# Elastix Certified Engineer

## Protocolos SIP/IAX/RTP

Laboratorios



Lab 6 Protocolos SIP / IAX/ RTP Elastix ECT Training

### Protocolos SIP / IAX/ RTP

#### Laboratorio 6.1

Descripción: Realizar la captura de una conversación utilizando la herramienta tcpdump.

Objetivo: Capturar una conversación realizada en nuestro servidor Elastix.

Tiempo Máximo: 15 minutos.

#### Instrucciones:

Tcpdump es una herramienta que permite capturar paquetes recibidos y transmitidos, en tiempo real, en la red en que se encuentra nuestro servidor. Más información sobre esta herramienta en: http://www.tcpdump.org/

Tcpdumb se ejecuta en la línea de comandos y se encuentra incluido en Elastix.

 Ingresamos a la consola como usuario root, y crearemos un directorio para guardar las capturas que realicemos en el servidor.

[root@elastix ~] # mkdir pruebaws

Realizaremos la captura desde el directorio pruebaws

[root@elastix ~] # cd pruebaws

Para realizar la captura utilizaremos el comando:

tcpdump -i any -s0 -w capturaXX.pcap

- Dónde:
- -i any significa que vamos a tomar capturas en todas las interfaces de red.
- -s0 significa que no voy a poner un límite en el tamaño de cada paquete a capturar.
- -w capturaXX.pcap por un lado la opción "-w" indica que los paquetes capturados van a ser almacenados en un archivo "capturaXX.pcap". El archivo puede tener un nombre arbitrario, solo que hay que tener cuidado porque la aplicación puede sobreescribir el archivo, por eso podemos usar XX como el número de captura: 01, 02, 03 .... etc. La extensión ".pcap" en el nombre del archivo.
- Una vez que ejecutemos el comando anterior, el equipo capturará paquetes de todas las interfaces de red. Inmediatamente podemos realizar una llamada desde una de las extensiones creadas (ej: 201 a 202).
- Una vez que terminemos de hablar y cerremos la extensión, presionamos "CTRL + C".
- Ahora copiaremos el archivo capturaXX.pcap para cargarlo posteriormente en wireshark.

#### Laboratorio 6.2

<u>Descripción</u>: En esta práctica utilizaremos la herramienta wireshark para analizar la conversación capturada en el laboratorio anterior.

<u>Objetivo:</u> Adiestrar al estudiante en el uso de sniffers para analizar tráfico RTP y generar y reproducir el payload de una captura de paquetes.

Tiempo Máximo: 10 minutos.

#### Instrucciones:

Wireshark es un programa open source desarrollado para el análisis de protocolos. Es similar en funcionalidad a tcpdump, con la ventaja de que cuenta con una interfaz gráfica y otras características adicionales que permiten un mejor análisis. Más información en: <u>http://www.wireshark.org/</u>

 Primero iniciamos Wireshark y hacemos clic en "Open a previously captured file" e importamos el archivo de captura de la práctica anterior.



**Nota:** Para obtener el archivo facilmente podemos usar un cliente SCP, como: WINSCP, Filezilla, Fugu (Mac)

- En la captura podemos observas diferentes tipos de paquetes, sin embargo nos interesa analizar SIP y RTP.
- Vamos a la pestaña "Telephony" → "VoIP Calls". Allí obtendremos un listado de las llamadas VoIP capturadas con tcpdump, al igual que sus resultados (COMPLETE, REJECTED, CANCEL). Es muy útil si queremos una vista rápida para buscar alguna anomalía en el funcionamiento del sistema, como un proveedor SIP que nos esté rechazando llamadas o problemas comunes como el one-way-audio.

File	Edit V	iew Go Capt	ure Analyze	Statistics Teleph	nony Tools Internals	Help					
E.	ä ()		🗅 🖂 🗶	C 🖴 🔾	( ) 1. 7.			<u>B</u> 🖌	2		
		😣 🗐 🗊 capti	ura01.pcap - Vo	DIP Calls							
Fil	ter:										
No.	Tin					Detected 2 V	oIP Calls. Selected 0 Calls.				
	3 0.0	Start Time 🔻	Stop Time	Initial Speaker	From		То	Protoco	Packets	State	Comments
	4 0.4	3,572059	36,136802	192.168.99.88	204		200	IAX2	66	REJECTED	
	5 1.6	3,842408	34,472885	192.168.99.29	"Juancito" <sip:204@19< td=""><td>92.168.99.29</td><td><sip:26431507@192.168.99.88:49555< td=""><td>SIP</td><td>11</td><td>COMPLETE</td><td>1</td></sip:26431507@192.168.99.88:49555<></td></sip:204@19<>	92.168.99.29	<sip:26431507@192.168.99.88:49555< td=""><td>SIP</td><td>11</td><td>COMPLETE</td><td>1</td></sip:26431507@192.168.99.88:49555<>	SIP	11	COMPLETE	1
	7 2 3										
	8 3.2										
	9 3.5				Total: Calls: 2	2 Start packet	s: 0. Completed calls: 3. Rejected calls: 1	n			
	10 3.5				iotal calor.	- Stare putitet					
	11 3.6		Prepare Filte		Flow		Player Seleccie	onar todo		Cerr	ar
	13 3.6	39331 127 6	0.0.1	127 0 0 1	тср	68 48894	> 5038 [ACK] Seg=1 Ack=223 Win=6	5127 Len=A	TSval=7650	3266 TSecr	=76503266
	15 5.0.				10.	00 10051	· Sobo [Ack] Seq 1 Ack 115 Hill C		15101 7051	-	-,0505200
► Fr	ame 1: 7	8 bytes on wi	re (624 bits)	, 78 bytes capt	tured (624 bits)						
⊳ In	ternet P	rotocol Versi	on 4. Src: 19	92.168.99.88 (19	92.168.99.88). Dst:	192.168.99.29	(192,168,99,29)				
► Tr	ansmissi	on Control Pr	otocol, Src F	Port: 41423 (414	423), Dst Port: ssh	(22), Seq: 1,	, Ack: 1, Len: θ				

 Podemos seleccionar cualquiera de las llamadas (inclusive más de una) e indicarle a Wireshark que realice un diagrama (Flow) de cada paquete intercambiado entre las partes.

ØØG			COO Capt	ura01.pcap - Vo						
File Ed	dit View G	o C						😣 🗆 💿 captura01.pc	ap - Graph Analysis	
	i 🙆 🔛	6					De	10		
		0	Start Time 🔻	Stop Time	Initial Speaker	From		Time	192.168.99.29	Commont
Filter:		_	3,572059	36,136802	192.168.99.88	204		2 942409	INVITE SDP (0711U 0711A GSN	SIP From: "Juancito" <sin:204@192.168.99.29 th="" to<=""></sin:204@192.168.99.29>
No.	Time	S	3,842408	34,472885	192.168.99.29	"Juancit	o" <sip:204@192.16< th=""><th>4 011792</th><th>(5060) 100 Trying</th><th>SIP Status</th></sip:204@192.16<>	4 011792	(5060) 100 Trying	SIP Status
3	3 0.073303	19						4.012269	(5060) 180 Ringing (49555)	SIP Status
4	4 0.403067	19						6.900770	200 OK SDP (g711U telephone	SIP Status
	5 1.695476	Re					Total: Calls: 2 Sta	6.901119	(5060) ACK (49555)	SIP Request
	7 2 315061	10						7.089154	(14314), BTP (07110) (50004)	RTP Num packets:840 Duration:26.840s SSRC:0x
	8 3.246665	19		Prepare Filte	2r	F	low	7.420992	(14314) BYE (50004)	SIP Request
9	9 3.572059	19	2.168.99.88	192.16	8.99.29	IAX2	110 IAX, so	32.127167	(5060) 200 OK (49555)	SIP Status
1/	9 3 572355	10	169 00 70	102 16	9 00 99	TAY2	76 TAY 50	33.069002	(5060) BYE (49555)	SIP Request
▶ Frame	1: 78 byte	s on	wire (624 bit	s), 78 bytes	captured (624	bits)		33.069164	(5060) 200 OK (49555)	SIP Status
Linux	cooked cap	ture	cion 4 Crc.	102 169 00 9	0 (102 169 00	00) Det.	102 169 00 20 /	34.472747	(5060) BYE (49555)	SIP Request
▶ Trans	mission Con	trol	Protocol Src	Port: 41423	(41423) Dst	oo), Ust: Port∙ ssh	(22) Sed: 1 A	34.472885	(5060) 200 OK (49555)	SIP Status
- Turis				10101 12120	(12125))) 550		(12), boq: 1, A			
								C	luardar como	Cerrar

 Como podemos observar, tenemos el diálogo completo entre Elastix y un SIP peer. Si seleccionamos cada paquete podemos analizarlo en detalle, lo que permite hacer un depuramiento intensivo fácilmente. Podemos visualizar los valores de los campos del header SIP e inclusive el SDP como payload del SIP en mensajes como INVITE y 200 OK.

800	captura01.	ncai		ura01 ocao - V							
File Edi	t View Co	C	Cape	anaon.peap - v	on caus				CO Captura01.p		
		<u>~</u>					Detected 2	VoIP Calls.			
	9		Charles Time a	Chas Times	to black and the	Con est		<b>T</b> -	Time	192.168.99.29	
Filtori			Start Time *	Stop Time	inicial Speaker	From		10	Time	192 168 99 88	Comment
Filler.		-	3,572059	36,136802	192.168.99.88	204		200	3.842408	INVITE SDP (9711U 9711A GSN	SIP From: "Juancito" <sip:204< td=""></sip:204<>
No.	Time	S	3,842408	34,472885	192.168.99.29	"Juancito" <sip:204@192< td=""><td>.168.99.29</td><td><sip:264< td=""><td>4.011792</td><td>(5060) (49555)</td><td>SIP Status</td></sip:264<></td></sip:204@192<>	.168.99.29	<sip:264< td=""><td>4.011792</td><td>(5060) (49555)</td><td>SIP Status</td></sip:264<>	4.011792	(5060) (49555)	SIP Status
2156	3.841875	12							4.012269	(5060) 180 Ringing (49555)	SIP Status
2157	3.841988	12							6.900770	200 OK SDP (g/110 telephone	SIP Status
2158	3.842014	12				Table Caller 2	Charles and all all		6.901119	(5060) ACK (49555)	SIP Request
2159	3.842408	19				TOLAL CAUS. 2	Start packe	.s. o comp	7.089154	(14314), BTP (071111), (50004)	RTP Num packets: 790 Durat
2160	3.842482	12		Prepare Filt	er	Flow		Player	7.420992	(14314) BYE	SIP Request
2161	3.842546	12							32 127167	(5060) 200 OK	SIP Status
2162	3.842688	127	.0.0.1	127.0.	.0.1	TCP 346 5038	> 48895 [P	SH, ACK]	33.069002	(5060) BYE (49555)	SIP Request
▶ User Da	tagram Pro	toco	l. Src Port:	sip (5060).	Dst Port: 4955	5 (49555)			33.069164	(5060) 200 OK (49555)	SIP Status
▼ Session	Initiatio	n Pr	otocol			()			34.472747	(5060) BYE (49555)	SIP Request
▶ Reque	st-Line: IM	IVITE	sip:2643150	7@192.168.99.	.88:49555 SIP/2	.Θ			34.472885	(5060) 200 OK (49555)	SIP Status
▼ Messa	ge Header										
▶ Via:	SIP/2.0/U	DP 19	92.168.99.29:	5060;branch=	z9hG4bK13ec770b	;rport					
Max-	Forwards:	70									
▶ From	: "Juancit	o" <:	sip:204@192.1	68.99.29>;ta	g=as000222ff						
▶ T0:	<s1p:26431< td=""><td>507@</td><td>192.168.99.88</td><td>:49555&gt;</td><td></td><td></td><td></td><td></td><td></td><td>· · ·</td><td></td></s1p:26431<>	507@	192.168.99.88	:49555>						· · ·	
Coll	act: <sip:< td=""><td>204@</td><td>192.168.99.29</td><td>:5000&gt;</td><td>02 168 00 20.50</td><td>060</td><td></td><td></td><td></td><td>Curred as a second</td><td>C</td></sip:<>	204@	192.168.99.29	:5000>	02 168 00 20.50	060				Curred as a second	C
	- 102 TNVT	TE	51/408/5100/4	4110774868@1	52.100.55.25.30	100				Guardar Como	Cerrai
User	-Agent: FP	BX-2	8.1(11.4.0)					l			
Date	: Sun. 23	Jun	2013 21:08:53	GMT							
Allo	w: INVITE,	ACK	CANCEL, OPT	IONS, BYE, R	EFER, SUBSCRIBE	, NOTIFY, INFO, PUBLIS	SH .				
Supp	orted: rep	lace	s, timer								
		1									
0000 00	04 00 01 0 60 03 7d e	0 00	52 54 00 8 00 00 40 1	5 <del>69 02</del> 00 00	3 63 1d F. 1d	.KI					
0020 00	a8 63 58 1	3 c4	c1 93 03 69	9 4d d2 49 4e	e 56 49cX.	iM.INVI					
0030 54					) 37 40 TE si	p:2 6431507@					
0040						******					



800												
File Edi	t View Go	С								😣 🗐 🗊 captura01.pca	p - Graph Analysis	
<b>B</b>		ளி					Del	tected 2 \	/oIP Calls.			
			Start Time 🔻	Stop Time	Initial Speaker	From			То	Time	192.168.99.29	Comment
Filter:			3,572059	36,136802	192.168.99.88	204			200	3 942409	INVITE SDP (0711U 0711A GSN	SIP From: "Juancito" <sin:204< td=""></sin:204<>
No.	Time	S	3,842408	34,472885	192.168.99.29	"Juancito	" <sip:204@192.168< td=""><td>3.99.29</td><td><sip:264< td=""><td>4.011792</td><td>(5060) 100 Trying (49555)</td><td>SIP Status</td></sip:264<></td></sip:204@192.168<>	3.99.29	<sip:264< td=""><td>4.011792</td><td>(5060) 100 Trying (49555)</td><td>SIP Status</td></sip:264<>	4.011792	(5060) 100 Trying (49555)	SIP Status
2104	5 502472	10								4.012269	180 Ringing (19555)	SIP Status
2194	5 657866	10								6.900770	200 OK <u>SDP (g711U tel</u> ephone	SIP Status
2196	5.700062	RC								6.901119	(5060) ACK (49555)	SIP Request
2197	6.900770	19					Total: Calls: 2 Sta	rt packet	s:0 Comp	7.089154	(14314), RTP (g711U) (50004)	RTP Num packets:840 Durat
2198	6.901119	19		Prepare Filt	er	F	ow		Player	7.420992	(14314) RTP (0/110) (50004)	RTP Num packets:790 Durat
2199	6.901265	12								32.126962	(5060) 200 OK (49555)	SIP Request
2200	6.901276	12	7.0.0.1	127.0.	0.1	TCP	68 48894 >	5038 [AG	CK] Seq=1	33,069002	(5060) BYE (49555)	SIP Request
-			1							33.069164	(5060) 200 OK (49555)	SIP Status
V Session	Initiatio									34.472747	(5060) BYE (49555)	SIP Request
▼ Messa	ne Header	/2.0	5 200 OK							34.472885	(5060) 200 OK (49555)	SIP Status
▶ Via:	SIP/2.0/U	)P 1	92.168.99.29:	5060:rport=5	060:received=19	92.168.99.	29:branch=z9hG4b	K13ec77	9b			
Call	-ID: 03b061	Ld47	8f74ca731be74	4f167748ea@1	92.168.99.29:50	960						
▶ From	: "Juancito	o" <	sip:204@192.1	68.99.29>;ta	g=as000222ff							
▶ To:	<sip:264315< td=""><td>507@</td><td>192.168.99.88</td><td>&gt;;tag=.CeTMw</td><td>BgHHQj2rN-KdWpI</td><td>WUIJtKsI92</td><td>5B</td><td></td><td></td><td></td><td></td><td></td></sip:264315<>	507@	192.168.99.88	>;tag=.CeTMw	BgHHQj2rN-KdWpI	WUIJtKsI92	5B					
► CSeq	: 102 INVI	ΓE									· · · · · · · · · · · · · · · · · · ·	
Serv	er: Blink (	9.3.	1 (Linux)							G	lardar como	Cerrar
ALLO	W: SUBSCRIE	5E,	NUTIFY, PRACK	, INVITE, AC	K, BYE, CANCEL	, UPDATE,	MESSAGE, REFER					
Supr	act: <sip: <="" td=""><td>2045 cel</td><td>replaces no.</td><td>99.00:493332&gt; refersub ar</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></sip:>	2045 cel	replaces no.	99.00:493332> refersub ar								
Cont	ent-Type: a	annl	ication/sdp	rerersus, gr	uu							
Cont	ent-Length	1	236									
▶ Messa	ge Body											
0000 00	00 00 01 0	0 06	i 2e 1d b5 3a	a al 79 00 00	08 00	:.v.						

 Wireshark también puede reproducir un audio con los paquetes RTP de la llamada seleccionada. Cerramos el diagrama, y hacemos clic "Player" en la llamada seleccionada y luego en "Decode".



- Como podemos observar, tenemos el audio completo, tanto el upstream y downstream que pasó por la interfaz de red de nuestro Elastix. Podemos analizar el flujo y hasta reproducir el mismo. Esto nos permite, por ejemplo, determinar que un problema de corte de llamadas no es por causa de Elastix.
- También podemos hacer un análisis sobre el flujo de RTP de cada llamada capturada. Vamos a "Telephony → RTP → Show All Streams" y allí tenemos todos los flujos de RTP capturados por tcpdump. Los mismos podemos diferenciarlos por su IP y SSRC.

File Edit	View Go Captur	e Analyze	Statistics Te	lephony To	ools Internal	Help							
🗐 🌺	🚉 🔍 🕍 📔	🗅 🔝 🗙	C 🔒 🛛	Q 🔇	> 🕹 Ŧ				• 🖬 🕅 🚦	3 💥 🕐			
Filter:					Expression	Clear Apr	olv Gua	rdar					
No.	😣 🗐 🗐 🛛 Wiresha	rk: RTP Str	eams										
2156 3				Detected		Chaosa ana far	Forward	and coverse d	lisection for analysi	-			
2157 3				Detected	Z RTP streams.	Choose one for	rorward	and reverse d	irrection for analysi	5			503468
2158 3	Src IP addr 🔻	Src port	Dst IP addr	Dst porl	SSRC	Payload	Packet	Lost	Max Delta (ms)	Max Jitter (m:	Mean Jitter (ms	Pb?	
2159 3	192.168.99.29	14314	192.168.99.88	50004	0x15EE844D	g711U	790	0 (0.0%)	99.78	41.17	32.38	х	
2160 3	192.168.99.88	50004	192.168.99.29	14314	0x33D7671C	g711U a	840	350 (29.4%)	1187.92	195.84	41.19	х	503469
2161 3													
2162 3													503469
▼ Messag	e												
▼ Sessi													
Ses	s												
► Own	e												
Ses	5												
► Con	n												
▶ Tim	e												
▶ Med	1				Select a for	ward stream wit	h left mo	use button, a	nd then				
▶ Med	1				Select a r	everse stream w	ith Ctrl +	left mouse bu	utton				
Med ▶ Med	1		Unse	elect F	Find Reverse	Guardar como	Mark	Packets P	repare Filter	Copiar A	Analyze Ce	rrar	
▶ Med	ia ALLTIDULE TAT:	rtomap:10	L Letephone-e	vent/8000									
► Med	ia Attribute (a):	fmtp:101 (	9-16	,									
▶ Med	ia Attribute (a):	ntime 20											

 Como podemos observar en la imagen, tenemos datos fundamentales acerca de la calidad de cada stream, como el porcentaje de paquetes perdidos, el diferencial de jitter, el máximo valor de jitter presente, etc. Además podemos analizar el stream paquete por paquete, para ello debemos seleccionar un stream y elegir "Analyze".

				Detected	2 RTP streams	Choose	one for forw	ard and reverse o	direction for	analysi	s		
Src IP addr 🛛 🔻	Src p	oort	Dst IP addr	Dst port	SSRC	Payload	Packe	t Lost	Max Delta	(ms)	Max Jitter (m:	Mean Jitter (ms	Pb?
192.168.99.29	1431	4	192.168.99.88	50004	0x15EE844D	g711U	790	0 (0.0%)	99.78		41.17	32.38	x
192.168.99.88	5000	4	192.168.99.29	14314	0x33D7671C	g711U	840	350 (29.4%)	1187.92		195.84	41.19	X
		80	Wireshar	k: RTP Stro	eam Analysis								
		Forw	ard Direction	Reverse	d Direction								
				Analysin	g stream from	192.168.9	99.88 port 50	004 to 192.168.9	99.29 port 14	4314 S	SRC = 0x33D7671C		
		Pack	▼ Sequen	Delta(n	Filtered Jitter	(ms)	Skew(ms)	IP BW(kbps	) Mar	k St	atus		
		2425	12187	1.12	23.99		55.26	44.80		[C	ik j		
		2426	12188	0.01	23.74		75.26	46.40		[C	lk ]		
		2435	12189	82.16	26.14		13.10	48.00		[0	ik ]		- 1
		2437	12190	0.28	25.74		32.82	49.60		[0	•k]		
		2438	12191	0.01	25.38		52.81	51.20		[0	lk]		
		2445	12192	0.55	25.01		72.27	52.80		[0	)k]		
		2454	12194	75.75	25.68		36.51	54.40		W	rong sequence nr.		_
e Description, a	tive	2455	12195	0.00	25.32		56.51	56.00		[0	•k ]		
lia Description, I	name	2461	12196	63.54	26.46		12.96	57.60		[0	lk]		
lia Attribute (a)	: rti	2464	12197	0.23	26.04		32.73	59.20		[0	k]		
lia Attribute (a)	: rtį	2465	12198	0.00	25.67		52.72	60.80		[0	k]		
lia Attribute (a)	: rtj	2481	12199	0.98	25.25		71.75	62.40		[0	k]		
lia Attribute (a)	fm:	2482	12200	0.00	24.92		91.74	64.00		[0	)k]		
lia Attribute (a)	Dt:	2487	12201	66.61	26.28		45.14	65.60		[0	k]		
lia Attribute (a)	sei	2492	12202	0.25	25.87		64.89	67.20		[0	k]		
04 00 01 00 06 5 60 03 7d 64 4d 0 a8 63 58 13 c4 c 45 20 73 69 70 3 me (frame), 909 byte	2 54 9 00 1 93 a 32			Max del Max jitt Max ske Total RT Duratio	ta = 1187.92 ms er = 195.84 ms. w = -5429.38 m P packets = 119 n 26.84 s (-3037	at packe Mean jitt 5. 10 (expe ms clock	et no. 4765 er = 41.19 m cted 1190) L drift, corres	ost RTP packets	= 350 (29.41 Hz (-11.32%)	%) Sec	juence errors = 79		

Como podemos observar, en este punto también podemos escuchar el Stream o descargarlo como un archivo de audio.

#### Laboratorio 6.3

<u>Descripción</u>: En este laboratorio configuraremos el uso de TLS (Seguridad en la Capa de Transporte) y SRTP (Encripción de la Voz) utilizando el softphone blink.

Objetivo: Configurar encriptación de audio en Elastix.

Tiempo Máximo: 40 minutos.

#### Instrucciones:

 Ingresamos a nuestra consola y nos colocamos en el directorio /etc/asterisk, una vez ahí debemos crear una carpeta llamadas keys. Para esto ejecutamos el siguiente comando:

mkdir keys

Luego nos dirigimos al siguiente directorio:

/usr/share/doc/asterisk-x.x.x/contrib/scripts/

Nota: el directorio asterisk-x.x.x corresponde a la versión de Asterisk actual. Para determinar con exactitud la versión podemos ejecutar el siguiente comando desde consola: asterisk vvvr, ejemplo: [root@ecte ~]# asterisk -vvvr Asterisk 1.8.20.0, Copyright (C) 1999 - 2012 Digium, Inc. and others. Created by Mark Spencer <markster@digium.com> Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details. This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details. \_\_\_\_\_ Connected to Asterisk 1.8.20.0 *cerembly* running on ecte (pid = 2903) Verbosity is at least 3 ecte\*CLI> Directorio: /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/

 Una vez que nos encontramos en el directorio, ejecutamos el siguiente comando para generar los certificados que serán utilizados por asterisk:

./ast\_tls\_cert -C pbx.mycompany.com -0 "mycompany" -d /etc/asterisk/keys

**Nota:** En este caso, pbx.mycompany.com es el hostname de nuestro servidor ("mycompany" es un comentario). Podemos verificar el hostname ingresando al archivo /etc/sysconfig/network. Es necesario además adicionar la siguente línea al final del archivo /etc/hosts: IP\_del\_servidor server server.example.com, donde server.example.com es el hostname, Ej: IP = 192.168.5.93, hostname = test.elastix.com -> 192.168.5.93 test test.elastix.com.

- Durante el proceso nos pedirá ingresar una clave y su validación un par de ocasiones, la escribimos y presionamos enter para continuar. Esta clave es la contraseña que utilizaran nuestros certificados de asterisk.
- Ahora, desde el mismo directorio, ejecutamos el siguiente comando para generar los certificados que serán utilizados por nuestros teléfonos:

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k
/etc/asterisk/keys/ca.key -C phone.mycompany.com -0 "mycompany" -d
/etc/asterisk/keys -o phone
```

**Nota:** Este comando crea certificados para los teléfonos que lo requieran, sin embargo hay muchos teléfonos que traen un certificado self signing. Tomando el ejemplo de hostname anterior (test.elastix.com), podemos reemplazar phone.mycompany.com por phone.elastix.com.

- Nos solicitará una clave, es la misma que usamos para Asterisk.
- Nos dirigimos al directorio /etc/asterisk/keys y validamos que los archivos estén generados:

```
[root@ecte keys]# 11
total 48
-rw------ 1 root root 1212 Jun 2 13:09 asterisk.crt
-rw------ 1 root root 574 Jun 2 13:09 asterisk.csr
-rw------ 1 root root 887 Jun 2 13:09 asterisk.key
-rw------ 1 root root 155 Jun 2 13:09 asterisk.pem
-rw------ 1 root root 1753 Jun 2 13:09 ca.crt
-rw------ 1 root root 3311 Jun 2 13:09 ca.key
-rw------ 1 root root 578 Jun 2 13:10 phone.crt
-rw------ 1 root root 887 Jun 2 13:10 phone.key
-rw------ 1 root root 2103 Jun 2 13:10 phone.pem
-rw------ 1 root root 124 Jun 2 13:10 tmp.cfg
```

Es necesario cambiar el propietario y el grupo de archivos a Asterisk, y habilitar todos los permisos

```
[root@test keys]# 11
total 48
-rwxrwxrwx 1 asterisk asterisk 1196 Feb 9 15:34 asterisk.crt
-rwxrwxrwx 1 asterisk asterisk 566 Feb 9 15:33 asterisk.csr
-rwxrwxrwx 1 asterisk asterisk 891 Feb 9 15:33 asterisk.key
-rwxrwxrwx 1 asterisk asterisk 2087 Feb 9 15:34 asterisk.pem
-rwxrwxrwx 1 asterisk asterisk 150 Feb 9 15:32 ca.cfg
-rwxrwxrwx 1 asterisk asterisk 1736 Feb 9 15:33 ca.crt
-rwxrwxrwx 1 asterisk asterisk 3311 Feb 9 15:33 ca.key
-rwxrwxrwx 1 asterisk asterisk 1204 Feb 9 15:40 phone.crt
-rwxrwxrwx 1 asterisk asterisk 887 Feb 9 15:40 phone.key
-rwxrwxrwx 1 asterisk asterisk 887 Feb 9 15:40 phone.key
-rwxrwxrwx 1 asterisk asterisk 2091 Feb 9 15:40 phone.pem
-rwxrwxrwx 1 asterisk asterisk 1204 Feb 9 15:40 phone.crt
```

 Ahora activamos TLS en Elastix. Para realizar esta tarea es necesario entrar a FreePBX, para lo cual activamos su acceso en la interfaz de administración de Elastix en "Seguridad → Configuraciones Avanzadas":

7	elastix									619	i * 1
		Sistema	Agenda	Correo Electrónico	Fax	PBX	IM	Seguridad 🧹			
	Cortafuegos Auditoría	Claves I	Débiles Config	juraciones Avanzadas							
)	🔀 Conf. Avanzada										★ ?
	Información:	a ba sido babil	itado								Dismiss
	Guardar										
	Habilitar accesos					Cambiar Con	traseña				
	Habilitar acceso directo (No	o embebido) a	FreePBX®:?	ON		Contraseña B	ase de Datos y	Administración We	b FreePBX®: <u>?</u>	[	
	Activar llamadas SIP anóni	mas:	[	OFF		Confirmación	de la Contrase	eña:			
				Elastix is licensed	under GPL by	PaloSanto Solution	ns. 2006 - 2015.				

- Una vez que activamos FreePBX ingresamos a la interfaz en el siguiente enlace: <u>https://ip-de-su-servidor/admin</u>, el usuario es admin y la contraseña es la que configuramos al instalar Elastix.
- Al ingresar vamos a la siguiente ruta "Settings → Asterisk SIP Settings".
- Primero configuramos la sección "NAT Settings" y seleccionamos la opción "Public IP".

NAT Settings			
NAT	yes no	never	route
IP Configuration	Public IP	Static IP	Dynamic IP

Luego en la sección "Advanced General Settings" ingresamos los siguientes parámetros:

tlsenable=yes tlsbindaddr=0.0.0.0 tlsdontverifyserver=yes tlscertfile=/etc/asterisk/keys/asterisk.pem tlscafile=/etc/asterisk/keys/ca.crt

Advanced General Settings		
Language Default Context Bind Address Bind Port Allow SIP Guests Allow Anonymous Inbound SIP Calls	Sí No Sí No	
SRV Lookup	Habilitado De	shabilitado
Call Events	Sí No	
Other SIP Settings	tisenable	= yes
	tlsbindaddr	= 0.0.0.0
	tlsdontverifyserver	= yes
	tlscertfile	= /etc/asterisk/keys/aster
	tlscafile	= /etc/asterisk/keys/ca.cr
	Add Field	
Enviar cambios		

Una vez que hemos ingresado los datos hacemos clic en "Enviar cambios" y luego aplicaciomos los cambios.

**Nota:** Si no aplicamos los cambios, los campos que hemos agregado no se incluirán en el archivo /etc/asterisk/sip\_general\_additional.conf

#### Encriptación con SRTP

 Ahora, en la interfaz de administración, vamos a PBX → Configuración PBX → Extensiones. Ingresamos a cualquiera de las extensiones y en la sección Device Options configuramos el campo "encryption" seleccionando "SRTP only":

transport <sup>©</sup>		UDP Only \$
avpf		No 🛊
icesupport <sup>@</sup>		No 🛊
encryption <sup>©</sup>	$\longrightarrow$	Yes (SRTP only) \$

- Para esta práctica usaremos cualquiera de las extensiones que hemos configurado anteriormente.
- Es importante mencionar que la habilitación de SRTP no es un standard en todos los endpoints. Cada endpoint puede tener una manera diferente de habilitar esta funcionalidad y es importante contactar al fabricante para verificar primero que el endpoint soporta SRTP y TLS y además como se configura.
- En el caso de un teléfono fanvil X5 la configuración se realiza en la sección advanced de la cuenta SIP en el campo "RTP Encryption", el cual se debe habilitar.

Fanvil		English 💠 Dial	Logout Answer	( admin ) Hang Up
	SIP Dial Peer Dial Plan Global Settings			
> SYSTEM	SIP Line SIP 2 +			
> NETWORK	Basic Settings >>			
> LINES	Codecs Settings >>			
	Advanced SIP Settings >>			
> PHONE	Always Forward Enable Hotline			
	Always Fwd Number Hotline Number			
	Busy Forward Warm Line Wait Time 0 (0~9)second(s)			
PHONEBOOK	Busy Fwd Number Keep Alive Type UDP +			
	No Answer Forward Keep Alive Interval 30 second(s)			
> CALL LOGS	NoAnswer Fwd Number BLF Server			
	No Ans. Fwd Wait Time 5 (0~120)second(s) Transfer Timeout 0 second(s)			
> FUNCTION KEY				
	SIP Encryption Enable Auto Answer			
	SIP Encryption Key Auto Answer Timeout 5 second(s)			
	RTP Encryption			
	RTP Encryption Key Session Timeout 0 second(s)			

 En el caso de un cliente Bria (Counterpath) para iOS, la configuración se realiza en la cuenta en Opciones avanzadas de la cuenta → Transporte y Seguridad → Encriptar audio

Opciones avanzadas d	e la cuenta
TRANSPORTE Y SEGURIDAD	
Transporte de SIP	UDP >
Encriptar audio	Nunca >
REGISTRO SIP	
Llamadas entrantes	
Intervalo de actualización W	900
Intervalo de actualización m	900
MANTENER ACTIVO	
Intervalo de Wi-Fi	30
Intervalo celular	30
Teléfono Contactos Historial	Configuración

- Configuraremos el softphone Blink para Windows, el cual incluye soporte para SRTP y TLS en sus versiones gratuitas.
- En la sección "Media", en el campo "sRTP Encryption" seleccionamos mandatory

G Blink Preferences	
Accounts	
💱 Bonjour	Account Information Media Server Settings Network Advanced
305@192.168.2.101	Audio Codecs Video Codecs
	✓ G722           ✓ speex           GSM           I.BC           ✓ PCMU           ✓ PCMA
	Reset Note: drag codecs to change their order Reset
	RTP Options
	Send inband DTMF
	sRTP Encryption: mandatory V
+ -	

Procedemos a configurar los siguientes parámetros en server settings

G Blink Preferences							- • •
Accounts Audio Logging Advanced							
😵 Bonjour	Account Information	Media	Server Settings	Network	Adv	anced	
305@192.168.2.101	SIP Proxy						
		Always	use my proxy for	outgoing sea	ssions		
	Outbound Proxy:	192.168.2	2.101		Port:	5060 ≑	Transport: UDP 🔻
	Auth Username:	305					
	MSRP Relay						
		Always	use my relay for o	utgoing ses	sions		
	MSRP Relay:	Relay add	ress taken from DN	IS	Port:	2855 🌲	Transport: TLS 🔻
	Extra Server Setting	js					
	Voicemail URI:	Discovere	d by subscribing to	305@192.1	.68.2.10	1	
	XCAP Root URL:	Taken from	n the DNS TXT reco	ord for xcap.	192.168	3.2.101	
	Server Tools URL:						
	Conference Server:						
+ -							]

• En la sección "Advanced", del menú "Accounts", editamos las opciones Register interval, Publish interval y Subscribe interval, tal como se muestra en la figura.

dar i a c	
G Blink Preferences	
Accounts Audio Logging Advanced	
😵 Boniour	Account Information Media Server Settings Network Advanced
305@192.168.2.101	
	SIP Settings
	Register interval: 600 🚔 seconds 🐼 Re-register
	Publish interval: 3600 🖉 seconds
	Subscribe interval: 3600 🛓 seconds
	Dialing landline and mobile numbers
	Replace preceding + with: +
	External line prefix: None
	TLS Settings
	Certificate File: Browse
	Verify server
+ -	

- Una vez que hemos realizado las configuraciones correspondientes, realizaremos una captura entre las extensiones de prueba usando tcpdumpba.
- Obtenemos el archivo de la captura desde nuestro servidor Elastix e iniciamos Wireshark, luego hacemos clic en "Open a previously captured file" y seleccionamos el archivo de la captura.

**Nota:** Es necesario obtener el archivo de nuestro servidor Elastix, cuando sea necesario. Al igual que en el laboratorio 6.2, podemos usar usar un cliente SCP.

📶 сар	tura1b.pcap [Wir	eshark 1.8.5 (SVN Rev 47350	from /trunk-1.8)]		
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statis</u>	tics Telephony <u>T</u> ools <u>I</u> nterr	nals <u>H</u> elp	
8		🖻 🐻 🗙 🎜 🛛	् 🐐 🔿 🖥 🛃		0. 🗹   🖉 🖻 🎭   💢
Filter:			▼ E	xpression Clear A	pply Save
No.	Time	Source	Destination	Protocol	Length Info
	1 0.000000	192.168.2.101	192.168.2.27		108 Encrypted response packet len=52
	2 0.000012	192.168.2.101	192.168.2.27	SSH	188 Encrypted response packet len=132
	3 -0.00003	9 192.168.2.27	192.168.2.101	TCP	62 55569 > ssh [ACK] Seq=1 Ack=53 Win=63676 Len=C
	4 0.012923	PortechC_01:00:	dc	ARP	62 Who has 192.168.1.13? Tell 192.168.1.130
	5 0.044122	X1amenye_13:b0:	8T	ARP	62 Who has 192.168.1.100? Tell 192.168.1.232
	7 0 067809	192.100.1.100	192.108.2.101	тср	68 34305 S http [ACK] Seg=1 Ack=50 Win=365 Len=0
	8 0 068095	192.168.1.168	192.168.2.101	тср	85 [TCP segment of a reassembled PDU]
	9 0.068108	192.168.2.101	192.168.1.168	TCP	68 34305 > http [ACK] Seg=1 Ack=67 Win=365 Len=0
	10 0.068520	192.168.1.168	192,168,2,101	TCP	109 [TCP segment of a reassembled PDU]
	11 0.068540	192.168.2.101	192.168.1.168	TCP	68 34305 > http [ACK] Seq=1 Ack=108 win=365 Len=0
	12 0.068804	192.168.1.168	192.168.2.101	TCP	92 [TCP segment of a reassembled PDU]
	13 0.068814	192.168.2.101	192.168.1.168	TCP	68 34305 > http [ACK] Seq=1 Ack=132 Win=365 Len=0
	14 0.069095	192.168.1.168	192.168.2.101	TCP	94 [TCP segment of a reassembled PDU]
	15 0.069104	192.168.2.101	192.168.1.168	TCP	68 34305 > http [ACK] Seq=1 Ack=158 Win=365 Len=0
	16 0.069357	192.168.1.168	192.168.2.101	TCP	70 [TCP segment of a reassembled PDU]
	17 0.069382	192.168.2.101	192.168.1.168	ICP	68 34305 > http  ACK  Seg=1 ACK=160 W1n=365 Len=0
·					,
🕀 Fra	ame 1: 108 b	ytes on wire (864 b	oits), 108 bytes captu	red (864 bits)	
0000	00 04 00 01	00 06 00 0d 97 f	7 cd 4f 00 00 08 00	0	
0010	45 10 00 50	d1 52 40 00 40 0	6 e3 68 c0 a8 02 65	F.,\.R@, @,.h.	e
0020	c0 a8 02 1	00 16 d9 11 d5 6	0 a6 67 0d 00 92 d8		•••
0030	50 18 32 40	) ad fd 00 00 fd 3	5 4e 16 94 e8 a8 ca	P.2@5N	
0040	bh 8h he di	3 4T 34 31 70 TO 3 5 d6 9F e3 F9 c3 d	0 37 93 34 Ta 20 0a 9 39 dc ed 8h h1 c1	504Qp .6W.4	. «]
0060	c1 07 d8 a	3 24 e3 a7 a7 10 1	0 f0 c8		
0	File: "C:\Users\Le	nín\Desktop\captura1b.pc	. Pa Profile: Default		

■ En Wireshark vamos a "Telephony → VoIP Calls", allí vamos a obtener un listado de las llamadas VoIP junto a su resultado (COMPLETE, REJECTED, CANCEL).

📶 captura1b.pcap -	VoIP Calls						- • •
			Detected 2	VoIP Calls. Selected 2 Calls			
Start Time 🔺	Stop Time 🔹	Initial Speaker	From	▲ To	Protocol     Packets	State Com	nments 🔹
176.529136	218.247960	192.168.2.27	"Lenín" <sip:305@192.< td=""><td>168 <sip:304@192.168.2.101< td=""><td>SIP</td><td>11 COMPLETED</td><td></td></sip:304@192.168.2.101<></td></sip:305@192.<>	168 <sip:304@192.168.2.101< td=""><td>SIP</td><td>11 COMPLETED</td><td></td></sip:304@192.168.2.101<>	SIP	11 COMPLETED	
179.240950	217.963572	192.168.2.101	"305" <sip:305@192.16< td=""><td>8.2. <sip:46372159@192.168< td=""><td>3.2.: SIP</td><td>6 COMPLETED</td><td></td></sip:46372159@192.168<></td></sip:305@192.16<>	8.2. <sip:46372159@192.168< td=""><td>3.2.: SIP</td><td>6 COMPLETED</td><td></td></sip:46372159@192.168<>	3.2.: SIP	6 COMPLETED	
•				III			•
	Prepare Filter	F	Total: Calls: 2 Start pack	ets: 0 Completed calls: 2 F	Rejected calls: 1 Select <u>A</u> ll	Close	

 Seleccionamos cualquiera de las dos llamadas y hacemos clic en "Player" y luego en "Decode". Al hacerlo nos damos cuenta que no es posible entender lo que los participantes de la llamada estaban conversando en el momento.

184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         184 s       185 s       186 s       187 s       188 s       189 s       190 s <t< th=""><th>daptura1b.pcap - VoIP - RTP Player</th><th></th><th></th><th></th><th></th><th></th><th>- • •</th></t<>	daptura1b.pcap - VoIP - RTP Player						- • •
184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         Image: From 192.168.2.27:54465 to 192.168.2.101:12428       Duration:34.65       Drop by Jitter Buff:0(0.0%)       Out of Seq: 1(0.1%)       Wrong Timestamp: 1723(99.9%)         Image: From 192.168.2.27:54465 to 192.168.2.101:12428       Duration:34.65       Drop by Jitter Buff:0(0.0%)       Out of Seq: 1(0.1%)       Wrong Timestamp: 1723(99.9%)         Image: From 192.168.2.27:54465       Transformed and the second							
From 192.168.2.27:54465 to 192.168.2.101:12428 Duration:34.65 Drop by Jitter Buff:0(0.0%) Out of Seq: 1(0.1%) Wrong Timestamp: 1723(99.9%)          184 s       185 s       186 s       187 s       188 s       189 s       190 s       191 s         • <td< td=""><td>184 s 185 s</td><td>186 s</td><td>187 s</td><td>188 s</td><td>189 s</td><td>190 s</td><td>191 s</td></td<>	184 s 185 s	186 s	187 s	188 s	189 s	190 s	191 s
From 192.168.2.27:54465 to 192.168.2.101:12428       Duration:34.65       Drop by Jitter Buff:0(0.0%)       Out of Seq: 1(0.1%)       Wrong Timestamp: 1723(99.9%)         Image: State Stat							
184  s  185  s  186  s  187  s  188  s  189  s  190  s  191	From 192.168.2.27:54465 to 192.168	3.2.101:12428 Duratio	on:34.65 Drop by	litter Buff:0(0.0%)	Out of Seq: 1(0.1%)	Wrong Time	stamp: 1723(99.9%
184 s         185 s         186 s         187 s         188 s         189 s         190 s         191 s           Image: Construction of the state of the						. <u></u>	
From 192.168.2.101:12428 to 192.168.2.27:54465 Duration:34.41 Drop by Jitter Buff:9(0.5%) Out of Seq: 0(0.0%) Wrong Timestamp: 1713(99.4%) View as time of day	184 s 185 s	186 s 1	87 s	188 s	189 s 1	90 s	191 s
From 192.108.2.101:12428 to 192.108.2.27:54465 Duration:34.41 Drop by Jitter Buff:9(0.5%) Out of Seq: 0(0.0%) Wrong Timestamp: 1/13(99.4%) View as time of day.				D	0		
View as time of day	From 192.108.2.101:12428 to 192.10	8.2.27:54465 Duratio	on:34.41 Drop by	htter Buff:9(0.5%)	Out of Seq: 0(0.0%)	wrong Time	stamp: 1713(99.47
	1		View as time	e of day			
Jitter buffer [ms] 50 🛓 🔲 Use RTP timestamp Decode Play Pause Stop Close	Jitter buffer [ms] 50 🛓 🔲 Use R	TP timestamp	Decode	<u>P</u> lay	P <u>a</u> use	<u>S</u> top	<u>C</u> lose
							н

La imagen anterior muestra la incorporación de ruido al canal de audio.

#### **Usando TLS**

- Ahora, usaremos TLS junto con SRTP y realizaremos una captura.
- Habilitamos transport=tls en la extension (PBX → PBX Configuration → Extensions) tal como se muestra en la figura.

transport	<b></b>	TLS Only \$
avpf		No 🛊
icesupport		No 🗘
encryption <sup>©</sup>		Yes (SRTP only) \$

 Es hora de subir el certificado creado en nuestro servidor Elastix en blink. Nos dirigimos a la parte superior al menú "Advanced", hacemos clic en "Browse" y subimos el archivo ca.crt.

G Blink Preferences			
Accounts Audio Loggi	ng Advanced		
SIP and RTP settings			
Transports:	Enable UDP UDP por	t: Auto 🌻 Note: set SIP ports to 0 for automatic allocation	
	Enable TCP TCP por	t: Auto 🜲	
	Enable TLS TLS por	t: Auto ≑	
RTP Ports:	500 🚔 starting a	t: 50000 🌩	
Session Timeout:	90 🚖 seconds		
RTP Timeout:	30 seconds		
TLS Settings			
Certificate Authority File:	C:\Users\Lenín\Desktop\ca.cr	t	Browse
Connection Timeout:	3,0 🚔 seconds		
L			

 Luego vamos a la cuenta y en la sección "Server Settings" editamos el puerto al 5061 y la opción TLS en "Transport".

🐨 Bonjour	Account Information	Media Server Settings	Network Ad	vanced	
305@192.168.2.101	SIP Proxy				
		Always use my proxy for a	outgoing sessions		
	Outbound Proxy:	192.168.2.101	Port:	5061 🚔 Trans	port: TLS
	Auth Username:	305			
	Мэкр кенау				
	MSDD Delay	Always use my relay for o	utgoing sessions	DOLL A Tranc	
	Moke Keldy:	Relay address taken from DN	Port	2855 V Irans	port: 115
	Extra Server Setting	5			
	Voicemail URI:	Discovered by subscribing to	305@192.168.2.1	01	
	XCAP Root URL:	Taken from the DNS TXT reco	rd for xcap. 192. 16	8.2.101	
	Server Tools URL:				
	Conference Server:				

Repetimos el procedimiento en ambas extensiones.

**Nota:** En el caso de la versión de Blink para Mac, la configuración se debe realizar en Avanzado  $\rightarrow$  Señalización SIP. En el campo proxy primario es necesario colocar IP\_Servidor:5061;transport=tls. Esta versión de Blink no requiere que subamos un certificado.

- En el caso de Bria (Counterpath) para iOS, no es necesario subir un certificado. Este cliente acepta el certificado sin intentar verificarlo, cuando la opción "Verficar certificado TLS", está en off. Tampoco es necesario especificar el puerto de transporte.
- Activamos el transporte por TLS en en la cuenta en Opciones avanzadas de la cuenta → Transporte y Seguridad → Transporte de SIP

Opciones avanzadas o	le la cuenta
TRANSPORTE Y SEGURIDAD	
Transporte de SIP	TLS >
Encriptar audio	Siempre >
REGISTRO SIP	
Llamadas entrantes	
Intervalo de actualización W	900
Intervalo de actualización m	900
MANTENER ACTIVO	
Intervalo de Wi-Fi	30
Intervalo celular	30
Teléfono Contactos Historial	Configuración

- Si no tenemos dos clientes endpoint que soporten TLS y SRTP, podemos hacer la práctica con una sola extensión.
- Iniciamos la capruta de paquetes, realizamos la llamada y obtenemos el archivo.
- Abrimos Wireshark y nos dirigimos a "Telephony → VoIP Calls".

	aptu	ıra2b.	pcap	[Wir	eshark	: 1.8.5	5 (S)	/N Re	v 473	50 fr	om /	/trun	(-1.8)	1																		x
File	Ec	tit ۱	/iew	Go	Capt	ure	Ana	alyze	Sta	tistic	s 1	elep	nony	Тоо	ls Ir	ternals	Help															
	-	0					8	2	-	0	2	<i>\</i>	<u>۔</u> ا	- 	F 4			Ð		0 🖻	]   🗎	I 🗹	1	*	đ							
Filt	er:														•	Expr	ession	Cle	ar Ap	ply S	ave											
No		Ti	me		s	ource						D	ectina	tion		_		Proto	col lu	enath	Info											
140.	4	40 0	. 010	0370	1	.92.	168	3.2.	101			1	92.	168.3	1.16	8		TCP	01 0	6	8 533	75 >	http	) [AC	к]	Seg=1	1 A	ck=1	1424	win=1	380 L	
	4	41 0	. 010	0374	1	.92.	168	3.1.	168			1	92.	168.3	2.10	1		тср		151	6 [тс	P se	gment	: of	ar	easse	emb	led	PDU]			
	4	42 0	.010	)379	1	.92.	168	3.2.	101			1	92.	168.3	1.16	8		тср		6	8 533	75 >	http	) [AC	к]	Seq=1	1 A	ck=1	2872	Win=2	)61 L	.6
	- 4	43 0	.010	0405	1	.92.	168	3.1.	168			1	92.3	168.3	2.10	1		тср		15	6 [тс	P Se	gment	: of	a r	reasse	emb	led	PDU]			
	4	44 0	.010	0411	1	.92.	168	3.2.	101			1	92.	168.3	2.27	_		SSH		10	8 Enc	rypt	ed re	espon	se	packe	et	len=	52			
_	4	45 0	.010	0414	1	.92.	168	3.2.	101			1	92.	168.1	1.16	8		тср		6	8 533	75 >	• http	) [AC	K]	Seq=1	1 A	ck=1	2960	Win=2	061 L	. e
		46 0	. 010	1418	1	.92.	168	5.2.	101			1	92.	168.	2.27			SSH		18	8 Enc	rypt	ed re	espon	se	packe	et	len=	132			
		4/0	. 010	)424 )428		02	160	5. <u>1</u> .	108			- 1	92.	168.1	2.10	0		TCP		121	0 LIC	P 56	gmerit		וא רא	Easse	emb 1 ^	rea ck=1	4409	win-2	242 1	
	-	19 0	010	1420	1	92.	168	2 1	168			1	92.	168	2 10	1		TCP		15	6 Гтс		ament	of	n j	-passe	emh	led		w111-2	142 L	
		50 0	. 000	0034	1	92.	168	3.2.	27			1	92.	168.3	2.10	1		тср		6	2 51 5	09 >	ssh	ΓΑCΚ	1 9	Sea=1	AC	k=18	5 Wir	1=254	en=0	)
		51 0	. 000	0064	1	92.	168	3.2.	101			1	92.	168.3	1.16	8		TCP		6	8 533	75 >	http	AC	к]	Seg=1	1 A	ck=1	4496	win=2	242 L	e
		52 0	. 000	0633	1	.92.	168	3.1.	168			1	92.	168.3	2.10	1		тср		58	0 [тс	P se	gment	of	a r	easse	emb	led	PDU]			
		530	. 000	0661	1	.92.	168	3.2.	101			1	92.	168.3	1.16	8		тср		6	8 533	75 >	http	) [AC	к]	Seq=1	1 A	ck=1	5008	Win=2	423 L	e
		54 0	. 001	L476	1	.92.	168	3.1.	168			1	92.	168.3	2.10	1		тср		151	6 [тс	P se	gment	: of	a r	easse	emb	led	PDU]			
		550	. 001	L490	1	.92.	168	3.2.	101			1	92.	168.3	1.16	8		тср		6	8 533	75 >	- http	) [AC	К]	Seq=1	1 A	ck=1	6456	Win=2	504 L	.e
		56 0	. 001	L495	1	.92.	168	3.1.	168			1	92.	168.3	2.10	1		тср		15	б Гтс	P Se	ament	: of	a r	easse	emb	led	PDUl			
< L																															'	
	in an	ne 1	: 11	L7 by	/tes	on	wi	re (	936	bi	ts)	, 1:	.7 k	ytes	cap	oture	d (93	6 bi	ts)													÷
000	0	00 (	0 00	0 01	00	06	00	0b	82	2b	43	38	00	00 0	8 00				+C8													_
001	0	45 (	0 00	0 65	60	43	40	00	40	06	54	f2	c0	a8 0	1 a8	Ε.	.e`C	ı. @	.т													
002	0	CU 1	18 0	2 65 h 50	00	50 4.8	00	/T	C4	01	00	46	00	79 C 72 d	0 9C		.е.р.	• •	F.y	•••												
004	ŏ	04	7b 7	8 e5	48	54	54	50	2f	31	2e	30	20	32 3	0 30	. 1	х. нтт	P /	1.0 2	00												
005	0	20 4	1f 4	b 00	0a	44	61	74	65	3a	20	46	72	69 2	0 41	ć	Dа	it e	: Fri	A												
006	0	20	2/2	3 00	39	20	31	32	зa	30	35	3a	35	30 2	0 32	01	291	.2 :	05:50	2												
007	•			5 00	vu											01																
0	F	ile: "(	C:\Us	ers\Le	nín\D	eskto	p\ca	ptura	2b.p	c	Pa.	P	ofile	Defau	ılt																	_
_							_				_														_		_					

Este es el resultado que obtenemos al usar TLS

🗖 captura2b.p	ocap - VoIP Calls							
				Detected 0 VoIP Calls. Selecte	d 0 Calls.			
Start Time	<ul> <li>Stop Time</li> </ul>	<ul> <li>Initial Speaker</li> </ul>	<ul> <li>From</li> </ul>	▲ To	Protocol	Packets 4 S	itate • Comment	5 <b>4</b>
-								•
			Total: Calls: 0	Start packets: 0 Completed of	alls: 0 Rejected calls: 0			
	Prepare Filter	1	Flow	Player	Select		Close	
				ridyer	Select		21030	

 TLS cifra completamente la señalización y como conclusión no se puede ver el diagrama de respuestas SIP como en la captura anterior.

#### Laboratorio 6.4 (Práctica recomendada)

Descripción: Algunos filtros útiles para tcpdump.

<u>Objetivo</u>: Adiestrar al estudiante en el uso de sniffers para analizar señalización y/o los paquetes RTP con mayor detalle.

Tiempo Máximo: 10 minutos.

Instrucciones:

- Ingresamos a la consola como usuario root
- Realizamos una captura de audio desde el directorio pruebaws

cd pruebaws

Vamos a realizar una captura de un host en concreto y de una interfaz de red en particular.
 Ejecutamos el siguiente comando:

tcpdump -i eth0 -s0 -w capturaXX.pcap udp port 5060 and host XXX.XXX.XXX

- Donde XXX.XXX.XXX.XXX debe ser la IP del teléfono IP. Esto nos permite capturar solamente los paquetes SIP cuyo origen/destino sea el host XXX.XXX.XXX.XXX.
- Con esto reducimos significativamente el tamaño del archivo capturado y podemos realizar una captura más extensa. Ideal para servidores Elastix con un alto flujo de llamadas.
- Para realizar una captura en IAX, de un host en concreto y de una interfaz de red en particular, ejecutamos el siguiente comando:

tcpdump -i eth0 -s0 -w capturaXX.pcap udp port 4569 and host xxx.xxx.xxx

 Para realizar la captura de paquetes UDP, de un host en concreto y de una interfaz de red en particular, ejecutamos el siguiente comando:

tcpdump -i eth0 -s0 -w capturaXX.pcap udp and host XXX.XXX.XXX.XXX

Analizar los archivos generados, usando lo aprendido en los laboratorios anteriores.

#### Laboratorio 6.5 (Práctica recomendada)

<u>Descripción</u>: En este laboratorio instalaremos el códec G.729 versión gratuita desde los repositorios de Asterisk.

Objetivo: Instalación del códec G.729

Tiempo Máximo: 20 minutos.

Instrucciones:

Digium distribuye una versión comercial del codec g729 y puede ser adquirida en el siguiente enlace:

http://www.digium.com/en/products/software/g729-codec

 En este laboratorio usaremos una versión no comercial para propósitos académicos. Nos dirigimos a la siguiente dirección:

http://asterisk.hosting.lv/

Bajo "Linux Binaries" encontramos tres categorías:

Asterisk 1.8 Asterisk 11 Asterisk 12

- Procedemos a revisar la versión de Asterisk instalada en el sistema, que es muy importante a la hora de elegir el códec requerido.
- En la consola de linux de nuestro Elastix ejecutamos

```
asterisk -vvvr
```

- Una vez que encontramos la versión hacemos clic en una de las categorías encontradas en la página web y obtendremos un listado de codecs disponibles. Hay varias alternativas.
- Para la selección del binario adecuado debemos tomar en consideración la arquitectura del sistema (32 bits, 64 bits) y el tipo de procesador que tenemos.

Para obtener información lo más precisa posible ejecutamos el siguiente comando desde consola:

```
cat /proc/cpuinfo
```

```
[root@ecte ~]# cat /proc/cpuinfo
processor
              : 0
vendor id
              : GenuineIntel
cpu family
              : 6
model
              : 23
              : Intel(R) Core(TM)2 Duo CPU
                                               P8600 @ 2.40GHz
model name
stepping: 10
              : 1714.448
cpu MHz
cache size
              : 6144 KB
fdiv bug: no
hlt bug
              : no
f00f bug: no
coma bug: no
fpu
               : yes
fpu exception : yes
cpuid level
              : 5
wp
              : yes
              : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat
flags
pse36 clflush mmx fxsr sse sse2 nx constant tsc up pni monitor ssse3
bogomips: 3428.89
```

 Basaremos nuestra selección en la información obtenida en el campo "model name" y el campo "flags". Además es importante revisar primero las notas que se incluyen en la página:

#### Notas

- Después de descargar revise MD5SUM.
- Use estructuras x86\_64 si está operando en modo de 64-bits. Los Binarios que no contienen x86\_64 en el nombre son de 32-bit.
- Use estructura Pentium 4 para Pentium D. Use Pentium 3 para VIA C3 y Pentium 4 para VIA C7.
- XEON es una rama de CPU para servidores de la familia Pentium3/Pentium4/Core. Celeron es Pentium3/Pentium4/Core con menor cache. Básicamente, hay 5 núcleos de software: MMX, SSE, SSE2, SSE3, SSE4. Escoger el más cercano CPU Intel y probarlo.
- GCC4, ICC todos los binarios son compatibles con estructuras de Asterisk creadas con otros compiladores, se debe usar el más rápido o mejor para usted.
- Las estructuras sse3 son para iteraciones Prescott de chips Pentium 4 con soporte SSE3, revisar por PNI en flag en /proc/cpuinfo.
- Núcleos ICC no siempre son más rápidos, revisar con '(core) show translation recalc 10' en la consola de Asterisk, asegúrese que el servidor esté desocupado o el timing puede ser incorrecto.
- En el caso de este ejemplo, el procesador es Core2 para el cual existen las siguientes opciones:

codec\_g729-ast18-gcc4-glibc-core2-sse4.so codec\_g729-ast18-gcc4-glibc-core2.so codec\_g729-ast18-icc-glibc-core2-sse4.so codec\_g729-ast18-icc-glibc-core2.so

 De acuerdo a la información obtenida en flags, nuestro servidor no tiene instrucciones sse4, por lo cual nuestras alternativas se reducen a dos:

codec\_g729-ast18-icc-glibc-core2.so

#### codec\_g729-ast18-gcc4-glibc-core2.so

 ICC y GCC4, son compiladores usados para compilar el binario, el primero es una versión comercial de Intel y el segundo es un compilador GNU de versión 4 que no tiene cargo. Aunque el primero debe producir mejores y optimizados binarios, podemos probar ambos en nuestro equipo y escoger el que tenga mejor timing.

**Nota:** En este ejemplo solo instalaremos el primero, pero usted puede instalar varias opciones y revisar el timing, lo cual se detallará al final de esta práctica.

- Una vez que seleccionamos el binario a instalar copiamos su enlace para usarlo posteriormente.
- Nos dirigimos al directorio /usr/lib/asterisk/modules desde ahí obtendremos el binario utilizando el comando wget y el link del binario que copiamos anteriormente.

wget http://asterisk.hosting.lv/bin/codec\_g729-ast18-icc-glibc-core2.so

Ahora debemos cambiar el nombre al codec (mv nombre\_actual.so nombre\_nuevo.so)

mv codec\_g729-ast18-icc-glibc-core2.so codec\_g729.so

- Reiniciamos Asterisk con service asterisk restart
- Ahora ingresamos a la consola de Asterisk y ejecutamos "core show translation"

[root@ecte modules]# asterisk -r									
Verbosity is at least 3									
ecte*CLI>	cone s	how tr	anslat	ion					
1	nansla	tion t	imes b	etweer	n formats	(in mi	crosed	conds)	for one
	Source	Forma	t (Row	s) Des	tination	Format	(Colu	umns)	
	g723	gsm	ulaw	alaw	g726aa12	adpcm	slin	lpc10	g729
g723									-
gsm			2	2	1001	2	1	1001	1001 1
ulaw		1001		1	1001	2	1	1001	1001
alaw		1001	1		1001	2	1	1001	1001
g726aa12		1999	1000	1000		1000	999	1999	1999 :
adpcm		1001	2	2	1001		1	1001	1001
slin		1000	1	1	1000	1		1000	1000
1pc10		2000	1001	1001	2000	1001	1000		2000
g729		1001	2	2	1001	2	1	1001	-
speex		1001	2	2	1001	2	1	1001	1001
ilbc		1001	2	2	1001	2	1	1001	1001
g726		2000	1001	1001	2000	1001	1000	2000	2000
g722		1001	2	2	1001	2	1	1001	1001
siren7									-
siren14									-
slin16		2001	1002	1002	2001	1002	1001	2001	2001
g719									-
speex16		3001	2002	2002	3001	2002	2001	3001	3001
testlaw		1001	2	2	1001	2	1	1001	1001

- Si todo salió bien podremos ver los tiempos de transcoding entre g729 y otros codecs.
- Una comprobación adicional se puede realizar habilitando g729 en una de las extensiones que estamos usando. Para hacerlo vamos a la interfaz de administración web de Elastix a PBX → Configuración PBX → Extensiones. Entramos a la extensión y editamos los campos disallow y allow en la sección "Device Options" como se muestra la imagen.

disallow	all
allow	g729

- Luego hacemos clic en "Submit" y aplicamos los cambios. Ahora haremos una prueba marcando 1234, deberíamos escuchar la voz de Allison Smith dándonos la bienvenida a Asterisk.
- Para verificar el timing ejecutamos desde la consola de Asterisk el siguiente comando: core show translation recalc 10
- En una prueba, fuera de laboratorio, hicimos la comparación de los datos obtenidos con los dos binarios disponibles para nuestro servidor y obtuvimos los siguientes resultados:

	g729			
Codec	Α	В		
gsm	1899	798		
ulaw	1600	500		
alaw	1600	500		
g726aa12	1899	798		
adpcm	1600	500		
slin	1599	499		
lpc10	1899	4098		
speex	1999	4498		
ilbc	4398	1298		
g726	1799	698		
g722	1699	898		
slin16	2298	2597		
speex16	3097	3496		
testlaw	1600	500		

Alternativa A) codec\_g729-ast18-icc-glibc-core2.so Alternativa B) codec\_g729-ast18-gcc4-glibc-core2.so

- Como podemos observar en el cuadro, el binario de la alternativa B, tiene un mejor timing para la traducción o transcoding hacia otros codecs, como por ejemplo g711 (ulaw, alaw), en cambio la alternativa A tiene un mejor tiempo de traducción con el codec speex y lpc10.
- Dependiendo el uso que tenga nuestra operación de telefonía debemos hacer la selección, si vamos a usar un porcentaje alto de extensiones con codec g711, entonces nos conviene usar la alternativa B.

#### Laboratorio 6.6 (Práctica Recomendada)

Descripción: Habilitar los codecs de video y probar video llamada con teléfonos grandstream.

Objetivo: Habilitar codecs de video

Tiempo Máximo: 10 minutos.

Instrucciones:

Habilitamos Ilamada de video editando el archivo

/etc/asterisk/sip\_general\_custom.conf

Una vez dentro del archivo agregamos las siguientes líneas:

```
videosupport=yes
allow=h264
allow=h263
allow=h263p
```

Proot@training:~	[	
allowguest=no videosupport=yes		*
allow=h264		
allow=h263		
allow=h263p		
~		
~		
~		
	5,1	All 🔻

 Ir a la interfaz Elastix y configurar las extensiones asociadas a los teléfonos y editar los campos disallow y allow en la sección "Device options":

disallow	all
allow	h264&ulaw&alaw

Deben de estar habilitados los codecs en el teléfono Grandstream

Preferred Vocoder :	Available G723.1 G726-32 GSM L16-256	<ul> <li></li></ul>	Selected PCMU PCMA G729A/B G722
Preferred Video Codec :	Available H263 H263+	<b>↑</b> <b>↓</b> <b>↓</b>	Selected H264

• Una vez realizado las siguientes configuraciones podremos realizar la video llamada.

#### Laboratorio 6.7 (Práctica Recomendada)

Descripción: Configurar el archivo sip\_nat.conf para solucionar problemas de NAT

Objetivo: Configurar el archivo sip\_nat.conf

Tiempo Máximo: 10 minutos.

Instrucciones:

- En ocasiones suele suceder que no podemos realizar o recibir llamadas aun cuando todo esté configurado correctamente.
- Esto puede suceder debido a problemas de NAT para lo cual recomendamos la siguiente configuración:
- Editar el siguiente archivo:

#### /etc/asterisk/sip\_nat.conf

Dentro de ese archivo incluir:

nat=yes externip=IP\_externa/mascara\_de\_red localnet=IP\_Interna/mascara\_de\_red

Ejemplo:

nat=yes
externip=200.4.5.23/255.255.255.255
Localnet=192.168.1.0/255.255.255.0

- Grabar y Salir (Esc  $\rightarrow$  :wq)
- Recargar asterisk: [root@elastix asterisk]# asterisk -rx "reload"

El contenido de este libro está sujeto a mejoramiento. Si usted encuentra errores, por favor envíe un email a <u>training@elastix.com</u> y recibirá una actualización gratis en la siguiente edición.