

Universidad Tecnica Federico Santa Maria

Departamento de Electrónica
ELO322 – Redes de Computadores
1er Semestre 2017

Proyecto Final

VoIP (Voz Sobre IP)

Nicolas Peñailillo
Javier Rebolledo
Javiera Rojas

8 de julio de 2017

1. Resumen

Voz sobre IP o VoIP, es un protocolo que apunta a la optimización en el envío de voz por medio de intercambio de paquetes de datos por internet, el cual nace como una alternativa más económica a la ya costosa red pública de telefonía. Bajo este contexto, se estudió TeamSpeak, software que se abrió paso en la industria gamer por ofrecer comunicación via VoIP de alta calidad, baja en ruido, lag y ancho de banda. El objetivo principal fue lograr comprender como es que se implementa VoIP y en particular como lo desarrolla TeamSpeak, exponiendo las características típicas del protocolo, las técnicas más comunes utilizadas y la captura de paquetes mediante Wireshark.

2. Introducción

Los protocolos que se conocen como protocolo VoIP o Voz Sobre IP, son el conjunto de recursos que hacen posible que una señal de voz viaje a través de internet empleando protocolo IP, o bien dicho de otra manera, que el mensaje de voz viaje de forma digital en paquetes de datos, en lugar de ser transmitida de forma analógica, como operan las redes PSTN de telefonía convencional. Quizá el software más conocido que aplica este protocolo es Skype, el cual se masificó por permitir realizar videoconferencias libre de cualquier costo. Sin embargo, este Software no es muy popular entre jugadores de video juegos. TeamSpeak es una de las elecciones más comunes entre jugadores online, el cual les permite establecer una comunicación fluida con sus equipos de juego, a un bajo ancho de banda, mejorando la experiencia de juego. En este trabajo primero se explica el protocolo VoIP, para luego intentar hacer un análisis del funcionamiento de TeamSpeak y lograr identificar, mediante estudio y captura de paquetes con Wireshark, como es que este logra cumplir con el servicio que promete.

3. VoIP y Aplicación en TeamSpeak

3.1. Cómo funciona VOIP

VoIP se define como el conjunto de normas, dispositivos y protocolos que permiten transmitir voz por protocolo IP. En la Tabla 1 se pueden ver los protocolos y funciones para cada capa del modelo OSI.

Numero de Capa OSI	Nombre de Capa OSI	Protocolos y funciones de VOIP
7	Aplicación	NetMeeting/Aplicaciones
6	Presentación	Codecs (Speex)
5	Sesión	H.323/MGCP/SIP/TeamSpeak/RTP
4	Transporte	TCP/UDP
3	Red	IP
2	Enlace de Datos	Frame Relay, ATM, Ethernet, PPP, MLP y más.

Tabla 1: Relacion de Modelo OSI con VoIP

VoIP comienza por comprimir el audio que viene de señales análogas desde SoftPhones (Computadores con software de VoIP). Esta señal de audio se comprime en la capa de presentación mediante codecs específicos usados para VoIP (Speex, GSM, etc) posteriormente la capa de sesión usa protocolos

que se encargan de establecer, gestionar y finalizar sesiones multimedia (SIP, H323). Finalmente se transporta por las redes basadas en IP. Al otro lado de la línea el receptor hace el mismo proceso invertido recibiendo por sus audífonos o parlantes la señal de audio generada por el emisor. En la figura 1 se muestra una Trama VOP, en ella se detallan los largos de cada trama.

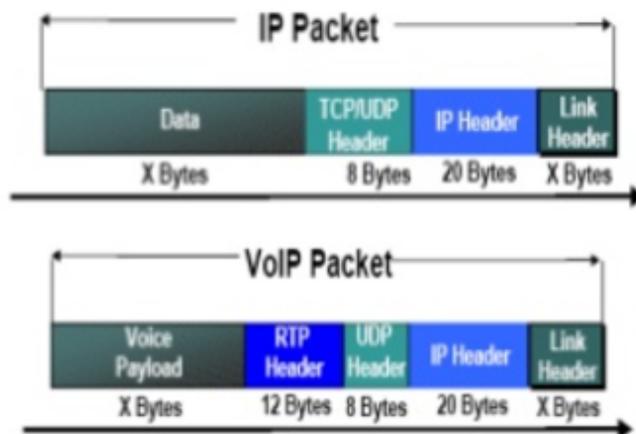


Figura 1: RTP header añadido a paquete IP

3.2. Estándares de control

Existen variados estándares de protocolos de control, cada uno diseñado por diferentes grupos de trabajo, con el fin de solucionar distintos aspectos en la comunicación. El desarrollo de estos ha permitido que la voz se codifique en paquetes cada vez más pequeños, requiriendo menor ancho de banda y diversas mejoras en el sistema. Algunos ejemplos son:

H.323: definido por la UIT (unión internacional de telecomunicaciones). Posee ventajas como controlar el tráfico de red, mejorando el rendimiento, es independiente del tipo de red física. Fue originalmente diseñado para el transporte de video conferencia. Es relativamente seguro ya que utiliza RTP.

SIP: Protocolo de Inicio de sesión, es utilizado para conferencias, telefonía y mensajería instantánea por Internet. Este protocolo considera a cada conexión como un par y se encarga de negociar las capacidades de ellos. Tiene una sintaxis simple, similar a HTTP.

MGCP: (media Gateway Control Protocol), inicialmente diseñado para simplificar en lo posible la comunicación con terminales como los teléfonos. Utiliza un modelo centralizado (arquitectura cliente-servidor, es decir la comunicación no es directa)

3.3. Codex VOIP

Para codificar la voz y ser transmitida por red IP, se hace uso de códecs que garantizan la codificación y compresión del audio para su posterior decodificación y descompresión.

Según el codec a utilizar en la transmisión, se utiliza mayor o menor ancho de banda. La cantidad de ancho de banda tiene relación directa con la cantidad de datos transmitidos.

algunos de los codecs más utilizados en VoIP son G.711, G.729 y Speex

Codex	Bandwidth/kbps	Comentarios
G.711	64	Entrega una transmisión precisa de audio. Bajos requerimientos de procesamiento. Es uno de los codecs más antiguos (1972) y funciona bien con un alto ancho de banda, lo que lo hace obsoleto para el internet pero es aún útil para LANs.
G.729	8	Excelente utilización de ancho de banda. Tolerante a los errores. Este es una mejora de los otros con similar nombre, pero es licenciado, lo que significa que no es gratis.
Speex	2.15 / 44	Minimiza el uso de ancho de banda usando una tasa variable de bits. Es uno de los codecs más preferidos por muchas apps VoIP

Tabla 2: Comparativa de Codex usados en VoIP

3.4. Futuro de VoIP

El servicio VoIP crecerá considerablemente en los próximos años, para ello se deben mejorar algunos aspectos que hagan de él un servicio confiable y eficaz.

1. En lo que respecta a la calidad de la llamada, esta aún es inferior a la llamada telefónica tradicional ya que en VoIP se tienen pérdida de paquetes y problemas de latencia. Para mejorar estos aspectos se debe trabajar en disminuir la latencia disminuyendo el uso de red y optimizar el envío de paquetes.
2. Se debe transformar en un servicio más confiable, ya que VoIP es propenso a el robo de datos por crackers, para ello se deben crear protocolos más seguros y encriptaciones más complejas.
3. Gracias al ancho de banda creciente a nivel mundial y la constante optimización de la capa 2 y 3, garantizaran que la comunicación en tiempo real de VoIP sea de mayor calidad.
4. Puede que la comunicación VoIP nunca supere la calidad de la llamada tradicional pero gracias a los costos asociados a VoIP muchas empresas y compañías optarían a futuro por comunicación VoIP dejando la telefonía tradicional de lado.

3.5. Arquitectura de Teamspeak

TeamSpeak es un servidor de comunicación por voz en grupo que permite que múltiples personas que se conectan por el cliente de Teamspeak entren a canales y puedan hablar simultáneamente con otras personas en el mismo canal. En esta arquitectura Cliente/servidor el cliente envía paquetes encapsulados con uno de los codex de VoIP al servidor usando unicast. Posteriormente el servidor se comunica con los demás clientes que están en el mismo canal por unicast como lo muestra la figura 2.

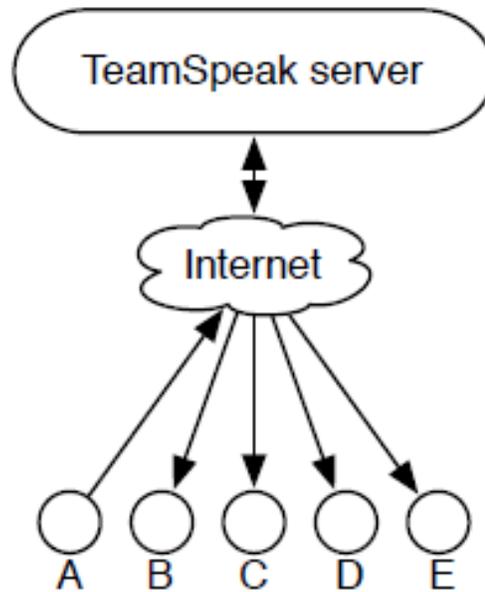


Figura 2: Arquitectura de Teamspeak

3.6. Formato de paquetes de Teamspeak

Entendiendo como es la estructura de un mensaje de voz en IP y analizando como es la comunicación entre usuarios de TeamSpeak, se puede esquematizar los paquetes de envío y recibo de la siguiente manera.

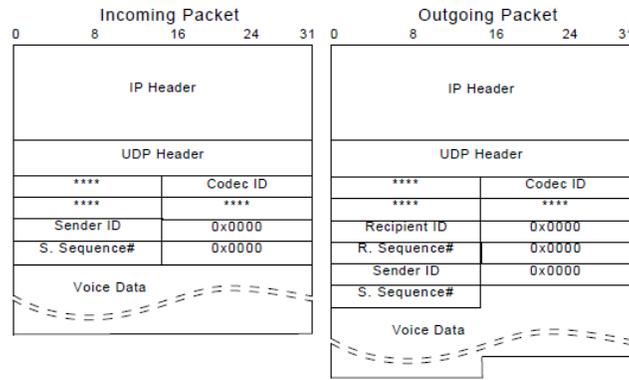


Figura 3: Solución Típica Basada en VoIP

De la figura anterior hay que destacar varios puntos, partiendo por la única diferencia en cuanto al tamaño del paquete. Se puede observar que el paquete enviado es más grande puesto que este contiene la IP de tanto emisor como receptor, mientras que un mensaje de entrada, solo contiene la IP de quien envía el mensaje. Respecto al encabezado, ya se había mencionado que este respeta los protocolos de IP y UDP, por lo tanto, no hay nada distinto en estos encabezados. Por lo tanto, solo resta intentar deducir el tipo de protocolo de control y codec utilizado por TeamSpeak.

4. Resultados Parte practica

Iniciando una conversación en Teamspeak y, mediante la captura de paquetes usando Wireshark, se obtuvo lo siguiente:

7	0.641918	192.168.0.7	131.221.33.13	UDP	135	61668	→	9987	Len=93
8	0.661870	192.168.0.7	131.221.33.13	UDP	126	61668	→	9987	Len=84
9	0.680610	192.168.0.7	131.221.33.13	UDP	134	61668	→	9987	Len=92
10	0.699595	192.168.0.7	131.221.33.13	UDP	135	61668	→	9987	Len=93
11	0.720192	192.168.0.7	131.221.33.13	UDP	133	61668	→	9987	Len=91
12	0.740184	192.168.0.7	131.221.33.13	UDP	130	61668	→	9987	Len=88
13	0.761343	192.168.0.7	131.221.33.13	UDP	122	61668	→	9987	Len=80
14	0.781645	192.168.0.7	131.221.33.13	UDP	122	61668	→	9987	Len=80
15	0.801670	192.168.0.7	131.221.33.13	UDP	126	61668	→	9987	Len=84
16	0.821766	192.168.0.7	131.221.33.13	UDP	127	61668	→	9987	Len=85

```

▶ Frame 9: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▶ Ethernet II, Src: LiteonTe_89:19:49 (30:10:b3:89:19:49), Dst: ArrisGro_30:4c:e1 (a4:15:88:30:4c:e1)
▶ Internet Protocol Version 4, Src: 192.168.0.7, Dst: 131.221.33.13
▶ User Datagram Protocol, Src Port: 61668, Dst Port: 9987
▶ Data (92 bytes)
    
```

0000	a4 15 88 30 4c e1 30 10 b3 89 19 49 08 00 45 00	...L.0. ...I..E.
0010	00 78 1a d5 00 00 80 11 ba 06 c0 a8 00 07 83 dd	.x.....
0020	21 0c f0 e4 27 03 00 64 23 52 05 94 b7 0e a9 1e	!...'d #R.....
0030	d8 4d 00 9f 00 46 c0 00 a0 04 48 87 a0 at 92 f2	.M...F... ..H....
0040	b5 5d 99 a0 fc c0 3a 14 29 fb cc 9a 8c 6d 9e 70	.].....:)....m.p
0050	08 a1 ca 9b 4c 36 19 44 69 c7 ea 50 c5 19 84 b1	...L6.D i..P....
0060	ce b1 6a e1 f1 ea 83 30 b9 12 a1 76 37 5c d7 32	...j....0 ...v7\..2
0070	7f 13 dd 40 a2 01 f4 e7 4f fa 6e c0 da 5b da 2d	...@.... 0.n..[-
0080	9b 54 e4 a0 17 0d	.T....

Figura 4: Captura de wireshark Usando TeamSpeak

Al analizar un paquete voz enviado por TeamSpeak, se observa que cumple con los tamaños indicados en el análisis de VoIP. Para el IP Header se tienen 20 bytes (en azul), UDP Header 8 bytes (en rojo) y lo correspondiente a el protocolo de sesion y audio es lo restante(en verde). Para calcular el ancho de banda solo necesitamos el largo de los paquetes de audio los cuales en promedio son de 85 bytes. El tiempo promedio en que llegan aquellos bytes es de 19ms. El ancho de banda puede calcularse de la siguiente forma:

$$\text{AnchoBanda} = \frac{\text{PaqueteAudio(bits)}}{\text{Tiempo(seg)}}$$

$$\text{AnchoBanda} = \frac{85 * 8}{0,019} = 35\text{kbps}$$

Por lo tanto el bitrate de Speex es el de 32Khz ultra-wideband.

5. Conclusiones

En este informe se expusieron las características y protocolos de propios de VoIP para entender el funcionamiento de TeamSpeak. La información recopilada ilustra lo útil y practico de este protocolo, que mejora día a día, al punto de competir y reemplazar a la telefonía clásica.

Por otra parte, el estudio y pruebas realizadas sobre TeamSpeak, reflejan lo versátil que puede ser VoIP en sus aplicaciones, siendo en este caso, una solución innovadora para un publico en especifico (gamers). Además, mediante la captura de paquetes se logro identificar el tipo de codec utilizado por el software y se descubrió que el valor agregado de TeamSpeak radica en su protocolo de control, siendo este privado.

Actualmente vivimos en la época del apogeo de los medios de comunicación y VoIP es un factor clave en las telecomunicaciones. No caben dudas que el futuro traerá nuevos protocolos y softwares dedicados a optimizar VoIp, por lo que su estudio y comprensión se vuelven cada día más relevante, especialmente, en la formación de un ingeniero Electrónico y/o telemático.

Referencias

- [1] A Location Aware P2P Voice Communication Protocol for Networked Virtual Environments
<http://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1494&context=etd>
- [2] Telefonía Voz IP
<http://www.telefoniavoz.com/voip/que-es-la-telefonía-ip.htm>
- [3] Wireshark: Listening to VoIP Conversations from Packet Captures
<https://cyberarms.wordpress.com/2012/05/21/wireshark-listening-to-voip-conversations-from-packet-captures/>
- [4] Technical aspects of network neutrality
<http://agents.usluge.tel.fer.hr/sites/default/files/ConTEL%202011%20-%20Technical%20aspects%20of%20network%20neutrality.pdf>