

Cómo hacer llamadas de Voz y Chat que no puedan grabarse.

MTIA Guillermo Canchola; Solution Architect Latin America



Agenda

Notas Curiosas

- Algunos casos recordados por la historia
- En México

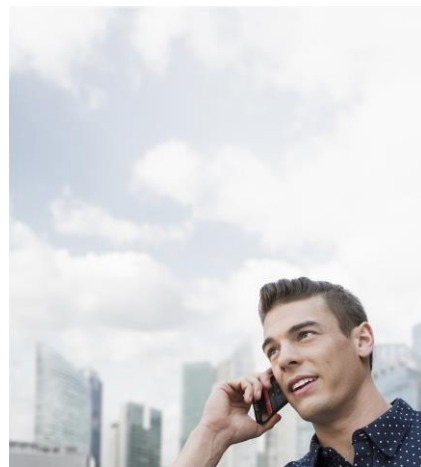
El origen del problema

La solución:

- Autenticación
- Encriptación
- Encapsulación

Seguridad vs Privacidad

Preguntas



Algunas notas curiosas





Algunos casos recordados por la historia

- Edward Snowden hace publicos los programas de vigilancia masiva de la NSA (Agencia de seguridad Nacional). Junio de 2013
- Voicemail de Donald Trump 'hackeado' por Anonymous.- 31 de Marzo, 2016.
- Conversación entre Dilma Rousseff y Lula da Silva .- 16 de Marzo, 2016.
- Mensajes entre Kate del Castillo y Joaquín Guzmán .- 12 de Enero 2016
- Whatsapp prohibido en Brasil por 24 horas.-17 diciembre 2015
- Whatsapp libera encriptación mundial.- 5 Abril 2016





En México

"¿Y cuánto nos va a tocar?"
"Si pierdo me voy a La Ching@(^@"

"cobarde"

"ratero" "te luces"

"Yo no soy la virgen de Guadalupe!"

"comes y te vas"

"mi Gober precioso!"

"patán"

"Y un saludo muy amoroso a que filtrá todas nuestras llamadas telefónicas, O sea"

"Aunque ustedes no lo crean,tengo 400 pares de zapatos"

El delito de intervención de comunicaciones privadas está previsto y sancionado en el artículo 177 del Código Penal Federal: "A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones **de 6 a 12 años de prisión y de 300 a 600 días de multa**".

De acuerdo a la ley, **sólo el CISEN y la PGR** pueden realizar intervenciones telefónicas mediante un permiso otorgado por un juez. Para ello **tienen que argumentar que se trata de casos de seguridad nacional o de investigaciones relacionadas con la delincuencia organizada.**

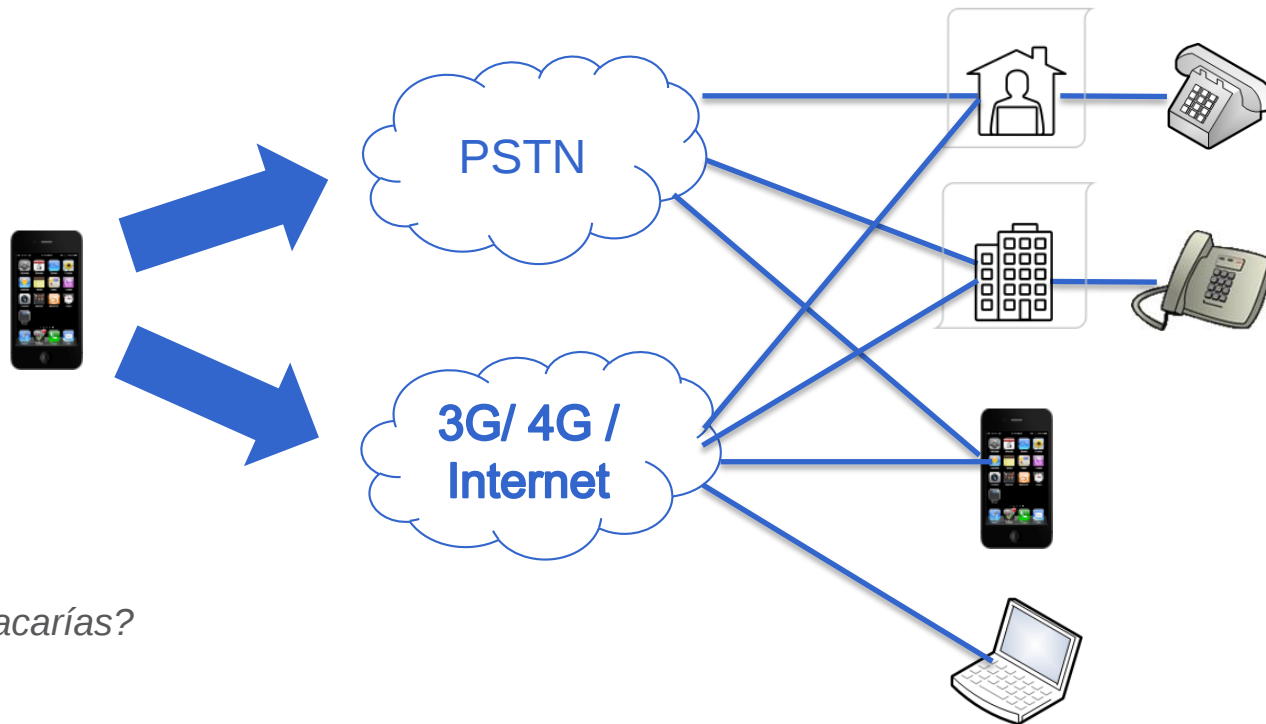
A group of business professionals are gathered on a rooftop terrace with a modern building in the background. In the foreground, a man in a suit is smiling while looking at a tablet held by another man. The tablet screen displays a ShoreTel software interface with a list of contacts and a chat window. Other people are seated at tables with white tablecloths, some looking at their devices. The scene is bright and sunny.

El Origen del problema

 **ShoreTel®**
Brilliantly simple™



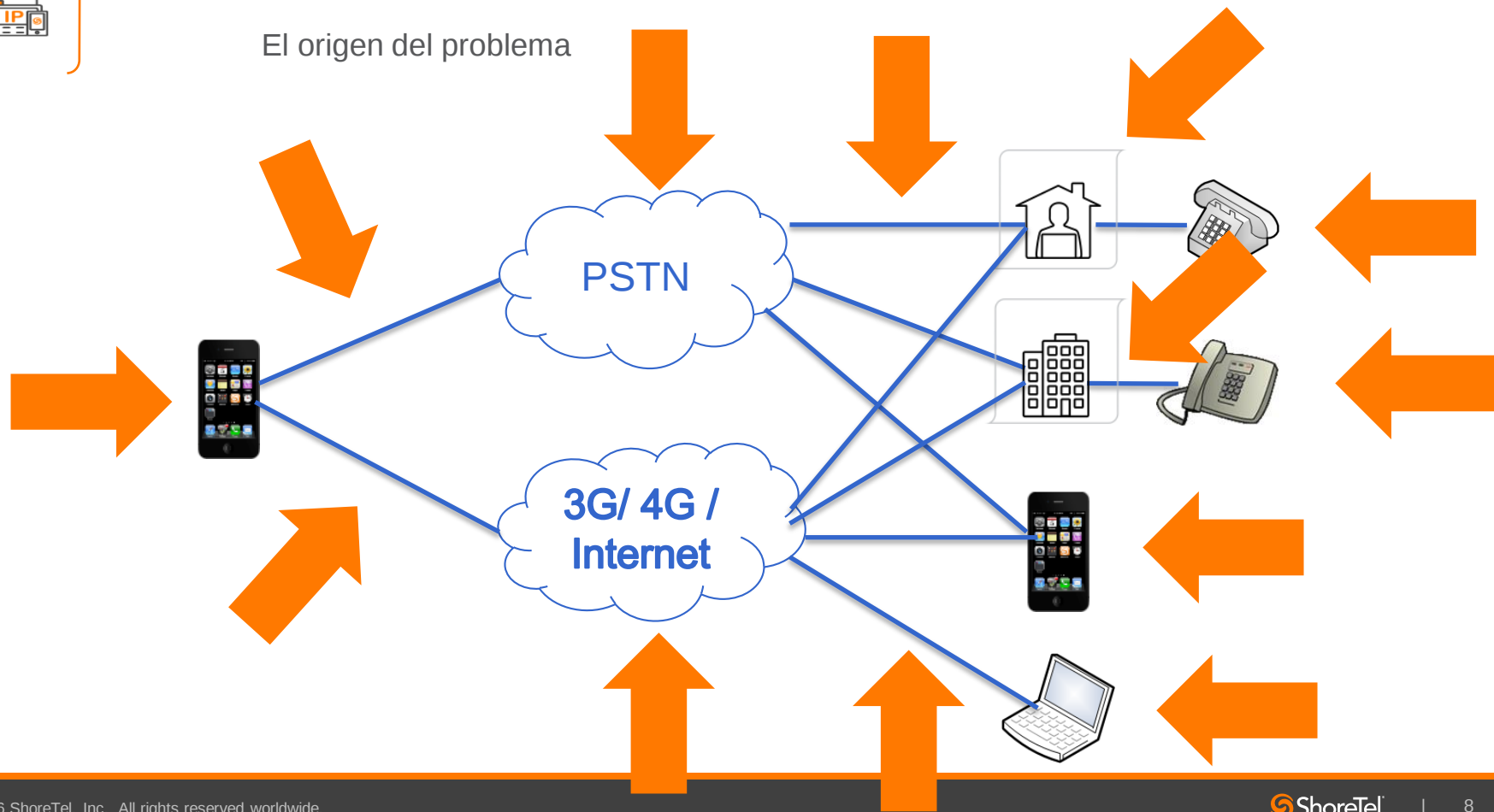
El origen del problema



En dónde atacarías?



El origen del problema



Amenazas en cualquier punto involucrado en la conversación.

Dispositivo móvil

Pérdida o robo del dispositivo

Virus, Malware, Botnet, Hoaxes, Spam, Rootkit.

Suplantación de identidad o 'spoofing'.

Acceso a información confidencial, archivos, conversaciones, imágenes.

Red celular (3G/4G)

Intrusiones tipo "hombre en medio" (Man in the middle).

Suplantar a la red o "IMSI Catcher".

Localización Geográfica

Negación de servicio.

Downgrade selectivo.

Malware, Botnet, Suplantación.

Red Publica (PSTN)

Intrusiones tipo "hombre en medio" (Man in the middle).

Suplantar a la red o "IMSI Catcher".

Negación de servicio. "Phreaking".

Tel. de escritorio

Malware, Botnet, Rootkit.

Suplantación de identidad o 'spoofing'.





Mecanismos de seguridad

1. Autenticación

2. Encriptación

3. Encapsulación



A man with a beard, wearing a dark suit, white shirt, and a blue and white striped tie, is holding a white smartphone to his ear. The phone's screen displays a Windows Phone-style interface with various app tiles. The background is a blurred office or modern building interior.

Solución de ShoreTel





Autenticación en ShoreTel

- Corroborar la identidad de un usuario representa más mecanismos que simplemente un usuario y password, por ejemplo: certificados cliente/servidor, identificación de dispositivos y controles de acceso.
- MAAGTICSI y la Estrategia Digital Nacional obliga a las Instituciones a instrumentar servicios de TIC con autenticación de certificados.

Generando un certificado en ShoreTel:

The screenshot displays the ShoreTel management interface. On the left, a navigation tree shows the following structure: Groups and Users, Policies, Voice, Mobility, UC, Clustering, and System. Under the 'System' category, several sub-items are listed: Networking, Certificate (expanded), Certificate Authority (selected), Mobility Router, Permit List, Authentication, Logging / Monitoring, Date / Time, and Licensing. The main content area on the right is titled 'Certificate Authority > Generate Certificate'. It contains a form with the following fields: Country Name (US), State or Province (California), Locality (Sunnyvale), Organization (Your company name), Organization Unit (Your unit name), Common Name (ramr-dev4.mobility.shoretel.com), and Key Length (bits) (1024). At the bottom of the form are two buttons: 'Generate' and 'Generate CSR'.



Autenticación en ShoreTel



**Configuration**

**Monitor**

**Maintenance**

**Troubleshooting**

Groups and Users
Policies
Voice
Mobility
UC
Clustering
System
 ▶ Networking
 ▼ Certificate
 ▶ Certificate Authority
 ▶ Mobility Router
 ▶ Permit List
 ▶ Authentication
 ▶ Logging / Monitoring
 ▶ Date / Time
 ▶ Licensing

➤ Certificate Authority
Certificate:
Data:
 Version: 3 (0x2)
 Serial Number: 1309402302 (0x4e0be4be)
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: C=US, ST=California, L=Sunnyvale, O=Your company name, OU=Your unit name, CN=raar-dev4.mobility.shoretel.com
 Validity
 Not Before: Jun 29 02:51:42 2011 GMT
 Not After : Jun 25 02:51:42 2031 GMT
 Subject: C=US, ST=California, L=Sunnyvale, O=Your company name, OU=Your unit name, CN=raar-dev4.mobility.shoretel.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
 Modulus (1024 bit):
 00:9b:ba:1d:b8:f7:28:c0:ec:09:58:df:a2:46:b3:
 d0:90:a2:c1:f4:fc:23:d9:76:d4:80:90:73:ea:d7:
 80:16:4a:77:3d:d0:ae:0a:b2:d9:2b:18:c0:9a:8c:
 6a:12:17:6d:06:67:f8:5f:31:e5:44:bd:dc:a3:10:
 c4:77:94:80:84:67:3a:61:85:e0:81:e2:74:31:20:
 16:4f:e7:ba:08:ec:bb:e0:73:ca:56:41:a6:e5:58:
 9d:80:40:6c:b0:c8:48:a4:76:a3:cd:42:66:fc:35:
 e6:60:4f:37:56:2c:6f:ba:1b:ef:e2:26:26:67:54:
 b7:a5:9b:14:25:b7:e8:74:a9
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Basic Constraints:
 CA: TRUE
 Netscape Cert Type:
 SSL Client, SSL Server, S/MIME, Object Signing
 Netscape Comment:
 RA Mobility Router Root Certificate
 X509v3 Subject Key Identifier:
 39:BB:4E:3E:F0:14:DE:91:6D:CF:36:02:66:82:A3:FA:84:0E:DC:9C
 X509v3 Authority Key Identifier:
 keyid:39:BB:4E:3E:F0:14:DE:91:6D:CF:36:02:66:82:A3:FA:84:0E:DC:9C
 DirName:/C=US/ST=California/L=Sunnyvale/O=Your company name/OU=Your unit name/CN=raar-

Generate

Import



Autenticación en ShoreTel

ShoreTel®

Configuration Monitor Maintenance Troubleshooting

Mobility R
Administration Portal v
14:59 Apr 18, 2016 America/I
Logged in as admin

Groups and Users

- Groups
- Users

Users > mmartinez

General Line

User Options

Maximum number of devices allowed for the user 2 (1 Used) Apply

User Devices

Primary	CC Device	Name	Number	Client Version	Description	Provisioning Status
✓	✓	iPhone 6	3338148161	9.0.82.115	iPhone	provisioned

Total Rows 1 Selected Rows 1

Add Delete Modify Make Primary Make Communicator Controlled Device Refresh

Device Details

Device Name: **iPhone 6**
Device ID: **107**
Primary Device: **True**
Communicator Controlled (CC) Device: **True**
Cellular Number: **3338148161**

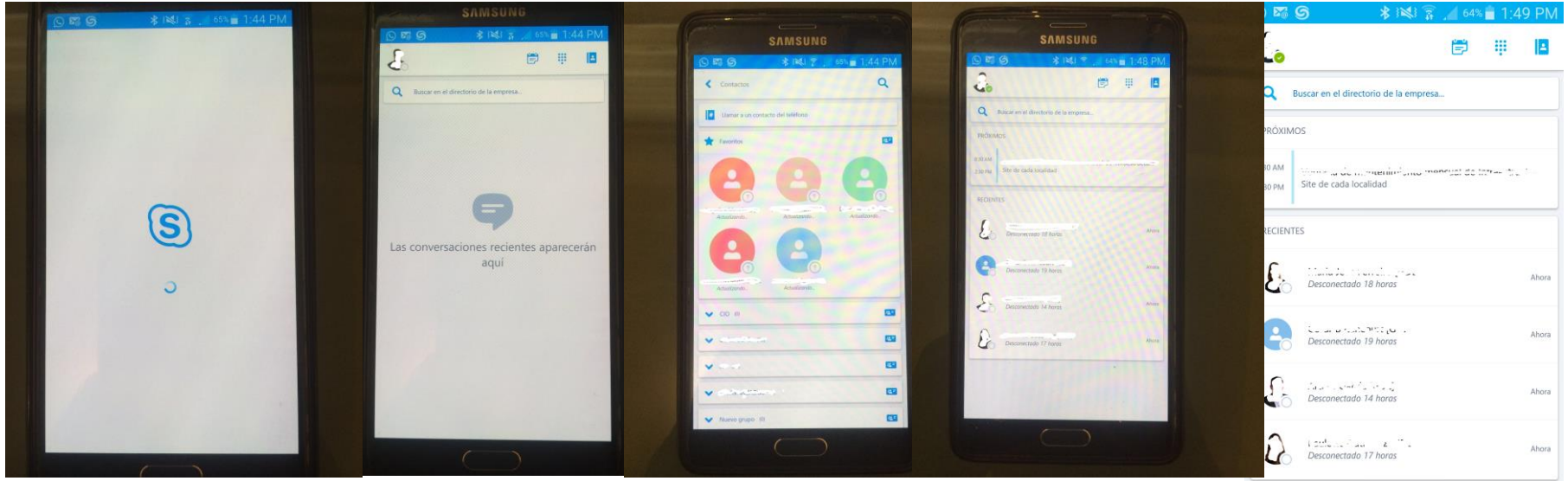
Description: **iPhone**
Provisioning Status: **provisioned**
Client Version: **9.0.82.115**

ROM Version: 9.3.1
IMEI / ESN: 79b078703ccc
IMSI: 334020011260204
MAC address: 79:80:78:70:3C:CC

Cellular Network Type: GSM
Caller ID via DTMF: Roaming
DTMF Error Correction: Disabled
Cellular Call Answer Confirmation: IVR



Una configuración mal aplicada...



Intercambiamos nuestros usuarios / passwords?



Cifrado en ShoreTel

- Existen diferencias entre cifrado de señalización y cifrado de contenido.
- MAAGTICSI y la Estrategia Digital Nacional obliga a las Instituciones a utilizar cifrado a 256 bits .

Habilitando cifrado en ShoreTel:

The screenshot shows the ShoreTel Configuration interface. On the left, the 'Groups and Users' sidebar is visible, with 'Remote Access' highlighted under the 'System' section. Two large orange arrows point from the sidebar to the 'Remote Access' configuration area. The main configuration area has tabs for 'General', 'Protocol', 'Client IP Pool', and 'Options'. The 'General' tab is selected, showing settings for 'Datagram TLS / UDP' and 'TLS / TCP'. Both sections have an 'Enable' checkbox checked and a 'Cipher' dropdown set to 'AES256-SHA'. The 'Datagram TLS / UDP' section also shows settings for Port (443), MTU (1376), Keep Alive (55), Session Timeout (600), and Renegotiation Time (1440). The 'TLS / TCP' section shows similar settings for Port (443), MTU (1376), Keep Alive (480), Session Timeout (600), and Renegotiation Time (1440). An 'Apply' button is at the bottom.



Una configuración mal aplicada...

7603 Calls 7601 - Call established then ended-1.pcap

Apply a display filter ... <36/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CompalCo_b0:61:1c	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.30
2	0.051833	192.168.100.30	192.168.100.70	ICMP	74	Echo (ping) request id=0x0001, seq=2627/17162, ttl=128 (reply in 3)
3	0.052421	192.168.100.70	192.168.100.30	ICMP	74	Echo (ping) reply id=0x0001, seq=2627/17162, ttl=64 (request in 2)
4	1.053824	192.168.100.30	192.168.100.70	ICMP	74	Echo (ping) request id=0x0001, seq=2628/17418, ttl=128 (no response found!)
5	2.546121	192.168.100.33	192.168.100.70	SIP/SDP	952	Request: INVITE sip:7603@192.168.100.70
6	2.575143	192.168.100.70	192.168.100.70			
7	2.583333	192.168.100.70	192.168.100.70			
8	2.6047511	192.168.100.33	192.168.100.70			
9	2.648859	192.168.100.33	192.168.100.70			
10	2.653333	192.168.100.70	192.168.100.70			
11	2.805702	192.168.100.70	192.168.100.70			
12	2.805964	CetisInc_01:07:9e	192.168.100.70			
13	2.806927	192.168.100.70	192.168.100.70			
14	2.855505	192.168.100.82	192.168.100.70			
15	2.858745	192.168.100.82	192.168.100.70			
16	2.895502	CompalCo_b0:61:1c	192.168.100.70			
17	2.906106	192.168.100.70	192.168.100.70			
18	2.948602	192.168.100.33	192.168.100.70			
19	2.972000	192.168.100.70	192.168.100.70			
20	3.499862	CompalCo_b0:61:1c	192.168.100.70			
21	3.735911	192.168.100.82	192.168.100.70			

[Response Time (ms): 101]

Message Header

Via: SIP/2.0/UDP 192.168.100.33:5060; rport; branch=z9HG4bK5cf000a

Transport: UDP

Sent-by Address: 192.168.100.33

Sent-by port: 5060

RPort: rport

Content-Type: application/sdp

Content-Disposition: inline

Content-Length: 12cc05cf-2dc-7828ac72

SIP Display info: "Extension 7603"

SIP from address: sip:7603@192.168.100.70

SIP from address User Part: 7603

SIP from address: sip:7603@192.168.100.70

From: "Extension 7603" <sip:7603@192.168.100.70>; tag=12cc05cf-2dc-7828ac72

To: "Extension 7603" <sip:7603@192.168.100.70>; tag=0.67

Call-ID: 1194896-92241745

Contact: "Extension 7603" <sip:7603@192.168.100.70>; tag=0.67

Content-Type: application/sdp

Content-Disposition: inline

Content-Length: 10192.16 8.100.70

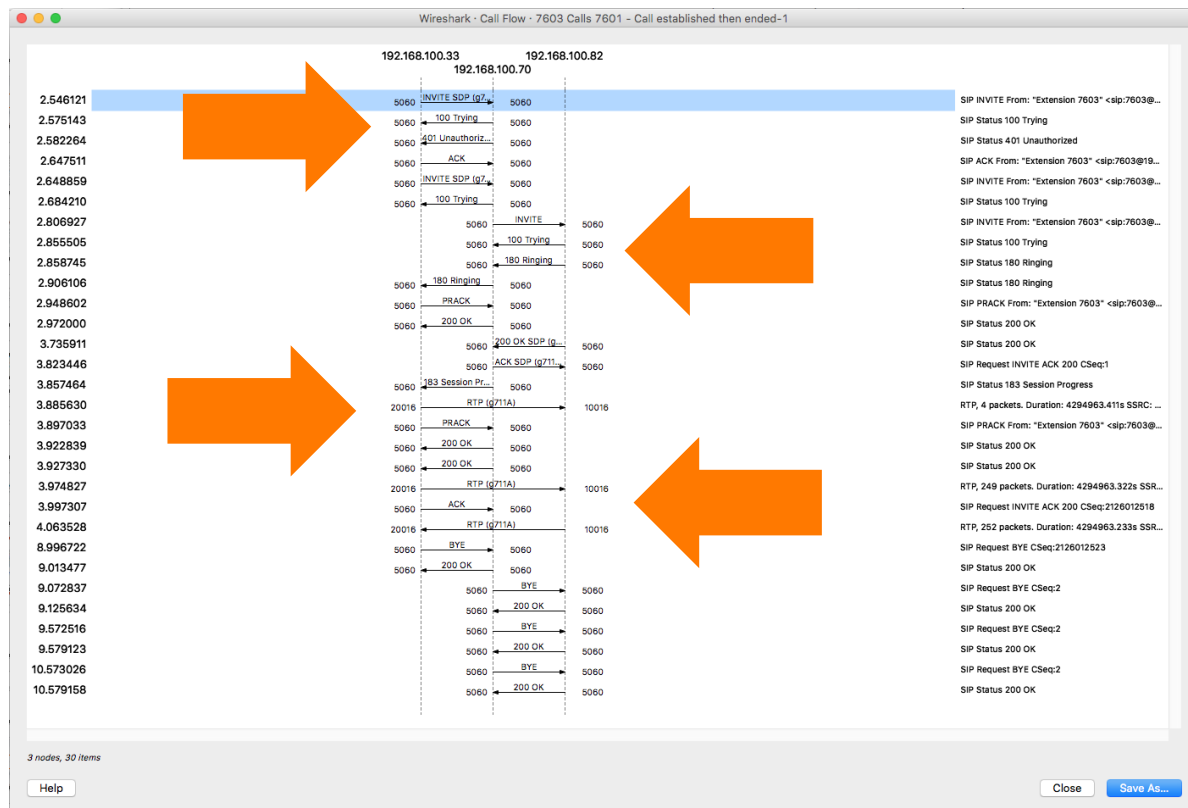
Sequence: 2 12601251

ACK: 12601251

Phone: 0 7.81.00.

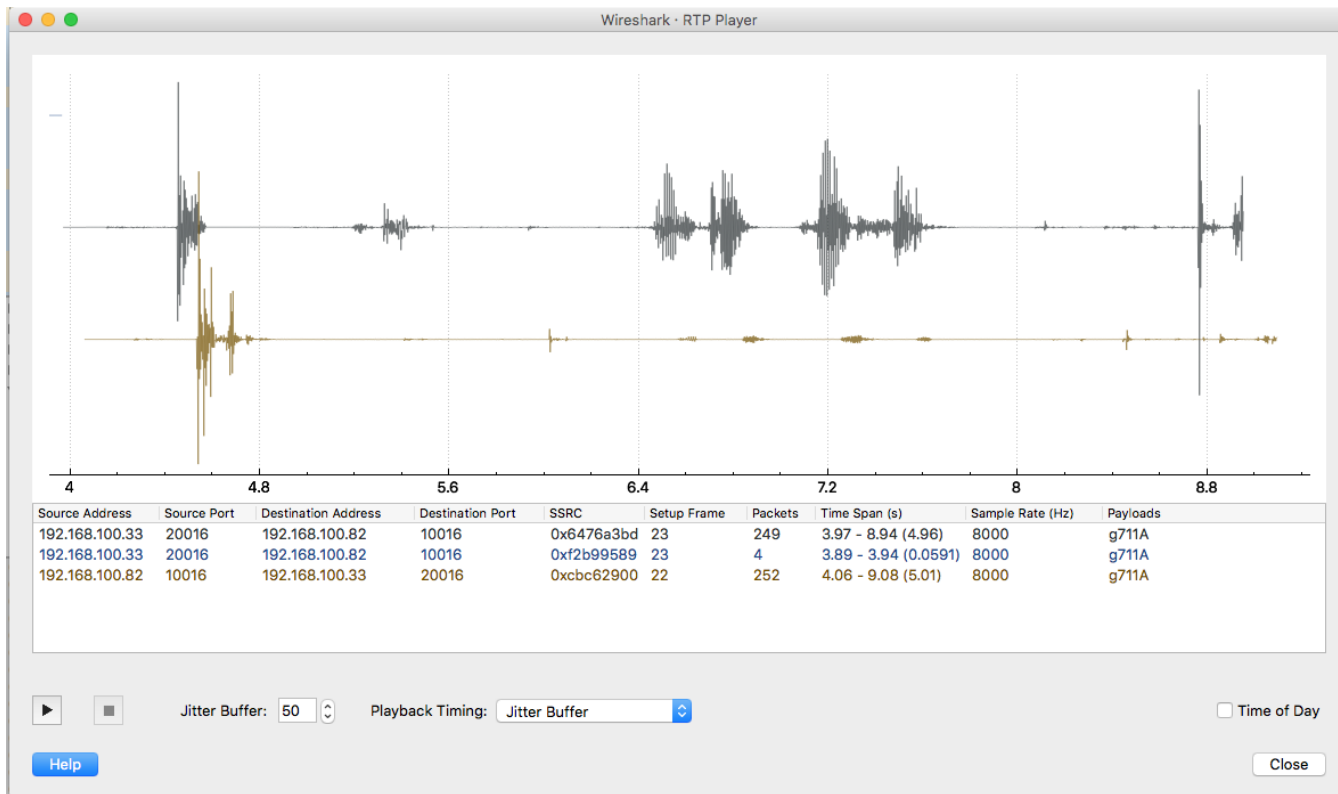


Una configuración mal aplicada...





Una configuración mal aplicada...





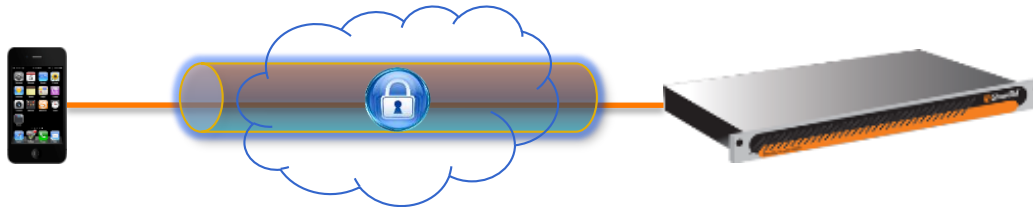
©2016 ShoreTel, Inc. All rights reserved worldwide.



Encapsulación

- Un túnel SSL es utilizado para asegurar la comunicación entre el SMR y los dispositivos móviles, los servicios empresariales (IM, directorio, etc.) también se encuentran dentro del túnel.

Generando una VPN con SSL en ShoreTel:





Una llamada en un tunel VPN

Thunderbolt Ethernet: en5

ip.addr==192.168.0.8

No.	Time	Source	Destination	Protocol	Length	Info
210	4.182131	192.168.0.8	12.167.101.103	QUIC	135	Payload (Encrypted), CID: 254, Seq: 0
211	4.213079	149.154.175.100	192.168.0.8	TCP	74	443 → 57039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=280472166 TSecr=1...
212	4.217722	192.168.0.8	149.154.175.100	TCP	66	57039 → 443 [ACK] Seq=1 Ack=1 Win=87680 Len=0 TSval=1601313 TSecr=280472166
213	4.218338	192.168.0.8	149.154.175.100	SSL	276	Continuation Data
214	4.291647	12.167.101.103	192.168.0.8	TLSv1	135	Application Data
215	4.291995	12.167.101.103	192.168.0.8	TLSv1	343	Application Data
216	4.293708	192.168.0.8	12.167.101.103	TCP	66	50234 → 443 [ACK] Seq=4873 Ack=2644 Win=4085 Len=0 TSval=1601328 TSecr=2647429496
217	4.301913	12.167.101.103	192.168.0.8	TLSv1	119	Application Data
218	4.303713	12.167.101.103	192.168.0.8	TLSv1	1399	Application Data
219	4.304957	12.167.101.103	192.168.0.8	TLSv1	1399	Application Data
220	4.306000	12.167.101.103	192.168.0.8	TLSv1	1399	Application Data
221	4.306344	12.167.101.103	192.168.0.8	TLSv1	359	Application Data
222	4.306780	12.167.101.103	192.168.0.8	TLSv1	503	Application Data
223	4.306861	192.168.0.8	12.167.101.103	TCP	66	50234 → 443 [ACK] Seq=4873 Ack=4030 Win=4085 Len=0 TSval=1601331 TSecr=2647429506
224	4.307787	192.168.0.8	12.167.101.103	TCP	66	50234 → 443 [ACK] Seq=4873 Ack=6696 Win=4085 Len=0 TSval=1601331 TSecr=2647429507
225	4.308315	192.168.0.8	12.167.101.103	TCP	66	50234 → 443 [ACK] Seq=4873 Ack=7426 Win=4085 Len=0 TSval=1601331 TSecr=2647429507

▶ Frame 213: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface 0

▶ Ethernet II, Src: SamsungEa2:39:42 (f4:09:d8:a2:39:42), Dst: ArrisGro_da:14:a1 (00:1d:d0:da:14:a1)

▶ Internet Protocol Version 4, Src: 192.168.0.8, Dst: 149.154.175.100

▶ Transmission Control Protocol, Src Port: 57039 (57039), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 210

Source Port: 57039

Destination Port: 443

Stream index: 61

[TCP Segment Len: 210]

Sequence number: 1 (relative sequence number)

[Next sequence number: 211 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 32 bytes

▶ Flags: 0x018 (PSH, ACK)

Window size value: 685

[Calculated window size: 87680]

[Window size scaling factor: 128]

▶ Checksum: 0x9d05 [validation disabled]

Urgent pointer: 0

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

▶ [SEQ/ACK analysis]

Secure Sockets Layer



Una llamada en un tunel VPN

Dashboard

- Calls
- Users
- System
 - Interfaces
 - Access Points
 - Remote Access Counters

Remote Access Counters

Handshake Attempts	56,546	Receive UDP Packets	4,976,102
Handshake Successes	27,076	Receive UDP Bytes	1,231,069,641
Handshake Failures	29,184	Certificate Authentication Successes	26,705
Authentication Attempts	359	Certificate Verify Failures	0
Authentication Successes	348	Session Start Successes	15,186
Authentication Failures	11	Session Start Failures	11,820
Out of IP Failures	0	Permit List Check Failures	27,682
Tunnel Interface Create Failures	0	Overlap Session Failures	3,839
Select Failures	0	Session Termination Failures	380
Packet Pool Size	200	Packet Pool Free	199

Summary Table:

Name	TLS	DTLS	Total
Total Sessions	55,434	1,132	56,566
Active Sessions	17	45	62
Max Active Sessions	57	46	103
Rx Packets	533,970	4,971,126	5,505,096
Tx Packets	1,277,124	6,854,584	8,131,708
Rx Bytes	229,097,108	937,665,741	1,166,762,849
Tx Bytes	518,097,127	1,119,102,243	1,637,199,370
Rx Dropped	21,793	552	22,345
Tx Dropped	0	0	0
SSL Reads	588,235	4,972,388	5,560,623
SSL Writes	1,286,692	6,854,584	8,141,276
Tx Keep Alive	25,474	1,239,591	1,265,065

[Refresh](#)



ShoreTel Mobility Router

ShoreTel Mobility Router



Scaling:

- 2000 Series: 10 - 100 users
- 4000 Series: 10 - 1,000 users
(Stackable for additional scaling)
- Virtual SMR – 1000 users

Core Functions:

- PBX and UC integration
- Security integration
- App layer security
- Policy management
- Reporting/trending

ShoreTel Mobility Client



Key Features:

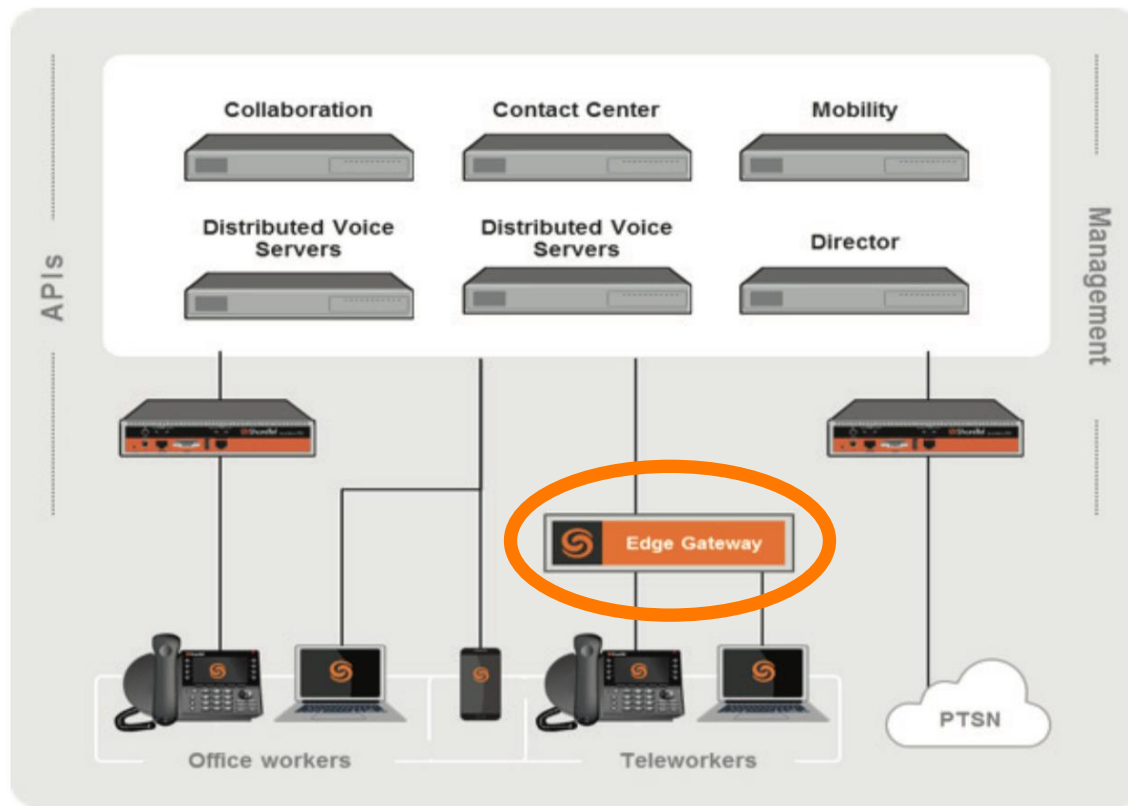
- Video Conferencing
- Desk phones and UC capabilities
- Integrated security
- Business and personal identities
- Calendar integration

Phone Types:

- Android
- Apple iOS
- Blackberry OS



Que pasa con los teléfonos de escritorio? Edge Gateway



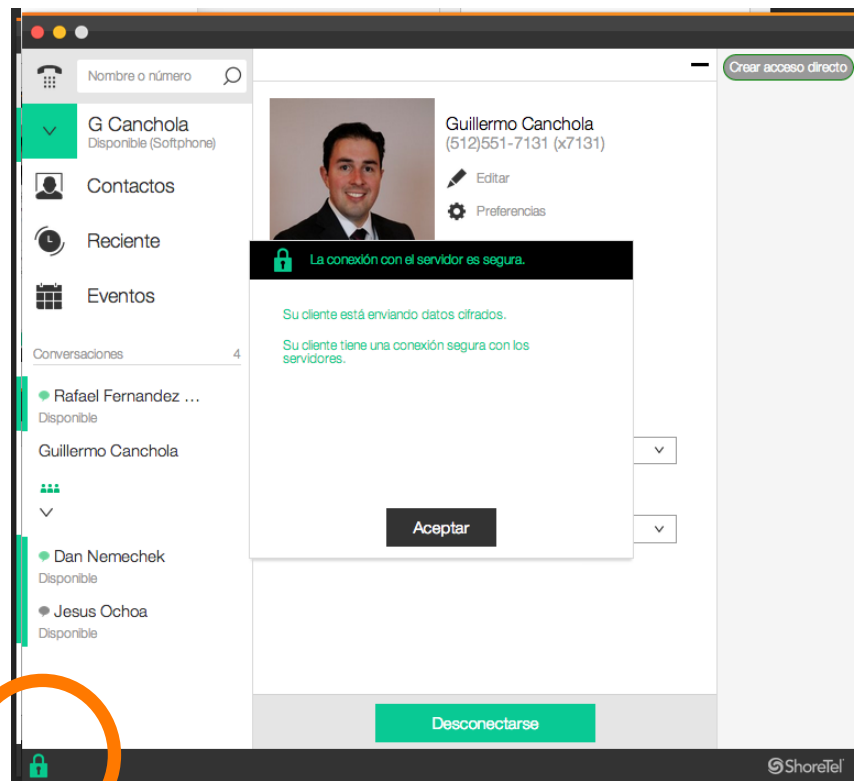


Edge Gateway



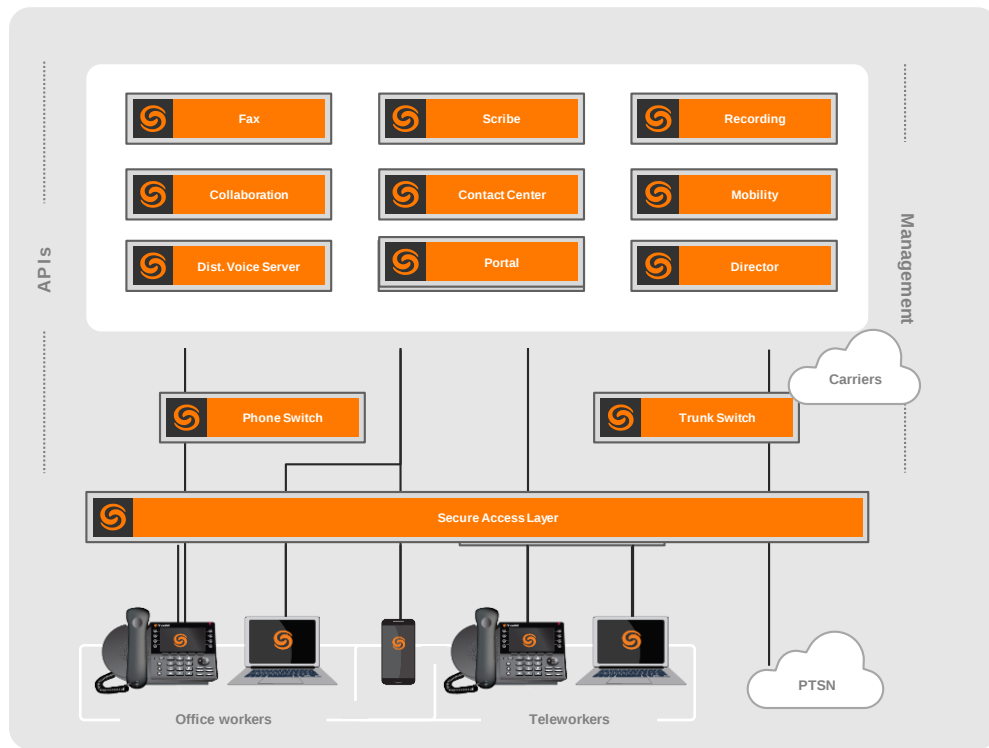


Edge Gateway





Que pasa con el video y otros servicios de comunicaciones?



Todas las comunicaciones entre los usuarios **dentro de tu red** ahora están seguras.



Seguridad VS Privacidad

c. [REDACTED] **Not Encrypted End-to-End.** Calls made through the [REDACTED] service are decrypted at [REDACTED] servers and are then routed without encryption through the public switched telephone network (PSTN) to their intended termination points. Calls made via [REDACTED] may be subject to lawful interception at the point where they are decrypted and at any point on the public telephone network. Member to member calls are fully encrypted end-to-end.

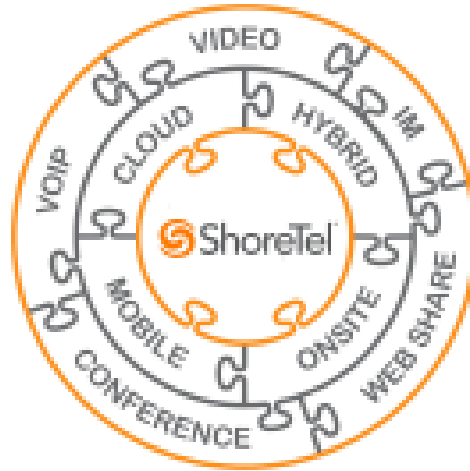
Log File Information: When you use the [REDACTED], our servers automatically record certain information that your web browser sends whenever you visit any website. These server logs may include information such as your web request, Internet Protocol ("IP") address, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, the date and time of your request, one or more cookies that may uniquely identify your browser, your phone number, phone number you are requesting the status of and various status information. When you use the [REDACTED] Service, our servers log certain general information that our application sends whenever a message is sent or received, or if you update or request any status information, including time and date stamps and the mobile phone numbers the messages were sent from and to.

[REDACTED] If you do not agree to our practices, please do not use the [REDACTED] Service.

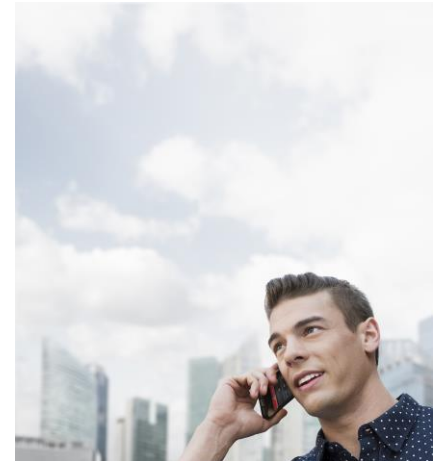
you. You are responsible for all activity that occurs under your Account, and you agree to maintain the security and secrecy of your Account username and password at all times. Unless otherwise permitted by [REDACTED] writing, you may only possess one Account.

[REDACTED] may, in [REDACTED] sole discretion, permit you from time to time to submit, upload, publish or otherwise make available to [REDACTED] through the Services textual, audio, and/or visual content and information, including commentary and feedback related to the Services, initiation of support requests, and submission of entries for competitions and promotions ("*User Content*"). Any User Content provided by you remains your property. However, by providing User Content to [REDACTED] you grant [REDACTED] a worldwide, perpetual, irrevocable, transferrable, royalty-free license, with the right to sublicense, to use, copy, modify, create derivative works of, distribute, publicly display, publicly perform, and otherwise exploit in any manner such User Content in all formats and distribution channels now known or hereafter devised (including in connection with the Services and [REDACTED] business and on third-party sites and services), without further notice to or consent from you, and without the requirement of payment to you or any other person or entity.

Preguntas?

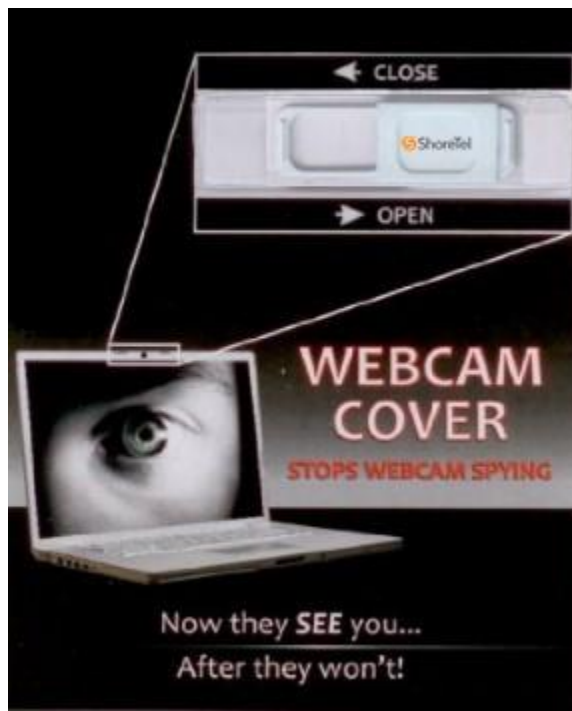


Contacto: gcanchola@shoretel.com
@MemoCancholaR
www.shoretel.com

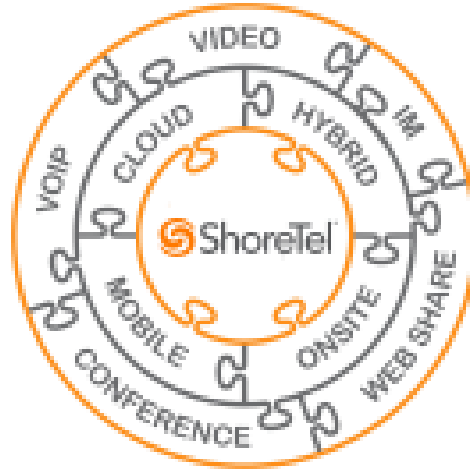




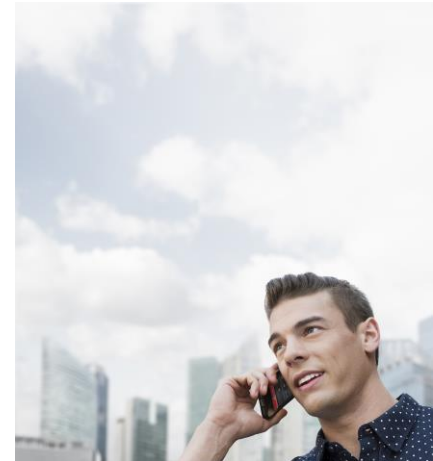
La mejor seguridad para el video.....



GRACIAS!!!!!!!!!!



Contacto: gcanchola@shoretel.com
@MemoCancholaR
www.shoretel.com



Cálculo de ancho de banda

Bandwidth Calculator for Secure Remote Voice

Device Type: **Android**

Codec	G.711 u-law	Sample Size	20
Transport Type	UDP	Encryption	AES-SHA

ETHERNET	14
IP	20
UDP	8
DTLS	13
AES-SHA	40
RAST	16
RTP	12
Tunneled UDP	8
Tunneled IP	20
G.711	160
Total bytes	311
Packet per sec	50
Data Rate (one-way)	124.4 kbps