bantuan software network protocol analyzer yang lain. Karena OS yang digunakan pada komputer yang akan digunakan untuk melakukan capture ini adalah windows 7, maka akan digunakan network protocol analyzer "Microsoft Network Monitor" karena software ini keluaran dari vendor yang sama seperti windows 7 yaitu Microsoft jadi banyak program di dalamnya yang saling sinkron.

Microsoft network monitor sendiri tidak berbeda jauh dari wireshark, terdapat kolom filter, paket yang tercapture, detail paket, dan detail paket dalam hexadecimal. Berikut tampilan dari Microsoft network Monitor

	_									
Microsoft Network Monitor 3.4 - K:\wifii.c	ар			possed	the second	-				
<u>File Edit View Frames Filter Expe</u>	erts <u>T</u> ools <u>H</u> e	lp								
📄 New Capture 😕 Open Capture 🛛 🕞 Sa	ave As 📔 🥯 Rea	ssemble						🔡 Layout 🔻 🍋 Pa	arser Profiles 💌 🔝 Options	🕜 How Do I 🤻
🌒 wfii.cap 🔥 Start Page 🐚 Parsers										
Network Conversations ×	Display Filter									×
🖃 🛄 All Traffic	X Apply X	Remove State	🕶 🏹 Load F	ilter 🔻					Save Filter	⊘ Clear Text
😑 🔜 Other Traffic									100	SZ
AvastSvc.exe (1500)										
DataProxy.exe (4852)										
B- System (0)										
svchost.exe (1048)	Frame Summa	ry								×
	🖓 Find 🔻 🖣	r 1						2	Color Rules 🖓 Aliases 🔻	III Columns 🔻
	Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description		*
	16	11:45:31 AM 7/4/2013	1.4022167		[647002 BD4040]	[*BROADCAS	it] WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 N	/bps, SSID = N
	17	11:45:31 AM 7/4/2013	1.5045428		[647002 BD4040]	[*BROADCAS	T] WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 N	tbps, SSID = N
	19	11:45:31 AM 7/4/2013	1.7093582		[647002 BD4040]	["BROADCAS	T] WIFI	WiFi: [ManagementBeacon]	. RSSI = -54 dBm, Rate = 1.0 N	Abps, SSID = N
	20	11:45:32 AM 7/4/2013	1.8117454		[647002 BD4040]	[*BROADCAS	T] WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 M	lbps, SSID = N
	22	11:45:32 AM 7/4/2013 11:45:32 AM 7/4/2013	2.0165575		[647002 BD4040]	[*BROADCAS	TI WIFI	WiFi: [ManagementBeacon]	. RSSI = -54 dBm, Rate = 1.0 M	4bos, SSID = N
	23	11:45:32 AM 7/4/2013	2.1187966		[647002 BD4040]	[*BROADCAS	T] WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 M	4bps, SSID = N
	24	11:45:32 AM 7/4/2013	2.2213231		[647002 BD4040]	[*BROADCAS	T] WIFI	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 N	tbps, SSID = N
	25	11:45:32 AM 7/4/2013	2.3435416	AvastSvc.exe	77.234.41.53	192, 168, 1, 21		HTTP:Response, HTTP/1,1, Statu	s: Ok. URL:	10ps, 5510 = N
	27	11:45:32 AM 7/4/2013	2.3494150	AvastSvc.exe	192.168.1.21	77.234.41.53	3 HTTP	HTTP:Request, GET /R/A0YKIDc0	NjIyOTZkM2FhODQ3MmJiMmY5	Y2I4OTcxM2U:
	28	11:45:32 AM 7/4/2013	2.4261596		[647002 BD4040]	["BROADCAS"	T] WIFI	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 N RSSI = -54 dBm, Rate = 1.0 N	Ibps, SSID = N
	30	11:45:32 AM 7/4/2013	2.6197782	AvastSvc.exe	77.234.41.53	192.168.1.21	L TCP	TCP:Flags=A, SrcPort=HTT	P(80), DstPort=50556, Payload	JLen=0, Seq=1
	31	11:45:32 AM 7/4/2013	2.6307918		[647002 BD4040]	[*BROADCAS	T] WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 M	lbps, SSID = N
	32	11:45:32 AM 7/4/2013 11:45:33 AM 7/4/2013	2.7333232		[647002 BD4040] [647002 BD4040]	[*BROADCAS	TJ WiFi	WiFi: [ManagementBeacon]	RSSI = -54 dBm, Rate = 1.0 M RSSI = -54 dBm, Pate = 1.0 M	lbps, SSID = N
	34	11:45:33 AM 7/4/2013	2.9382051		[647002 BD4040]	[*BROADCAS	T] WIFI	WiFi: [ManagementBeacon]	. RSSI = -54 dBm, Rate = 1.0 N	Abps, SSID = N T
	•									F.
	Frame Details					x	Hex Details			×
	Frame: Num	uber = 25, Capture	ed Frame	Length = 3	26, MediaTy	pe = 1	late in t			
	WiFi: [Ma	nagementBeacon]	R	SSI = -54	dBm, Rate =	1.0 1	121 Decode As	Width ♥ Prot Off: 0 (0x00)	Frame Off: 0 (0x00)	Sel Bj
	. MetaDat	a: RSSI = -54 dBm	, Rate =	1.0 Mbps			0000 02 20		0 00 00	••••
	FrameCo	ntrol: Version 0,	Managemer	nt, Beacon	,(0x	:80)	000A 00 06		0 00 CAV.	Day
	Duration	n: 0 (0x0)					0014 FF FF	80 00 00 00 FF F	0 71 70 71 0 0 7 7 7 7 7 7	000
	DA: *BR	DADCAST					0028 FF FF		0 64 70 ÿÿdp.%@	Ødp
	- SA: 647	002 BD4040					0032 02 BD		1 6A 1C .800 w.	áj.
	BSSID:	647002 BD4040					003C 02 00		4 00 02d.	••••
	1		- **	- 1010		+	🧾 Frame Commen	ts [#E] Hex Details		
Version 3.4.2350.0							🕵 Displa	yed: 280 Captured: 280	Focused: 25 Seler	cted: 1

Pada gambar tersebut terlihat jika MNM dapat melakukan capture terhadap protocol 802.11 dimana pada gambar tersebut ditunjukan dengan nama protocol wifi. Di situ *Komunitas eLearning IlmuKomputer.Com* 4 *Copyright* © 2003-2007 *IlmuKomputer.Com*



sebenarnya juga sudah terdapat paket detail dari setiap paket yang ada meskipun agak sedikit berbeda tampilanya dengan tampilan yang ada pada wireshark.

Untuk melihat protocol tersebut melalui wireshark, pertama-tama stop dulu proses capture yang sedang berlangsung dengan cara klik stop pada toolbar

💯 Microsoft Network Monitor 3.4					
File Edit View Frames Capture Filter Experts Tools Help					
📄 New Capture 👏 Open Capture 🔚 Save As 🐺 Capture Settings 🕨 Start 🛽	Pause 🥃 Stop				
🔵 Capture1 💿 wifii.cap 🚮 Start Page 🐚 Parsers	Stop Capture F7				
Network Conversations × Display Filter					

Kemudian save hasil capture protokol wifi tersebut dengan format yang bisa dibaca oleh wireshark yaitu format .cap

😥 Save As		Same in the second		X		
Save in:	👝 Data E (E:)		• 🎯 🌶 📂 🛄 •			
(Ang	Name	*	Date modified	Туре 🔺		
Recent Places	Blog capture bts		6/19/2013 8:07 AM 5/7/2013 12:31 AM	File fol File fol		
	🍌 CCNA		4/19/2013 6:43 PM 6/24/2013 9:24 AM	File fol = File fol		
Desktop	📗 database ars	/ad	6/27/2013 11:19 AM	File fol		
F 0	퉬 Files		5/5/2013 5:01 AM	File fol		
	lorensics-pro	otocols	6/2/2013 6:25 AM	File fol		
Libraries	퉬 foto pantula	n	7/2/2013 7:50 PM	File fol		
	퉬 gadget dege	neration	6/14/2013 12:59 PM	File fol		
	퉬 Gambar		6/23/2013 11:05 AM	File fol		
Computer	퉬 instalasi dan	pengukuran jar radio	4/23/2013 2:34 PM	File fol		
	퉬 jarak ke bts		5/14/2013 2:24 AM	File fol		
	iob Teknik M	lultimedia	5/6/2013 11:22 AM	File fol		
Network	•			P		
	File name:	wifi	E	Save		
	Save as type:	Capture File (*.cap)	•	Cancel		
Frame selection						
<u>All captured frames</u>						
◎ <u>D</u> isplayed frames						
© Selected frames						
Frame range (eg. 1,3,5-12):						
[√] Regord display filter in capture file						

Save file tersebut pada folder yang diinginkan kemudian bukalah wireshark dan buka file .cap yang telah di-save tadi dengan cara klik file, open kemudian cari di folder tempat menyimpan file tersebut kemudian klik open.

📶 wifi	.cap [Wiresha	k 1.8.6 (SVN Rev 48142 from	/trunk-1.8)]		president in						
Eile	dit <u>V</u> iew <u>G</u>	<u>Capture</u> <u>A</u> nalyze <u>S</u> tatist	ics Telephony <u>T</u> ool	s Internals <u>H</u> elp							
8		🖻 🐻 🗙 🔁 占	् 🗢 🔿 🖥		🔍 🔍 🔍 🖭 👹	🗹 🕵 🎇	Ħ				
Filter:				 Expression 	Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length Info						
	1 0.000000	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1824	, FN=0,	Flags=,	BI=100,	SSID=NN	
	2 0.102535	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1828	, FN=0,	Flags=,	BI=100,	SSID=NN	
	3 0.204917	00 тр-Linkт_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1832	, FN=0,	Flags=,	BI=100,	SSID=NN	
	4 0.307315	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1836	, FN=0,	Flags=,	BI=100,	SSID=NN	
	5 0.409792	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1840	, FN=0,	Flags=,	BI=100,	SSID=NN	
	6 0.511986	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1844	, FN=0,	Flags=,	BI=100,	SSID=NN	
	7 0.614344	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1848	, FN=0,	Flags=,	BI=100,	SSID=NN	
	8 0.716923	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1852	, FN=0,	Flags=,	BI=100,	SSID=NN	
	9 0.819389	00 тр-Linkт_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1856	, FN=0,	Flags=,	BI=100,	SSID=NN	
	LO 0.921769	00 тр-Linkт_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1860	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L1 1.029172	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1864	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L2 1.126527	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1868	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L3 1.228911	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1872	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L4 1.331377	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1876	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L5 1.433703	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1880	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L6 1.536029	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1884	, FN=0,	Flags=,	BI=100,	SSID=NN	
	L7 1.638519	00 Tp-LinkT_bd:40:40	Broadcast	802.11	326 Beacon fra	ame, SN=1888	, FN=0,	Flags=,	BI=100,	SSID=NN	
	19 1 740004	OO TO LIDET bd-40-40	Prondenet	203 11	276 Poscon fr		EN-0	close-	PT_100	CCTD_NN	
•											
🗉 Ena	me 9: 326	bytes on wire (2608	bits), 326 bytes	s captured (260	8 bits)						
Net	Mon 802.11	capture header									
IEI IEI	E 802.11 E	eacon frame, Flags:									1
😑 IEEE 802.11 wireless LAN management frame											
🗄 Fixed parameters (12 bytes)											
⊟ Tagged parameters (254 bytes)											
⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]											
🗄 Tag: DS Parameter set: Current Channel: 1											
🗄 Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]											
Tag: Country Information: Country Code ID, Environment Unknown (0x00)											
E	Tag: AP C	hannel Report: Regul	atory Class 32,	Channel List :	1, 2, 3, 4, 5, 6	6, 7,					
E	Tag: AP C	hannel Report: Regul	atory Class 33,	Channel List :	5, 6, 7, 8, 9, 1	10, 11,					
E	∃Tag: Traf	fic Indication Map (TIM): DTIM 0 of	0 bitmap							
	T-0. COD	Information									
0000	05 00 19	00 dd 1a 00 50 f2 0	1 01 00 00 50 f2	02P	···· P··						
0000	20 18 01	50 + 2 + 02 + 00 + 50 + 2 + 00 + 20 + 00 + 0	+ 01 00 00 50 72	02PP	· · · · · P · ·						
JUEU	ac 04 01	00 00 0f ac 02 00 0	0 dd 18 00 50 f7	02	P						0
10f0					1 DCA						
00f0 100	01 01 00)003a40000 27a	4 00 00 42 43 56		· · · DC/.						
00f0	01 01 00 67 77 76	00 03 a4 00 00 27 a	4 00 00 42 43 Se	00	BCA.						

Gambar di atas merupakan tampilan dari hasil capture protocol wifi yang telah dilakukan pada MNM tadi melalui wireshark. Disitu terlihat nama protokolnya tidak lagi wifi melainkan protokol 802.11. berikut merupakan detail dari paket yang telah tercapture tersebut

■ Frame 2: 326 bytes on wire (2608 bits), 326 bytes capt	ured (2608 bits)					
□ NetMon 802.11 capture header						
Header revision: 2						
Header length: 32	12 1 126527000 To LinkT bd/40/40 Propderet 902 11 226 Paper frame SNL-1969 ENL-0 Elage PL-100					
Operation mode: 0x0000008	12 1.120327000 [p-tink1_bd.40.40 broadcast doz.11 520 beacon name, 514=1008, FN=0, Flags=, BI=100					
PHY type: 802.11g (6)						
Center frequency: 2422 Mhz						
RSSI: -54 dBm	Chieffen 002 11 contine beader					
Data rate: 1.000000 Mb/s	H NELMON 802.11 Capture neader					
Timestamp: 130173867304094222	TEFE 802 11 Person frame Flags:					
IEEE 802.11 Beacon frame, Flags:	* TEEE 602.11 Beacon name, Frays					
Type/Subtype: Beacon frame (0x08)	TEEE 802 11 wireless LAN management frame					
	E IEEE 002.11 WHEress EAN management in ame					
.000 0000 0000 0000 = Duration: 0 microseconds						
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)						
Source address: Tp-LinkT_bd:40:40 (64:70:02:bd:40:40)					
BSS Id: Tp-LinkT_bd:40:40 (64:70:02:bd:40:40)						
Fragment number: 0						
Sequence number: 1828						
	be 0x2c20e6b9]					
IEEE 802.11 wireless LAN management frame						
Fixed parameters (12 bytes)						
Timestamp: 0x00000021C4a10Td						
Beacon Interval: 0.102400 [Seconds]						
Gapabilties Information: 0x0411						
□ lagged parameters (234 bytes)						
■ lag: SSLU parameter set: NN						
□ Jag: Supported Rates 1(5), 2(5), 5.5(8), 11(8), 9, 18, 36, 54, [MDIT/Sec]						
Tag: DS Parameter Set: Current Channel: 1	(soc]					
Tag: Country Information: Country Code ID Environ	/secj ment unknown (0x00)					
Tag: AB Chappel Report: Regulatory Class 22 Chapp	$\begin{bmatrix} 0 & 1 \\ 1 $					
B Tag. AP Channel Report: Regulatory Class 32, Channel List. 5, 6, 7, 8, 9, 0, 7,						
B Tag: Traffic Indication Map (TIM): DTM 0 of 0 bitmap						
Tage interfect interfect of a state of						
B Tag: HT cabilities (802.11n D1.10)						
B Tag: HT Information (802.11n D1.10)						
Tagi and an and a second secon						
I Tag: Vendor Specific: Microsof: WPA Information Element						
B Tag: RSN Information						
■ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element						

Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com

IlmuKomputer.Com

Ikatlah limu dengan menuliskannya

Pada gambar tersebut terdapat empat layer pada detail paketnya yaitu frame, netmon 802.11 capture header, IEEE 802.11 beacon frame, dan IEEE 802.11 Wireless LAN Management Frame. Pada gambar terlihat jika frame tersebut merupakan frame ke 12 dan jika dilihat pada keterangan di dalamnya, terdapat detail-detail dari frame tersebut seperti frame number, frame length, capture length, dll.

Kemudian selanjutnya adalah netmon 802.11 capture header, berisi parameter-parameter dari protokol 802.11 yang digunakan. Disitu terlihat jika PHY type yang digunakan adalah 802.11g. PHY type merupakan tipe dari physical layer yang digunakan. Berarti paket tersebut menggunakan 802.11g sebagai layer fisiknya dimana seperti yang telah diketahui pada teori di atas jika 802.11g merupakan protokol 802.11 yang memiliki frekuensi 2,4Ghz dan Maksimum bandwidth yang bisa dicapai sebesar 54Mbps. Hal itu ditunjukan pada keterangan dibawahnya pada "center frequency" yang menunjukan 2422 MHz (2.422GHz) yang berarti komunikasi data yang digunakan pada pengiriman paket data tersebut bekerja pada frekuensi 2.4 GHz. Selain itu terdapat juga keterangan RSSI, Data rate, dan Timestamp.

RSSI merupakan besarnya sinyal radio yang diterima oleh komputer penerima, disitu tertulis besarnya RSSI adalah -54 dBm yang berarti sinyal yang diterima cukup kuat dan bisa digunakan untuk komunikasi data. Kemudian data rate pada gambar tersebut tertulis 1.0000 Mb/s yang berarti data yang dikirim dengan menggunkan sinyal radio tersebut bisa mengirim 1Mb data pada setiap detiknya. Dan timestamp sendiri merupakan suatu tanda yang diberikan ke tiap paket oleh WinPcap.

Referensi

http://wiki.wireshark.org/CaptureSetup/WLAN#Management_Packets http://www.khaerulanwar.com/jaringan/2012/03/24/23/protokol--wlan/ http://budi.insan.co.id/courses/ec7010/dikmenjur/hari-report.doc



Biografi Penulis

Arsyad Dwiyankuntoko. Sedang menjalankan program D4 Teknik Telekomunikasi di Politeknik Negeri Semarang angkatan 2010

Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com