

Apéndice E - Estudio de seguridad y roaming

E1. Estadísticas completas del estudio de seguridad sin *roaming* utilizando la herramienta Intel PROset/ Wireless Wifi

WPA 2 Empresa en 802.11b sin roaming					
Tipo de autenticación	Protocolo de autenticación	Codificación de datos	Identidad de movilidad Certificación-Validación	Promedio de tiempo en codificación	Promedio de tiempo en tipo de autenticación
PEAP	GTC	TKIP	Usuario -Con-Con	3,835016	3,258713
		AES	Dominio/Usuario -Con-Sin	2,770966	
	MSCHAP v2	TKIP	Dominio/Usuario -Con-Con	3,272262	
		AES	Dominio/Usuario -Con-Con	3,156609	
TTLS	PAP	TKIP	Dominio/Usuario -Sin-Sin	3,059898	2,828770
		AES	Usuario -Sin-Sin	2,968747	
	CHAP	TKIP	Usuario -Con-Sin	2,439644	
		AES	Usuario -Con-Sin	2,653706	
	MSCHAP	TKIP	Dominio/Usuario -Con-Con	3,005530	
		AES	Usuario -Con-Sin	2,845096	
TLS		TKIP	Ninguno -Sin-Sin	3,580577	3,226355
		AES	Ninguno -Con-Sin	2,872134	
WPA 2 Empresa en 802.11g sin roaming					
Tipo de autenticación	Protocolo de autenticación	Codificación de datos	Identidad de movilidad Certificación-Validación	Promedio de tiempo en codificación	Promedio de tiempo en tipo de autenticación
PEAP	GTC	TKIP	Usuario -Con-Sin	3,800514	3,445824
		AES	Dominio/Usuario -Con-Con	3,714832	
	MSCHAP v2	TKIP	Usuario -Con-Sin	3,35306	
		AES	Usuario -Sin-Sin	2,91589	
TTLS	PAP	TKIP	Dominio/Usuario -Con-Sin	3,129671	2,727446
		AES	Dominio/Usuario -Sin-Sin	2,664324	
	CHAP	TKIP	Dominio/Usuario -Con-Con	2,975566	
		AES	Dominio/Usuario -Con-Con	2,488374	
	MSCHAP	TKIP	Dominio/Usuario -Sin-Sin	2,748979	
		AES	Usuario -Con-Sin	2,357765	
TLS		TKIP	Ninguno -Con-Sin	2,621419	2,625980
		AES	Ninguno -Con-Con	2,630542	

Tabla E1 Promedio de tiempos para WPA 2 Empresa sin *roaming*

WPA Empresa en 802.11b sin roaming					
Tipo de autenticación	Protocolo de autenticación	Codificación de datos	Identidad de movilidad Certificación-Validación	Promedio de tiempo en codificación	Promedio de tiempo en tipo de autenticación
PEAP	GTC	TKIP	Dominio/Usuario -Sin-Sin	3,22226	3,04941
		AES	Usuario -Sin-Sin	2,80979	
	MSCHAP v2	TKIP	Dominio/Usuario -Con-Sin	3,08426	
		AES	Dominio/Usuario -Con-Con	3,08131	

TTLS	PAP	TKIP	Usuario -Sin-Sin	2,448277	2,6527525
		AES	Usuario -Con-Con	2,522143	
	CHAP	TKIP	Dominio/Usuario -Sin-Sin	2,540223	
		AES	Usuario -Con-Con	2,602702	
	MSCHAP	TKIP	Dominio/Usuario -Sin-Sin	2,95482	
		AES	Usuario -Con-Con	2,84835	
WPA Empresa en 802.11g sin roaming					
Tipo de autenticación	Protocolo de autenticación	Codificación de datos	Identidad de movilidad Certificación-Validación	Promedio de tiempo en codificación	Promedio de tiempo en tipo de autenticación
PEAP	GTC	TKIP	Usuario -Sin-Sin	2,730486	3,0592915
		AES	Usuario -Sin-Sin	3,116744	
	MSCHAP v2	TKIP	Dominio/Usuario -Con-Sin	3,006565	
		AES	Dominio/Usuario -Con-Con	3,383371	
TTLS	PAP	TKIP	Usuario -Con-Sin	2,964768	2,9457475
		AES	Dominio/Usuario -Con-Con	2,757703	
	CHAP	TKIP	Usuario -Con-Sin	3,006429	
		AES	Usuario -Con-Con	2,787541	
	MSCHAP	TKIP	Usuario -Con-Con	2,783973	
		AES	Dominio/Usuario -Con-Sin	3,374071	
TLS		TKIP	Ninguno -Con-Sin	2,713774	2,9393835
		AES	Ninguno -Con-Sin	3,164993	

Tabla E2 Promedio de tiempos para WPA Empresa sin *roaming*

WPA 2 Personal en 802.11g sin roaming				
Tipo de autenticación	Tamaño de la clave de codificación	Promedio codificación	Promedio tipo	Promedio total
TKIP	10ASCII	3,6519898	2,724512	2,841154
	20ASCII	2,1408466		
	30ASCII	1,870924		
	40ASCII	1,8793286		
	50ASCII	3,2470996		
	63ASCII	3,5568836		
AES	10ASCII	2,7513698	2,957797	
	20ASCII	3,0889892		
	30ASCII	2,3704324		
	40ASCII	3,2599696		
	50ASCII	3,3605438		
	63ASCII	2,9154806		
WPA 2 Personal en 802.11b sin roaming				
Tipo de autenticación	Tamaño de la clave de codificación	Promedio codificación	Promedio tipo	Promedio total
TKIP	10ASCII	2,9611618	2,566261	2,540296
	20ASCII	1,9964082		
	30ASCII	2,8662162		

	40ASCII	2,9548164		
	50ASCII	3,1901672		
	63ASCII	1,4287964		
AES	10ASCII	3,1946018	2,514332	
	20ASCII	2,4459752		
	30ASCII	1,9654974		
	40ASCII	2,6865792		
	50ASCII	2,4118522		
	63ASCII	2,3814874		

Tabla E3 Promedio de tiempos para WPA 2 Personal sin *roaming*

WPA Personal en 802.11g sin <i>roaming</i>				
Tipo de autenticación	Tamaño de la clave de codificación	Promedio codificación	Promedio tipo	Promedio total
TKIP	10ASCII	3,6519898	2,724512	2,841154
	20ASCII	2,1408466		
	30ASCII	1,870924		
	40ASCII	1,8793286		
	50ASCII	3,2470996		
	63ASCII	3,5568836		
AES	10ASCII	2,7513698	2,957797	
	20ASCII	3,0889892		
	30ASCII	2,3704324		
	40ASCII	3,2599696		
	50ASCII	3,3605438		
	63ASCII	2,9154806		
WPA Personal en 802.11b sin <i>roaming</i>				
Tipo de autenticación	Tamaño de la clave de codificación	Promedio codificación	Promedio tipo	Promedio total
TKIP	10ASCII	2,83166	2,688632	2,855502
	20ASCII	2,1160138		
	30ASCII	3,1775464		
	40ASCII	2,1062406		
	50ASCII	2,768904		
	63ASCII	3,1314324		
AES	10ASCII	3,202373	3,022371	
	20ASCII	2,9005058		
	30ASCII	3,074297		
	40ASCII	3,2932542		
	50ASCII	2,8322288		
	63ASCII	2,831573		

Tabla E4 Promedio de tiempos para WPA Personal sin *roaming*

E2. Promedios del estudio de seguridad sin *roaming* utilizando la herramienta Intel PROset/ Wireless Wifi

El siguiente estudio de promedios es el resultado del análisis de la sección E1 vista anteriormente. Se observó los tiempos de autenticación, identidad de itinerancia, certificación y validación, luego según este criterio se creó esta sección en donde se presenta los valores más relevantes y las configuraciones de seguridad que lo permitieron.

Estudio sin seguridad y sin roaming.				
Tipo	Banda de transmisión	Rango de tiempo de asignación de dirección IP	Promedio de banda	Promedio sin seguridad
Sin seguridad	802.11g	0,363844 Hasta 2,356137	1,36448	1,27355
	802.11b	0,377078 Hasta 2,382642	1,18263	

Tabla E5 Estudio de autenticación en configuración abierta con Intel PROset.

Estudio de autenticación tipo empresa sin roaming.					
Característica evaluada		WPA		WPA 2	
Banda de transmisión		802.11b	802.11g	802.11b	802.11g
Rango de tiempo de autenticación		0,316959 Hasta 5,599978	0,407953 Hasta 5,706783	0,217683 Hasta 6.414367	0,372271 Hasta 5,828502
Mejor tipo de autenticación		TTLS	TLS	TTLS	TLS
Mejor protocolo de autenticación		PAP	TTLS+PAP	CHAP	TTLS+MSCHAP
Mejor codificación de datos		AES	TKIP	AES	AES
Mejor identidad de movilidad		**LO\AA	**LO\AA	*AA	**LO\AA
Mejor combinación de seguridad	Certificación	Con	Con	Con	Con
	Validación	Sin	Sin	Sin	Sin
Mejor tiempo promedio alcanzado		1,45128	1,59557	1,06272	1,03992
Mejor tiempo promedio de codificación		2,44827	2,71377	2,43964	2,35776
Mejor tiempo promedio de protocolo		2,44852	2,86123	2,54667	2,55337
Mejor tiempo promedio de tipo		2,65275	2,93938	2,82877	2,62598
Tiempo promedio de banda de Tx		2,78934	2,98147	3,10463	2,93316
Tiempo promedio de WPA ó WPA 2		2,885405		3,018895	
Tiempo promedio de WPA y WPA 2 empresa		2,95215			
Tiempo promedio de autenticación = Tiempo promedio de WPA y WPA 2 empresa – Tiempo de asignación de dirección IP				1,6786	
**LO\AA = LOWENBRAUN\Andres Arce = Dominio\Usuario ↔ *AA = Andres Arce = Usuario: La identidad de movilidad es la Información brindada por el usuario que es necesaria para la autenticación y que es confrontada por el RADIUS en el archivo users.					

Tabla E6 Estudio de autenticación tipo empresa con Intel PROset.

Estudio de autenticación tipo personal sin roaming.					
Característica Evaluada		WPA		WPA 2	
Banda de transmisión		802.11b	802.11g	802.11b	802.11g
Rango de tiempo de autenticación		0,165776 Hasta 4,989438	0,095377 Hasta 5,098085	0,122325 Hasta 4,740382	0,490553 Hasta 4,836425
Mejor codificación de datos		TKIP	TKIP	TKIP	TKIP
Incidencia de tamaño de clave de codificación	Mejor	20 ASCII	40 ASCII	63 ASCII	30 ASCII
	Medio	50 ASCII	63 ASCII	Ninguno	Ninguno
	Bajo o Nulo	40 ASCII y 63 ASCII	10 ASCII y 30 ASCII	30 ASCII y 20 ASCII	40 ASCII y 20 ASCII
Tamaño de la clave de codificación	Mejor	40 ASCII con 2,10624	40 ASCII con 1,21701	63 ASCII con 1,42879	30 ASCII con 1,87092
	Medio	20 ASCII con 2,11601	40 ASCII con 1,40179	30 ASCII con 1,96549	40 ASCII con 1,87933
	Bajo	50 ASCII con 2,76890	63 ASCII con 1,43348	20 ASCII con 1,99640	20 ASCII con 2,14084
Mejor tiempo promedio alcanzado		2,10624	1,21701	1,42879	1,87092
Mejor tiempo promedio de codificación		2,68863	2,24651	2,51433	2,72451
Tiempo promedio de banda de Tx		2,8555	2,42089	2,54029	2,84115
Tiempo promedio de WPA ó WPA 2		2,638195		2,69072	
Tiempo promedio de WPA y WPA 2 personal				2,6644575	
Tiempo promedio de autenticación = Tiempo promedio de WPA y WPA 2 personal – Tiempo de asignación de dirección IP				1,3909	

Tabla E7 Estudio de autenticación tipo personal con Intel PROset.

E3. Estadísticas completas del estudio de seguridad sin *roaming* utilizando Windows XP para la gestión Wi-Fi

Estudio sin seguridad y sin roaming.				
Tipo	Banda de transmisión	Rango de tiempo de asignación de dirección IP	Promedio de banda	Promedio sin seguridad
Sin seguridad	802.11g	0,004175 Hasta 0,546707	0,11517	0,332255
	802.11b	0,010178 Hasta 1,569089	0,54934	

Tabla E8 Estudio de autenticación sin seguridad con Windows.

Estudio de autenticación tipo empresa sin roaming.					
Característica Evaluada		WPA		WPA 2	
Banda de transmisión		802.11b	802.11g	802.11b	802.11g
Rango de tiempo de autenticación		0,108553 Hasta 4,850788	0,106963 Hasta 4,527906	0,105522 Hasta 4,987696	0,127180 Hasta 4,800777
Mejor tipo de autenticación		PEAP	PEAP	PEAP	PEAP
Mejor protocolo de autenticación		MSCHAPV2	MSCHAPV2	MSCHAPV2	MSCHAPV2
Mejor codificación de datos		AES	TKIP	TKIP	TKIP
Mejor identidad de movilidad		**LOVAA	**LOVAA	**LOVAA	**LOVAA
Mejor combinación de seguridad	Certificación	Con	Con	Con	Con
	Validación	Sin	Sin	Sin	Sin

Mejor tiempo promedio alcanzado	0,125357	0,124403	0,12212	0,18677
Mejor tiempo promedio de codificación	0,133354	0,140847	0,65622	0,29489
Mejor tiempo promedio de protocolo	0,21874	0,17092	0,71343	0,63129
Mejor tiempo promedio de tipo	0,21874	0,17092	0,71343	0,63129
Tiempo promedio de banda de Tx	1,38481	1,26715	1,80275	1,66217
Tiempo promedio de WPA ó WPA 2	1,32598		1,73246	
Tiempo promedio de WPA y WPA 2 empresa	1,52922			
Tiempo promedio de autenticación = Tiempo promedio de WPA y WPA 2 empresa – Tiempo de asignación de dirección IP			1,196965	
**LO\AA = LOWENBRAUN\Andres Arce = Dominio\Usuario ↔ *AA = Andres Arce = Usuario: La identidad de movilidad es la Información brindada por el usuario que es necesaria para la autenticación y que es confrontada por el RADIUS en el archivo users.				

Tabla E9 Estudio de autenticación tipo empresa con Windows.

Estudio de autenticación tipo personal sin roaming.					
Característica Evaluada		WPA		WPA 2	
Banda de transmisión		802.11b	802.11g	802.11b	802.11g
Rango de tiempo de autenticación		0,042491 Hasta 5,002628	0,056421 Hasta 4,919293	0,070114 Hasta 4,930975	0,114502 Hasta 4,922479
Mejor codificación de datos		TKIP	TKIP	TKIP	TKIP
Incidencia de tamaño de clave de codificación	Mejor	63 ASCII	40 ASCII	50 ASCII	40 ASCII
	Medio	Ninguno	Ninguno	30 ASCII	63 ASCII
	Bajo o Nulo	10 ASCII Y 20 ASCII	30 ASCII y 50 ASCII	40 ASCII Y 20 ASCII	10 ASCII Y 30 ASCII
Tamaño de la clave de codificación	Mejor	63 ASCII con 1,61776	30 ASCII con 1,55223	50 ASCII con 0,82833	40 ASCII con 1,53178
	Medio	10 ASCII con 1,65418	40 ASCII con 1,84122	30 ASCII con 1,70922	40 ASCII con 1,67407
	Bajo	20 ASCII con 1,75573	40 ASCII con 2,08102	40 ASCII con 1,81668	10 ASCII con 1,85882
Mejor tiempo promedio alcanzado		1,61776	1,55223	0,82833	1,53178
Mejor tiempo promedio de codificación		2,03186	2,25498	2,20193	2,19038
Tiempo promedio de banda de Tx		2,2698	2,33085	2,40194	2,37304
Tiempo promedio de WPA ó WPA 2		2,300325		2,38749	
Tiempo promedio de WPA y WPA 2 personal				2,3439	
Tiempo promedio de autenticación = Tiempo promedio de WPA y WPA 2 personal – Tiempo de asignación de dirección IP				2,011645	

Tabla E10 Estudio de autenticación tipo personal con Windows.

E4. Estadísticas completas del estudio de seguridad con *roaming* utilizando la herramienta Intel PROset/ Wireless Wifi

Autenticación WPA tipo empresa con <i>roaming</i>.									
Banda de transmisión		802.11g				802.11b			
Tipo de autenticación		TLS		PEAP		TTLS		PEAP	
Protocolo de autenticación				MSCHAPV2		PAP		GTC	
Codificación de los datos		TKIP	TKIP	AES	AES	TKIP	TKIP	TKIP	TKIP
Combinación de seguridad	Certificación	Con	Con	Con	Con	Con	Con	Con	Con
	Validación	Sin	Sin	Sin	Sin	Sin	Sin	Sin	Sin
Secuencia de las pruebas		1	2	1	2	1	2	1	2
Tiempo de autenticación en <i>roaming</i> (seg)		0,673	0,587	0,971	0,757	0,614	0,647	1,430	1,376
Tiempo promedio de autenticación en <i>roaming</i> (seg)		0,63		0,864		0,635		1,403	
Tiempo promedio total de autenticación en <i>roaming</i> (seg)		0,883							
Evento de continuidad paquetes perdidos en <i>roaming</i>		2	2	2	1	1	1	3	3
Paquetes perdidos (%)		3	4	4	1	3	2	5	7
Retardo (ms)		32	46	33	38	52	34	70	42
Ancho de banda (Mbits/sec)		3,69	2,8	4,5	4,14	2,34	2,39	1,75	1,73
Señal RSSI en el <i>roaming</i> (dbm)	AP1 (DD-WRT1) Disponible	-86	-88	-83	-77	-85	-82	-89	-84
	AP2 (DD-WRT2) Conectado	-89	-91	-93	-87	-93	-90	-93	-93
Calidad de movilidad		0,658	-1,22	0,469	3,113	-0,67	0,360	-3,26	-5,29
Calidad de <i>roaming</i>		1,658	0,778	2,469	3,113	1,320	1,360	-1,26	-1,29

Tabla E11 Autenticación WPA tipo empresa con *roaming*.

Autenticación WPA tipo personal con <i>roaming</i>.									
Banda de transmisión		802.11g				802.11b			
Tamaño de la clave de codificación		40 ASCII		20 ASCII		20 ASCII		30ASCII	
Codificación de los datos		TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP
Secuencia de las pruebas		1	2	1	2	1	2	1	2
Tiempo de autenticación en <i>roaming</i> (seg)		0,018	0,105	0,022	0,009	0,098	0,179	0,013	0,009
Tiempo promedio de autenticación en <i>roaming</i> (seg)		0,0615		0,0155		0,1385		0,011	
Tiempo promedio total de autenticación en <i>roaming</i> (seg)		0,056							
Evento de continuidad paquetes perdidos en <i>roaming</i>		1	1	2	0	0	0	0	0

Paquetes perdidos (%)	6	3	3	3	3	4	1	1	
Retardo (ms)	32	41	31	33	38	41	39	39	
Ancho de banda (Mbits/sec)	3,45	3,91	4,07	3,99	2,89	2,94	2,88	2,81	
Señal RSSI en el <i>roaming</i> (dbm)	AP1 (DD-WRT1) Disponible	-83	-83	-84	-82	-84	-82	-83	-83
	AP2 (DD-WRT2) Conectado	-93	-93	-93	-91	-92	-91	-91	-91
Calidad de movilidad	-2,58	0,885	1,037	0,959	-0,13	-1,08	1,854	1,784	
Calidad de <i>roaming</i>	2,418	2,885	2,037	3,959	2,863	2,915	2,854	2,784	

Tabla E12 Autenticación WPA tipo personal con *roaming*.

Autenticación WPA 2 tipo empresa con <i>roaming</i> .									
Banda de transmisión		802.11g				802.11b			
Tipo de autenticación		TLS		PEAP		TTLS		PEAP	
Protocolo de autenticación				GTC		CHAP		GTC	
Codificación de los datos		TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP
Combinación de seguridad	Certificación	Con	Con	Con	Con	Con	Con	Con	Con
	Validación	Sin	Sin	Sin	Sin	Sin	Sin	Sin	Sin
Secuencia de las pruebas		1	2	1	2	1	2	1	2
Tiempo de autenticación en <i>roaming</i> (seg)		0,301	0,676	0,428	1,153	0,905	0,773	1,133	0,608
Tiempo promedio de autenticación en <i>roaming</i> (seg)		0,4885		0,7905		0,839		0,8705	
Tiempo promedio total de autenticación en <i>roaming</i> (seg)		0,747							
Evento de continuidad paquetes perdidos en <i>roaming</i>		1	1	3	3	2	1	3	3
Paquetes perdidos (%)		1	1	6	4	5	2	5	5
Retardo (ms)		136	40	51	36	39	55	42	41
Ancho de banda (Mbits/sec)		2,86	3,62	3,67	3,35	2,39	2,3	1,92	1,78
Señal RSSI en el <i>roaming</i> (dbm)	AP1 (DD-WRT1) Disponible	-85	-76	-83	-86	-82	-84	-83	-84
	AP2 (DD-WRT2) Conectado	-91	-88	-92	-92	-91	-93	-92	-92
Calidad de movilidad		1,852	2,595	-2,34	-0,67	-2,63	0,281	-3,10	-3,24
Calidad de <i>roaming</i>		1,852	2,595	0,650	0,322	0,364	1,281	-1,10	-1,24

Tabla E13 Autenticación WPA 2 tipo empresa con *roaming*.

Autenticación WPA 2 tipo personal con <i>roaming</i>.									
Banda de transmisión		802.11g				802.11b			
Tamaño de la clave de codificación		30 ASCII		50 ASCII		63 ASCII		10ASCII	
Codificación de los datos		TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP	TKIP
Secuencia de las pruebas		1	2	1	2	1	2	1	2
Tiempo de autenticación en <i>roaming</i> (seg)		0,175	0,006	0,009	0,004	0,054	0,052	0,078	0,069
Tiempo promedio de autenticación en <i>roaming</i> (seg)		0,0905		0,0065		0,053		0,0735	
Tiempo promedio total de autenticación en <i>roaming</i> (seg)		0,0558							
Evento de continuidad paquetes perdidos en <i>roaming</i>		0	1	1	1	1	0	0	0
Paquetes perdidos (%)		4	3	3	4	1	5	0	2
Retardo (ms)		58	43	33	40	35	35	32	32
Ancho de banda (Mbits/sec)		3,88	2,83	4,27	4,36	2,93	2,93	2,91	2,83
Señal RSSI en el <i>roaming</i> (dbm)	AP1 (DD-WRT1) Disponible	-85	-84	-84	-83	-83	-83	-82	-83
	AP2 (DD-WRT2) Conectado	-93	-93	-92	-90	-91	-93	-90	-91
Calidad de movilidad		-0,13	-0,19	1,239	0,335	1,901	-2,09	2,878	0,798
Calidad de <i>roaming</i>		3,862	1,806	3,239	3,335	1,901	2,901	2,878	2,798

Tabla E14 Autenticación WPA 2 tipo personal con *roaming*.