



**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**Facultad de Ingeniería en Electricidad y Computación**

**“ANÁLISIS DE EFICIENCIA DE PROTOCOLOS DE ENRUTAMIENTOS EN  
IMPLEMENTACIÓN DE RED INALÁMBRICA MESH EN INSTALACIONES  
DE LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y  
COMPUTACIÓN (FIEC)”**

**INFORME DE  
PROYECTO DE GRADUACION**

Previa a la obtención del Título de:

**INGENIERO EN ELECTRONICA Y  
TELECOMUNICACIONES**

Presentada por:

**EVELYN STEPHANIA JIMENEZ BRAVO**

**JOSE EDUARDO ZERNA TORRES**

GUAYAQUIL – ECUADOR

2011

# AGRADECIMIENTO

A Dios, a mis padres por todo el apoyo brindado durante toda mi formación académica, por no dejarme caer ante los obstáculos.

***Evelyn S. Jiménez Bravo***

A mis padres y hermanos porque gracias a ellos he logrado llegar hasta donde estoy ahora, y a Dios sin cuyo consentimiento no cae una hoja de un árbol.

***José E. Zerna Torres***

Agradecemos al Centro de Investigación, Desarrollo e Innovación de Sistemas (CIDIS) por las facilidades brindadas al trabajar en sus instalaciones y con sus equipos, al Ing Juan Carlos Basurto y al Ing, Roberto Riggio por el apoyo brindado en el desarrollo del presente proyecto

# DEDICATORIA

A mi abuelita que desde el cielo siempre guiará mis pasos, a toda mi familia, a mis queridos amigos quienes juntos recorrimos esta etapa y me ayudaron a culminarla.

***Evelyn S. Jiménez Bravo***

A mis padres, hermanos y amigos, quienes constituyen el pilar más importante de mi vida.

***José E. Zerna Torres***

# TRIBUNAL DE SUSTENTACIÓN

---

Ing. Jorge Aragundi.

**SUB-DECANO FIEC**

---

Ing. Patricia Chávez B.

**DIRECTOR DE PROYECTO**

---

Ing. Albert Espinal.

**MIEMBRO PRINCIPAL**

# DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este trabajo, nos corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”.

(Reglamento de exámenes y títulos profesionales de la ESPOL)

---

Evelyn Stephanía Jiménez Bravo

---

José Eduardo Zerna Torres

# RESUMEN

En la actualidad las redes Wireless Mesh (redes malladas inalámbricas) se han convertido en una nueva área de la tecnología destinada a jugar un papel importante en el escenario de las redes inalámbricas de banda ancha debido a las ventajas que nos ofrece este tipo de redes, lo cual ha permitido un amplio aumento de aplicaciones tanto como una plataforma de investigación y como una tecnología que puede ser explotada comercialmente.

No obstante, uno de los principales retos en la investigación de este tipo de redes Inalámbricas Malladas es poder ofrecer escalabilidad, es decir, mientras mayor sea el área, mayor debe ser el número de usuarios que pueden acceder a ella. Es por este motivo, que la calidad de servicio (QoS) es un factor importante en su implementación, el aumento de nodos implica que se produzca un aumento del retardo, ya que los paquetes deben atravesar más nodos hasta su destino final. Para evitar esto, se hace uso de métricas que sean adecuadas para cada tipo de servicio.

Este proyecto se basará en analizar las redes Inalámbricas Malladas usando cuatro protocolos de enrutamiento mallado, empleando las dos clases representativas de los mismos: proactivos y reactivos. Para ello, se verificara la calidad de servicio (QoS) que cada uno de ellos nos brinda. Los

parámetros que serán analizados en el proyecto serán: el consumo de ancho de banda, jitter, retraso, pérdida de paquetes.

En el primero capítulo se procederá a describir los antecedentes, el problema planteado, los objetivos alcanzados y la justificación de porqué se realiza la implantación de la red inalámbrica mallada.

En el segundo capítulo, se procederá a describir el marco teórico, explicando qué son las redes inalámbricas malladas, la funcionalidad de este tipo de redes, los estándares que las rigen, los protocolos de enrutamiento de malla usados para el envío de información entre los nodos, establecer las diferencias entre ellos, análisis detallado de cada protocolo que será utilizado en este proyecto, explicación de los parámetros que determinará el protocolo más eficiente.

En el tercer capítulo, se describen las herramientas utilizadas para la implementación de la red, la descripción de la posición de cada enrutador dentro de las instalaciones de la Facultad, así como la instalación, configuración y desarrollo de cada uno de los protocolos que serán analizados en el proyecto.

En el cuarto capítulo, se detallan las pruebas realizadas con cada protocolo de enrutamiento de malla por medio de la captura de paquetes para su posterior análisis de la calidad de servicio (QoS) que cada uno de ellos ofrece.

En el quinto Capítulo, se procederá a realizar el análisis comparativo de los protocolos proactivos y reactivos de la red inalámbrica mallada con el objetivo de determinar el más eficiente.

# INDICE GENERAL

RESUMEN

ÍNDICE GENERAL

ABREVIATURAS

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

<b>1. ANTECEDENTES Y JUSTIFICACION</b> .....	1
1.1 Antecedentes .....	1
1.2 Definición del problema .....	5
1.3 Objetivos .....	6
1.4 Justificación .....	7
<b>2. ANALISIS CONCEPTUAL Y DISEÑO</b> .....	10
2.1 Redes Wireless Mesh.....	10
2.1.1 Funcionalidad.....	14
2.2 Protocolos de enrutamiento Mesh .....	17
2.2.1 Clases de protocolos .....	18
2.3 Protocolo de mejor aproximación a la Adhoc móvil (B.A.T.M.A.N) .....	19
2.4 Protocolo Roofnet .....	23
2.5 Protocolo Wing.....	25
2.6 Protocolo Optimización del estado del enlace (O.L.S.R.).....	28
2.7 Parámetros a evaluar con la finalidad de determinar el protocolo más eficiente .....	31
2.7.1 Pérdida de paquetes .....	31
2.7.2 Jitter .....	33
2.7.3 Paquetes VOIP .....	34

2.7.1 Retardo .....	35
<b>3. HERRAMIENTAS DE IMPLEMENTACIÓN.....</b>	<b>39</b>
3.1 Tipos de dispositivos a utilizar en la red Mesh .....	39
3.2 Análisis de la posición de cada router en instalaciones de la FIEC.. .....	52
3.3 Instalación y configuración del firmware (OPENWRT) .....	57
3.4 Instalación de Asterisk en servidor .....	72
3.5 Instalación y configuración de B.A.T.M.A.N .....	75
3.5 Instalación y configuración de Roofnet.....	80
3.5 Instalación y configuración de Wing .....	85
3.5 Instalación y configuración de O.L.S.R.....	98
<b>4. PRUEBAS DE CALIDAD DE SERVICIO.....</b>	<b>113</b>
4.1 Pruebas empleando B.A.T.M.A.N como protocolo de enrutamiento inalámbrico Mesh .....	113
4.1.1 Pérdida de paquetes, jitter, ancho de banda, retardo ..	114
4.2 Pruebas empleando Roofnet como protocolo de enrutamiento inalámbrico Mesh .....	125
4.2.1 Pérdida de paquetes, jitter, ancho de banda, retardo ..	125
4.3 Pruebas empleando Wing como protocolo de enrutamiento inalámbrico Mesh .....	129
4.3.1 Pérdida de paquetes, jitter, ancho de banda, retardo ..	129
4.4 Pruebas empleando OLSR como protocolo de enrutamiento inalámbrico Mesh .....	141
4.4.1 Pérdida de paquetes, jitter, ancho de banda, retardo .	141
<b>5. ANALISIS DE LOS RESULTADOS.....</b>	<b>211</b>
5.1 Análisis comparativo de los protocolos proactivos y reactivos en la red implementada.....	211

CONCLUSIONES

RECOMENDACIONES

GLOSARIO

ANEXOS

BIBLIOGRAFÍA

# ABREVIATURAS

WMN	Wireless Mesh Network Red Inalámbrica Mallada
QoS	Quality of Service Calidad de Servicio
MANET	Mobile Ad Hoc Network Red Móvil Ad Hoc
WLAN	Wireless Lan Network Red Inalámbrica de área local
WPAN	Wireless Personal Area Network Red Inalámbrica de área personal
WMAN	Wireless Metropolitan Area Network Red Inalámbrica de área metropolitana
ISP	Internet Service Provider Proveedor de Servicios de Internet
OLSR	Optimized Link State Routing Protocolo optimización del estado del enlace
WING	Wireless Mesh Network for Next-Generation Internet Red inalámbrica de próxima generación de Internet
BATMAN	Better Approach To Mobile Adhoc Networking

	Protocolo de Mejor aproximación a la red ad hoc móvil
RTP	Real-time Transport Protocol Protocolo de Transporte de Tiempo real
LAN	Local Area Network Red de area local
SSH	Secure Shell Intérprete de órdenes seguras
VLAN	Virtual Local Area Network Red de Área Local Virtual
PBX	Private Branch Exchange Ramal privado de conmutación automática
SSID	Service Set Identifier Servicio de Identificador de Conjunto

# INDICE DE FIGURAS

Figura 2.1: Red en malla .....	11
Figura 2.2: Red inalámbrica en malla .....	12
Figura 2.3: Compartición de Internet en una WMN .....	14
Figura 2.4: Logo del protocolo B.A.T.M.A.N .....	19
Figura 2.5: Logo de OLSR .....	28
Figura 2.6: Propagación de mensajes de enrutamiento por OLSR .....	29
Figura 3.1: Arquitectura de una red de malla inalámbrica .....	43
Figura 3.2: Enrutador Linksys WRT54GL .....	45
Figura 3.3: Enrutador Meraki Outdoor .....	45
Figura 3.4: Enrutador D- Link DIR-825 .....	46
Figura 3.5: Logo Wireshark .....	48
Figura 3.6: Softphone X-Lite .....	50
Figura 3.7: Red WMN implementada Protocolo Batman, OLSR y Wing .....	53
Figura 3.8: Red WMN implementada Protocolo Roofnet .....	54
Figura 3.9: Distribución de zonas en protocolo BATMAN .....	55
Figura 3.10: Distribución de zonas en protocolo Roofnet .....	56
Figura 3.11: Presentación inicial de OpenWrt en Linksys WRT54GL .....	60
Figura 3.12: Presentación inicial de OpenWrt en D-Link Dir 825.....	68
Figura 3.13: Logo de Elastix .....	73
Figura 3.14: Extensiones en servidor Elastix .....	74
Figura 3.15: Captura de paquetes BATMAN en Wireshark .....	80

Figura 3.16: Inicio de sesión en página de Meraki .....	81
Figura 3.17: Nodos de la Red WMN Roofnet .....	82
Figura 3.18: Administración de la Red WMN Roofnet .....	83
Figura 3.19: Propagación de la señal del Meraki Outdoor .....	84
Figura 3.20: Rutas creadas dinámicamente- Enrutador 1 .....	94
Figura 3.21: Rutas creadas dinámicamente- Enrutador 2 .....	95
Figura 3.22: Rutas creadas dinámicamente- Enrutador 3 .....	96
Figura 3.23: Rutas creadas dinámicamente- Enrutador 4 .....	97
Figura 3.24: Captura de paquetes O.L.S.R. en Wireshark .....	104
Figura 3.25: Rutas creadas O.L.S.R - Enrutador 1 .....	105
Figura 3.26: Rutas creadas O.L.S.R - Enrutador 2.....	106
Figura 3.27: Rutas creadas O.L.S.R. - Enrutador 3.....	107
Figura 3.28: Rutas creadas dinámicamente- Enrutador 4 .....	108
Figura 4.1: Captura de paquetes del enrutador 1 en Zona 1 (BATMAN)	113
Figura 4.2: Captura de paquetes del enrutador 2 en Zona 1 (BATMAN)	114
Figura 4.3: Captura de paquetes del enrutador 2 en Zona 1-cliente Softphone (BATMAN).....	114
Figura 4.4: Steam RTP en el cliente en la dirección de avance en Zona 1 (BATMAN) .....	115
Figura 4.5: Steam RTP en el cliente en la dirección de reversa en Zona 1 (BATMAN) .....	115
Figura 4.6: Captura de paquetes del enrutador 1 en Zona 2 (BATMAN)	116
Figura 4.7: Captura de paquetes del enrutador 2 en Zona 2 (BATMAN)	116
Figura 4.8: Captura de paquetes del enrutador 3 en Zona 2 (BATMAN)	117
Figura 4.9: Captura de paquetes del cliente en Zona 2 (BATMAN).....	117
Figura 4.10: Steam RTP en el cliente en la dirección de avance en	

Zona 2 (BATMAN) .....	118
Figura 4.11: Steam RTP en el cliente en la dirección de reversa en Zona 2 (BATMAN) .....	118
Figura 4.12: Captura de paquetes del enrutador 1 en Zona 3 (BATMAN) .....	119
Figura 4.13: Captura de paquetes del enrutador 2 en Zona 3 (BATMAN) .....	119
Figura 4.14: Captura de paquetes del enrutador 3 en Zona 3 (BATMAN) .....	120
Figura 4.15: Captura de paquetes del cliente en Zona 3 (BATMAN) .....	120
Figura 4.16: Steam RTP en el cliente en la dirección de avance en Zona 3 (BATMAN) .....	121
Figura 4.17: Steam RTP en el cliente en la dirección de reversa en Zona 3 (BATMAN) .....	121
Figura 4.18: Captura de paquetes del enrutador 1 en Zona 4 (BATMAN) .....	122
Figura 4.19: Captura de paquetes del cliente en Zona 4 (BATMAN).....	122
Figura 4.20: Steam RTP en el cliente en la dirección de avance en Zona 4 (BATMAN) .....	123
Figura 4.21: Steam RTP en el cliente en la dirección de reversa en Zona 4 (BATMAN) .....	123
Figura 4.22: Captura de paquetes del cliente en Zona 1(Roofnet) .....	124
Figura 4.23: Captura de paquetes del cliente 2 en Zona 1 (Roofnet) ....	125
Figura 4.24: Captura de paquetes del cliente 1 en Zona 2 (Roofnet) ....	125
Figura 4.25: Captura de paquetes del cliente 2 en Zona 2 (Roofnet) ....	126

Figura 4.26: Captura de paquetes del cliente 1 en Zona 3 (Roofnet) ....	126
Figura 4.27: Captura de paquetes del cliente 2 en Zona 3 (Roofnet) ....	127
Figura 4.28: Captura de paquetes del cliente 1 en Zona 4 (Roofnet) ....	127
Figura 4.29: Captura de paquetes del cliente 2 en Zona 4 (Roofnet) ....	128
Figura 4.30: Captura de paquetes del enrutador 1 en Zona 1(WING)...	129
Figura 4.31: Captura de paquetes del enrutador 2 en Zona 1 (WING)..	129
Figura 4.32: Captura de paquetes del cliente 1 en Zona 1 (WING).....	130
Figura 4.33: Steam RTP en el cliente en la dirección de avance en Zona 1 (WING) .....	130
Figura 4.34: Steam RTP en el cliente en la dirección de reversa en Zona 1 (WING) .....	131
Figura 4.35: Captura de paquetes del enrutador 1 en Zona 2 (WING)..	131
Figura 4.36: Captura de paquetes del enrutador 2 en Zona 2 (WING)..	132
Figura 4.37: Captura de paquetes del enrutador 3 en Zona 2 (WING)..	132
Figura 4.38: Captura de paquetes del cliente 1 en Zona 2 (WING).....	133
Figura 4.39: Steam RTP en el cliente en la dirección de avance en Zona 2 (WING) .....	133
Figura 4.40: Steam RTP en el cliente en la dirección de reversa en Zona 2 (WING) .....	134
Figura 4.41: Captura de paquetes del enrutador 1 en Zona 3 (WING)..	134
Figura 4.42: Captura de paquetes del enrutador 2 en Zona 3 (WING)..	135
Figura 4.43: Captura de paquetes del enrutador 3 en Zona 3 (WING)..	135
Figura 4.44: Captura de paquetes del enrutador 4 en Zona 3 (WING)..	136
Figura 4.45: Captura de paquetes del cliente en Zona 3 (WING).....	136
Figura 4.46: Steam RTP en el cliente en la dirección de avance en Zona 2 (WING) .....	137

Figura 4.47: Steam RTP en el cliente en la dirección de reversa en Zona 2 (WING) .....	137
Figura 4.48: Captura de paquetes del enrutador 1 en Zona 4 (WING)..	138
Figura 4.49: Captura de paquetes del cliente en Zona 4 (WING).....	138
Figura 4.50: Steam RTP en el cliente en la dirección de avance en Zona 4 (WING) .....	139
Figura 4.51: Steam RTP en el cliente en la dirección de reversa en Zona 4 (WING) .....	139
Figura 4.52: Captura de paquetes del enrutador 1 en Zona 1(WING)...	140
Figura 4.53: Captura de paquetes del enrutador 2 en Zona 1(OLSR)...	141
Figura 4.54: Captura de paquetes del cliente en Zona 1 (OLSR).....	141
Figura 4.55: Steam RTP en el cliente en la dirección de avance en Zona 1 (OLSR) .....	142
Figura 4.56: Steam RTP en el cliente en la dirección de reversa en Zona 1 (OLSR) .....	142
Figura 4.57: Captura de paquetes del enrutador 1 en Zona 2 (OLSR)..	143
Figura 4.58: Captura de paquetes del enrutador 2 en Zona 2 (OLSR)..	143
Figura 4.59: Captura de paquetes del enrutador 3 en Zona 2 (OLSR)..	144
Figura 4.60: Captura de paquetes del enrutador 4 en Zona 2 (OLSR) .	144
Figura 4.61: Captura de paquetes del cliente en Zona 2 (OLSR).....	145
Figura 4.62: Steam RTP en el cliente en la dirección de avance en Zona 2 (OLSR) .....	145
Figura 4.63: Steam RTP en el cliente en la dirección de reversa en Zona 2 (OLSR) .....	146
Figura 4.64: Captura de paquetes del enrutador 1 en Zona 3 (OLSR)..	146
Figura 4.65: Captura de paquetes del enrutador 2 en zona 3 (OLSR) ..	147

Figura 4.66: Captura de paquetes del enrutador 3 en zona 3 (OLSR) ..	147
Figura 4.67: Captura de paquetes del enrutador 4 en zona 3 (OLSR) ..	148
Figura 4.68: Captura de paquetes del cliente en zona 3 (OLSR) .....	148
Figura 4.69: Steam RTP en el cliente en la dirección de avance en Zona 3 (OLSR) .....	149
Figura 4.70: Steam RTP en el cliente en la dirección de reversa en Zona 3 (OLSR) .....	149
Figura 4.71: Captura de paquetes del enrutador 1 en Zona 4 (OLSR)..	150
Figura 4.72: Captura de paquetes del cliente en Zona 4 (OLSR).....	150
Figura 4.73: Steam RTP en el cliente en la dirección de avance en Zona 4 (OLSR) .....	151
Figura 4.74: Steam RTP en el cliente en la dirección de reversa en Zona 4 (OLSR) .....	151
Figura 4.75: Exportación a Excel de los paquetes de cada protocolo de enrutamiento capturados con Wireshark .....	152
Figura 4.76: Información de estadística descriptiva para OLSR en la zona 1 .....	154
Figura 4.77: Histograma de frecuencias para el retardo de OLSR en la zona 1 .....	154
Figura 4.78: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 1 .....	155
Figura 4.79: Histograma de frecuencias para el Jitter de OLSR en la zona 1 .....	155
Figura 4.80: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 1.....	156
Figura 4.81: Histograma de frecuencias para el Ancho de Banda	

de OLSR en la zona 1 .....	156
Figura 4.82: Resultado de prueba de intervalos de confianza para el Ancho de Banda de OLSR en la zona 1 .....	157
Figura 4.83: Información de estadística descriptiva para BATMAN en la zona 1 .....	157
Figura 4.84: Histograma de frecuencias para el retardo de BATMAN en la zona 1 .....	158
Figura 4.85: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 1 .....	158
Figura 4.86: Histograma de frecuencias para el Jitter de BATMAN en la zona 1 .....	159
Figura 4.87: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 1 .....	159
Figura 4.88: Histograma de frecuencias para el Ancho de Banda de BATMAN en la zona 1 .....	160
Figura 4.89: Resultado de prueba de intervalos de confianza para el Ancho de Banda de BATMAN en la zona 1 .....	160
Figura 4.90: Información de estadística descriptiva para Roofnet en la zona 1 .....	161
Figura 4.91: Histograma de frecuencias para el Retardo de Roofnet en la zona 1 .....	161
Figura 4.92: Resultado de prueba de intervalos de confianza para el retardo de Roofnet en la zona 1 .....	162
Figura 4.93: Histograma de frecuencias para el Jitter de Roofnet en la zona 1 .....	162
Figura 4.94: Resultado de prueba de intervalos de confianza	

para el jitter de Roofnet en la zona 1 .....	163
Figura 4.95: Histograma de frecuencias para el Ancho de Banda de Roofnet en la zona 1 .....	163
Figura 4.96: Resultado de prueba de intervalos de confianza para el Ancho de Banda de Roofnet en la zona 1 .....	164
Figura 4.97: Información de estadística descriptiva para WING en la zona 1 .....	164
Figura 4.98: Histograma de frecuencias para el retardo de WING en la zona 1 .....	165
Figura 4.99: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 1 .....	165
Figura 4.100: Histograma de frecuencias para el jitter de WING en la zona 1 .....	166
Figura 4.101: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 1 .....	166
Figura 4.102: Histograma de frecuencias para el ancho de banda de WING en la zona 1 .....	167
Figura 4.103: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 1 .....	167
Figura 4.104: Información de estadística descriptiva para OLSR en la zona 2 .....	168
Figura 4. 105: Histograma de frecuencias para el retardo de OLSR en la zona 2 .....	168
Figura 4.106: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 2 .....	169
Figura 4.107: Histograma de frecuencias para el jitter de OLSR	

en la zona 2 .....	169
Figura 4.108: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 2.....	170
Figura 4.109: Histograma de frecuencias para el ancho de banda de OLSR en la zona 2 .....	170
Figura 4.110: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 2.....	171
Figura 4.111: Información de estadística descriptiva para BATMAN en la zona 2 .....	171
Figura 4.112: Histograma de frecuencias para el retardo de BATMAN en la zona 2 .....	172
Figura 4.113: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 2.....	172
Figura 4.114: Histograma de frecuencias para el jitter de BATMAN en la zona 2 .....	173
Figura 4.115: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 2 .....	173
Figura 4.116: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 2 .....	174
Figura 4.117: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 2.....	174
Figura 4.118: Información de estadística descriptiva para ROOFNET en la zona 2 .....	175
Figura 4.119: Histograma de frecuencias para el retardo de ROOFNET en la zona 2 .....	175
Figura 4.120: Resultado de prueba de intervalos de confianza	

para el retardo de ROOFNET en la zona 2 .....	176
Figura 4.121: Histograma de frecuencias para el jitter de ROOFNET en la zona 2 .....	176
Figura 4.122: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 2 .....	177
Figura 4.123: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 2 .....	177
Figura 4.124: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 2 .....	178
Figura 4.125: Información de estadística descriptiva para WING en la zona 2 .....	178
Figura 4.126: Histograma de frecuencias para el retardo de WING en la zona 2 .....	179
Figura 4.127: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 2 .....	179
Figura 4.128: Histograma de frecuencias para el jitter de WING en la zona 2 .....	180
Figura 4.120: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 2 .....	180
Figura 4.130: Histograma de frecuencias para el ancho de banda de WING en la zona 2 .....	181
Figura 4.131: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 2 .....	181
Figura 4.132: Información de estadística descriptiva para OLSR en la zona 3 .....	182
Figura 4.133: Histograma de frecuencias para el retardo de OLSR	

en la zona 3 .....	182
Figura 4.134: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 3 .....	183
Figura 4.135: Histograma de frecuencias para el jitter de OLSR en la zona 3 .....	183
Figura 4.136: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 3 .....	184
Figura 4.137: Histograma de frecuencias para el ancho de banda de OLSR en la zona 3 .....	184
Figura 4.138: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 3 .....	185
Figura 4.139: Información de estadística descriptiva para BATMAN en la zona 3 .....	185
Figura 4.140: Histograma de frecuencias para el retardo de BATMAN en la zona 3 .....	186
Figura 4.141: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 3 .....	186
Figura 4.142: Histograma de frecuencias para el jitter de BATMAN en la zona 3 .....	187
Figura 4.143: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 3 .....	187
Figura 4.144: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 3 .....	188
Figura 4.145: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 3 .....	188
Figura 4.146: Información de estadística descriptiva para ROOFNET	

en la zona 3 .....	189
Figura 4.147: Histograma de frecuencias para el retardo de ROOFNET en la zona 3 .....	189
Figura 4.148: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 3 .....	190
Figura 4.149: Histograma de frecuencias para el jitter de ROOFNET en la zona 3 .....	190
Figura 4.150: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 3 .....	191
Figura 4.151: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 3 .....	191
Figura 4.152: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 3 .....	192
Figura 4.153: Información de estadística descriptiva para WING en la zona 3 .....	192
Figura 4.154: Histograma de frecuencias para el retardo de WING en la zona 3 .....	193
Figura 4.155: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 3 .....	193
Figura 4.156: Histograma de frecuencias para el jitter de WING en la zona 3 .....	194
Figura 4.157: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 3 .....	194
Figura 4.158: Histograma de frecuencias para el ancho de banda de WING en la zona 3 .....	195
Figura 4.159: Resultado de prueba de intervalos de confianza	

para el ancho de banda de WING en la zona 3.....	195
Figura 4.160: Información de estadística descriptiva para OLSR en la zona 4.....	196
Figura 4.161: Histograma de frecuencias para el retardo de OLSR en la zona 4.....	196
Figura 4.162: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 4.....	197
Figura 4.163: Histograma de frecuencias para el jitter de OLSR en la zona 4.....	197
Figura 4.164: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 4.....	198
Figura 4.165: Histograma de frecuencias para el ancho de banda de OLSR en la zona 4.....	198
Figura 4.166: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 4.....	199
Figura 4.167: Información de estadística descriptiva para BATMAN en la zona 4.....	199
Figura 4.168: Histograma de frecuencias para el retardo de BATMAN en la zona 4.....	200
Figura 4.169: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 4.....	200
Figura 4.170: Histograma de frecuencias para el jitter de BATMAN en la zona 4.....	201
Figura 4.171: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 4.....	201
Figura 4.172: Histograma de frecuencias para el ancho de banda	

de BATMAN en la zona 4 .....	202
Figura 4.173: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 4.....	202
Figura 4.174: Información de estadística descriptiva para ROOFNET en la zona 4 .....	203
Figura 4.175: Histograma de frecuencias para el retardo de ROOFNET en la zona 4 .....	203
Figura 4.176: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 4 .....	204
Figura 4.171: Histograma de frecuencias para el jitter de ROOFNET en la zona 4 .....	204
Figura 4.178: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 4.....	205
Figura 4.179: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 4.....	205
Figura 4.180: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 4 .....	206
Figura 4.181: Información de estadística descriptiva para WING en la zona 4 .....	206
Figura 4.182: Histograma de frecuencias para el retardo de WING en la zona 4 .....	207
Figura 4.183: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 4 .....	207
Figura 4.184: Histograma de frecuencias para el jitter de WING en la zona 4 .....	208
Figura 4.185: Resultado de prueba de intervalos de confianza	

para el jitter de WING en la zona 4.....	208
Figura 4.186: Histograma de frecuencias para el ancho de banda de WING en la zona 4 .....	209
Figura 4.187: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 4.....	209
Figura 5.1: Retardo en Zona 1.....	238
Figura 5.2: Retardo en Zona 2.....	238
Figura 5.3: Retardo en Zona 3.....	238
Figura 5.4: Retardo en Zona 4.....	238
Figura 5.5: Jitter en Zona 1.....	240
Figura 5.6: Jitter en Zona 2.....	240
Figura 5.7: Jitter en Zona 3.....	240
Figura 5.8: Jitter en Zona 4.....	240
Figura 5.9: Ancho de Banda consumido en Zona 1.....	242
Figura 5.10: Ancho de Banda consumido en Zona 2.....	242
Figura 5.11: Ancho de Banda consumido en Zona 3.....	242
Figura 5.12: Ancho de Banda consumido en Zona 4.....	242

# INDICE DE TABLAS

Tabla I	– Especificación de cliente de malla .....	47
Tabla II	– Especificación de cliente fijo .....	48
Tabla III	– Extensiones utilizadas .....	51
Tabla VI	– Distribución de las zonas .....	57
Tabla V	– Distribución de las direcciones IP .....	57
Tabla VI	– Especificaciones del servidor .....	74
Tabla VII	– Direcciones Ip's Protocolo Wing .....	93
Tabla VIII	– Zona 1 Valores obtenidos de Retardo .....	244
Tabla IX	– Zona 2 Valores obtenidos de Retardo .....	245
Tabla X	– Zona 3 Valores obtenidos de Retardo .....	246
Tabla XI	– Zona 4 Valores obtenidos de Retardo .....	246
Tabla XII	– Zona 1 Valores obtenidos de Jitter .....	247
Tabla XIII	– Zona 2 Valores obtenidos de Jitter .....	248
Tabla XIV	– Zona 3 Valores obtenidos de Jitter .....	249
Tabla XV	– Zona 4 Valores obtenidos de Jitter .....	249
Tabla XVI	– Zona 1 Valores obtenidos de Ancho de Banda .....	250
Tabla XVII	– Zona 2 Valores obtenidos de Ancho de Banda .....	251
Tabla XVIII	– Zona 3 Valores obtenidos de Ancho de Banda .....	252
Tabla XIX	– Zona 4 Valores obtenidos de Ancho de Banda .....	253
Tabla XX	– Pérdida de paquetes por zona para cada protocolo .....	253

# INTRODUCCIÓN

Actualmente, los investigadores han centrado su trabajo principalmente en explorar y explotar la industria de la tecnología y la comunicación por lo cual encontramos un incremento en el despliegue de tecnologías cada vez más complejas en las redes inalámbricas que mejoran muchos los aspectos de la vida cotidiana.

Las redes inalámbricas de malla de sus siglas en inglés (WMN) es una prometedora tecnología para múltiples aplicaciones comerciales emergentes tales como: implementar comunidades y vecindarios a una misma red, creación de sistemas de transporte inteligente razón por la cual los proveedores de internet han centrado toda su atención puesto que brinda a sus usuarios finales acceso fiable a los servicios inalámbricos de banda ancha a un costo razonable en comparación con las otras tecnologías, además las WMN ofrecen un mantenimiento fácil de la red, robustez y en combinación con tecnologías avanzadas de radio permite el manejo de múltiples interfaces de radio y antenas inteligentes.

Este tipo de redes al poseer características únicas generan todo tipo de investigaciones acerca diseño de la arquitectura y los protocolos de enrutamiento de la red que van desde la capa de aplicación hasta la capa física.

Los protocolos de enrutamiento de malla deben ser lo suficientemente eficiente para permitir la auto-configuración de la red, la auto recuperación en caso de falla de algún nodo, brindar la seguridad de todo los nodos existentes, tolerar la interoperabilidad e integración de redes heterogéneas, aceptar la escalabilidad de la red y cumplir con los parámetros de calidad de servicio los cuales son de vital importancia en una configuración de redes inalámbricas malladas.

Este proyecto plantea la implementación de una WMN la cual consta de una serie de enrutadores dentro de las instalaciones de la FIEC con el objetivo de determinar el protocolo de enrutamiento que sea más eficiente y que cumpla con las características que previamente fueron descritas para lo cual se procederá a medir el ancho de banda usado, la pérdida de paquetes experimentada, el jitter y retraso que presentó la red y los paquetes VOIP perdidos.

# CAPITULO 1

## 1. ANTECEDENTES Y JUSTIFICACION

En este capítulo se provee información acerca de los antecedentes sobre los cuáles se plantearon los objetivos, una explicación más detallada del problema a tratar y la justificación del presente trabajo.

### 1.1 Antecedentes

El objetivo de las redes inalámbricas malladas es mejorar o ampliar la cobertura de las redes inalámbricas tradicionales, lo cual permite abarcar aquellas zonas en las que no es posible instalar cableado para proporcionar conectividad de red a los puntos de acceso razón por la cual tuvieron su origen principalmente para los entornos militares con lo cual se permitía

a los soldados tener comunicación confiable de banda ancha en cualquier lugar.

La telefonía móvil de red Ad-Hoc de sus siglas en inglés (MANET) es una red dinámica formada por dispositivos móviles sin necesidad de cualquier infraestructura existente o de la configuración previa de la red. Una red de malla inalámbrica (WMN) es un tipo particular de una MANET, las cuales tienen como objetivo permitir el acceso total de la banda ancha para un gran número de usuarios (1).

Las redes inalámbricas de malla (WMNS) se componen de dos elementos principales: los enrutadores de malla y los clientes de malla; en la cual los enrutadores de malla se encargan de formar una infraestructura inalámbrica / backbone y también de interactuar con las redes cableadas para proporcionar conectividad inalámbrica de Internet de múltiples saltos para los clientes de malla.

Al igual que las MANETS, las WMN también tienen las habilidades de auto-organización, auto-descubrimiento, auto-recuperación y auto-configuración lo cual proporciona conectividad inalámbrica de Internet adaptable y flexible a los usuarios móviles, sin embargo

las WMN son comunes encontrarlas como una configuración estática de enrutadores. En este tipo de redes se pueden utilizar para diferentes tecnologías de acceso inalámbrico tales como los estándares IEEE 802.11, 802.15, 802.16, basados en la red de área local inalámbrica (WLAN), redes inalámbricas de áreas personales (WPAN), y la red inalámbrica de área metropolitana (WMAN) respectivamente (2).

Las WMN basan su estructura de red principalmente en los protocolos de enrutamiento los cuales son más importantes para que la red funcione que las conexiones físicas, puesto que permiten la comunicación entre los nodos que pertenecen a la red, razón por la cual éstos son diseñados por capas con funciones independiente del resto de las capas. De esta manera cuando se quiere transmitir un mensaje que se origina en la capa más baja va atravesando las diferentes capas hasta llegar a la más alta.

Los protocolos de enrutamiento de malla tienen como objeto revelar las rutas de la red, realizar el encaminamiento adecuado de los datos y controlar el mantenimiento de las rutas.

A lo largo de los años se ha ido desarrollando y mejorando los protocolos de enrutamiento para ofrecer cada vez más un mejor servicio. Es así que en el 2003, LugoMesh, un proyecto de Grupo de Usuarios de Software Libre de la ciudad de Rosario, crea una red comunitaria, no dependiente de ISP's y que utiliza exclusivamente Software Libre en sus implementaciones.

A mediados del 2007, implementan una Red inalámbrica utilizando tecnología mallada. El proyecto tomó el nombre de LUGRo-Mesh, y cuenta con 27 nodos y 2035 usuarios.

En un comienzo, trabajaron con BerlinRoofnet, Wing y Robin. Sin embargo, su trabajo no fue tan simple ni tan eficiente, y pasaron a trabajar con B.A.T.M.A.N. bajo Nightwing.

WING empezó hace apenas 3 años como un proyecto en redes inalámbricas malladas. Parte del software desarrollado es construido sobre Roofnet, una red mallada 802.11b/g experimental. WING extiende el proyecto original añadiendo soporte para interfaces para múltiples radios.

Existen varias implementaciones para el Protocolo Optimización del Estado del Enlace (OLSR) que comenzaron como un borrador IETF

escrito en el INRIA en Francia. La implementación de olsr.org comenzó como la tesis de máster de Andreas Toennesen en la Universidad Unik. OLSR se modificó con base en la experiencia práctica de las redes comunitarias gratuitas. El OLSR actual difiere significativamente del borrador original porque incluye un mecanismo denominado Link Quality Extension (Extensión de la Calidad del Enlace) que mide la cantidad de paquetes perdidos entre los nodos y calcula las rutas de acuerdo con esta información.

## **1.2 Definición del problema**

Las redes WMN ofrecen múltiples ventajas en el manejo de las redes, sin embargo, presentan dificultades al momento de ofrecer QoS de óptima calidad por lo cual no garantiza seguridad y robustez (3). Por esta razón es importante tener un protocolo de enrutamiento que permita tener escalabilidad, fiabilidad, flexibilidad y sobretodo calidad de servicio que es un factor esencial para poder realizar la selección de las mejores rutas para diferentes clases de tráfico.

El objetivo del presente proyecto es determinar el protocolo de enrutamiento que sea más eficiente, usado en la implementación de una red inalámbrica mallada dentro de la Facultad, con la finalidad de evitar el consumo innecesario de recursos, para lo cual se procederá a medir el

ancho de banda consumido, la pérdida de paquetes experimentada, el jitter y retraso que presentó la red y los paquetes VOIP perdidos.

### 1.3 Objetivos

La implementación de una red inalámbrica mallada (WMN) usando diversos puntos de las instalaciones de la Facultad de Ingeniería en Electrónica y Telecomunicaciones fue planteado para proporcionar un reporte detallado de la calidad de servicio (QoS) de los protocolos de enrutamiento de malla utilizados para poder determinar el más eficiente. Con la finalidad de lograr esto se trazaron los siguientes objetivos:

- ✓ Comparar la calidad de servicio que ofrecen los protocolos inalámbricos de malla, tanto de tipo proactivo como reactivo. Para ello, se tomarán cuatro protocolos de enrutamiento: B.A.T.M.A.N, Roofnet, Wing, OLSR.
- ✓ Tomar medición de la cantidad de paquetes perdidos, el ancho de banda consumido, el jitter, el retardo producido y los paquetes VOIP perdidos, empleando la herramienta de captura de paquetes Wireshark.

## 1.4 Justificación

Las redes inalámbricas de malla proponen una nueva tecnología en las redes inalámbricas, permitiendo conectar con eficacia, de forma inalámbrica, ciudades enteras utilizando esta tecnología de bajo costo. Resuelven los dos problemas principales que se presentan cuando se quiere desplegar una red en un área densamente poblada:

- 1.- La interferencia resultante de usar espectro libre.
- 2.- La necesidad de que todas las estaciones de usuario tengan línea de vista con la estación base.

Otras ventajas es que las estaciones transmiten a menor potencia y por lo tanto pueden emplear mayores velocidades de transmisión, y además se facilita distribuir el acceso a Internet en varios puntos.

### **Ventajas principales:**

- ✓ Disminuye la interferencia.
- ✓ Facilidad de crecimiento y de sostenimiento.
- ✓ Organización y modelo de negocio cooperativo.

- ✓ Red robusta y flexible.
- ✓ Integración con otro tipo de redes.
- ✓ Ambientes urbanos y rurales
- ✓ Permite eliminar el cableado de las redes alámbricas.
- ✓ Es la única solución actual que permite la total movilidad de los usuarios.

### **Elementos de enrutamiento de malla**

- ✓ Cálculo de las rutas
  - Manejo de direcciones IP
  - Manejo de la red troncal (uplink, backhaul)
- ✓ Descubrimiento de nodos.
- ✓ Descubrimiento de la frontera.

Los protocolos de enrutamiento permiten a los enrutadores dirigir o enrutar los paquetes hacia diferentes redes usando tablas de enrutamiento. Para realizar este cálculo, utilizan diferentes criterios según

el protocolo a usar los cuales pueden ser: la métrica, la distancia administrativa, vector distancia, entre otros.

### **Tipos de protocolos de enrutamiento de malla**

Existen dos tipos:

- ✓ Proactivos o basados en tablas. Buscan rutas periódicamente, suponiendo que serán útiles Ejemplo: OLSR, B.AT.M.A.N
- ✓ Reactivos o por demanda. Buscan una ruta solo cuando se necesita Ejemplo: AODV, DSR.

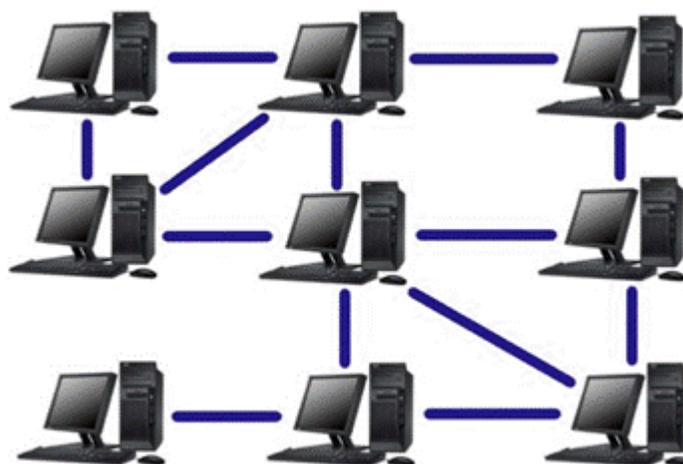
# **CAPITULO 2**

## **2. ANÁLISIS CONCEPTUAL Y DISEÑO**

### **2.1 Redes Wireless Mesh**

Una red en malla es simplemente una topología de red en la cual cada uno de los nodos que la componen está conectado a todos los demás nodos de la red. Es así, que la información puede ir de un nodo a otro a través de diversas rutas.

Una red inalámbrica mallada, no es más que una red en malla que ha sido implementada sobre una red inalámbrica LAN, conservando así los mismos atributos de una red mallada cableada, pero con las ventajas (y también con sus debidas desventajas) que provee una red inalámbrica.

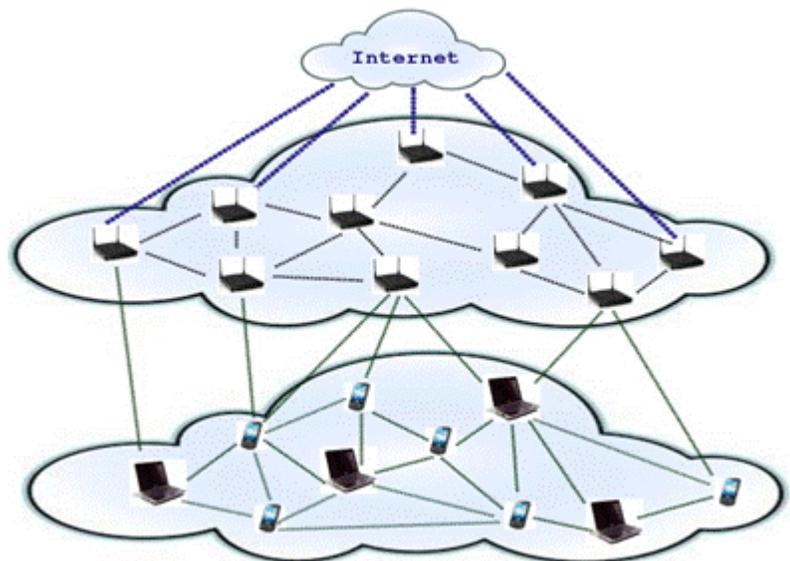


*Figura. 2.1: Red en malla*

Las redes inalámbricas en malla, o WMN de sus siglas en inglés (Wireless Mesh Networks), pueden incluso comunicar ciudades enteras usando tecnología relativamente de bajo costo ya existente. Mientras las redes comunes se basan en tener un pequeño número de puntos de acceso, cada uno con su cableado respectivo, en una WMN la conexión se propaga por medio de decenas o incluso cientos de nodos inalámbricos mallados que se comunican entre sí para compartir la conexión a la red a través del área de cobertura. Además, en una WMN, únicamente un nodo necesita estar conectado físicamente a Internet, por ejemplo a través de un módem DSL. Y es este único nodo, el que

comparte dicha conexión de manera inalámbrica a los nodos cercanos a él. Estos nodos, a su vez, comparten la conexión de manera inalámbrica a los nodos en sus vecindades. De esta manera, mientras más nodos existan en la red, mayor será la distancia que se esparcirá

la conexión.



**Figura 2.2: Red inalámbrica en malla**

En un ámbito general, entre las ventajas que las redes inalámbricas en malla nos ofrecen, constan las siguientes:

- ✓ Mientras más nodos se empleen, más grande y rápida se

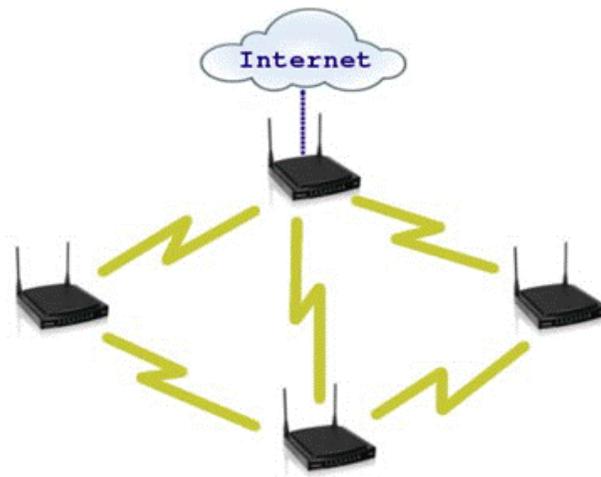
tornará la red inalámbrica.

- ✓ Utilizan los mismos estándares WiFi (802.11a, 802.11b, 802.11g, 802.11n) que son utilizados en la mayoría de las redes inalámbricas.
- ✓ Los nodos son fáciles de instalar y desinstalar, lo que permite que la red sea adaptable y escalable, en los eventuales casos en que se necesite mayor o menor cobertura.
- ✓ No es necesario realizar grandes obras para canalizaciones, puesto que sólo se necesita que un nodo esté conectado a Internet.
- ✓ El hecho de usar menos cables reduce significativamente los costos de instalar la red, especialmente cuando se trata de áreas de cobertura muy grandes.
- ✓ Se mitiga la interferencia.
- ✓ Es más fácil de instalar tanto en entornos urbanos como en rurales. Esto es conveniente especialmente donde no se puedan hacer conexiones de Ethernet en las paredes.
- ✓ La red automáticamente encuentra la ruta más fácil y más confiable para enviar los datos, incluso si algún nodo

perdiese la señal o estuviese bloqueado.

### 2.1.1 Funcionalidad

La figura 2-3 muestra el funcionamiento de una red inalámbrica en malla cuando se comparte una conexión a Internet a través de una LAN. Como se puede apreciar, únicamente un nodo está conectado directamente a Internet. Es éste nodo comparte esta conexión de manera inalámbrica con los nodos de su vecindad, los cuales, a su vez, la comparten con los nodos de sus respectivas vecindades y así sucesivamente.



**Figura. 2.3: Compartición de Internet en una WMN**

Esto implica que no se necesita que cada uno de los nodos esté conectado con cables a Internet. En realidad, no requieren estar conectados a ninguna parte alamburada, excepto su respectiva fuente de alimentación y están listos para funcionar.

Es por este motivo, que la compartición de Internet a través de una WMN es extremadamente eficiente. Mientras más nodos existan en la red, habrá mayor cobertura, y la conexión a Internet para los usuarios finales será más rápida y mejor.

La conexión mejora por dos motivos principales:

- ✓ Si una laptop se encuentra en el rango de cobertura de 4 nodos, hay disponible 4 veces el ancho de banda de un enrutador inalámbrico tradicional.
- ✓ La distancia juega un papel extremadamente importante en cuanto a la intensidad de la señal. Si se reduce a la mitad la distancia que hay entre el dispositivo final y el nodo, la intensidad de la señal será 4 veces más fuerte.

Cabe recalcar que los nodos pueden también proveer Internet a dispositivos en la red que necesiten de cables para funcionar; como por ejemplo: teléfonos IP, cámaras, servidores. Incluso, si

los nodos proveen de la tecnología de alimentación por Internet o PoE (Power over Internet), estos dispositivos no necesitan conectarse a tomas de corriente.

Incluso en una red inalámbrica en malla, llega un momento en que la información debe llegar a un punto de acceso con cableado, para llegar a Internet. El hacer llegar la información de regreso al punto de acceso, es lo que se conoce con el nombre de backhaul. Cuando la red es pequeña, el backhaul puede manejarse sin mayor complicación; pero, cuando la red es muy grande, únicamente ciertos nodos deben comportarse como nodos de backhaul. Todos los demás nodos envían la información a uno de los nodos de backhaul, el cual a su vez, la envía al punto de acceso con cableado.

Otro punto a acotar respecto a las WMN, es que las tarjetas de red de los dispositivos pueden comunicarse entre sí, incluso cuando están conectadas a diferentes puntos de acceso. Esto permite que los paquetes puedan ir directamente a de un dispositivo a otro hasta llegar a su destino, sin necesidad de pasar por el punto de acceso cercano al dispositivo de origen.

Para poder realizar eficientemente este paso de paquetes, es necesario contar con un protocolo de enrutamiento que permita enviar estos paquetes de la manera más eficiente, ya sea con el menor número de saltos, o con un número suficientemente bueno, aunque haya mayor cantidad de saltos que el mínimo; y que, además, sea tolerante a fallos en la red, debido a la caída de algún nodo.

## **2.2 Protocolos de Enrutamiento Mesh**

Los protocolos de enrutamiento definen varias maneras en que los enrutadores se comunican entre sí, con la finalidad de determinar la mejor ruta hacia cada destino.

Las funciones que un protocolo de enrutamiento debe realizar son:

- ✓ Aprender información sobre las rutas de enrutadores vecinos.
- ✓ Dar a conocer información sobre sus rutas a los enrutadores vecinos.
- ✓ Si más de una ruta posible existe a una subred, escoger la mejor ruta basada en la métrica.

- ✓ Si la topología de la red cambia -por ejemplo, un enlace falla- debe reaccionar dando a conocer que algunas rutas han fallado, y escoger una nueva mejor ruta. Este proceso se conoce como convergencia.

### 2.2.1 Clases de protocolos de enrutamiento mesh

Existen varios protocolos con la finalidad de enrutar paquetes a través de una red en malla. Estos se pueden clasificar de la siguiente manera:

**Protocolos reactivos:** Este tipo de protocolos buscan una ruta, únicamente cuando es necesario. Por ello, también se los conoce como protocolos bajo demanda. Entre ellos, se puede nombrar a AODV y a DSR.

Sus características principales son:

- ✓ Se asume latencia alta para el primer paquete.
- ✓ Si la topología cambia, la ruta individual se mantiene con vida por cierto tiempo.
- ✓ Las rutas tienen cierto grado de independencia entre ellas.

- ✓ La relación entre el número de rutas útiles y todas las rutas posibles es alta.

**Protocolos proactivos:** Estos protocolos buscan rutas de manera periódica, bajo la suposición de que sean de utilidad. Entre ellos figura OLSR.

Sus características principales son:

- ✓ Implican alguna variación de los protocolos de Estado de Enlace.
- ✓ Resulta primordial una respuesta rápida.
- ✓ Si se modifica una ruta, esta puede afectar a cualquier nodo.
- ✓ La relación entre el número de rutas útiles y todas las rutas posibles es relativamente baja.

### 2.3 Protocolo de mejor aproximación a la Adhoc móvil (B.A.T.M.A.N.)



Fuente: <http://en.wikipedia.org/wiki/B.A.T.M.A.N.>

**Figura 2.4: Logo del protocolo B.A.T.M.A.N**

El Protocolo de Mejor Aproximación a la Adhoc Móvil, o B.A.T.M.A.N. por sus siglas en inglés Better Approach To Mobile Adhoc Network, es un protocolo de enrutamiento bajo el desarrollo de la comunidad Freifunk, con la finalidad de sustituir al protocolo OLSR. Esta comunidad notó que OLSR tenía muchos defectos en su desempeño cuando la red era muy grande (aproximadamente 300 nodos).

B.A.T.M.A.N. se encarga de mantener proactivamente información sobre la existencia de todos los nodos en la malla, a los cuales se puede acceder con uno o varios saltos.

El algoritmo de este protocolo se basa en definir para cada destino dentro de la malla, un vecino de un salto, el cual es considerado como el mejor gateway para comunicarse con dicho nodo destino. Cada nodo realiza este procedimiento, hasta llegar al nodo final. Es decir, no es necesario calcular la ruta completa; lo importante, es aprender cuál es el próximo mejor salto para cada destino. De esta manera, se obtiene una implementación bastante rápida y eficiente.

B.A.T.M.A.N. realiza un análisis estadístico de la pérdida de paquetes del protocolo y velocidad de propagación, sin depender del estado de los nodos o de su información topológica. Las decisiones de enrutamiento no

se basan en la información contenida en el tráfico recibido del protocolo, puesto que el mismo puede tener retrasos o incluso puede perderse; más bien, se basan en el conocimiento sobre la falta o existencia de información. Es por este motivo, que los paquetes de este protocolo son muy pequeños y contienen muy poca información, y la pérdida de paquetes del protocolo debido a enlaces no confiables son detectados con la finalidad de tomar mejores decisiones de enrutamiento. Cada nodo individualmente toma su decisión de enrutamiento y B.A.T.M.A.N. elige la ruta más confiable basándose en ellas.

El algoritmo de B.A.T.M.A.N consiste en particionar el conocimiento de la mejor ruta entre nodos, a TODOS los nodos que conforman la malla. Así, cada nodo tiene la información sobre el próximo mejor salto hacia cada uno de los otros nodos. Es por ello, que se torna superfluo el conocimiento global sobre los cambios en la topología. Además, B.A.T.M.A.N contiene un mecanismo de inundación basado en eventos, el cual asegura que no existan lazos de capa de red, y limita el número de mensajes de topología que inunda la malla.

Puede resumirse el algoritmo del protocolo de la siguiente manera:

1. Cada nodo envía mensajes de difusión (broadcast), para que sus

vecinos sepan de su existencia. Estos mensajes se denominan Mensajes Originadores (OGM) y tienen un tamaño típico de 52 bytes, incluyendo el encabezado IP y UDP.

2. Los vecinos retransmiten los OGMs para informar a sus vecinos sobre la existencia del nodo que originó el OGM, y así sucesivamente.
3. Así, la red es inundada con OGMs. Cada uno de estos mensajes contiene, por lo menos, la dirección del nodo que originó el OGM, la dirección del nodo que retransmite el paquete, un tiempo de vida (TTL) y un número de secuencia.
4. Si el OGM sigue un ruta donde el enlace tiene una pobre calidad o esta saturado, habrán pérdida de paquetes o retrasos. Mientras que los OGMs que viajan por enlaces de buena calidad no tendrán inconvenientes y, evidentemente, llegarán antes.
5. Cada uno de los nodos retransmite, al menos una vez, cada mensaje originador que ha recibido; y únicamente envía hacia el nodo que originó el OGM, aquellos mensajes recibidos del vecino que ha sido identificado como el mejor próximo salto.
6. Así, los mensajes originadores son inundados en la red de manera selectiva y se emplean para que los nodos que los reciben tengan

conocimiento de otros nodos.

De esta manera, un nodo A tendrá conocimiento de la existencia de un nodo B cuando los OGMs del nodo B sean retransmitidos por su vecino de un salto. Ahora bien, si el nodo A tiene más de un vecino, para determinar cuál de ellos elige para enviar mensajes al nodo distante, se toman en cuenta los OGMs que recibe de manera más rápida y confiable.

Con este procedimiento, el algoritmo elige cuál vecino es el mejor próximo salto hacia el originador del mensaje y configura su respectiva tabla de enrutamiento.

#### **2.4 Protocolo de la Red Experimental Roofnet (Scrrr)**

Roofnet es el nombre que se le dio a una red 802.11b mallada experimental desarrollada por el MIT. El software de este proyecto está disponible gratuitamente como código abierto.

La característica principal de Roofnet es que no necesita configuración y por ende es sencillo de implementar y expandir. Un nuevo usuario puede simplemente encender un nuevo nodo y empezar a usarlo para acceder a Internet sin mayor configuración que el hecho de instalar el hardware.

El protocolo de enrutamiento que usa ROOFNET se llama ScrRR. La finalidad de este protocolo es encontrar las rutas con el rendimiento (throughput) más alto. Su diseño se basa en el Protocolo de Fuente de Enrutamiento Dinámico (DSR por sus siglas en inglés). Cuando un nodo A intenta encontrar una ruta hacia un nodo B, se envía un mensaje de difusión para consultar acerca del nodo B. Cada nodo X que recibe el mensaje, reenvía la consulta añadiendo su propio identificador en la ruta origen del paquete. Cada vez que el nodo B escucha una consulta sobre sí mismo, envía una respuesta al nodo A a lo largo de la ruta que se va creando. El nodo A, y todos los nodos que ven la consulta o la respuesta a la consulta, añade todos los enlaces mencionados en la respuesta a una base de datos que contiene los estados de enlaces locales y usa el algoritmo de Dijkstra en esa base de datos, para encontrar la mejor ruta. De esta manera, cuando el nodo A envía un paquete al nodo B, incluye esa ruta como ruta de origen en el paquete.

Principalmente, lo que diferencia a ScrRR de DSR es el hecho de que ScrRR emplea la métrica ETX para escoger rutas en buen estado. ETX continuamente hace mediciones de la tasa de pérdidas en ambos sentidos entre un nodo y sus vecinos, utilizando mensajes de difusión periódicos. Asigna a cada enlace una métrica que estima el número de

veces que un paquete necesita ser retransmitido para que sea recibido exitosamente.

## **2.5 Protocolo Wireless Mesh Network For Next- Generation Internet (Wing)**

WING de sus siglas en ingles (Red inalámbrica de próxima generación de Internet) es un proyecto de investigación que inició hace 3 años aproximadamente, con el auspicio del Ministerio italiano de Universidad e Investigación (MIUR-Ministero dell'Università e della Ricerca) y liderado por el centro de investigación sin fines de lucro CREATE-NET y el Instituto Technion

El proyecto fue creado con la finalidad de promover la cooperación científica entre CREATE-NET y Technion. Para ello, se creó a un equipo de investigación internacional de alto nivel en el área de algoritmos y protocolos de redes inalámbricas.

Parte del software desarrollado fue construido sobre Roofnet, una WMN experimental desarrollada por el MIT en Cambridge, Massachusetts. Wing modifica el proyecto original y le añade soporte para múltiples interfaces de radio, métrica de enrutamiento WCETT, y asignación automática de

canal. El software, en su totalidad, está disponible para toda la comunidad investigadora.

En sí, WING mantiene la misma configuración de Roofnet pero con módulos adicionales que son responsables de:

- ✓ **Adición adaptiva del tráfico:** Sistema que permite mejorar notablemente la capacidad de voz en la red, a través de la concatenación de paquetes.
- ✓ **Programación oportuna:** Un programador oportuno de direccionamiento de anomalías en el desempeño de la IEEE 802.11.
- ✓ **Provisionamiento de Calidad de Servicio (QoS):** Un marco que se basa en Servicios Diferenciados (DiffServ) para ofrecer límites más tenues de QoS.
- ✓ **Multi-Radio:** Un sistema de selección dinámica de canales que es capaz de explotar el uso de múltiples radios con la finalidad de construir y mantener el backhaul inalámbrico.

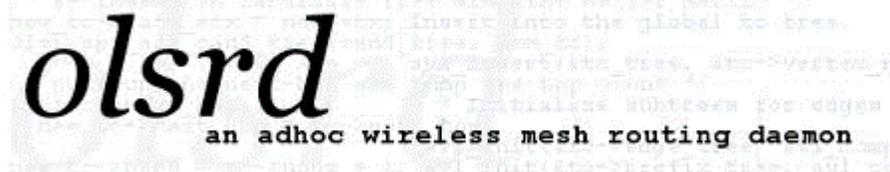
Los nodos de WING pueden detectar automáticamente si son simples nodos o si son puertas de enlace. El nodo se configura a sí mismo

automáticamente como puerta de enlace si se puede obtener una dirección IP mediante DHCP a través de uno de sus enlaces de subida (uplink) soportados. WING, en la actualidad, soporta Ethernet (*eth0* es la interfaz por defecto empleada por los nodos), IEEE 802.11 y UMTS.

La conectividad a Internet la proveen las puertas de enlace, empleando enlaces cableados o inalámbricos. Las puertas de enlace de la WMN pueden emplear WiFi, WiMax o UMTS para sus enlaces inalámbricos en la conexión punto a multipunto.

En cuanto a la Calidad de Servicio, WING implementa diversos avances destinados a mejorar la capacidad de voz del sistema, y métodos de aislamiento de flujos similares en el rendimiento, en ambientes con demasiado ruido.

## 2.6 Protocolo de Optimización del Estado de Enlace (O.L.S.R.)



Fuente: <http://www.olsr.org/>

**Figura 2.5: Logo de OLSR**

OLSR es un protocolo de enrutamiento de tipo proactivo desarrollado en un principio por investigadores de Instituto Nacional francés de Investigación en Informática y Automática, INRIA por sus siglas en francés. Posteriormente, OLSR fue estandarizado por el IETF y es descrito en el RFC3626. Es considerado, de hecho, como uno de los protocolos más prometedores y estables.

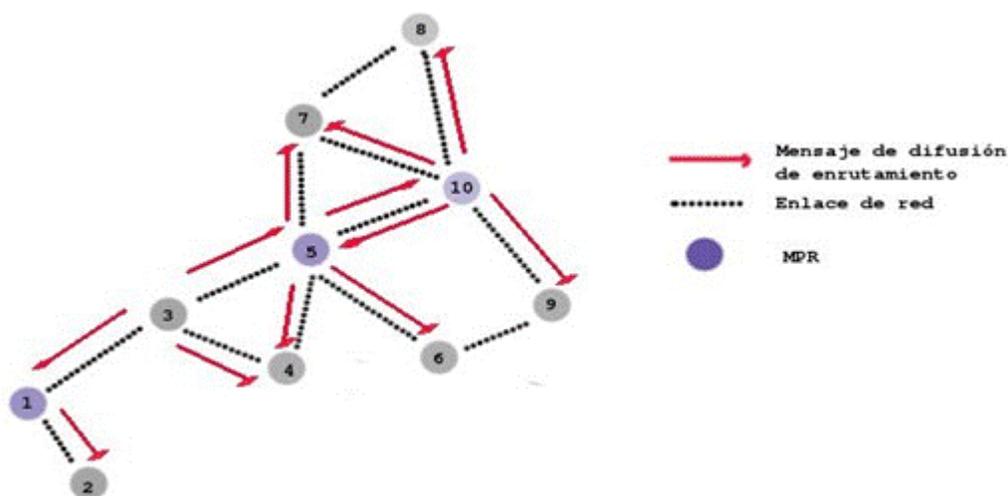
Para su funcionamiento, OLSR trabaja con un mecanismo denominado Relés Multipunto o MPR (de sus siglas en inglés MultiPoint Relays). Los MPR de un nodo A son sus vecinos que cumplen con la condición de que cada vecino de dos saltos de A es un vecino de un salto de al menos un MPR de A. Cada nodo transmite su lista de vecinos en señales periódicas, de tal manera que todos los nodos pueden conocer sus vecinos de 2 saltos, con la finalidad de elegir los MPRs.

De esta manera, OLSR reduce el encabezado de información de inundación de estado de enlace, al requerir menor cantidad de nodos para enviar la información. Un mensaje de difusión del nodo A es transmitido únicamente por sus MPRs.

La Figura 2.6.2. muestra cómo el protocolo de enrutamiento OLSR propaga mensajes de enrutamiento desde el nodo 3 por la red, a través de los MPRs seleccionados.

El código fuente de OLSR que es ejecutado en una red inalámbrica, puede hacer uso de dos tipos de métricas de enrutamiento:

- ✓ El RFC de OLSR hace uso de la métrica en enrutamiento de



Fuente: [http://wirelessafrica.meraka.org.za/wiki/images/9/98/Batman\\_ifip.pdf](http://wirelessafrica.meraka.org.za/wiki/images/9/98/Batman_ifip.pdf)

**Figura 2.6: Propagación de mensajes de enrutamiento por OLSR**

histéresis, para calcular la calidad del enlace entre dos nodos.

- ✓ La métrica de Conteo de Transmisión Esperada o ETX (Expected Transmission Count), es una métrica propuesta por el MIT, que también ha sido incorporada al código fuente para OLSR, pero que no es oficialmente parte del RFC. es considerada ampliamente como una métrica de enrutamiento superior a la de histéresis.

ETX calcula el número esperado de retransmisiones requeridas para que un paquete viaje desde y hacia un destino. La calidad del enlace,  $LQ$ , representa la fracción de paquetes exitosos que fueron recibidos por nosotros desde un vecino, en un período de ventana. La calidad del enlace de vecino,  $NLQ$ , representa la fracción de paquetes exitosos que fueron recibidos por el vecino de parte de nosotros, en un período de ventana. En base a esto, el ETX es calculado de la siguiente manera:

$$ETX = \frac{1}{LQ \times NLQ} \quad (1)$$

Donde un enlace es perfecto cuando ETX es igual a 1.

Para el control de tráfico, OLSR emplea básicamente dos tipos de mensajes:

- ✓ Mensajes HELLO, los cuales cada nodo envía de manera periódica

a sus nodos vecinos. Estos mensajes no son retransmitidos más allá del primer salto desde su emisor.

- ✓ Mensajes de control de topología (TC), los cuales se envían de manera periódica y asíncrona usando el mecanismo de MPRs. Estos mensajes, en cambio, deben llegar a todos los nodos de la red y permiten a cada nodo tener conocimientos de la topología, elaborar el árbol de caminos mínimos usando el algoritmo de Dijkstra y construir la tabla de enrutamiento.

## **2.7 Parámetros A Evaluar Con La Finalidad De Determinar El Protocolo Más Eficiente.**

### **2.7.1 Pérdida de paquetes**

La pérdida de paquetes ocurre cuando uno o más paquetes que viajan a través de una red, no llegan a su destino final.

Esto puede deberse a varios factores, tales como:

- ✓ Malas conexiones.
- ✓ Interferencia electromagnética.
- ✓ Equipos defectuosos.

- ✓ Cables en muy mal estado.
- ✓ Pequeños cortos circuitos entre los pares de cobre.
- ✓ Tormentas de difusión.
- ✓ Colisiones debido a que varios equipos comparten el mismo medio, sin el debido control.
- ✓ Otras consideraciones, como relación señal a ruido, distancia entre transmisor y receptor.

La pérdida de paquetes puede reducir notablemente el desempeño de la red y producir también fluctuaciones (jitter) en aplicaciones como Voz sobre IP, juegos en línea, videoconferencias, etc. y afectará en menor grado otro tipo de aplicaciones. Sin embargo, la pérdida de paquetes no implica siempre un problema, puesto que si hay un nivel aceptable de pérdidas no habrá un cambio drástico en el desempeño de la red.

Hay que tomar en cuenta que la fracción de pérdida de paquetes incrementa a medida que la intensidad de tráfico incrementa. Y este nivel de pérdidas será aceptable dependiendo de la aplicación para la cual está siendo empleada la red. No es lo mismo tener un 10% de pérdida de paquetes cuando se realiza

una videoconferencia que cuando se carga una página web. Es así que para aplicaciones tales como el tráfico de Voz sobre IP, perder uno o dos paquetes cada cierto tiempo no afecta la calidad de la conversación, mientras que pérdidas entre 5% y 10% afectarán significativamente la calidad del servicio.

### **2.7.2 Jitter**

El jitter es un efecto que se produce en una red no orientada a la conexión. Es, básicamente, la variación en el tiempo de llegada de los paquetes. Esto se puede producir debido a que cada paquete puede tomar una ruta distinta para llegar a su destino, o a una congestión en la red.

Se puede entender el concepto de jitter asociándolo a la palabra precisión. Como se mencionó ya, la información se envía en paquetes; toda la señal se particiona en pequeñas porciones que se transmiten a un dispositivo receptor que las debe volver a ensamblar. Si ocurre jitter, la sincronización se complica y el dispositivo receptor tendrá dificultades para volver a ensamblar la información entrante.

En todas las aplicaciones reales, el jitter tiene un componente aleatorio; es por ello, que debe ser especificado empleando términos estadísticos. El jitter aleatorio, también llamado jitter gaussiano es básicamente ruido electrónico impredecible, y típicamente sigue una distribución Gaussiana o Normal. Se cree que el jitter aleatorio tiene una distribución de este tipo puesto que la mayor parte del ruido en un circuito se debe al ruido térmico, el cual sigue una distribución Gaussiana.

### **2.7.3 Retardo**

El retardo es una medida muy importante a considerar en una red de telecomunicaciones. El retardo en una red no es más que una medida de cuánto tiempo le toma a un bit de datos viajar a través de la red desde un nodo a otro. Al ser una medida de tiempo, se mide en segundos; aunque usualmente estos valores suelen ser muy bajos y rara vez son mayores a 1 segundo.

Se acostumbra tomar en cuenta dos valores de retardo: el valor máximo de retardo de la red y el valor promedio. Si se consideran correctamente estos valores, se puede lograr que el desempeño

de la red sea bastante aceptable. Así, es posible que no se perciba mayormente la diferencia de tiempo existente entre el momento que se envía el flujo de información y el momento en que se lo recibe.

#### **2.7.4 Paquetes VoIP**

Voz sobre Protocolo de Internet o Voz sobre IP (VoIP por sus siglas en inglés: Voice over IP) es una tecnología que permite que la voz viaje a través de Internet empleando para ello un protocolo de red (IP).

En la actualidad existen dos arquitecturas de VoIP para la transmisión de voz por Internet que se utilizan de manera abundante:

- ✓ Protocolo de Inicio de Sesión (SIP de sus siglas en inglés: Session Initiation Protocol): Es un estándar desarrollado por la IETF y definido en el RFC 3261. Es un protocolo de señalización y control para establecer llamadas y conferencias en una red IP.

SIP realiza la comunicación empleando dos protocolos: RTP, el cual transporta los datos en tiempo real, y SDP que es usado para la negociación de las capacidades de los clientes.

Este protocolo de VoIP fue diseñado de acuerdo al modelo de Internet, trabaja en la capa de Aplicación y se basa en mensajes de petición y respuesta.

- ✓ H.323: Es el primer estándar internacional de comunicaciones multimedia y tenía la función específica de proveer a los usuarios teleconferencias con capacidades de voz, vídeo y datos sobre redes de conmutación de paquetes.

Hay que considerar, que la comunicación de la voz es analógica, mientras las redes de datos son digitales. Por ello, es necesario contar con un sistema de codificación/decodificación para poder llevar a cabo una comunicación VoIP. Este proceso es llevado a cabo por los denominados códecs.

Hay diversas maneras de convertir la voz de analógica a digital, siendo el más sencillo y conocido el procedimiento de Modulación por Codificación de Pulsos (PCM por sus siglas en inglés). De

hecho, muchas de las otras formas son variaciones o mejoras de PCM.

Entre los códecs más conocidos se puede citar: G.711, G.721, G.723, G.726, G.727, G.729, iLBC, EVRC, DVI, entre otros. De ellos, los más empleados más usualmente son G.711, G.723 y G.729.

Dado que las comunicaciones VoIP ocurren en tiempo real, es importante tomar en cuenta que los parámetros mencionados anteriormente (jitter, delay, pérdida de paquetes) constituyen una preocupación inherente en este tipo de comunicaciones, y su debido control y atenuación es imprescindible para lograr ofrecer una buena calidad de servicio.

- ✓ Pérdida de paquetes: Dado que las comunicaciones en tiempo real se basan en el protocolo UDP (no orientado a la conexión), si ocurre una pérdida de algún paquete, este no se reenvía. De igual manera, si un paquete no llega a tiempo al destino, es descartado.

No obstante, la voz es, en cierta manera, predictiva. Si se pierden paquetes de manera aislada, la voz puede recomponerse y los

resultados aún así son óptimos. El verdadero inconveniente ocurre cuando se pierden varios paquetes consecutivos.

Se recomienda que el porcentaje de paquetes perdidos sea menor al 1%. De esta manera la comunicación no se degrada. Este valor depende en gran medida del códec que se emplee.

- ✓ Jitter: Las comunicaciones en tiempo real son especialmente sensibles a este efecto. Frecuentemente, se debe a enlaces lentos o congestionados. Se recomienda que el jitter entre punto inicial y final de la comunicación esté en valores menores a 100 milisegundos. Si se cumple esta condición, el jitter puede ser compensado de manera apropiada.
  
- ✓ Retardo: Este es un inconveniente de las redes de telecomunicaciones en general, no solamente de las redes orientadas a la conexión, pero las comunicaciones VoIP son bastante sensibles a este efecto, que se debe a enlaces lentos o congestionados, al igual que el jitter.

El oído humano promedio puede detectar retardos de 250 milisegundos, si supera este valor la comunicación se torna molesta; pero, se recomienda que el valor del retardo entre el punto inicial y el punto final de una comunicación sea inferior a 150 milisegundos.

# CAPITULO 3

## 3. HERRAMIENTAS DE IMPLEMENTACIÓN

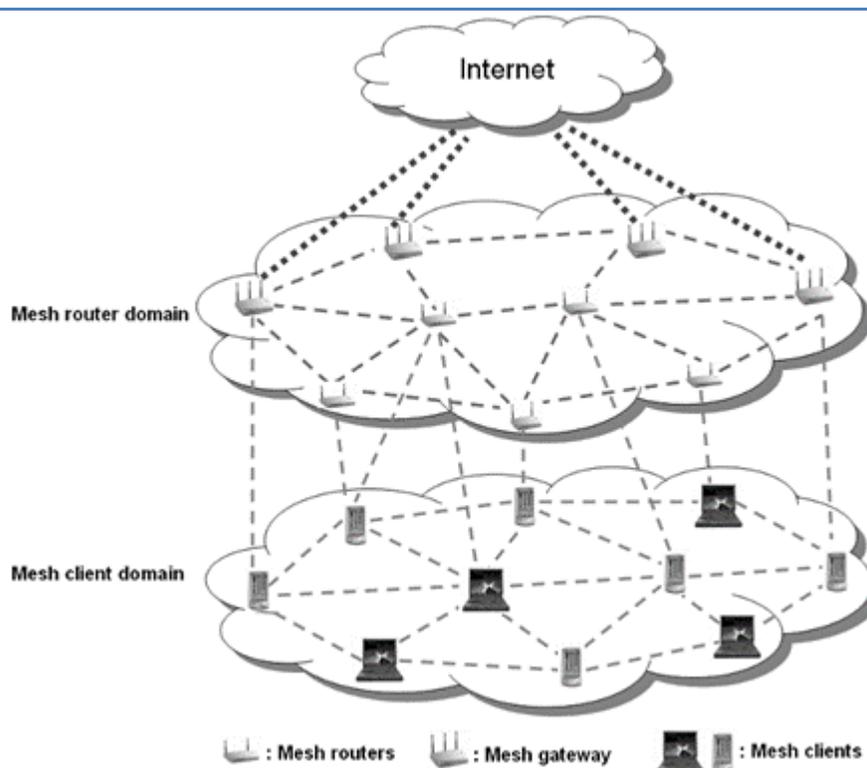
Para este capítulo se detallarán las herramientas usadas en el desarrollo del proyecto, el análisis a detalle de la configuración de cada protocolo y firmware utilizado, además del estudio de la posición de cada enrutador en los diferentes espacios de la facultad.

### 3.1 Tipos de dispositivos a utilizar en la red Mesh

Las WMN tradicionales se basan en una red de enrutadores estáticos de malla inalámbricos que son los que formarán el backbone, es decir, aquella zona por donde fluirá toda la información importante y a la cual

los clientes acceden a través de éstos enrutadores de malla, tal como se muestra en la Figura 3.1.1 .

Los enrutadores contienen las funciones avanzadas de enrutamiento para brindar soporte de red de malla, esto se cumple puesto que los enrutadores son nodos fijos, sin limitaciones en el suministro de energía al estar conectados directamente a líneas de energía eléctrica, contando con múltiples interfaces inalámbricas ya sea para él en el mismo o en diferentes tecnologías de acceso inalámbrico (4). En este tipo de arquitectura algunos de los enrutadores son llamados *gateways* o puertas de enlace los cuales tienen la característica de estar conectados a Internet. Por el contrario los clientes de malla cumplen el rol de nodos móviles por lo cual generalmente generan consumo limitado de energía por tener que usar baterías.



Fuente: Wireless Mesh Networks Architectures and Protocols Ekram Hossain-- Kin Leung Pag. 26

### ***Figura 3.1: Arquitectura de una red de malla inalámbrica***

La tecnología usada para estos dos tipos de dispositivos: enrutadores y clientes de malla es el estándar IEEE 802.11 (a/b/e/g/n), el cual es reconocido por las Redes de Área local inalámbricas (WLAN), por esta razón la amplia variedad de dispositivos 802.11 permite que se produzcan rápidos despliegues de redes inalámbricas de malla. Sin embargo para poder utilizar esta característica debemos tomar en cuenta las modificaciones que requieren tanto los enrutadores como los clientes de malla y de las limitaciones y restricciones que nos presenta el hardware existente (5).

### **Enrutadores de malla**

Los enrutadores de malla o nodos fijos utilizados para la implementación de la red inalámbrica mallada realizada hemos utilizado diferentes tipos de enrutadores según las limitaciones y exigencias que los protocolos de enrutamiento requerían.

De este modo tenemos tres tipos de enrutadores:

✓ **Linksys WRT54GL:** Para la implementación de la red utilizando los protocolos BATMAN y OLSR se utiliza cuatro enrutadores de este tipo los cuales representan una versión mejorada del WRT54G, tiene una banda de radio común de 2.4GHZ, soporta también trabajar con equipos Wireless-B de 11 Mbps por lo cual permite migrar estas redes al estándar Wireless-G. La potencia de transmisión es de 15dBm, soporta velocidades de 54Mbps. El resultado final depende de algunos factores, condiciones y variables como por ejemplo la distancia desde el punto de acceso, el volumen del tráfico de la red, la fabricación y materiales, el sistema operativo utilizado, la combinación de productos inalámbricos utilizados, las interferencias y otras condiciones adversas (6).



Fuente: <http://www.linksysbycisco.com/EU/es/products/WRT54GL>

**Figura 3.2: Enrutador Linksys WRT54GL**

- ✓ **Meraki Outdoor:** La red implementada haciendo uso del protocolo Roofnet utiliza cuatro enrutadores Meraki Outdoor, los mismos que son resistentes para ambientes externos brindando grandes distancias de cobertura entre 150 a 350m lo cual permite el fácil despliegue de redes comunitarias, posee una antena omnidireccional que transmite 2dBi. Permite aumentar la señal recibida en caso de que esta sea baja o prácticamente nula. Acepta hasta 54 Mbps de datos útiles (7).



Fuente: <http://www.pcmag.com/article2/0,2817,2340318,00.asp>

**Figura 3.3: Enrutador Meraki Outdoor**

✓ **D-Link DIR-825:** El protocolo WING exigía el uso de enrutadores de gran capacidad y este tipo de enrutadores cubrían la necesidad. Los enrutadores D-Link Dir 825 cubren las frecuencias de 2.4 Ghz y 5 Ghz, siendo compatibles con las normas inalámbricas previas. Su principal característica es la función de calidad de servicio QoS puesto que, detectan automáticamente los contenidos de tipo audio, vídeo juego transmitidos en la red y dándoles prioridad. Soportan los estándares 802.11 a/b/g/n **(8)**.



Fuente: <http://es.engadget.com/tag/D-Link+DIR-825/>

**Figura 3.4: Enrutador D- Link DIR-825**

### **Ciente de malla**

Los clientes de malla constituyen los usuarios que se conectan a la red mallada inalámbrica lo cual implica que se producirán envíos de paquetes e información a los nodos fijos provocando que se produzca congestión en la red. Para la implementación realizada utilizamos una laptop que capturaba los paquetes que se enviaban entre los diferentes nodos.

<b>Equipo</b>	<b>Dirección IP</b>	<b>Características</b>
Laptop	DHCP	Toshiba. Intel Atom 2.0Ghz 2GB Ram.

***Tabla 1 - Especificación de cliente de malla***

### **Ciente fijo**

En la implementación se procedió a utilizar una computadora la cual estaba ubicada dentro de las instalaciones del CIDIS que era empleada para realizar llamadas usando el servidor de Asterisk registrando dos extensiones, una era usada en la laptop y otra por la computadora; para poder realizar las llamadas correspondimos a emplear softphones.

Equipo	Dirección IP	Características
Computadora	192.168.5.10	Intel Core 2 Duo 2.0 Ghz 2 Gb RAM DDR3.

**Tabla II - Especificación de cliente fijo**

### Software utilizado

Básicamente en la implementación se utilizó dos tipos de software uno para medir la calidad de servicio obtenida por cada uno de los protocolos (wireless site survey) y otro para realizar las llamadas VoIP desde la laptop hasta la computadora.

### Wireshark



Fuente: <http://comandante-linux.blogspot.com/2011/02/analisis-de-trafico-con-wireshark.html>

**Figura 3.5: Logo Wireshark**

Este software es un rastreador que permite realizar un análisis a detalle del tráfico que circula por las redes, permitiendo al usuario interactuar

con los paquetes en tiempo real (9), en la implementación se utilizó Wireshark con el objetivo de poder analizar los parámetros de pérdida de paquetes, jitter, retardo y pérdida de paquetes VoIP previamente detallados en el Capítulo 2 en base a los paquetes que fluctuaban por la WMN tanto en los enrutadores de malla como en la computadora al momento que se realizaban llamadas las cuales tenían duración de 1 minuto.

Wireshark tiene la funcionalidad de poder realizar análisis estadísticos y gráficos en base a la información recibida, pero este tipo de gráficos no suelen ser exactos por lo cual se procedió a capturar los paquetes RTP para posteriormente ser exportados y poder realizar un programa en Matlab el cual nos presenta esquemas mucho más precisos. El código empleado en Matlab se encuentra incluido en la sección de Anexos.

## X-Lite



Fuente: <http://martinromero.org/vozipsystem.net/xlite.html>

**Figura 3.6: Softphone X-Lite**

X-Lite es un software gratuito de VoIP que utiliza el Protocolo de Inicio de Sesión (SIP) (10). Este software es una herramienta muy valiosa la cual permite establecer comunicaciones de voz en redes inalámbricas. Además permite realizar videoconferencias y envío de mensajes instantáneos en una sola interfaz. Es compatible con GSM, G.711 y G.723. Para poder hacer el registro de las extensiones se procedió a usar el servidor Asterisk instalado en las oficinas del CIDIS. En la Tabla III se pueden observar las extensiones empleadas en la implementación

Servidor Asterisk Box	Equipo	Dirección IP	Extensión
200.126.12.116	Laptop	DHCP	1006
	Computadora	192.168.5.10	1007

**Tabla III - Extensiones utilizadas**

### 3.2 Análisis de la posición de cada router en instalaciones de la FIEC.

La presente tesis La función principal de los protocolos de enrutamiento es de suministrar herramientas que permitan descubrir nuevos caminos hacia el destino final en caso de falla de los enlaces, permitir que exista el balanceo de cargas proporcionando calidad de servicio, en base al tipo de red inalámbrica mallada que se desee implementar, las WMN tienen la particularidad de tener distintos caminos para llegar a un mismo destino, razón por la cual los protocolos de enrutamiento deben suministrar métricas que permitan establecer que la calidad de servicio estará presente a lo largo de la transmisión de la información. Estas métricas deben proveer información sobre el estado del enlace, ya que la variación de un enlace inalámbrico es alta a causa de las condiciones de propagación y de la presencia de los nodos adyacentes que pueden ser los que conforman la red o pueden ser redes cercanas que producen interferencias en las comunicaciones.

La red WMN implementada tiene como objetivo determinar el protocolo de enrutamiento sea éste proactivo o reactivo que cumpla con las características previamente descritas para obtener una comunicación más eficiente en un ambiente compartido con otras redes inalámbricas transmitiendo a la vez en varios canales 802.11.

Para la realización de las pruebas fue necesario que los enrutadores tengan buena línea de vista entre ellos, puesto que la presencia de personas cercanas al lugar provocaba interferencia causando que muchas veces no logran comunicarse entre sí.

Al momento de ponerlos en una ubicación elevada dejo de presentarse este inconveniente. Se realizó dos tipos de topología una empleada para los protocolos WING, OLSR y BATMAN como se puede observar en la Figura 3.7 y otra para el protocolo Roofnet Figura 3.8.

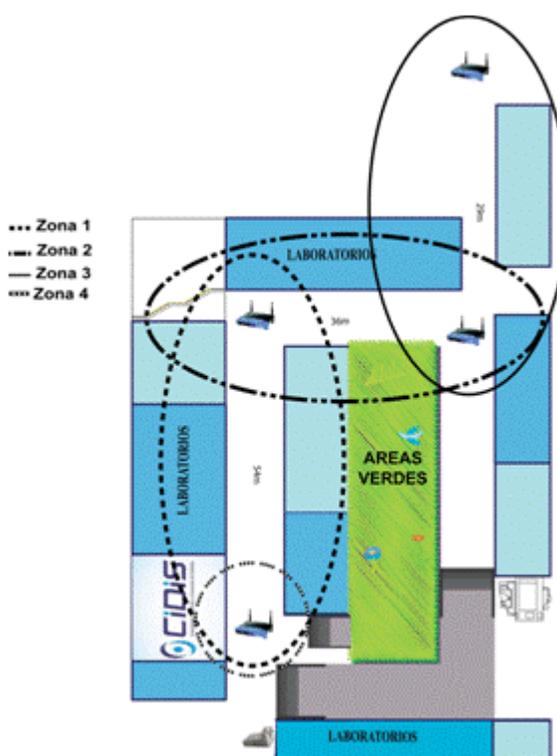


*Figura 3.7: Red WMN implementada  
Protocolo Batman, OLSR y Wing*

Cabe acotar que la topología empleada para el protocolo Roofnet fue diferente de la del resto de los protocolos puesto que los enrutadores Meraki Outdoor no lograban comunicarse en la topología ya planteada debido a que eran sensibles al tráfico existente en el camino.

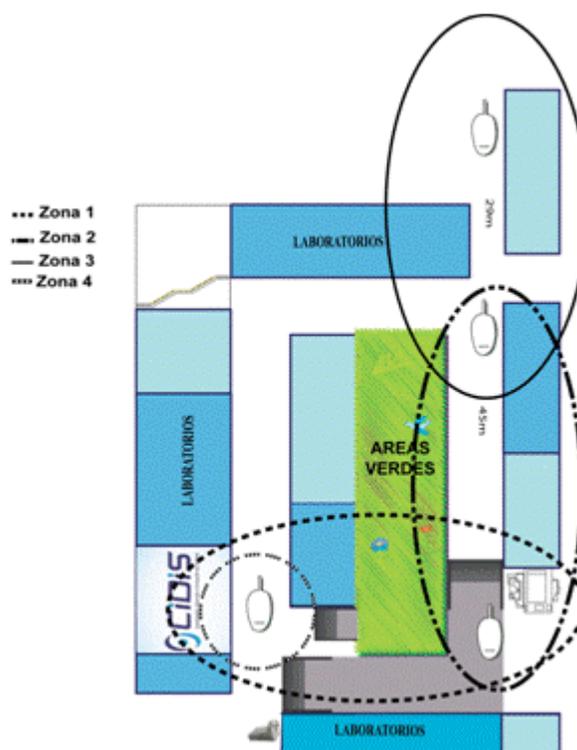


servicio brindada por los protocolos. En la Figura 3.9 se puede observar las de la topología de BATMAN el cual utiliza los enrutadores Linksys WRT54GL descritos previamente.



**Figura 3.9: Distribución de zonas en protocolo BATMAN**

La distribución de las zonas para la topología del protocolo Roofnet se puede observar en la Figura 3.10 .



**Figura 3.10: Distribución de zonas en protocolo Roofnet**

Las zonas realizadas en las dos topologías se encuentran distribuidas tal como se muestra en la tabla IV.

Zona 1	Zona 2	Zona 3	Zona 4
Enrutador 1-2	Enrutador 2-3	Enrutador 3-4	Enrutador 1

**Tabla IV - Distribución de las zonas**

Así mismo las direcciones ip asignadas para cada enrutador las podemos observar en la Tabla V, siendo el enrutador 1 el Gateway para las topologías realizadas para los protocolos OLSR, WING y Roofnet; por el contrario para el protocolo BATMAN se asignó el Enrutador 3 como Gateway:

Enrutador	Dirección IP
Enrutador 1	10.0.1.1
Enrutador 2	10.0.1.2
Enrutador 3	10.0.1.3
Enrutador 4	10.0.1.4

**Tabla V - Distribución de las direcciones IP**

### 3.3 Instalación y configuración del firmware (OPENWRT)

OpenWrt es descrito como una entrega de Linux para dispositivos embebidos, porque este firmware no es estático sino que provee un sistema de archivos enteramente configurable por medio del uso de paquetes, permitiendo adaptarse a cualquier tipo de aplicaciones; de esta manera constituye para el desarrollador poder para crear una aplicación sin tener que construir un firmware completo alrededor de ella

y para los usuarios significa la capacidad de personalización completa, para utilizar el dispositivo en múltiples maneras (11).

Este firmware se lo puede trabajar de dos maneras: mediante línea de comandos y mediante una interfaz web grafica web. Existe otro firmware Dd-wrt el cual es un derivado directo de OpenWrt, y la su principal diferencia radica en que Openwrt es más ligero, liviano y por lo tanto necesita menos espacio en Ram y Rom para ser ejecutado o instalado.

En la página web oficial de OpenWrt encontramos un conjunto de paquetes que pueden ser instalados según las características del enrutador que poseemos de esta manera para el desarrollo del proyecto investigamos aquellos paquetes que sean adecuados a los enrutadores a emplear (12).

### **Linksys WRT54GL**

- Dirigirse a la página de descargas de OpenWrt y buscar la versión Kamikaze 8.09 la cual presenta más estabilidad para trabajar. El paquete del firmware escogido fue `openwrt-wrt54g-squashfs.bin`

- Asignar la dirección de red 192.168.1.2/255.255.255.0 a la computadora en que estemos trabajando para poder conectarse al enrutador por medio del puerto LAN.
- Ingresar vía web al firmware por defecto del enrutador por medio de la dirección:

```
http://192.168.1.1/Upgrade.asp
```

- Dar click en navegar y seleccionar la imagen del firmware que previamente fue descargada. Presionar upgrade, es importante que el enrutador permanezca encendido mientras se realice este proceso para evitar daños al equipo.
- Una vez terminado este proceso el enrutador deja de parpadear, proceder a ingresar al enrutador vía Telnet por medio de la dirección ip 192.168.1.1 usando el programa Putty para configurar una clave de acceso.

```
root@openwrt:~$ passwd
Changing password for root
New password:
Retype password:
Password for root changed by root
root@openwrt:~$
```



- Modificar el fichero Firewall el cual es muy importante para habilitar los puertos de acceso para los distintos servicios de OpenWrt, el cual encontramos en el siguiente directorio:

```
root@openwrt:~# /etc/config/firewall
```

El mismo procedimiento se realiza en los cuatro enrutadores de la red WMN. Se procede a cambiar los parámetros de Entrada, Salida y Reenvío habilitándolos para permitir el flujo de los paquetes en el puerto Lan así como en las configuraciones por defecto.

```
config defaults
    option syn_flood 1
    option input      ACCEPT
    option output     ACCEPT
    option forward    ACCEPT

config zone
    option name       lan
    option input      ACCEPT
    option output     ACCEPT
    option forward    ACCEPT

config zone
    option name       wan
    option input      ACCEPT
    option output     ACCEPT
    option forward    ACCEPT
    option masq       1
```

- Se agrega el campo de la interfaz “wifi” que en el fichero Network; la cual previamente fue creada para permitir el envío de paquetes vía inalámbrica.

```
config 'zone'  
  option 'name' 'wifi'  
  option 'input' 'ACCEPT'  
  option 'output' 'ACCEPT'  
  option 'forward' 'ACCEPT'
```

- Agregar dos campos de “forwarding” para aceptar el envío y recepción de datos desde LAN a WAN (viceversa) y desde wifi a WAN (viceversa).

```
config forwarding  
  option src      lan  
  option dest     wan  
  option mtu_fix  1  
  
config forwarding  
  option src      wifi  
  option dest     wan  
  option mtu_fix  1
```

- En el fichero *Wireless* se refiere a los dispositivos de radio físicos presentes en el sistema. En él se describen las propiedades comunes de las redes inalámbricas tales como la selección de la antena, el canal a trabajar.

```
root@@openwrt:~# /etc/config/wireless
```

- Para la configuración final de OpenWrt en los enrutadores Linksys WRT54GL es descargar los siguientes paquetes que son dependencias necesarias para que empiece a funcionar el firmware para lo cual se dirige a la siguiente dirección:

```
http://downloads.openwrt.org/kamikaze/8.09/brcm-2.4/packages/
```

- a. - libpthread\_0.9.29-14\_mipsel.ipk
- b. - kernel\_2.6.25.17-brcm47xx-1\_mipsel.ipk
- c. -kmod-tun\_2.6.25.17-brcm47xx-1\_mipsel.ipk
- d. - tcpdump\_3.9.8-1\_mipsel.ipk

- Se procede a instalar las dependencias:

```
root@OpenWrt:/tmp# opkg install libpthread_0.9.29-14_mipsel.ipk
Installing libpthread (0.9.29-14) to root...
Configuring libpthread
root@OpenWrt:/tmp#
```

```
root@OpenWrt:/tmp# opkg install kernel_2.6.25.17-brcm47xx-
1_mipsel.ipk
Multiple packages (kernel and kernel) providing same name marked
HOLD or PREFER.
  Using latest.
Upgrading kernel on root from 2.4.35.4-brcm2.4-1 to 2.6.25.17-
brcm47xx-1...
Configuring kernel
root@OpenWrt:/tmp#
```

```
root@OpenWrt:/tmp# opkg install kmod-tun_2.6.25.17-brcm47xx-
1_mipsel.ipk
Installing kmod-tun (2.6.25.17-brcm47xx-1) to root...
Configuring kmod-tun
root@OpenWrt:/tmp#
```

```
root@OpenWrt:/tmp# opkg install tcpdump_3.9.8-1_mipsel.ipk
Installing tcpdump (3.9.8-1) to root...
Configuring tcpdump
root@OpenWrt:/tmp#
```

- Cambiar el nombre de cada nodo , para evitar confusiones en el momento de tener toda la red funcional

```
root@@openwrt:~# /etc/config/system
```

El campo hostname se lo cambia por el nombre deseado:

```
config system
    option hostname    Mesh1
    option timezone    UTC
```

- Es importante reiniciar el enrutador luego de hacer los cambios para que se realicen los mismos.

```
root@@openwrt:~# reboot
```

## D-Link Dir 825

Hay dos versiones de OpenWrt que pueden ser instalados en este tipo de enrutadores: la última versión (Backfire 10.03.1-rc4 en el momento de la escritura) o la última generación nocturna (nightly build) también llamado Bleeding edge. Hay ventajas y desventajas para ambas opciones (13).

La diferencia común entre estas versiones es que la generación nocturna contiene las últimas actualizaciones y correcciones y permite utilizar todas las características de OpenWrt soportadas actualmente en el enrutador. Sin embargo, esto implica que se puede ser víctima del denominado “bug” que se introdujo recientemente en el firmware. La última versión permite probar más a fondo, y suele ser más seguro. En general, si no se desean correr riesgos se aconseja instalar la última versión, por el contrario si se desea experimentar y escribir scripts instalar la generación nocturna.

Este enrutador tiene el modo de recuperación del firmware lo cual le permite arrancar desde un firmware alternativo y re-flash del enrutador, incluso si se bloquea. Esto lo hace más seguro si se utiliza la generación nocturna. Par el desarrollo del proyecto se escogió la versión nocturna, de esta manera:

- Dirigirse a la página de descargas de OpenWrt y buscar la versión indicada para este tipo de enrutadores, para el caso fue Snaphots

```
http://downloads.openwrt.org/snapshots/trunk/ar71xx/
```

- Escoger el paquete del firmware OpenWrt:

```
openwrt-ar71xx-generic-dir-825-b1-jffs2-factory.bin
```

- Asignar la dirección de red 192.168.0.2/255.255.255.0 a la computadora en que estemos trabajando para poder conectarse al enrutador por medio del puerto LAN.
- Entrar vía web al enrutador (D-Link recomienda usar Internet Explorer) por medio de la dirección 192.168.0.1. El navegador solicita un usuario y clave el cual viene configurado por defecto de fabrica: Usuario: admin y Password: dejarlo en blanco
- Una vez realizado el inicio de sesión se procede a cargar el firmware nuevo. Para ello, dirigirse a:

Tools → Firmware Update

- Escoger el archivo del firmware previamente descargada seleccionando la ubicación donde fue guardado. Presionar upgrade, no olvidar que no debemos apagar o desconectar

del puerto al enrutador mientras realiza esto debido a que podemos dañarlo definitivamente.

- Ingresar vía Telnet para realizar el cambio de contraseña pero con la dirección 192.168.1.1 debido a que el enrutador cambia su dirección ip después de ingresarle el nuevo firmware, sin olvidar cambiar la dirección de la computadora en la red 192.168.1.0/24

```
root@openwrt:~$ passwd
Changing password for root
New password:
Retype password:
Password for root changed by root
```

- Ingresar por medio de SSH usando como usuario root. La presentación de OpenWrt es:



```

root@OpenWrt:/tmp# opkg install wpad-mini_20110421-1_ar71xx.ipk
Installing wpad-mini (20110421-1) to root...
Configuring wpad-mini
root@OpenWrt:/tmp#

```

- Proceder a modificar el fichero *Wireless* ingresando al directorio:

```

root@@openwrt:~# /etc/config/wireless

```

Este tipo de enrutadores poseen dos radios los cuales manejan las bandas de 2,4Ghz y 5Ghz. Se procedió a configurar un radio en 2,4Ghz y el otro en 5Ghz debido a que este radio funcionará como modo monitor.

```

config wifi-device radio0
  option type mac80211
  #option device radio0
  option channel 11
  option macaddr 00:18:e7:f8:67:1d
  option hwmode 11ng
  option htmode HT20
  list ht_capab SHORT-GI-40
  list ht_capab TX-STBC
  list ht_capab RX-STBC1
  list ht_capab DSSS_CCK-40
  # REMOVE THIS LINE TO ENABLE WIFI:
  #option disabled 1

config wifi-device radiol1
  option type mac80211
  option channel 36
  option macaddr 00:18:e7:f8:67:1e
  option hwmode 11ng
  option htmode HT20
  list ht_capab SHORT-GI-40
  list ht_capab TX-STBC
  list ht_capab RX-STBC1
  list ht_capab DSSS_CCK-40
  # REMOVE THIS LINE TO ENABLE WIFI:
  #option disabled 1

```

- Modificar el fichero Firewall para habilitar el envío y recepción de datos por medio de los diferentes puertos y también vía inalámbrica.

```
root@@openwrt:~# /etc/config/firewall
```

- Anadir el campo de “wifib” habilitando la entrada, salida de datos; además agregar campos de “forwarding” para aceptar el envío y recepción de datos desde wifib a wan (viceversa) y desde wifib a lan (viceversa) y entre wifib.

```
config 'defaults'
    option 'syn_flood' '1'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'

config 'zone'
    option 'name' 'lan'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'

config 'zone'
    option 'name' 'wan'
    option 'input' 'REJECT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'
    option 'masq' '1'
    option 'mtu_fix' '1'

config 'zone'
    option 'name' 'wifib'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'
```

```
config 'forwarding'  
    option 'src' 'lan'  
    option 'dest' 'wan'  
  
config 'forwarding'  
    option 'src' 'lan'  
    option 'dest' 'wifib'  
  
config 'forwarding'  
    option 'src' 'wifib'  
    option 'dest' 'wifib'  
  
config 'forwarding'  
    option 'src' 'wifib'  
    option 'dest' 'wan'  
  
config 'rule'  
    option 'src' 'wan'  
    option 'proto' 'udp'  
    option 'dest_port' '68'  
    option 'target' 'ACCEPT'  
  
config 'rule'  
    option 'src' 'wifib'  
    option 'proto' 'tcp'  
    option 'dest_port' '5001'  
    option 'target' 'ACCEPT'  
  
config 'rule'  
    option 'src' 'wan'  
    option 'proto' 'icmp'  
    option 'icmp_type' 'echo-request'  
    option 'target' 'ACCEPT'  
  
config 'rule'  
    option 'src' 'wifib'  
    option 'proto' 'udp'  
    option 'dest_port' '698'  
    option 'target' 'ACCEPT'  
  
config 'rule'  
    option 'src' 'wan'  
    option 'proto' 'icmp'  
    option 'icmp_type' 'echo-request'  
    option 'target' 'ACCEPT'  
  
config 'rule'  
    option 'src' 'wifib'  
    option 'proto' 'icmp'  
    option 'icmp_type' 'echo-request'  
    option 'target' 'ACCEPT'  
  
config 'include'  
    option 'path' '/etc/firewall.user'
```

- Descargar e instalar las dependencias de la página de descargas de OpenWrt <http://downloads.openwrt.org/snapshots/trunk/ar71xx/>
  - a `.- libpcap_1.0.0-2_ar71xx.ipk`
  - b `.- tcpdump_4.0.0-3_ar71xx.ipk`

```
root@OpenWrt:/tmp# opkg install libpcap_1.0.0-2_ar71xx.ipk
Installing libpcap (1.0.0-2) to root...
Configuring libpcap.
root@OpenWrt:/tmp# opkg install tcpdump_4.0.0-3_ar71xx.ipk
Installing tcpdump (4.0.0-3) to root...
Configuring tcpdump.
```

### 3.4 Instalación de Asterisk en servidor

Para las pruebas de llamadas fue necesario utilizar Asterisk, el cual es una implementación de software libre que funciona como una PBX en una computadora, el cual actúa en Linux permitiendo que se realicen llamadas VoIP en tres protocolos: ADSI, SIP y H323 y puede interoperar con equipos de telefonía estándar básicas usando un hardware relativamente sin costo.

Elastix es una aplicación de software libre con ciertas restricciones puesto que tiene licencia GPL que integra en una única interface la cual es muy manejable, junto con las mejores herramientas disponibles para centrales telefónicas PBX basadas en Asterisk. Agrega su propio conjunto de utilitarios que permiten la creación de módulos de terceros. Estas características junto con la capacidad de generar reportes lo hace una buena opción para la implementación de una PBX basada en Asterisk.



Fuente: <http://www.elastix.org/>

**Figura 3.13: Logo de Elastix**

Las características de la computadora donde fue instalado el servidor de Elastix se las puede observar en la tabla VI:

Característica	Valor
CPU	GenuineIntel Intel(R) Celeron(R) CPU 2.00GHz
Disco Duro	80 GB
Memoria RAM	512
Sistema Operativo	CentOS 5

**Tabla VI - Especificaciones del Servidor**

Las extensiones (1006 y 1007) que fueron creadas en el servidor Elastix para la implementación se las puede observar en la Figura 3.4.2, las cuales fueron previamente descritas en el capítulo 2.

The screenshot displays the Elastix web interface. At the top, there is a navigation bar with the Elastix logo and various menu items like System, PBX, Fax, Email, IM, Reports, Extras, Agenda, Seminario Telematica, and Call Center. Below this is a secondary navigation bar with options like PBX Configuration, Flash Operator Panel, Voicemails, Monitoring, Endpoint Configuration, Conference, Extensions Batch, and Tools. The main content area is titled 'Add an Extension' and contains a form with a 'Device' dropdown menu set to 'Generic SIP Device' and a 'Submit' button. On the right side, there is a list of existing extensions: Roxanna <1001>, Estefania <1002>, Fernando <1005>, Evelyn <1006>, Jose <1007>, and sipp <2005>.

**Figura 3.14: Extensiones en servidor Elastix**

### 3.5 Instalación y configuración de B.A.T.M.A.N.

- Dirigirse a la página de descargas de OpenWrt

```
http://downloads.openwrt.org/kamikaze/8.09/brcm-2.4/
```

- Descargar la dependencia battool necesaria para poder instalar el protocolo y desacargar el paquete de B.A.T.M.A.N

a.- battool\_r1176-1\_mipsel.ipk

b.- batmand\_r1206-1\_mipsel.ipk

- Instalar la dependencia:

```
root@Mesh1:/tmp# opkg install battool_r1176-1_mipsel.ipk
Installing battool(2 r1176-1) to root...
Configuring battool
```

- Instalar el paquete que contiene a B.A.T.M.A.N:

```
root@Mesh1:/tmp# opkg install batmand_r1206-1_mipsel.ipk
Installing batmand(2 r1206-1) to root...
Configuring batmand
```

- Ingresar al fichero:

```
/etc/init.d/batmand
```

Cambiar el valor de START a 99 segundos debido a que el valor por defecto es 43 es un tiempo muy corto debido a que BATMAN aún se está iniciando luego del reinicio.

- Escribir el comando de habilitación de BATMAN seguido del “&” que permite mantener activo el protocolo.

```
root@Mesh1:~# /etc/init.d/batmand enable &
```

- Para modificar la red se ingresa al directorio:

```
root@@openwrt:~# /etc/config/network
```

Se configuran las direcciones IP de cada enrutador del puerto LAN, loopbacks y VLANs. Se agrega la sección de “wifi” para proceder a activar la parte inalámbrica del enrutador puesto que por defecto viene desactivado.

La diferencia entre la puerta de enlace y los enrutadores radica en que en el campo de configuración de la interfaz wifi, la puerta de enlace tiene la línea de “option DNS” para poder conectarse a Internet.

- **Configuración del Gateway:**

```
#### VLAN configuration
config switch eth0
    option vlan0      "0 1 2 3 5*"
    option vlan1      "4 5"

#### Loopback configuration
config interface loopback
    option ifname     "lo"
    option proto      static
    option ipaddr     127.0.0.1
    option netmask    255.0.0.0

#### LAN configuration
config interface lan
    option type       bridge
    option ifname     "eth0.0"
    option proto      static
    option ipaddr     192.168.0.1
    option netmask    255.255.255.0

#### WAN configuration
config interface wan
    option ifname     "eth0.1"
    option proto      dhcp

config interface wifi
    option proto      static
    option ipaddr     10.0.1.3
    'netmask' 255.255.255.0
    option ifname     "eth0.2"
    option 'dns'      8.8.8.8
```

La dirección de la interfaz inalámbrica es 10.0.1.3 y la dirección del DNS 8.8.8.8

- **Configuración de enrutadores de malla**

**Enrutador 10.0.1.1**

```
config interface wifi
  option proto static
  option ipaddr 10.0.1.1
  option 'netmask' 255.255.255.0
  option 'gateway' 10.0.1.3
```

**Enrutador 10.0.1.2**

```
config interface wifi
  option proto static
  option ipaddr 10.0.1.2
  option 'netmask' 255.255.255.0
  option 'gateway' 10.0.1.3
```

**Enrutador 10.0.1.4**

```
config interface wifi
  option proto static
  option ipaddr 10.0.1.4
  option 'netmask' 255.255.255.0
  option 'gateway' 10.0.1.3
```

- **Modificar el fichero de las interface inalámbricas ingresando al fichero `/etc/config/wireless` añadiendo lo siguiente:**

```
config wifi-device w10
  option type      broadcom
  option channel  1

config 'wifi-iface'
  option 'device' 'w10'
  option 'network' 'wifi'
  option 'mode' 'adhoc'
  option 'ssid' 'PTTnet'
  option 'encryption' 'none'
```

Una vez realizado los cambios necesarios se pueden observar que los paquetes de BATMAN se están enviando por medio de comandos que permiten observar la depuración en sus cinco diferentes niveles:

- 0 depuración deshabilitada
- 1 lista los vecinos
- 2 lista de puertas de enlace
- 3 permite observar el envío de paquetes BATMAN
- 4 observe permite observar el envío de paquetes BATMAN con más detalle.
- 5 memoria en uso

```
root@Mesh1:~# batmand -d 1 wl0
```

Los paquetes de BATMAN capturados por el programa Wireshark se los observa de la siguiente manera:

No.	Time	Source	Destination	Protocol Info
48	0.287498	10.0.1.1	10.0.1.255	BAT_BATSeq=2
422	4.510825	10.0.1.3	10.0.1.255	BAT_BATSeq=10
84	0.377493	10.0.1.1	10.0.1.255	BAT_BATSeq=6
423	4.527714	10.0.1.1	10.0.1.255	BAT_BATSeq=10
217	1.300180	10.0.1.1	10.0.1.255	BAT_BATSeq=3
216	1.297486	10.0.1.1	10.0.1.255	BAT_BATSeq=7
55	0.310995	10.0.1.3	10.0.1.255	BAT_BATSeq=2
517	6.667440	10.0.1.1	10.0.1.255	BAT_BATSeq=10
65	0.346200	10.0.1.3	10.0.1.255	BAT_BATSeq=6
620	8.637478	10.0.1.1	10.0.1.255	BAT_BATSeq=12
35	0.267453	10.0.1.2	10.0.1.255	BAT_BATSeq=2
87	0.386123	10.0.1.4	10.0.1.255	BAT_BATSeq=6
220	1.305447	10.0.1.3	10.0.1.255	BAT_BATSeq=3
221	1.306829	10.0.1.4	10.0.1.255	BAT_BATSeq=7
431	4.640837	10.0.1.3	10.0.1.255	BAT_BATSeq=8
426	4.577483	10.0.1.1	10.0.1.255	BAT_BATSeq=8

Frame 48: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 Ethernet II, Src: Cisco-Li\_27:b8:60 (68:7f:74:27:b8:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.1.255 (10.0.1.255)  
 User Datagram Protocol, Src Port: batman (4305), Dst Port: batman (4305)  
 B.A.T.M.A.N., orig: 10.0.1.4 (10.0.1.4)

**Figura 3.15: Captura de paquetes BATMAN en Wireshark**

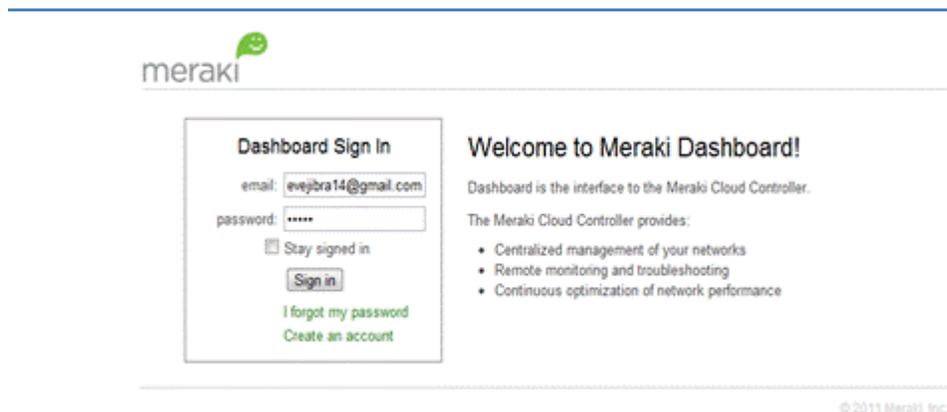
### 3.6 Instalación y configuración de Roofnet.

Existen diversas aplicaciones comerciales para el protocolo de enrutamiento Roofnet, tales como la empresa Meraki la cual ha desarrollado diversos dispositivos basados exclusivamente en este protocolo tales como: mini repetidores de bajo costo, antenas resistentes

a efectos ultravioletas, enrutadores para ambientes internos como externos como es el caso del enrutador Meraki Outdoor que es el utilizado en la implementación realizada. Este tipo de enrutadores no solo permiten el despliegue sencillo de la WMN sino también ampliarla fácilmente y de forma barata. Meraki no es un ambiente abierto como lo es OpenWrt por lo cual para poder capturar los paquetes que circulan por la red únicamente se capturan los que pasan por la laptop y por la computadora al momento de realizar las llamadas. Para empezar a utilizar los enrutadores se procede de la siguiente manera:

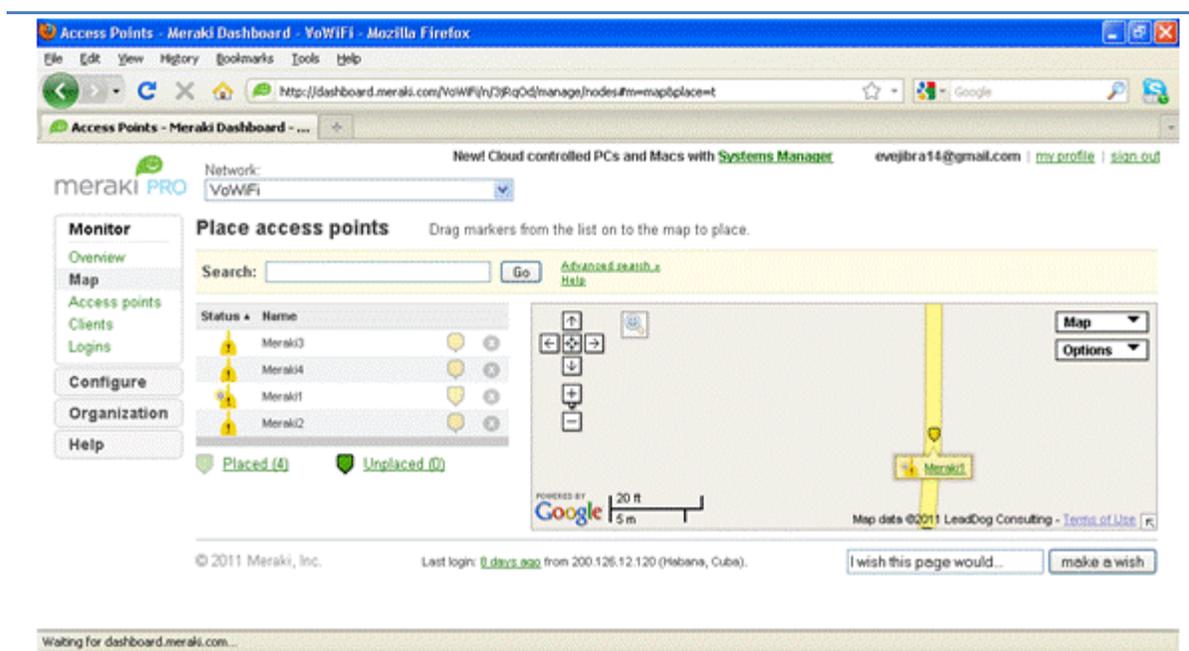
- Ingresar a la página de Meraki y proceder a crearse una cuenta para poder realizar el inicio de sesión.

<http://dashboard.meraki.com>



**Figura 3.16: Inicio de sesión en página de Meraki**

- Una vez realizado el inicio de sesión, registrar cada uno de los enrutadores escribiendo la dirección MAC de cada uno de ellos la cual se encuentra en la parte posterior del enrutador.
- Los Meraki Outdoor se auto- configuran y aparece un mapa de Google en donde se pueden observar los nodos desplegados como se puede observar en la Figura 3.6.2 .



**Figura 3.17: Nodos de la Red WMN Roofnet**

La administración de la red se la hace por entero en este panel Dashboard tales como: configurar varios aspectos de la red, el SSID de la

red, el canal de frecuencia que utiliza. El panel indica también cuántos usuarios están conectados y la cantidad de datos que han descargado en conjunto tal y como se observa en la Figura 3.6.3

The screenshot shows the Meraki Dashboard interface for a VoWiFi network. The 'Access Points' section is active, displaying a list of 4 access points. All four are in an 'Alerting' state, indicated by yellow warning icons and red connectivity bars. The table below provides details for each access point.

Status	Name	Contacted at	Usage	Clients	Connectivity	Mesh speed
Alerting	Meraki1	now	none	0	Red bar	N/A
Alerting	Meraki2	now	none	0	Red bar	N/A
Alerting	Meraki3	now	none	0	Red bar	N/A
Alerting	Meraki4	now	none	0	Red bar	N/A

**Figura 3.18: Administración de la Red WMM Roofnet**

- Ingresando vía browser a la dirección 10.128.128.128 podemos interactuar con cada enrutador para lo cual se debe iniciar sesión:

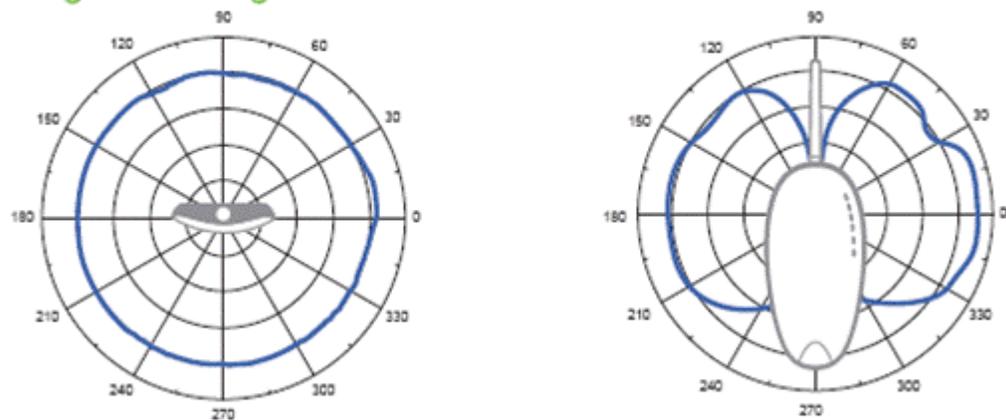
User: Meraki  
Password: Dirección Mac de cada enrutador

- Por este medio se puede configurar la dirección IP de cada

enrutador y como observar los nodos adyacentes para cada uno de ellos.

- Es preferible que la posición de los enrutadores sea vertical para que la propagación de la señal sea más eficiente y pueda tener más cobertura el enrutador como se detalla en la Figura 3.6.4

### ➤ Signal Coverage Pattern



Fuente: <http://meraki.com/products/hotzones/od2#tech-specs>

**Figura 3.19: Propagación de la señal del Meraki Outdoor**

### 3.7 Instalación y configuración de Wing

- Dirigirse a la página de descargas de OpenWrt y buscar la versión que corresponde al enrutador (14).

```
http://downloads.openwrt.org/snapshots/trunk/ar71xx/packages/
```

- Descargar las dependencias necesarias para la instalación del protocolo:
  - a. `kmod-tun_2.6.37.6-1_ar71xx.ipk`
  - b. `libpcap_1.0.0-2_ar71xx.ipk`
  - c. `libstdcpp_linaro-68_ar71xx.ipk`
- Instalar las dependencias previamente descargadas:

```
root@Mesh1:/tmp# opkg install kmod-tun_2.6.37.6-1_ar71xx.ipk
Installing kmod-tun (2.6.37.6-1) to root...
Configuring kmod-tun
```

```
root@Mesh1:/tmp# opkg install libpcap_1.0.0-2_ar71xx.ipk
Installing libpcap (1.0.0-2) to root...
Configuring libpcap
```

```
root@Mesh1:/tmp# opkg install libstdcpp_linaro-68_ar71xx.ipk
Installing libstdcpp_linaro(68) to root...
Configuring libpcap
```

- Descargar el paquete del protocolo Wing que se encuentra en la página de descargas previamente mencionada:

```
wing_20110329-2_ar71xx.ipk
```

- Proceder a instalar el paquete

```
root@Mesh1:/ opkg install wing_20110329-2_ar71xx.ipk
Installing wing (20110329-2) to root...
Configuring wing
```

- Ingresar al fichero de red:

```
root@@openwrt:~# /etc/config/network
```

Para la puerta de enlace se procede a modificar la dirección del campo WAN añadiéndole la opción de DNS, opción de máscara y opción de puerta de enlace para poder conectarse a direcciones IP públicas, además agregar el campo “interface wifib” para configurar la dirección inalámbrica del enrutador así como la opción de DNS. Además se agrega el campo *interface mesh* el mismo que contiene el soporte para el protocolo Wing; quedando configurado de la siguiente manera:

## Configuración de la puerta de enlace

```
config 'interface' 'loopback'
  option 'ifname' 'lo'
  option 'proto' 'static'
  option 'ipaddr' '127.0.0.1'
  option 'netmask' '255.0.0.0'

config 'interface' 'lan'
  option 'ifname' 'eth0.1'
  option 'type' 'bridge'
  option 'proto' 'static'
  option 'ipaddr' '192.168.1.1'
  option 'netmask' '255.255.255.0'

config 'interface' 'wan'
  option 'ifname' 'eth1'
  option 'proto' 'dhcp'
  option proto      static
  option 'ipaddr' '200.126.12.117'
  option 'netmask' '255.255.255.0'
  option 'gateway' '200.126.12.1'
  option 'dns' ' 200.9.176.5 192.188.59.2 192.188.59.2'

config 'interface' 'wifib'
  option 'proto' 'static'
  option 'ipaddr' '10.0.1.1'
  option 'netmask' '255.255.255.0'
  option 'dns' '8.8.8.8'

config 'switch'
  option 'name' 'rtl8366s'
  option 'reset' '1'
  option 'enable_vlan' '1'

config 'switch_vlan'
  option 'device' 'rtl8366s'
  option 'vlan' '1'
  option 'ports' '0 1 2 3 5t'

config 'interface' 'mesh'
  option 'proto' 'wing'
  option 'profile' 'bulk'
  option 'rc' 'minstrel'
  option 'ls' 'fcfs'
  option 'metric' 'wcett'
  option 'prefix' '6'
  option 'period' '10000'
  option 'tau' '100000'
  option 'debug' 'true'
```

En los enrutadores de malla difiere únicamente en su configuración los campos de Wan y la interface “wifib”.

### Enrutador 10.0.1.2

```
config 'interface' 'wan'  
  option 'ifname' 'eth1'  
  option 'proto' 'dhcp'  
  
config interface wifib  
  option proto      static  
  option ipaddr     10.0.1.2  
  option netmask    255.255.255.0  
  option gateway    10.0.1.1  
  option dns 8.8.8.8
```

### Enrutador 10.0.1.3

```
config 'interface' 'wan'  
  option 'ifname' 'eth1'  
  option 'proto' 'dhcp'  
  
config interface wifib  
  option proto      static  
  option ipaddr     10.0.1.3  
  option netmask    255.255.255.0  
  option gateway    10.0.1.1  
  option dns 8.8.8.8
```

### Enrutador 10.0.1.4

```
config 'interface' 'wan'  
  option 'ifname' 'eth1'  
  option 'proto' 'dhcp'  
  
config interface wifib  
  option proto      static  
  option ipaddr     10.0.1.4  
  option netmask    255.255.255.0  
  option gateway    10.0.1.1  
  option dns 8.8.8.8
```

No es necesario configurar *ifname* para esta interfaz, pues automáticamente este se deriva del nombre definido en *interface*. Así, el nombre en este caso será **wing-mesh**.

La dirección IP es generada automáticamente por los scripts de inicialización utilizando los últimos 3 bytes de la primera interfaz inalámbrica que se utiliza para construir la red de backhaul. Las interfaces de red que usan este protocolo están asociadas a una interfaz de TAP, que se configura como \$prefijo.X.X.X para el caso de la implementación empezara con 6.X.X.X

- Modificar el fichero */etc/config/wireless* en donde este protocolo exige que al menos una interfaz debe operar en modo monitor y la otra en modo ad-hoc (15). Con lo cual se obtiene:

```
config wifi-device radio0
option type mac80211
#option device radio0
option channel 11
option macaddr 00:18:e7:f8:67:1d
option hwmode 11ng
option htmode HT20
list ht_capab SHORT-GI-40
list ht_capab TX-STBC
list ht_capab RX-STBC1
list ht_capab DSSS_CCK-40
# REMOVE THIS LINE TO ENABLE WIFI:
#option disabled 1

config wifi-iface
option device radio0
option network wifib
option mode adhoc
option ssid Prueba_wing
#option encryption none
```

```

config wifi-device radiol
    option type      mac80211
    option channel   36
    option macaddr   00:18:e7:f8:67:1e
    option hwmode    11ng
    option htmode    HT20
    list ht_capab    SHORT-GI-40
    list ht_capab    TX-STBC
    list ht_capab    RX-STBC1
    list ht_capab    DSSS_CCK-40
    # REMOVE THIS LINE TO ENABLE WIFI:
    #option disabled 1

config wifi-iface
    option device    radiol
    option network   wific
    option mode      monitor
    option ssid      WingTest

```

- Modificar el fichero Firewall `/etc/config/firewall` añadiendo el campo que incluye la interface mallada con lo cual el fichero queda configurado finalmente de esta manera:

```

config 'defaults'
    option 'syn_flood' '1'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'

config 'zone'
    option 'name' 'lan'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' ''ACCEPT'

config 'zone'
    option 'name' 'wan'
    option 'input' 'REJECT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'
    option 'masq' '1'
    option 'mtu_fix' '1'

```

```
config 'zone'
  option 'name' 'wifib'
  option 'input' 'ACCEPT'
  option 'output' 'ACCEPT'
  option 'forward' 'ACCEPT'

config 'forwarding'
  option 'src' 'lan'
  option 'dest' 'wan'

config 'forwarding'
  option 'src' 'lan'
  option 'dest' 'wifib'

config 'forwarding'
  option 'src' 'wifib'
  option 'dest' 'wifib'

config 'forwarding'
  option 'src' 'wifib'
  option 'dest' 'wan'

config 'rule'
  option 'src' 'wan'
  option 'proto' 'udp'
  option 'dest_port' '68'
  option 'target' 'ACCEPT'

config 'rule'
  option 'src' 'wifib'
  option 'proto' 'tcp'
  option 'dest_port' '5001'
  option 'target' 'ACCEPT'

config 'rule'
  option 'src' 'wan'
  option 'proto' 'icmp'
  option 'icmp_type' 'echo-request'
  option 'target' 'ACCEPT'

config 'rule'
  option 'src' 'wifib'
  option 'proto' 'udp'
  option 'dest_port' '698'
  option 'target' 'ACCEPT'

config 'rule'
  option 'src' 'wan'
  option 'proto' 'icmp'
  option 'icmp_type' 'echo-request'
  option 'target' 'ACCEPT'
```

```

config 'rule'
    option 'src' 'wifib'
    option 'proto' 'icmp'
    option 'icmp_type' 'echo-request'
    option 'target' 'ACCEPT'

config 'include'
    option 'path' '/etc/firewall.user'

config 'zone'
    option 'name' 'mesh'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'
    option 'masq' '1'

config 'forwarding'
    option 'src' 'lan'
    option 'dest' 'mesh'

config 'forwarding'
    option 'src' 'mesh'
    option 'dest' 'wan'

```

- Una vez realizados los cambios necesarios en los ficheros se levanta la interfaz de malla con el comando:

```
root@Mesh1:~# ifup mesh
```

- Los controladores del protocolo se denominan *handler* con ellos se puede escribir, leer rutas, gateways; siendo los comandos usados  
 It.routes Solo de lectura, permite conocer los vecinos adyacentes al enrutador.

It.links Solo de lectura, indica los enlaces conocidos para el enrutador actualmente

.It.hosts Solo de lectura, lista los hosts que conoce actualmente el nodo local.

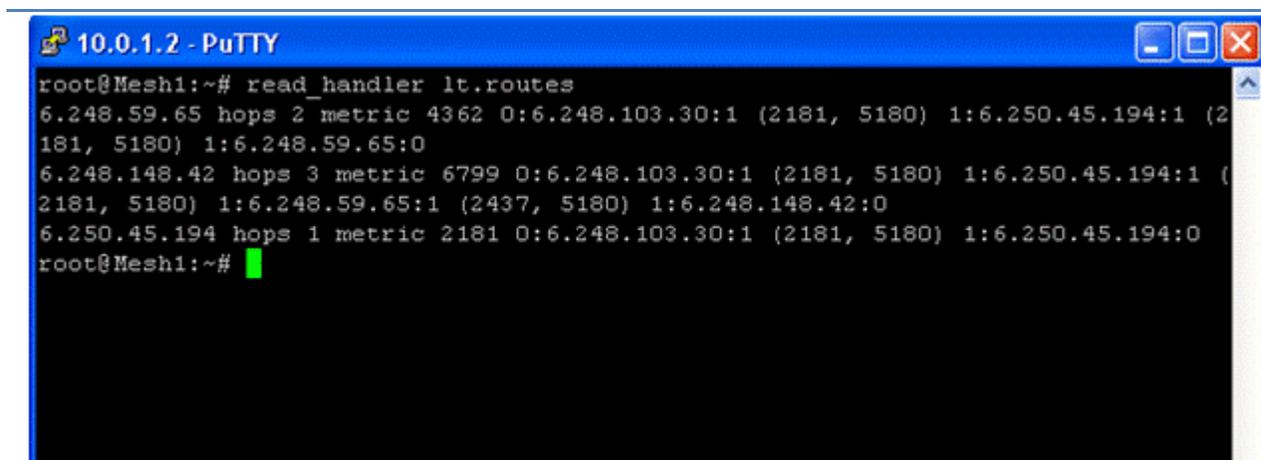
Las Ip's asignadas dinámicamente para cada enrutador son:

Equipo	Dirección IP
Enrutador 1	6.248.103.30
Enrutador 2	6.250.45.194
Enrutador 3	6.248.58.65
Enrutador 4	6.248.148.42

**Tabla VII: Direcciones Ip's Protocolo Wing**

Los controladores permiten observar el correcto funcionamiento de la red WMN con Wing, debido a que éste protocolo aun no cuenta con un filtro para poder ser observado por medio de Wireshark. Los resultados obtenidos para cada enrutador solo los siguientes:

## Enrutador 1

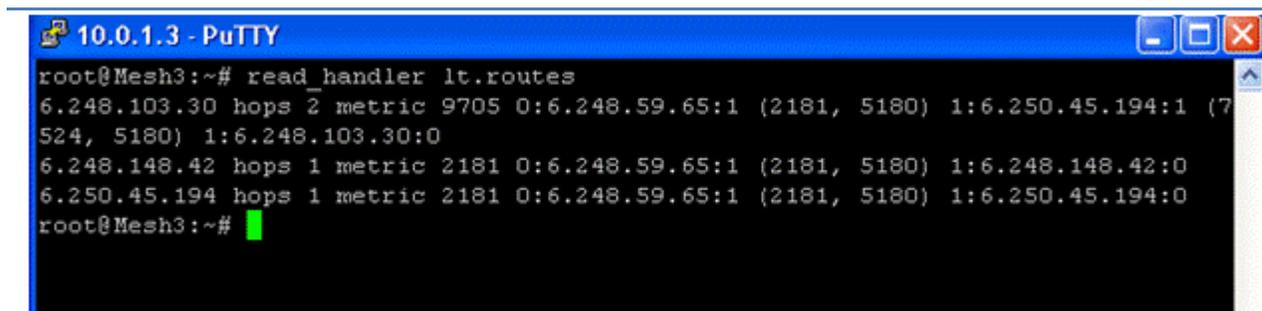


```
10.0.1.2 - PuTTY
root@Mesh1:~# read_handler lt.routes
6.248.59.65 hops 2 metric 4362 O:6.248.103.30:1 (2181, 5180) 1:6.250.45.194:1 (2
181, 5180) 1:6.248.59.65:0
6.248.148.42 hops 3 metric 6799 O:6.248.103.30:1 (2181, 5180) 1:6.250.45.194:1 (
2181, 5180) 1:6.248.59.65:1 (2437, 5180) 1:6.248.148.42:0
6.250.45.194 hops 1 metric 2181 O:6.248.103.30:1 (2181, 5180) 1:6.250.45.194:0
root@Mesh1:~#
```

*Figura 3.20: Rutas creadas dinámicamente- Enrutador 1*



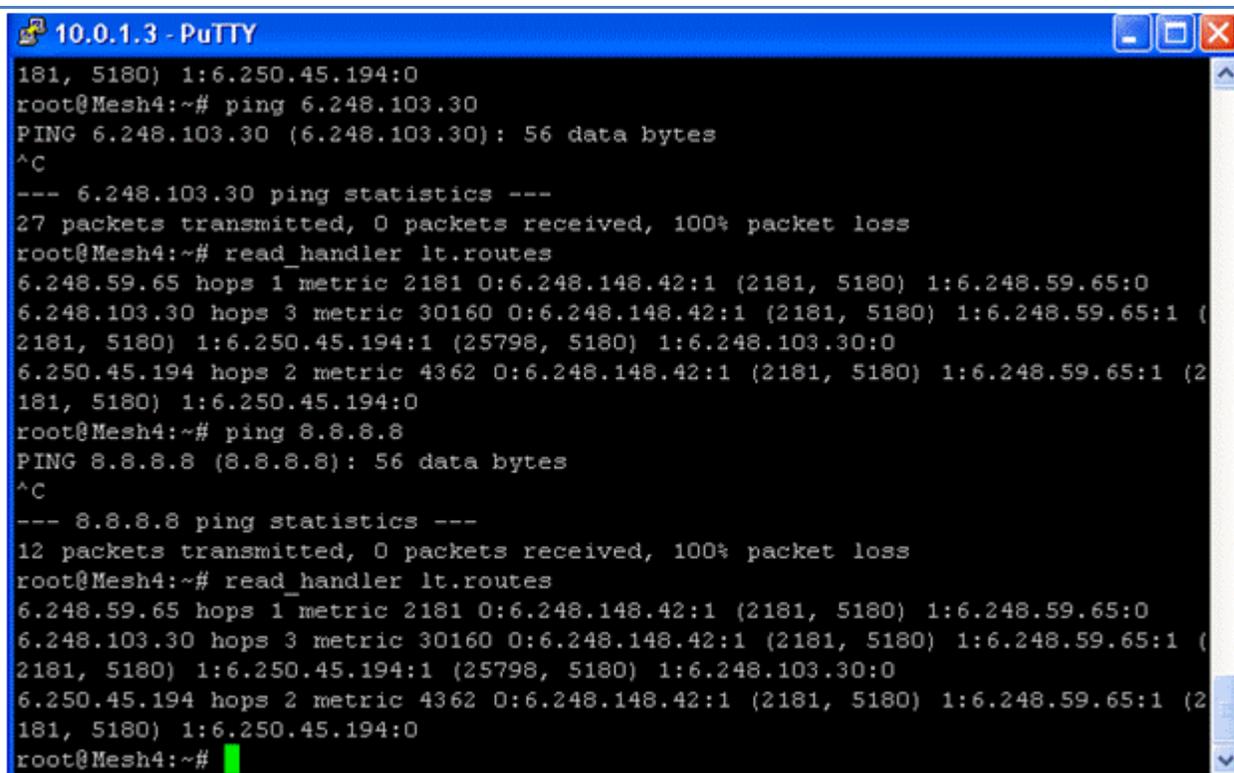
### Enrutador 3



```
10.0.1.3 - PuTTY
root@Mesh3:~# read_handler lt.routes
6.248.103.30 hops 2 metric 9705 0:6.248.59.65:1 (2181, 5180) 1:6.250.45.194:1 (7
524, 5180) 1:6.248.103.30:0
6.248.148.42 hops 1 metric 2181 0:6.248.59.65:1 (2181, 5180) 1:6.248.148.42:0
6.250.45.194 hops 1 metric 2181 0:6.248.59.65:1 (2181, 5180) 1:6.250.45.194:0
root@Mesh3:~#
```

*Figura 3.22: Rutas creadas dinámicamente- Enrutador 3*

## Enrutador 4



```
10.0.1.3 - PuTTY
181, 5180) 1:6.250.45.194:0
root@Mesh4:~# ping 6.248.103.30
PING 6.248.103.30 (6.248.103.30): 56 data bytes
^C
--- 6.248.103.30 ping statistics ---
27 packets transmitted, 0 packets received, 100% packet loss
root@Mesh4:~# read_handler lt.routes
6.248.59.65 hops 1 metric 2181 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:0
6.248.103.30 hops 3 metric 30160 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:1 (
2181, 5180) 1:6.250.45.194:1 (25798, 5180) 1:6.248.103.30:0
6.250.45.194 hops 2 metric 4362 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:1 (2
181, 5180) 1:6.250.45.194:0
root@Mesh4:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
^C
--- 8.8.8.8 ping statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
root@Mesh4:~# read_handler lt.routes
6.248.59.65 hops 1 metric 2181 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:0
6.248.103.30 hops 3 metric 30160 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:1 (
2181, 5180) 1:6.250.45.194:1 (25798, 5180) 1:6.248.103.30:0
6.250.45.194 hops 2 metric 4362 0:6.248.148.42:1 (2181, 5180) 1:6.248.59.65:1 (2
181, 5180) 1:6.250.45.194:0
root@Mesh4:~#
```

*Figura 3.23: Rutas creadas dinámicamente- Enrutador 4*

### 3.8 Instalación y configuración de O.L.S.R.

- Descargar el paquete de O.L.S.R. desde la página de descargas de OpenWrt correspondiente a la versión de Kamikaze que se esté utilizando(16):

```
olsrd_0.5.6-r3-2_mipsel.ipk
```

- Instalar el paquete:

```
root@Mesh1:/tmp# opkg install olsrd_0.5.6-r3-2_mipsel.ipk
Installing olsrd (0.5.6-r3-2) to root...
Configuring olsrd
```

- Ingresar al fichero `/etc/config/wireless` y modificar la interface inalámbrica que será utilizada para la red WMN el cual `wl0` es el identificador interno para OpenWrt que indica que es un dispositivo inalámbrico, y `broadcom` indica el tipo de driver a usar.

```
config wifi-device wl0
  option type      broadcom
  option channel   11

# REMOVE THIS LINE TO ENABLE WIFI:
#option disabled 1

config 'wifi-iface'
  option 'device' 'wl0'
  option 'network' wifi
  option 'mode' 'adhoc'
  option 'ssid' 'MeshTest'
  option 'encryption' 'none'
```

- Modificar el fichero `/etc/config/network` el cual difiere entre la configuración que se realiza en el Gateway y para la configuración de los enrutadores de malla con lo que se obtiene:

### Configuración de la puerta de enlace

```
#### VLAN configuration
config switch eth0
    option vlan0      "0 1 2 3 5*"
    option vlan1      "4 5"
    option vlan2      "5"
    option vlan3      "5"

#### Loopback configuration
config interface loopback
    option ifname     "lo"
    option proto      static
    option ipaddr     127.0.0.1
    option netmask    255.0.0.0

#### LAN configuration
config interface lan
    option type       bridge
    option ifname     "eth0.0"
    option proto      static
    option ipaddr     192.168.1.1
    option netmask    255.255.255.0

#### WAN configuration
config interface wan
    option ifname     "eth0.1"
#    option proto     dhcp
    option proto      static
    option 'ipaddr'   '200.126.12.119'
    option 'netmask'  '255.255.255.0'
    option 'gateway'  '200.126.12.1'
    option 'dns'      ' 200.9.176.5 192.188.59.2 192.188.59.2'
```

```
config interface wifi
  option proto static
  option ipaddr 10.0.1.1
  option 'netmask' 255.255.255.0
```

Los enrutadores que conforman la red difieren en su configuración en el campo de la interface *WAN* y la interface de *wifi*

### Enrutador 2

```
#### WAN configuration
config interface wan
  option ifname      "eth0.1"
  option proto       dhcp

config interface wifi
  option proto static
  option ipaddr 10.0.1.2
  option gateway 10.0.1.1
  option dns 200.9.176.5
  option 'netmask' 255.255.255.0
```

### Enrutador 3

```
#### WAN configuration
config interface wan
  option ifname      "eth0.1"
  option proto       dhcp

config interface wifi
  option proto static
  option ipaddr 10.0.1.3
  option gateway 10.0.1.1
  option dns 200.9.176.5
  option 'netmask' 255.255.255.0
```

## Enrutador 4

```
#### WAN configuration
config interface wan
    option ifname      "eth0.1"
    option proto       dhcp

config interface wifi
    option proto static
    option ipaddr 10.0.1.4
    option gateway 10.0.1.1
    option dns 200.9.176.5
    option 'netmask' 255.255.255.0
```

- El fichero *Firewall* queda configurado de la siguiente manera:

```
config defaults
    option syn_flood 1
    option input      ACCEPT
    option output     ACCEPT
    option forward    REJECT

config 'zone'
    option 'name' 'wifi'
    option 'input' 'ACCEPT'
    option 'output' 'ACCEPT'
    option 'forward' 'ACCEPT'

config zone
    option name      lan
    option input ACCEPT
    option output    ACCEPT
    option forward   REJECT

config zone
    option name      wan
    option input ACCEPT
    option output    ACCEPT
    option forward   REJECT
    option masq      1
    option mtu_fix   1
```

```
config forwarding
    option src      lan
    option dest     wan

config forwarding
    option src      wifi
    option dest     wan

config rule
    option src      wan
    option proto    udp
    option dest_port 68
    option target   ACCEPT

config rule
    option src      wifi
    option proto    udp
    option dest_port 698
    option target   ACCEPT

config rule
    option src      wifi
    option proto    udp
    option dest_port 1978
    option target   ACCEPT

config include
    option path /etc/firewall.user

# port redirect port coming in on wan to lan
config redirect
    option src      wan
    option src_dport 8477
    option dest     wifi
    option dest_ip   10.0.0.50
    option dest_port 8477
    option proto     tcp
```

- Editar la carpeta que se encuentra en la dirección: */etc/olsrd.conf* donde se observa la línea *Interface* colocar el nombre de la interfaz inalámbrica a usar en nuestro caso “*wl0*”. Obteniendo:

```
DebugLevel 0
IpVersion 4

ClearScreen yes

Interface "wl0"
{
    AutoDetectChanges yes
}

Hna4
{
    10.0.1.0
    255.255.255.0
}

AllowNoInt yes

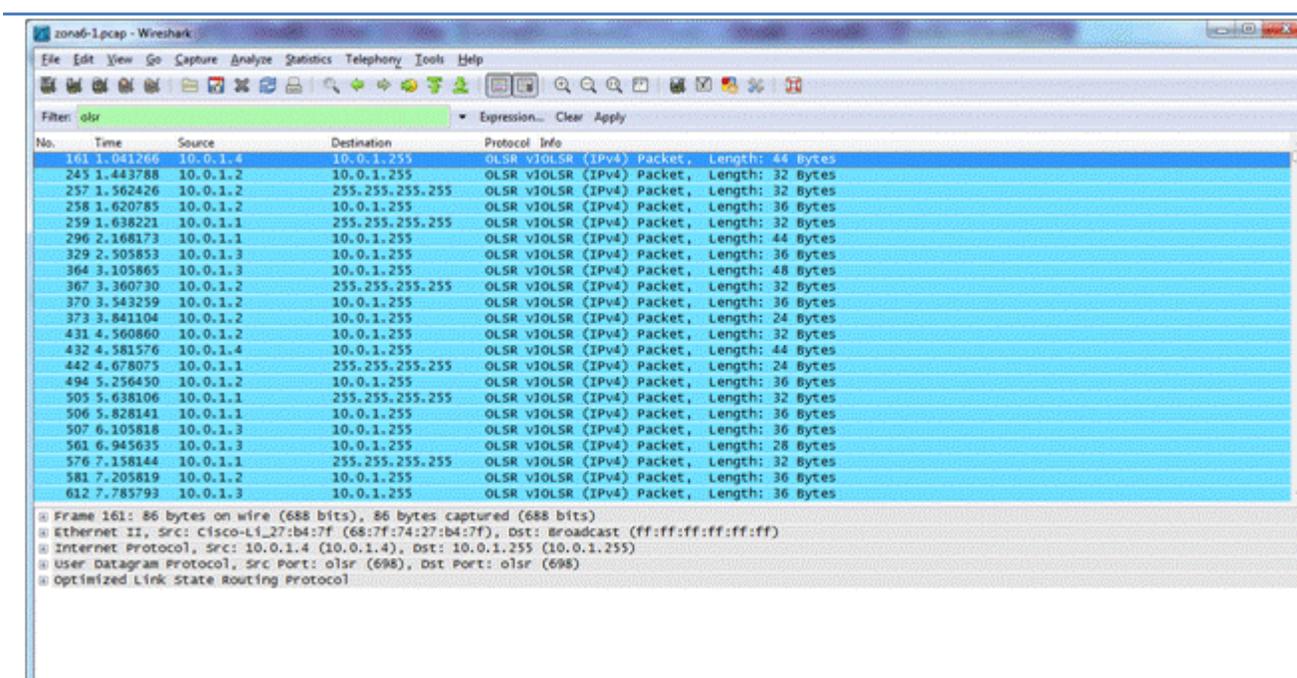
IpcConnect
{
    MaxConnections 0
    Host 127.0.0.1
}

UseHysteresis yes
HystScaling 0.50
HystThrHigh 0.80
HystThrLow 0.30
LinkQualityLevel 0
Pollrate 0.05
NicChgsPollInt 3.0
```

- Por último para habilitar el protocolo se escribe el comando

```
root@Mesh1 :~# /etc/init.d/olsrd start
```

Los paquetes enviados por la red por medio de este protocolo se los puede observar con el programa Wireshark los mismos que se observan en la Figura 3.8.1



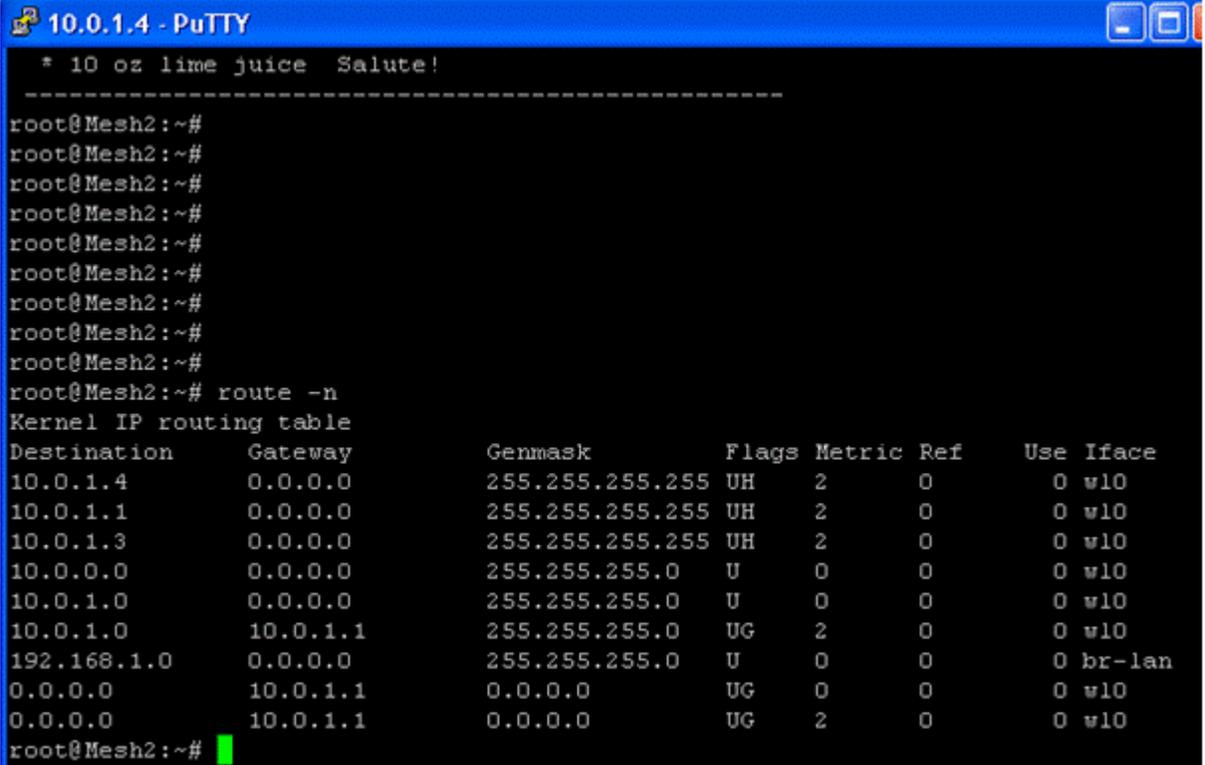
**Figura 3.24: Captura de paquetes O.L.S.R. en Wireshark**

Las rutas creadas dinámicamente en cada enrutador se observan por medio del comando:

```
root@Mesh1:~# route -n
```



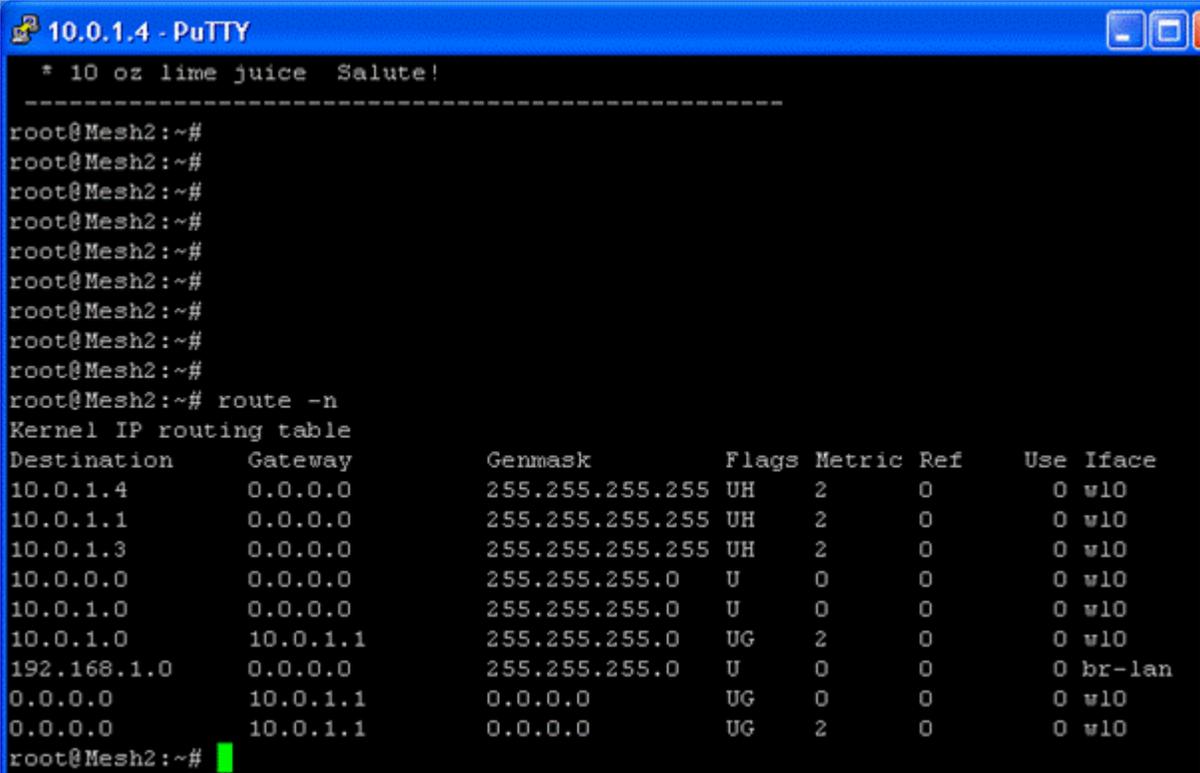
## Enrutador 2



```
10.0.1.4 - PuTTY
* 10 oz lime juice Salute!
-----
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.0.1.4         0.0.0.0         255.255.255.255 UH    2     0     0 w10
10.0.1.1         0.0.0.0         255.255.255.255 UH    2     0     0 w10
10.0.1.3         0.0.0.0         255.255.255.255 UH    2     0     0 w10
10.0.0.0         0.0.0.0         255.255.255.0   U     0     0     0 w10
10.0.1.0         0.0.0.0         255.255.255.0   U     0     0     0 w10
10.0.1.0         10.0.1.1       255.255.255.0   UG    2     0     0 w10
192.168.1.0     0.0.0.0         255.255.255.0   U     0     0     0 br-lan
0.0.0.0         10.0.1.1       0.0.0.0         UG    0     0     0 w10
0.0.0.0         10.0.1.1       0.0.0.0         UG    2     0     0 w10
root@Mesh2:~#
```

*Figura 3.26: Rutas creadas O.L.S.R - Enrutador 2*

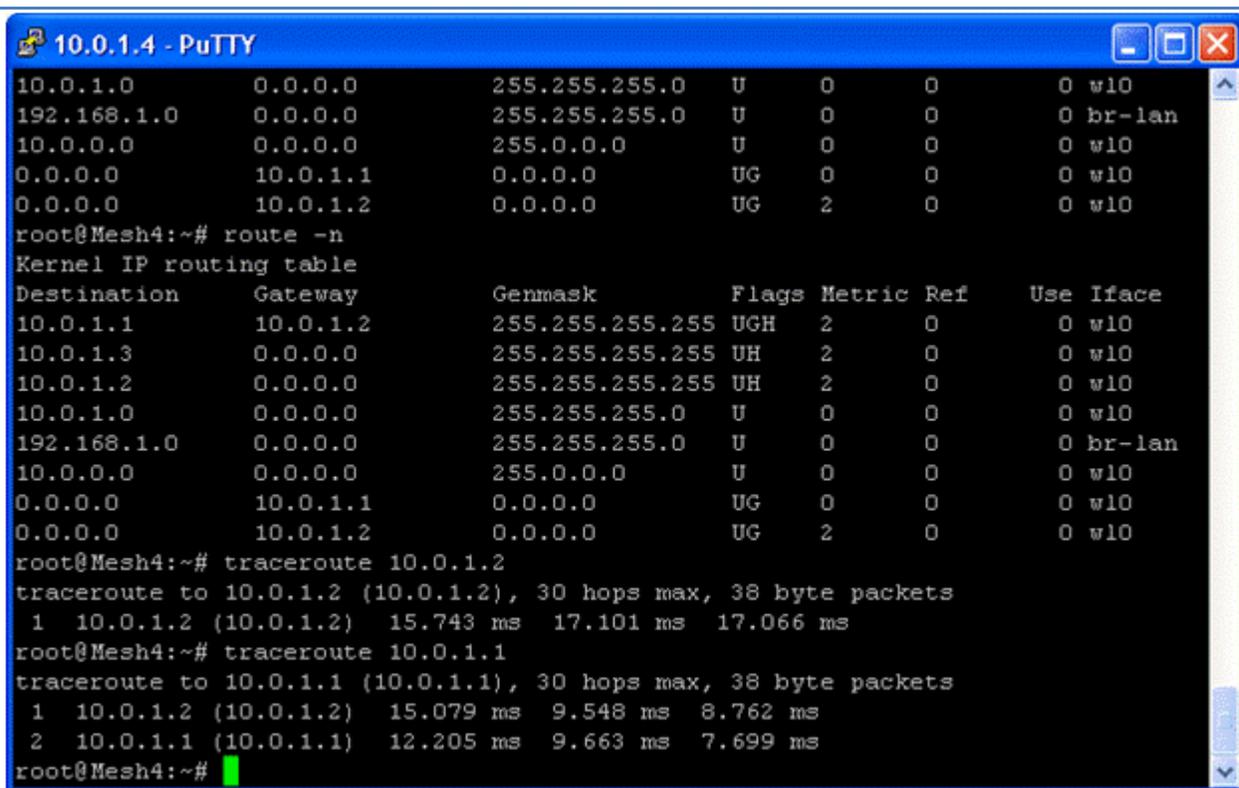
### Enrutador 3



```
10.0.1.4 - PuTTY
* 10 oz lime juice Salute!
-----
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~#
root@Mesh2:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.1.4         0.0.0.0        255.255.255.255 UH    2     0     0   w10
10.0.1.1         0.0.0.0        255.255.255.255 UH    2     0     0   w10
10.0.1.3         0.0.0.0        255.255.255.255 UH    2     0     0   w10
10.0.0.0         0.0.0.0        255.255.255.0   U     0     0     0   w10
10.0.1.0         0.0.0.0        255.255.255.0   U     0     0     0   w10
10.0.1.0         10.0.1.1       255.255.255.0   UG    2     0     0   w10
192.168.1.0     0.0.0.0        255.255.255.0   U     0     0     0   br-lan
0.0.0.0         10.0.1.1       0.0.0.0         UG    0     0     0   w10
0.0.0.0         10.0.1.1       0.0.0.0         UG    2     0     0   w10
root@Mesh2:~#
```

*Figura 3.27: Rutas creadas O.L.S.R. - Enrutador 3*

## Enrutador 4



```

10.0.1.0      0.0.0.0      255.255.255.0  U   0   0       0 w10
192.168.1.0  0.0.0.0      255.255.255.0  U   0   0       0 br-lan
10.0.0.0     0.0.0.0      255.0.0.0       U   0   0       0 w10
0.0.0.0     10.0.1.1     0.0.0.0         UG  0   0       0 w10
0.0.0.0     10.0.1.2     0.0.0.0         UG  2   0       0 w10
root@Mesh4:~# route -n
Kernel IP routing table
Destination   Gateway       Genmask       Flags Metric Ref    Use Iface
10.0.1.1     10.0.1.2     255.255.255.255 UGH   2     0     0    w10
10.0.1.3     0.0.0.0      255.255.255.255 UH    2     0     0    w10
10.0.1.2     0.0.0.0      255.255.255.255 UH    2     0     0    w10
10.0.1.0     0.0.0.0      255.255.255.0  U     0     0     0    w10
192.168.1.0  0.0.0.0      255.255.255.0  U     0     0     0    br-lan
10.0.0.0     0.0.0.0      255.0.0.0       U     0     0     0    w10
0.0.0.0     10.0.1.1     0.0.0.0         UG   0     0     0    w10
0.0.0.0     10.0.1.2     0.0.0.0         UG   2     0     0    w10
root@Mesh4:~# traceroute 10.0.1.2
traceroute to 10.0.1.2 (10.0.1.2), 30 hops max, 38 byte packets
 1 10.0.1.2 (10.0.1.2) 15.743 ms 17.101 ms 17.066 ms
root@Mesh4:~# traceroute 10.0.1.1
traceroute to 10.0.1.1 (10.0.1.1), 30 hops max, 38 byte packets
 1 10.0.1.2 (10.0.1.2) 15.079 ms 9.548 ms 8.762 ms
 2 10.0.1.1 (10.0.1.1) 12.205 ms 9.663 ms 7.699 ms
root@Mesh4:~#

```

**Figura 3.28: Rutas creadas dinámicamente- Enrutador 4**

Por medio de la depuración se puede observar el trabajo que realiza el protocolo por medio del Algoritmo de Dijkstra, escogiendo la ruta de menor costo para llegar al destino. A continuación se detalla la depuración realizada al enrutador 4.

--- 15:42:49.321294 -----

---- DIJKSTRA

KERN: Adding 10.0.1.3/32 from 10.0.1.3 via 10.0.1.3, cost 0.000,  
metric 1, v 20

KERN: ERROR adding 10.0.1.3/32 from 10.0.1.3 via 10.0.1.3, cost  
0.000, metric 1, v 20: File exists

KERN: Adding 10.0.1.1/32 from 10.0.1.1 via 10.0.1.3, cost 0.000,  
metric 2, v 20

--- 15:42:49.327746 -----

----- LINKS

IP address	hyst	LQ	ETX
10.0.1.1	0.749	0.000/0.000	INFINITE
10.0.1.2	1.000	0.000/0.000	INFINITE
10.0.1.3	1.000	0.000/0.000	INFINITE

--- 15:42:49.332608 ----- TWO-HOP NEIGHBORS

IP addr (2-hop)	IP addr (1-hop)	Total cost
10.0.1.2	10.0.1.1	INFINITE
	10.0.1.3	INFINITE
10.0.1.1	10.0.1.2	INFINITE
	10.0.1.3	INFINITE
10.0.1.3	10.0.1.1	INFINITE
	10.0.1.2	INFINITE

--- 15:42:49.334709 -----

---- TOPOLOGY

Source IP addr	Dest IP addr	LQ	ETX
10.0.1.1	10.0.1.3	0.039/0.000	0.000
10.0.1.2	10.0.1.1	0.039/0.000	0.000
10.0.1.2	10.0.1.3	0.039/0.000	0.000
10.0.1.3	10.0.1.1	0.039/0.000	0.000
10.0.1.3	10.0.1.2	0.008/0.906	0.000
10.0.1.3	10.0.1.4	0.039/0.000	0.000
10.0.1.4	10.0.1.1	0.000/0.000	0.000
10.0.1.4	10.0.1.2	0.000/0.000	0.000
10.0.1.4	10.0.1.3	0.000/0.000	0.000

HYST[10.0.1.1] HELLO timeout 0.374267

|

```

*** olsr.org - 0.5.6-r3 (2009-12-06 03:47:50 on arrakis)
***

--- 15:42:50.460738 -----
---- DIJKSTRA

KERN: Deleting 10.0.1.2/32 via 10.0.1.3
KERN: Adding 10.0.1.3/32 from 10.0.1.3 via 10.0.1.3, cost 0.000,
metric 1, v 21
KERN: ERROR adding 10.0.1.3/32 from 10.0.1.3 via 10.0.1.3, cost
0.000, metric 1, v 21: File exists

--- 15:42:50.466632 -----
----- LINKS

IP address      hyst          LQ           ETX
10.0.1.1        0.374  0.000/0.000  INFINITE
10.0.1.2        1.000  0.000/0.000  INFINITE
10.0.1.3        1.000  0.000/0.000  INFINITE

--- 15:42:50.471750 ----- TWO-HOP NEIGHBORS

IP addr (2-hop)  IP addr (1-hop)  Total cost
10.0.1.2         10.0.1.1         INFINITE
                  10.0.1.3         INFINITE
10.0.1.1         10.0.1.2         INFINITE
                  10.0.1.3         INFINITE
10.0.1.3         10.0.1.1         INFINITE
                  10.0.1.2         INFINITE

--- 15:42:50.473891 -----
---- TOPOLOGY

Source IP addr  Dest IP addr      LQ           ETX
10.0.1.1        10.0.1.3          0.039/0.000  0.000
10.0.1.3        10.0.1.1          0.039/0.000  0.000
10.0.1.3        10.0.1.2          0.008/0.906  0.000
10.0.1.3        10.0.1.4          0.039/0.000  0.000
10.0.1.4        10.0.1.1          0.000/0.000  0.000
10.0.1.4        10.0.1.2          0.000/0.000  0.000
10.0.1.4        10.0.1.3          0.000/0.000  0.000
/

*** olsr.org - 0.5.6-r3 (2009-12-06 03:47:50 on arrakis)
***
Setting 10.0.1.3 as MPR

```

```
--- 15:42:50.781327 -----
----- LINKS
```

IP address	hyst	LQ	ETX
10.0.1.1	0.687	0.000/0.000	INFINITE
10.0.1.2	1.000	0.000/0.000	INFINITE
10.0.1.3	1.000	0.000/0.000	INFINITE

```
--- 15:42:50.785872 ----- TWO-HOP NEIGHBORS
```

IP addr (2-hop)	IP addr (1-hop)	Total cost
10.0.1.2	10.0.1.3	INFINITE
10.0.1.1	10.0.1.2	INFINITE
	10.0.1.3	INFINITE
10.0.1.3	10.0.1.1	INFINITE
	10.0.1.2	INFINITE

```
--- 15:42:50.787763 -----
----- TOPOLOGY
```

Source IP addr	Dest IP addr	LQ	ETX
10.0.1.1	10.0.1.3	0.039/0.000	0.000
10.0.1.3	10.0.1.1	0.039/0.000	0.000
10.0.1.3	10.0.1.2	0.008/0.906	0.000
10.0.1.3	10.0.1.4	0.039/0.000	0.000
10.0.1.4	10.0.1.1	0.000/0.000	0.000
10.0.1.4	10.0.1.2	0.000/0.000	0.000
10.0.1.4	10.0.1.3	0.000/0.000	0.000

```
*** olsr.org - 0.5.6-r3 (2009-12-06 03:47:50 on arrakis)
```

```
***
```

```
Setting 10.0.1.3 as MPR
```

# **CAPITULO 4**

## **4. PRUEBAS DE CALIDAD DE SERVICIO**

### **4.1. Pruebas Empleando B.A.T.M.A.N. como Protocolo De Enrutamiento Inalámbrico Mesh**

En esta sección se detallan las pruebas llevadas a cabo en la red inalámbrica mallada empleando el protocolo de enrutamiento B.A.T.M.A.N.

#### 4.1.1. Pérdida De Paquetes, Jitter, Ancho De Banda, Retardo

Se realizaron las pruebas en cada zona, usando el protocolo de enrutamiento B.A.T.M.A.N, realizando llamadas telefónicas y capturando los paquetes que viajaban en la red usando la herramienta de captura de paquetes Wireshark. Los detalles se muestran a continuación:

##### Zona 1:

##### a) Enrutador 1:

No. -	Time	Source	Destination	Protocol	Info
73	2.137064	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=68
74	2.147351	10.0.1.3	10.0.1.255	BAT_BATM	Seq=5
75	2.152230	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=532
76	2.152468	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=5389 win=32693 Len=0
77	2.203292	10.0.1.1	10.0.1.255	BAT_BATM	Seq=5
78	2.208567	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=356
79	2.332157	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=5745 win=32648 Len=0
80	2.399114	200.126.12.116	10.0.1.22	SIP	Status: 200 OK[Packet size limited during capture]
81	2.446033	10.0.1.22	200.126.12.116	UDP	Source port: 51521 Destination port: 12159
82	2.482375	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
83	2.498916	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
84	2.520367	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
85	2.539205	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
86	2.540321	10.0.1.1	10.0.1.255	BAT_BATM	Seq=7
87	2.547938	10.0.1.22	200.126.12.116	SIP	Request: ACK sip:10070200.126.12.116[Packet size limited during capture]
88	2.553182	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=1300
89	2.556811	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
90	2.557109	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=7097 win=32768 Len=0
91	2.558599	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=116
92	2.559750	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=68
93	2.560913	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
94	2.562317	10.0.1.3	10.0.1.255	BAT_BATM	Seq=7
95	2.562718	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=7281 win=32745 Len=0
96	2.563268	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
97	2.566252	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
98	2.566308	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=7385 win=32732 Len=0
99	2.567252	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
100	2.569005	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=292
101	2.569349	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=89 Ack=7729 win=32689 Len=0
102	2.578914	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
103	2.594714	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
104	2.618714	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
105	2.634682	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
106	2.658899	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
107	2.674495	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158
108	2.690983	10.0.1.22	200.126.12.116	UDP	Source port: 51520 Destination port: 12158

[Frame 1 (106 bytes on wire, 96 bytes captured)]  
 [Ethernet II, Src: Cisco-L1\_27:b8:60 (68:7f:74:27:b8:60), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)]  
 [Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.1.22 (10.0.1.22)]  
 [Transmission Control Protocol, Src Port: ssh (22), Dst Port: camac (3545), Seq: 1, Ack: 1, Len: 52]  
 [SSH Protocol]  
 [Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 68 7f 74 27 b8 60 08 00 45 10  .#...h. t'...E.
0010 00 3c a2 f1 40 00 40 06 81 84 0a 00 01 0a 00  .\..@.....
0020 01 16 00 16 0d d9 4b 6d eb 10 92 88 eb 7e 50 18  ....Km .....P.
0030 19 20 9c 3e 00 00 3b 6f 9a a6 d3 e2 4b 55 6c df  .>..;o...kUl.
0040 49 9a 58 42 a6 ec bb 57 ef 52 50 4d 97 6d da ef  .ZB...RV...m..
0050 de ec 87 48 8e 26 d3 4f 4e d3 53 ed a0 44 ab b0  ...H.&O N.S.D..
  
```

File: C:\Users\Joehward\esool\PROYECTO... \ Packets: 3573 Displayed: 3573 Marked: 0

**Figura 4.1: Captura de paquetes del enrutador 1 en Zona 1 (BATMAN)**

b) Enrutador 2:

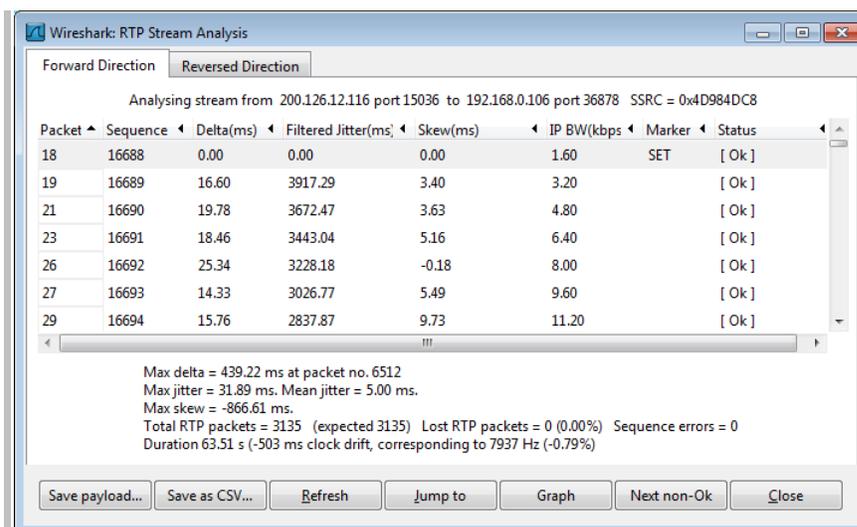
No.	Time	Source	Destination	Protocol	Info
2	0.000000	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
3	0.001820	10.0.1.3	10.0.1.22	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=105 win=32690 Len=0
4	0.002679	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
5	0.003763	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
6	0.004411	10.0.1.3	10.0.1.22	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=209 win=32677 Len=0
7	0.005201	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
8	0.006286	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
9	0.007332	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
10	0.008022	10.0.1.3	10.0.1.3	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=313 win=32664 Len=0
11	0.008812	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
12	0.009435	10.0.1.3	10.0.1.22	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=417 win=32651 Len=0
13	0.010276	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
14	0.011477	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
15	0.012147	10.0.1.3	10.0.1.22	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=537 win=32636 Len=0
16	0.012988	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
17	0.023819	10.0.1.22	10.0.1.3	TCP	telumat-rms > ssh [ACK] Seq=1 Ack=589 win=32629 Len=0
18	0.242132	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=68
19	0.251622	10.0.1.3	10.0.1.255	BAT_BATM	Seq=5
20	0.256656	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=532
21	0.257908	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=1 Ack=601 win=32693 Len=0
22	0.309833	10.0.1.1	10.0.1.255	BAT_BATM	Seq=5
23	0.313554	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=356
24	0.437594	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=1 Ack=957 win=32648 Len=0
25	0.504246	200.126.12.116	10.0.1.22	SIP	Status: 200 OK[Packet size limited during capture]
26	0.551470	10.0.1.22	200.126.12.116	UDP	source port: 51521 Destination port: 12159
27	0.587797	10.0.1.22	200.126.12.116	UDP	source port: 51520 Destination port: 12158
28	0.604338	10.0.1.22	200.126.12.116	UDP	source port: 51520 Destination port: 12158
29	0.625816	10.0.1.22	200.126.12.116	UDP	source port: 51520 Destination port: 12158
30	0.644670	10.0.1.22	200.126.12.116	UDP	source port: 51520 Destination port: 12158
31	0.646830	10.0.1.1	10.0.1.255	BAT_BATM	Seq=7
32	0.657437	10.0.1.22	200.126.12.116	SIP	Request: ACK sip:1007@200.126.12.116[Packet size limited during capture]
33	0.657981	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=1300
34	0.661884	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=52
35	0.662533	10.0.1.22	10.0.1.3	TCP	bmc-onekey > ssh [ACK] Seq=1 Ack=2309 win=32768 Len=0
36	0.663650	10.0.1.3	10.0.1.22	SSH	Encrypted response packet len=16

Figura 4.2: Captura de paquetes del enrutador 2 en Zona 1 (BATMAN)

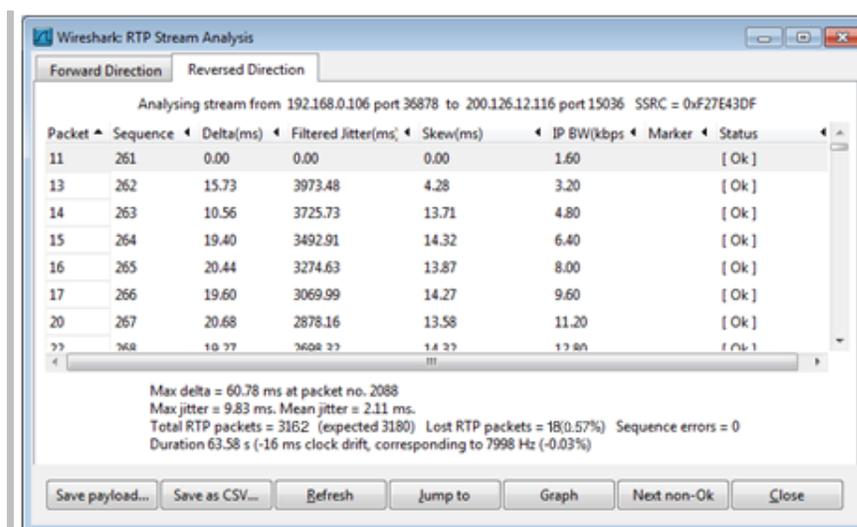
c) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.106	72.247.238.43	TCP	8004 > http [FIN, ACK] Seq=1 Ack=1 win=255 Len=0
2	0.000019	192.168.0.106	72.247.238.43	TCP	8004 > http [RST, ACK] Seq=2 Ack=1 win=0 Len=0
3	0.000442	192.168.0.106	62.41.70.114	TCP	8032 > https [FIN, ACK] Seq=1 Ack=1 win=255 Len=0
4	0.000443	192.168.0.106	62.41.70.114	TCP	57969 > https [FIN, ACK] Seq=1 Ack=1 win=254 Len=0
5	0.208329	62.41.70.114	192.168.0.106	TCP	https > 8002 [ACK] Seq=1 Ack=2 win=417 Len=0
6	0.221428	192.168.0.106	200.126.12.116	UDP	source port: 36879 Destination port: 15037
7	0.263350	62.41.70.114	192.168.0.106	TCP	https > 57969 [ACK] Seq=1 Ack=2 win=295 Len=0
8	0.279057	192.168.0.106	200.126.12.116	UDP	source port: 36878 Destination port: 15036
9	0.288197	192.168.0.106	200.126.12.116	SIP	Request: ACK sip:1007@200.126.12.116[Instance=70878958451cb31
10	0.321911	192.168.0.106	200.126.12.116	SIP/SDP	Status: 200 OK, with session description
11	0.322636	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=261, Time=1864020
12	0.323334	200.126.12.116	192.168.0.106	RTP	Request: ACK sip:1007@200.126.12.116[Instance=70878958451cb31
13	0.338361	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=262, Time=1864180
14	0.348924	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=263, Time=1864340
15	0.368320	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=264, Time=1864500
16	0.388765	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=265, Time=1864660
17	0.408369	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=266, Time=1864820
18	0.411695	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16688, Time=3095600, Mark
19	0.428293	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16689, Time=3095760
20	0.429053	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=267, Time=1864980
21	0.448069	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16690, Time=3095920
22	0.448320	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=268, Time=1865140
23	0.466533	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16691, Time=3096080
24	0.467685	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=269, Time=1865300
25	0.488471	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=270, Time=1865460
26	0.491874	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16692, Time=3096240
27	0.506207	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16693, Time=3096400
28	0.507724	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=271, Time=1865620
29	0.521959	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16694, Time=3096560
30	0.528354	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=272, Time=1865780
31	0.546016	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16695, Time=3096720
32	0.547722	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=273, Time=1865940
33	0.561970	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16696, Time=3096880
34	0.568460	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=274, Time=1866100
35	0.586167	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4D984D8C, Seq=16697, Time=3097040
36	0.587777	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x27E43D0, Seq=275, Time=1866260

Figura 4.3: Captura de paquetes del enrutador 2 en Zona 1-cliente Softphone (BATMAN)



**Figura 4.4: Steam RTP en el cliente en la dirección de avance en Zona 1 (BATMAN)**



**Figura 4.5: Steam RTP en el cliente en la dirección de reversa en Zona 1 (BATMAN)**

### Zona 2:

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.1	10.0.1.22	SSH	Encrypted response packet len=52
2	0.022544	200.126.12.116	10.0.1.22	SIP	Status: 200 OK[packet size limited during capture]
3	0.046782	10.0.1.22	10.0.1.1	TCP	gprs-cube > ssh [ACK] Seq=1 Ack=1 Win=32654 Len=0
4	0.047121	10.0.1.22	10.0.1.2	TCP	rb1checkd > ssh [ACK] Seq=1 Ack=1 Win=32768 Len=0
5	0.047698	10.0.1.22	10.0.1.1	TCP	tcpdataserver > ssh [ACK] Seq=1 Ack=53 Win=32677 Len=0
6	0.048038	10.0.1.1	10.0.1.22	SSH	Encrypted response packet len=536
7	0.057657	10.0.1.22	200.126.12.116	UDP	Source port: 36639 Destination port: 12148
8	0.096239	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
9	0.117277	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
10	0.122887	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
11	0.137763	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
12	0.152354	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
13	0.161402	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
14	0.163822	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
15	0.165027	10.0.1.22	200.126.12.116	SIP	Request: ACK sip:1007@200.126.12.116[packet size limited during capture]
16	0.180633	10.0.1.22	10.0.1.1	TCP	tcpdataserver > ssh [ACK] Seq=1 Ack=589 Win=32610 Len=0
17	0.183075	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
18	0.184008	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
19	0.203124	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
20	0.204602	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
21	0.223009	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
22	0.227224	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
23	0.243089	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
24	0.246378	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
25	0.261886	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
26	0.267077	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
27	0.281236	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
28	0.284678	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
29	0.302892	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
30	0.304067	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
31	0.321248	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
32	0.324650	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
33	0.334535	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
34	0.341852	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638
35	0.354277	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
36	0.364246	200.126.12.116	10.0.1.22	UDP	Source port: 12148 Destination port: 36638

[Frame 1 (106 bytes on wire, 96 bytes captured)]  
 [Ethernet II, Src: Cisco-Li\_27:b8:60 (68:7f:74:27:b8:60), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)]  
 [Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.1.22 (10.0.1.22)]  
 [Transmission Control Protocol, Src Port: ssh (22), Dst Port: tcpdataserver (3805), Seq: 1, Ack: 1, Len: 52]  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 68 7f 74 27 b8 60 08 00 45 10  .#...h.t'...E.
ffff 00 5c 64 76 00 00 00 00 00 00 00 00 00 00 00 00
  
```

**Figura 4.6: Captura de paquetes del enrutador 1 en Zona 2 (BATMAN)**

### b) Enrutador 2:

No. -	Time	Source	Destination	Protocol	Info
630	11.102093	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
639	11.199477	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
640	11.202876	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
641	11.208090	10.0.1.22	10.0.1.22	SSH	Encrypted response packet len=68
642	11.217564	10.0.1.22	10.0.1.255	BAT_BATM	seq=26
643	11.222050	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
644	11.228774	10.0.1.22	10.0.1.22	SSH	Encrypted response packet len=120
645	11.238072	10.0.1.22	10.0.1.2	TCP	rb1checkd > ssh [ACK] Seq=89 Ack=13561 Win=32607 Len=0
646	11.243103	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
647	11.252740	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
648	11.274351	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
649	11.292389	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
650	11.314324	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
651	11.342105	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
652	11.365246	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
653	11.382180	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
654	11.402769	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
655	11.436980	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
656	11.442100	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
657	11.462290	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
658	11.482951	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
659	11.490150	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
660	11.512222	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
661	11.532839	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
662	11.554334	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
663	11.583121	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
664	11.602360	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
665	11.642001	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
666	11.642712	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
667	11.662692	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
668	11.664310	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
669	11.702493	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
670	11.722341	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
671	11.733416	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
672	11.755317	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
673	11.778592	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148

[Frame 1 (106 bytes on wire, 96 bytes captured)]  
 [Ethernet II, Src: Cisco-Li\_27:b8:ba (68:7f:74:27:b8:ba), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)]  
 [Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.22 (10.0.1.22)]  
 [Transmission Control Protocol, Src Port: ssh (22), Dst Port: neto-dcs (3814), Seq: 1, Ack: 1, Len: 52]  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 68 7f 74 27 b8 ba 08 00 45 10  .#...h.t'...E.
ffff 00 5c 64 76 00 00 00 00 00 00 00 00 00 00 00
  
```

**Figura 4.7: Captura de paquetes del enrutador 2 en Zona 2 (BATMAN)**

c) Enrutador 3:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
2	0.020335	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
3	0.077564	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
4	0.079858	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
5	0.083053	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
6	0.096434	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
7	0.112307	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
8	0.133127	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
9	0.202263	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
10	0.204463	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
11	0.206318	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
12	0.229438	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
13	0.334699	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
14	0.337330	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
15	0.413114	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
16	0.417244	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
17	0.418186	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
18	0.433642	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
19	0.530086	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
20	0.591627	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
21	0.674371	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
22	0.675312	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
23	0.676037	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
24	0.676765	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
25	0.677611	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
26	0.678339	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
27	0.679287	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
28	0.679934	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
29	0.680641	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
30	0.681468	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
31	0.682426	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
32	0.683163	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
33	0.683883	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
34	0.684652	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
35	0.685478	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148
36	0.704004	10.0.1.22	200.126.12.116	UDP	Source port: 36638 Destination port: 12148

[Frame 1 (214 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f), Dst: Cisco-Li\_27:b8:b1 (68:7f:74:27:b8:b1)  
 Internet Protocol, Src: 10.0.1.22 (10.0.1.22), Dst: 200.126.12.116 (200.126.12.116)  
 User Datagram Protocol, Src Port: 36638 (36638), Dst Port: 12148 (12148)  
 Data (54 bytes)

```

0000  68 7f 74 27 b8 b1 00 23 08 b3 04 8f 00 00 45 00  h.t...#.....E.
0010  00 c8 91 4a 00 00 80 11 c8 02 0a 00 01 16 c8 7e  ...J.....~
0020  0c 74 8f 1e 2f 74 00 b4 16 8a 80 1c 70 00 09 2  ..../.....P
0030  d6 34 35 78 6a d4 b7 cb 50 3a 3a b0 f6 ad aa aa  .45kj...P.....
0040  ba cd 40 48 39 35 24f 3f ca b8 d6 e0 d8 5e 4d 54  ...H54?.....M
0050  d7 d0 4f 3f 37 47 da c1 3e 4b 4c 4a 4e 3e 36  ...756...z&LJN66
  
```

File: C:\Users\joedward\espo\PROYECTO... Packets: 7844 Displayed: 7844 Marked: 0

Figura 4.8: Captura de paquetes del enrutador 3 en Zona 2 (BATMAN)

d) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
37	0.945182	192.168.0.106	72.246.43.33	TCP	58672 > http [ACK] Seq=1 Ack=416 win=255 Len=0
38	0.948236	72.246.43.33	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
39	0.948246	72.246.43.33	192.168.0.106	TCP	http > 58673 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
40	0.948249	72.246.25.74	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
41	0.948252	72.246.25.74	192.168.0.106	TCP	http > 58677 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
42	0.948444	192.168.0.106	72.246.43.33	TCP	58673 > http [ACK] Seq=1 Ack=416 win=255 Len=0
43	0.948500	192.168.0.106	72.246.25.74	TCP	58677 > http [ACK] Seq=1 Ack=416 win=255 Len=0
44	0.954396	72.246.25.74	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
45	0.954409	72.246.25.74	192.168.0.106	TCP	http > 58676 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
46	0.954604	192.168.0.106	72.246.25.74	TCP	58676 > http [ACK] Seq=1 Ack=416 win=255 Len=0
47	0.969293	72.246.25.74	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
48	0.969303	72.246.25.74	192.168.0.106	TCP	http > 58674 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
49	0.969306	72.246.25.74	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
50	0.969310	72.246.25.74	192.168.0.106	TCP	http > 58675 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
51	0.969531	192.168.0.106	72.246.25.74	TCP	58674 > http [ACK] Seq=1 Ack=416 win=255 Len=0
52	0.969627	192.168.0.106	72.246.25.74	TCP	58675 > http [ACK] Seq=1 Ack=416 win=255 Len=0
53	0.970953	206.57.13.32	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
54	0.970964	206.57.13.32	192.168.0.106	TCP	http > 58661 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
55	0.971204	192.168.0.106	206.57.13.32	TCP	58661 > http [ACK] Seq=1 Ack=416 win=255 Len=0
56	1.089277	23.1.79.139	192.168.0.106	TCP	http > 58709 [FIN, ACK] Seq=1 Ack=1 win=257 Len=0
57	1.089444	192.168.0.106	23.1.79.139	TCP	58709 > http [ACK] Seq=1 Ack=2 win=255 Len=0
58	1.220052	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
59	1.254007	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
60	1.284296	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
61	1.293994	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
62	1.313461	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
63	1.333947	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
64	1.338059	72.246.43.33	192.168.0.106	HTTP	HTTP/1.0 408 Request Time-out (text/html)
65	1.338075	72.246.43.33	192.168.0.106	TCP	http > 58668 [FIN, ACK] Seq=415 Ack=1 win=183 Len=0
66	1.338332	192.168.0.106	72.246.43.33	TCP	58668 > http [ACK] Seq=1 Ack=416 win=255 Len=0
67	1.353507	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
68	1.374111	192.168.0.106	200.126.12.116	UDP	Source port: 15658 Destination port: 10534
69	1.376794	192.168.0.106	200.126.12.116	SIP/SDP	Status: 200 ok with session description
70	1.384838	200.126.12.116	192.168.0.106	SIP	Request: ACK sip:1007@200.126.12.109:61888;rinstance=e70878958451cb31
71	1.393756	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xc774AF0E, Seq=4691, Time=1349520
72	1.414011	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xc774AF0E, Seq=4692, Time=1349600

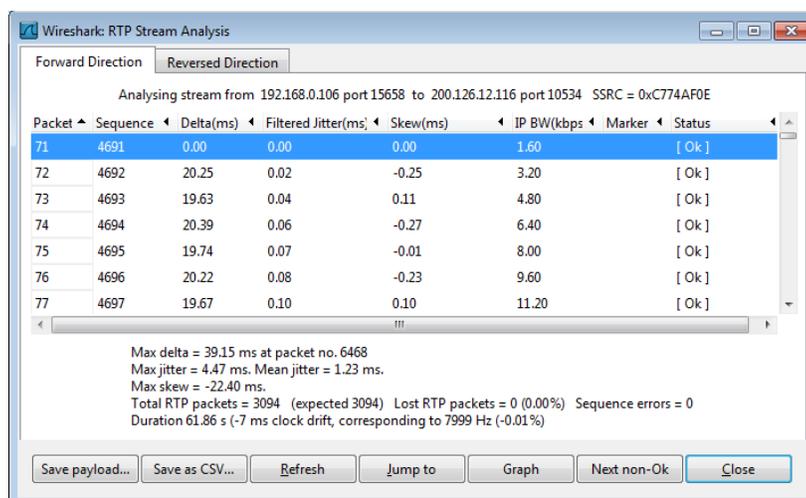
[Frame 1 (468 bytes on wire, 468 bytes captured)  
 Ethernet II, Src: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96), Dst: CameoCom\_3d:cb:0a (00:40:f4:3d:cb:0a)  
 Internet Protocol, Src: 208.44.23.112 (208.44.23.112), Dst: 192.168.0.106 (192.168.0.106)  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 58660 (58660), Seq: 1, Ack: 1, Len: 414  
 Hypertext Transfer Protocol  
 Line-based text data: text/html

```

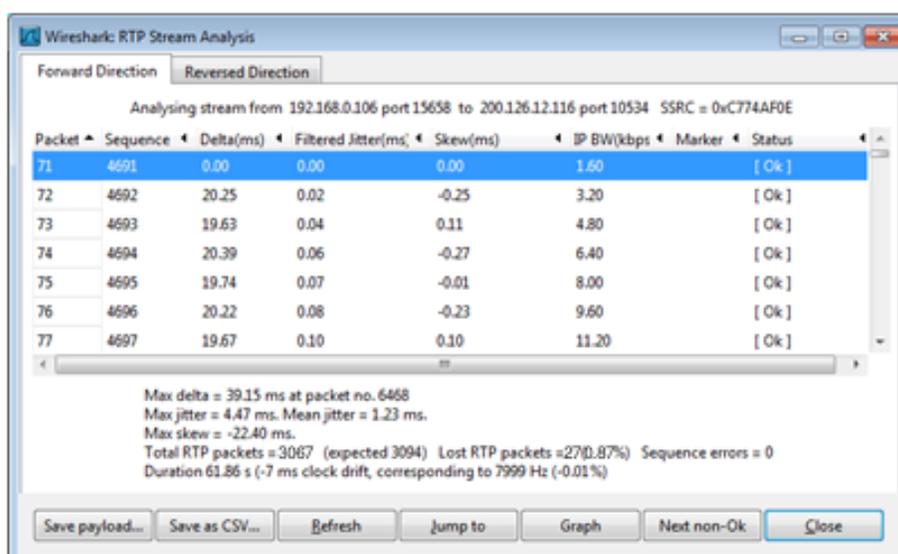
0000  00 40 f4 3d cb 0a 00 17 9a 2a 7f 96 08 00 45 00  .@.F.d.cb.O.17.9a.2a.7f.96.08.00.45.00  .@.....E.
0010  01 c5 08 4c 40 00 32 06 c5 a6 0c 17 70 c0 a8  ..C.....P.
0020  00 6a 00 50 e5 24 b0 d9 30 71 4c b1 7e a0 50 18  .j.....P.
0030  00 b7 63 61 00 48 54 54 50 2f 31 2e 30 20 34  .ca..HTP/1.0 4
0040  39 20 52 63 71 75 65 73 74 20 58 68 65 21 70  .88 Reque st Time-
0050  6f 75 74 04 0a 53 65 72 76 65 72 3a 20 41 6b 61  out..Ser ver: Aka
0060  64 61 60 47 48 f2 72 74 0d 0a 64 60 6d 65 74 56  markCo nt: v
  
```

File: C:\Users\joedward\espo\PROYECTO... Packets: 6806 Displayed: 6806 Marked: 0

Figura 4.9: Captura de paquetes del cliente en Zona 2 (BATMAN)



**Figura 4.10: Steam RTP en el cliente en la dirección de avance en Zona 2 (BATMAN)**



**Figura 4.11: Steam RTP en el cliente en la dirección de avance**

Zona 3:

a) Enrutador 1:

No.	Time	Source	Destination	Protocol	Info
2	0.004441	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
3	0.020842	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
4	0.024818	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
5	0.044338	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
6	0.049442	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
7	0.064854	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
8	0.067940	10.0.1.22	10.0.1.1	TCP	pxc-p1r-ft > ssh [ACK] seq=1 ack=1 win=12664 Len=0
9	0.068298	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=388
10	0.070142	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
11	0.084377	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
12	0.091192	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
13	0.104939	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
14	0.111175	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
15	0.124457	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
16	0.129542	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
17	0.144736	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
18	0.150113	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
19	0.164490	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
20	0.170544	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
21	0.183802	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
22	0.190158	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
23	0.201771	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
24	0.204291	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
25	0.223821	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
26	0.230230	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
27	0.238874	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
28	0.244718	10.0.1.4	10.0.1.255	BAT_BATM	seq=2
29	0.245073	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
30	0.251396	10.0.1.3	10.0.1.22	SSH	encrypted response packet len=692
31	0.251662	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=740
32	0.258386	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
33	0.261196	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=1044
34	0.264003	200.126.12.116	10.0.1.22	UDP	source port: 16596 destination port: 12538
35	0.267453	10.0.1.2	10.0.1.255	BAT_BATM	seq=2
36	0.268714	10.0.1.22	10.0.1.1	TCP	osmswanmer > sch [ACK] seq=1 ack=1781 win=12768 len=0
Frame 1 (214 bytes on wire, 96 bytes captured)					
Ethernet II, Src: Cisco-Li_27:b8:ba (68:7f:74:27:b8:ba), Dst: Cisco-Li_27:b8:ba (68:7f:74:27:b8:ba)					
Internet Protocol, Src: 10.0.1.22 (10.0.1.22), Dst: 200.126.12.116 (200.126.12.116)					
User Datagram Protocol, Src Port: 12538 (12538), Dst Port: 16596 (16596)					
Data (54 bytes)					
0000 68 7f 74 27 b8 ba 08 00 45 00 h.t'.h. t'....E.					
0010 00 c8 fe cd 00 00 7f 11 3c 4f 0a 00 01 16 c8 7e ..U...Z.....					
0020 0c 74 30 fa 40 04 00 b4 90 87 80 00 16 46 00 29 .to.8...:..F..					
0030 c2 60 f8 8f a8 cb 7d 0b 60 66 6f 75 7f ef e9 b .....}k...F...					
0040 e7 f3 74 75 7f 7d 73 71 75 7b fa 7c 7d f3 f2 f7 ..tu.)sq u{.}....					
0050 ba b7 bb c7 e3 5f 55 4f 48 3f 3c 3e 4a 64 ee fb .....wmu yy.....					
File: "C:\Users\joedw\respo\PROYECTO... \Packets: 3060 Displayed: 3060 Marked: 0					

Figura 4.12: Captura de paquetes del enrutador 1 en Zona 3 (BATMAN)

b) Enrutador 2:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
2	0.000287	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
3	0.019555	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
4	0.019840	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
5	0.049906	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
6	0.050174	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
7	0.060440	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
8	0.060713	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
9	0.079251	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
10	0.079526	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
11	0.100229	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
12	0.100502	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
13	0.129985	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
14	0.130261	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
15	0.139811	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
16	0.140083	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
17	0.159299	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
18	0.159570	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
19	0.184689	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
20	0.184965	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
21	0.189590	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
22	0.189864	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
23	0.199695	10.0.1.22	10.0.1.2	SSH	encrypted request packet len=88
24	0.210314	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
25	0.210598	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
26	0.233468	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
27	0.233743	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
28	0.259853	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
29	0.260130	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
30	0.269617	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
31	0.269890	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
32	0.290377	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
33	0.290656	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
34	0.319453	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
35	0.319730	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
36	0.349704	10.0.1.22	200.126.12.116	UDP	source port: 12538 destination port: 16596
Frame 1 (214 bytes on wire, 96 bytes captured)					
Ethernet II, Src: Arcadyan_lb3:04:8f (00:23:08:b3:04:8f), Dst: Cisco-Li_27:b8:ba (68:7f:74:27:b8:ba)					
Internet Protocol, Src: 10.0.1.22 (10.0.1.22), Dst: 200.126.12.116 (200.126.12.116)					
User Datagram Protocol, Src Port: 12538 (12538), Dst Port: 16596 (16596)					
Data (54 bytes)					
0000 68 7f 74 27 b8 ba 00 23 08 b3 04 8f 08 00 45 00 h.t'...'# .....E.					
0010 00 c8 ff 55 00 00 80 11 5a c7 0a 00 01 16 c8 7e ..U...Z.....					
0020 0c 74 30 fa 40 04 00 b4 90 87 80 00 16 46 00 29 .to.8...:..F..					
0030 c2 60 f8 8f a8 cb 7d 0b 60 66 6f 75 7f ef e9 b .....}k...F...					
0040 e7 f3 74 75 7f 7d 73 71 75 7b fa 7c 7d f3 f2 f7 ..tu.)sq u{.}....					
0050 f8 fb fe fe 77 6e 6d 75 79 79 f7 ec e2 f8 fd .....wmu yy.....					
Invalid filter Packets: 8200 Displayed: 8200 Marked: 0					

Figura 4.13: Captura de paquetes del enrutador 2 en la zona 3 (BATMAN)

c) Enrutador 3:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
2	0.009556	10.0.1.3	10.0.1.255	BAT_BATM	Seq=7
3	0.009914	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
4	0.030584	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
5	0.049947	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
6	0.079989	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
7	0.089775	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
8	0.110486	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
9	0.130225	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
10	0.160074	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
11	0.167374	10.0.1.22	10.0.1.3	SSH	Encrypted request packet len=88
12	0.169792	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
13	0.190558	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
14	0.210705	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
15	0.241800	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
16	0.249936	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
17	0.270585	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
18	0.290237	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
19	0.320274	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
20	0.330496	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
21	0.350598	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
22	0.370585	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
23	0.400390	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
24	0.410111	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
25	0.429627	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
26	0.450475	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
27	0.459945	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
28	0.480876	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
29	0.503924	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
30	0.530332	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
31	0.539995	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
32	0.560635	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
33	0.589782	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
34	0.610615	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
35	0.640591	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596
36	0.651548	10.0.1.22	200.126.12.116	UDP	source port: 12538 Destination port: 16596

[Frame 1 (214 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:b8:ba (68:7f:74:27:b8:ba), Dst: Cisco-L1\_27:b8:b1 (68:7f:74:27:b8:b1)  
 Internet Protocol, Src: 10.0.1.22 (10.0.1.22), Dst: 200.126.12.116 (200.126.12.116)  
 User Datagram Protocol, Src Port: 12538 (12538), Dst Port: 16596 (16596)

Figura 4.14: Captura de paquetes del enrutador 3 en la zona 3 (BATMAN)

e) Cliente softphone:

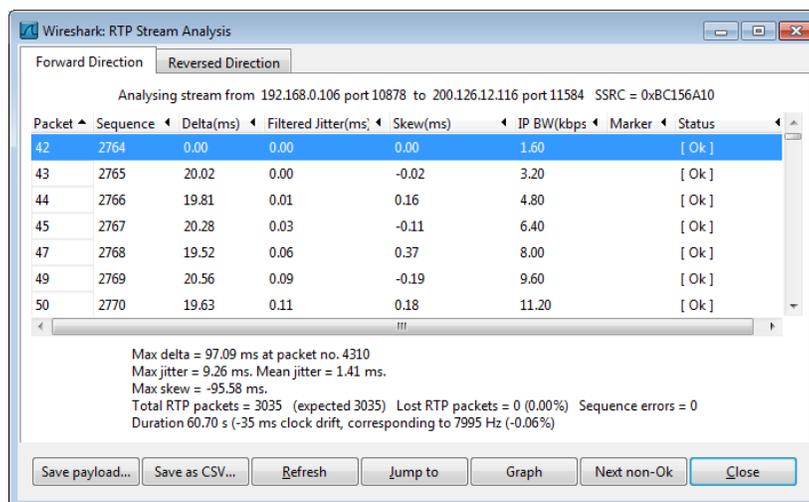
No.	Time	Source	Destination	Protocol	Info
19	1.142943	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
20	1.142953	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
21	1.142959	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
22	1.146697	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
23	1.146707	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
24	1.146711	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	1.146714	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
26	1.146717	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
27	1.148500	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
28	1.154337	74.125.91.18	192.168.0.106	TLSv1	Application Data
29	1.159755	74.125.91.18	192.168.0.106	TLSv1	Application Data
30	1.159929	192.168.0.106	74.125.91.18	TCP	57704 > https [ACK] Seq=179 Ack=124 Win=3692 Len=0
31	1.202150	69.63.180.47	192.168.0.106	TCP	http > 59053 [ACK] Seq=1 Ack=2 Win=12 Len=0
32	1.202162	69.63.180.47	192.168.0.106	TCP	http > 59054 [ACK] Seq=1 Ack=2 Win=12 Len=0
33	1.202165	69.63.180.47	192.168.0.106	TCP	http > 59051 [ACK] Seq=1 Ack=2 Win=12 Len=0
34	1.202168	69.63.180.47	192.168.0.106	TCP	http > 59055 [ACK] Seq=1 Ack=2 Win=12 Len=0
35	1.202172	69.63.180.47	192.168.0.106	TCP	http > 59056 [ACK] Seq=1 Ack=2 Win=12 Len=0
36	1.202685	69.63.180.47	192.168.0.106	TCP	http > 59052 [ACK] Seq=1753 Ack=1081 Win=47 Len=0
37	2.264594	192.168.0.106	200.126.12.116	UDP	source port: 10879 Destination port: 11585
38	2.289964	192.168.0.106	200.126.12.116	UDP	source port: 10878 Destination port: 11584
39	2.309328	192.168.0.106	200.126.12.116	UDP	source port: 10878 Destination port: 11584
40	2.336061	192.168.0.106	200.126.12.116	SIP/SDP	status: 200 OK, with session description
41	2.338241	200.126.12.116	192.168.0.106	SIP	request: ACK sip/1007@200.126.12.109:61888;rinstance=70878958451cb31
42	2.339798	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2764, Time=2946620
43	2.359822	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2765, Time=2946780
44	2.379634	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2766, Time=2946940
45	2.399912	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2767, Time=2947100
46	2.411927	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5D98A9A, Seq=3116, Time=2693600, Mark
47	2.419432	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2768, Time=2947260
48	2.438982	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5D98A9A, Seq=3117, Time=2693760
49	2.439987	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2769, Time=2947420
50	2.459616	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2770, Time=2947580
51	2.462861	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5D98A9A, Seq=3118, Time=2693820
52	2.470529	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5D98A9A, Seq=3119, Time=2694080
53	2.480263	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8136A10, Seq=2771, Time=2947740
54	2.480547	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5D98A9A, Seq=3120, Time=2694240

[Frame 1 (1514 bytes on wire, 1514 bytes captured)  
 Ethernet II, Src: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96), Dst: Camecom\_3d:cb:0a (00:40:f4:3d:cb:0a)  
 Internet Protocol, Src: 69.63.180.47 (69.63.180.47), Dst: 192.168.0.106 (192.168.0.106)  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 59052 (59052), Seq: 1, Ack: 1, Len: 1460

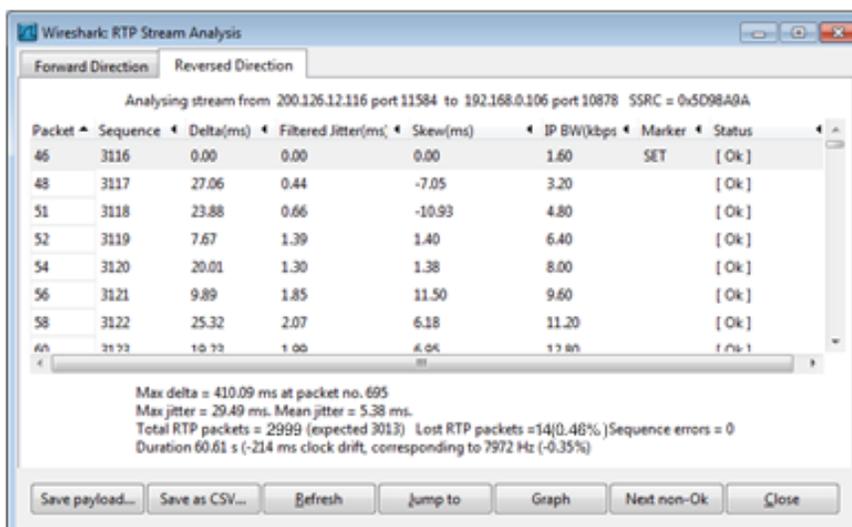
```

0000 00 40 f4 3d cb 0a 00 17 9a 2a 7f 96 08 00 45 00 .@.....@...E.
0010 05 dc 71 96 40 00 e7 06 62 04 43 3f b4 2f c0 a8 .,q@...bE?/.
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Figura 4.15: Captura de paquetes del cliente en Zona 3 (BATMAN)



**Figura 4.16: Steam RTP en el cliente en la dirección de avance en la Zona 3 (BATMAN)**



**Figura 4.17: Steam RTP en el cliente en la dirección de reversa en la Zona 3 (BATMAN)**

**Zona 4:**

**a) Enrutador 1:**

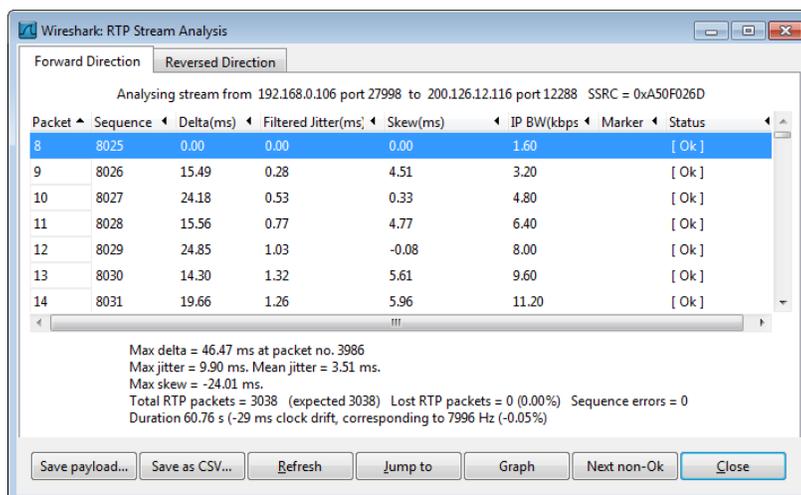
No.	Time	Source	Destination	Protocol	Info
73	2.347940	10.0.1.1	10.0.1.255	BAT_BATN	Seq=4
74	2.351841	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=356
75	2.354774	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=64
76	2.356333	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=1 Ack=6053 win=32723 Len=0
77	2.357188	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=1 Ack=9649 win=32717 Len=0
78	2.372302	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=68
79	2.772537	10.0.1.1	10.0.1.255	BAT_BATN	Seq=1
80	2.772986	200.126.12.116	10.0.1.22	SIP	Status: 200 OK(packet size limited during capture)
81	2.777684	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=532
82	2.779698	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=820
83	2.785103	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=532
84	2.787524	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=1 Ack=1403 win=32768 Len=0
85	2.793919	10.0.1.22	200.126.12.116	UDP	source port: 35397 destination port: 12971
86	2.808241	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=68
87	2.817647	10.0.1.1	10.0.1.255	BAT_BATN	Seq=1
88	2.818981	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=148
89	2.827685	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=108
90	2.831145	10.0.1.22	200.126.12.116	UDP	source port: 35397 destination port: 12971
91	2.831479	10.0.1.1	10.0.1.22	SSH	encrypted response packet len=68
92	3.01155	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=89 Ack=7621 win=32741 Len=0
93	3.012180	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=89 Ack=7621 win=32741 Len=0
94	3.012180	10.0.1.22	10.0.1.1	TCP	opencore > ssh [ACK] Seq=89 Ack=7621 win=32741 Len=0
95	3.012572	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
96	3.022024	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
97	3.022450	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
98	3.028159	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
99	3.031481	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
100	3.035066	10.0.1.22	200.126.12.116	SIP	Request: ACK sip:100/8200,126.12.116(packet size limited during capture)
101	3.035629	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
102	3.042991	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
103	3.043439	10.0.1.22	200.126.12.116	SIP	Request: ACK sip:100/8200,126.12.116(packet size limited during capture)
104	3.046942	10.0.1.1	10.0.1.22	TCP	ssh > opencore [ACK] Seq=7929 Ack=89 win=6432 Len=0
105	3.050695	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
106	3.062056	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970
107	3.071038	10.0.1.22	200.126.12.116	UDP	source port: 35396 destination port: 12970

**Figura 4.18: Captura de paquetes del enrutador 1 en la zona 4 (BATMAN)**

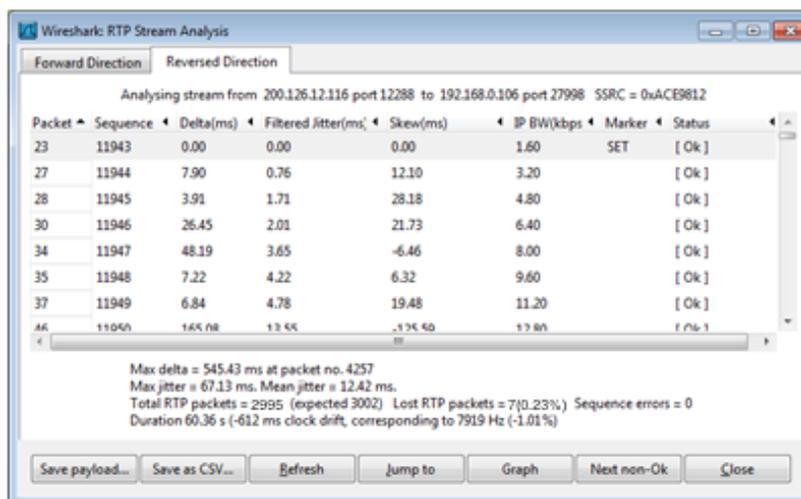
**b) Cliente softphone:**

No.	Time	Source	Destination	Protocol	Info
3	0.000010	69.63.180.47	192.168.0.106	HTTP	HTTP/1.1 200 OK (application/json)
4	0.000205	192.168.0.106	69.63.180.47	TCP	59052 > http [ACK] Seq=1 Ack=1753 win=256 Len=0
5	0.916213	192.168.0.106	74.125.91.18	TLSv1	Application Data
6	0.916529	192.168.0.106	74.125.91.18	TLSv1	Application Data
7	1.026838	192.168.0.106	69.63.180.47	TCP	59053 > http [FIN, ACK] Seq=1 Ack=1 win=256 Len=0
8	1.027048	192.168.0.106	69.63.180.47	TCP	59051 > http [FIN, ACK] Seq=1 Ack=1 win=256 Len=0
9	1.027243	192.168.0.106	69.63.180.47	TCP	59054 > http [FIN, ACK] Seq=1 Ack=1 win=256 Len=0
10	1.027463	192.168.0.106	69.63.180.47	TCP	59055 > http [FIN, ACK] Seq=1 Ack=1 win=256 Len=0
11	1.027615	192.168.0.106	69.63.180.47	TCP	59056 > http [FIN, ACK] Seq=1 Ack=1 win=256 Len=0
12	1.038608	192.168.0.106	69.63.180.47	HTTP	GET /AJAX/3583758055/068734455/false/pj_81802230423 HTTP/1.1
13	1.039427	74.125.91.18	192.168.0.106	TCP	https > 57704 [ACK] Seq=1 Ack=92 win=1002 Len=0
14	1.039435	74.125.91.18	192.168.0.106	TCP	https > 57704 [ACK] Seq=1 Ack=179 win=1002 Len=0
15	1.140088	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
16	1.140098	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
17	1.140101	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
18	1.142922	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
19	1.142943	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
20	1.142953	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
21	1.142959	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
22	1.146697	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
23	1.146707	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
24	1.146711	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	1.146714	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
26	1.146717	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
27	1.148500	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
28	1.154337	74.125.91.18	192.168.0.106	TLSv1	Application Data
29	1.159755	74.125.91.18	192.168.0.106	TLSv1	Application Data, Application Data
30	1.159929	192.168.0.106	74.125.91.18	TCP	57704 > https [ACK] Seq=179 Ack=124 win=3692 Len=0
31	1.202150	69.63.180.47	192.168.0.106	TCP	http > 59053 [ACK] Seq=1 Ack=2 win=12 Len=0
32	1.202162	69.63.180.47	192.168.0.106	TCP	http > 59054 [ACK] Seq=1 Ack=2 win=12 Len=0
33	1.202165	69.63.180.47	192.168.0.106	TCP	http > 59051 [ACK] Seq=1 Ack=2 win=12 Len=0
34	1.202168	69.63.180.47	192.168.0.106	TCP	http > 59055 [ACK] Seq=1 Ack=2 win=12 Len=0
35	1.202172	69.63.180.47	192.168.0.106	TCP	http > 59056 [ACK] Seq=1 Ack=2 win=12 Len=0
36	1.203685	69.63.180.47	192.168.0.106	TCP	http > 59052 [ACK] Seq=1753 Ack=1081 win=47 Len=0
37	2.264594	192.168.0.106	200.126.12.116	UDP	source port: 10879 destination port: 11585

**Figura 4.19: Captura de paquetes del cliente en Zona 4 (BATMAN)**



**Figura 4.20: Steam RTP en el cliente en la dirección de avance en la Zona 4 (BATMAN)**



**Figura 4.21: Steam RTP en el cliente en la dirección de reversa en la Zona 4 (BATMAN)**

## 4.2. Pruebas Empleando Roofnet como Protocolo De Enrutamiento Inalámbrico Mesh

En esta sección se detallan las pruebas llevadas a cabo en la red inalámbrica mallada empleando el protocolo de enrutamiento de Roofnet.

### 4.2.1. Pérdida de Paquetes, Jitter, Ancho De Banda, Retardo

Se realizaron las pruebas en cada zona, usando el protocolo de enrutamiento de ROOFNET, realizando llamadas telefónicas y capturando los paquetes que viajaban en la red usando la herramienta de captura de paquetes Wireshark. Los detalles se muestran a continuación:

#### Zona 1:

##### a) Cliente softphone en PC de escritorio:

No.	Time	Source	Destination	Protocol	Info
2	0.200050	192.168.0.106	74.125.229.53	TCP	56803 > http [ACK] Seq=1 Ack=28 win=16396 Len=0
3	1.002679	192.168.0.106	200.126.12.116	SIP/SDP	Request: INVITE sip:10068200.126.12.116, with session description
4	1.007989	200.126.12.116	192.168.0.106	SIP	Status: 407 Proxy Authentication Required
5	1.010662	192.168.0.106	200.126.12.116	SIP	Request: ACK sip:10068200.126.12.116
6	1.025029	192.168.0.106	200.126.12.116	SIP/SDP	Request: INVITE sip:10068200.126.12.116, with session description
7	1.027792	200.126.12.116	192.168.0.106	SIP	Status: 100 Trying
8	2.603916	200.126.12.116	192.168.0.106	SIP	Status: 180 Ringing
9	4.864325	74.125.229.53	192.168.0.106	HTTP	Continuation of non-HTTP traffic
10	4.866864	74.125.229.53	192.168.0.106	HTTP	Continuation of non-HTTP traffic
11	4.867071	192.168.0.106	74.125.229.53	TCP	56803 > http [ACK] Seq=1 Ack=400 win=16303 Len=0
12	5.186050	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
13	5.186592	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
14	5.186597	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
15	5.187831	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
16	5.188788	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
17	5.189042	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
18	5.189818	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
19	5.191061	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
20	5.191389	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
21	5.192210	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
22	5.193395	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
23	5.193640	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
24	5.194574	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	9.513835	200.126.12.116	192.168.0.106	SIP/SDP	Status: 200 OK, with session description
26	9.521080	192.168.0.106	200.126.12.116	RTCP	Receiver Report Source description
27	9.541059	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0XDE9FD4A, Seq=6194, Time=2455400, Mark
28	9.558448	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0X2E55C2DC, Seq=39690, Time=3225880
29	9.566807	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0XDE9FD4A, Seq=6195, Time=2455560
30	9.571644	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0X2E55C2DC, Seq=39691, Time=3226040
31	9.580972	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0XDE9FD4A, Seq=6196, Time=2455720
32	9.592143	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0X2E55C2DC, Seq=39692, Time=3226200
33	9.601440	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0XDE9FD4A, Seq=6197, Time=2455880
34	9.610136	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0X2E55C2DC, Seq=39693, Time=3226360
35	9.620740	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0XDE9FD4A, Seq=6198, Time=2456040
36	9.626800	192.168.0.106	200.126.12.116	RTP	Request: ACK <in>10068200.126.12.116

Frame 1 (81 bytes on wire, 81 bytes captured)  
 Ethernet II, Src: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96), Dst: CameoCom\_3d:cb:0a (00:40:f4:3d:cb:0a)  
 Internet Protocol, Src: 74.125.229.53 (74.125.229.53), Dst: 192.168.0.106 (192.168.0.106)  
 Transmission Control Protocol, Src Port: http (80), Dst Port: 56803 (56803), Seq: 1, Ack: 1, Len: 27  
 Hypertext Transfer Protocol

```

0000 00 40 f4 3d cb 0a 00 17 9a 2a 7f 96 08 00 45 00 .E.....E.
0010 00 43 04 f0 00 00 33 06 c1 ff 4a fd e5 35 c0 a8 .].P.....f.P.
0020 00 6a 00 50 dd e3 b8 95 f5 07 6a 46 97 0a 50 18 .].P.....f.P.
0030 01 ea 9f 86 00 00 31 35 0d 0a 31 38 0a 5b 5b 34 .....15]18.[4
0040 37 2c 5b 22 6e 6f 6f 70 22 5d 0a 5d 0a 0d 7[...noop]...
0050 0a
  
```

Invalid filter      Packets: 8098 Displayed: 8098 Marked: 0

Figura 4.22: Captura de paquetes del cliente en Zona 1 (Roofnet)

b) Cliente softphone en laptop:

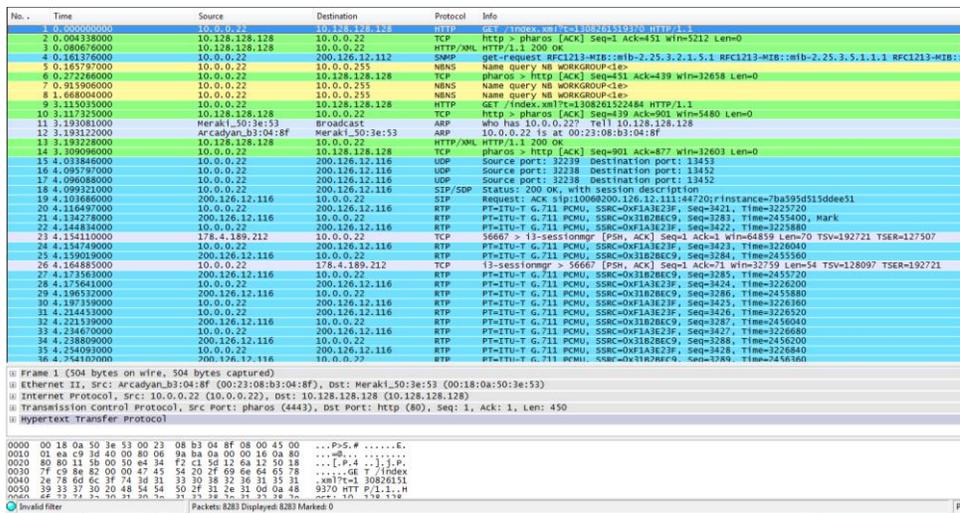


Figura 4.23: Captura de paquetes del cliente 2 en Zona 1 (Roofnet)

Zona 2:

a) Cliente softphone en PC de escritorio:

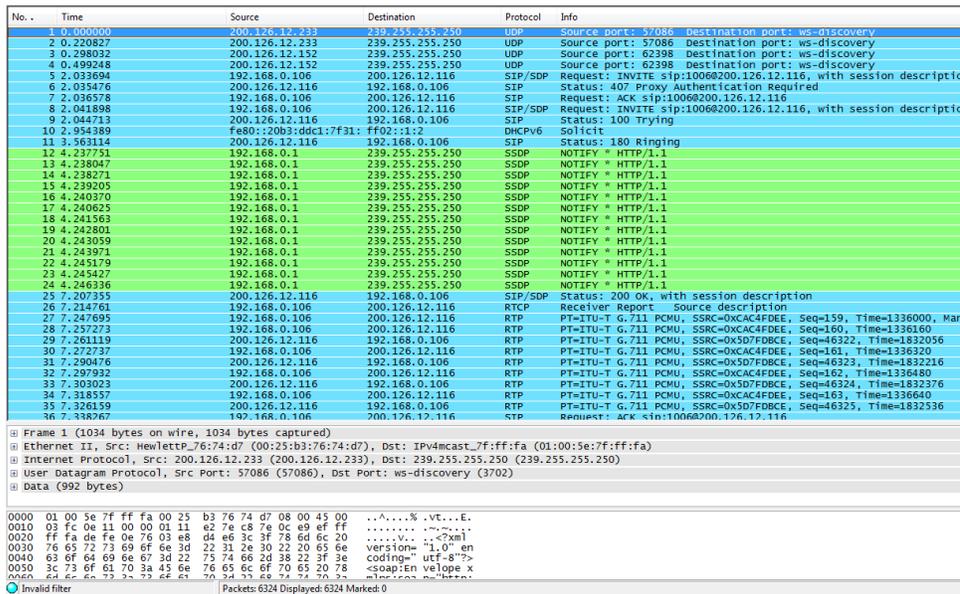


Figura 4.24: Captura de paquetes del cliente 1 en Zona 2 (Roofnet)



b) Cliente softphone en laptop:

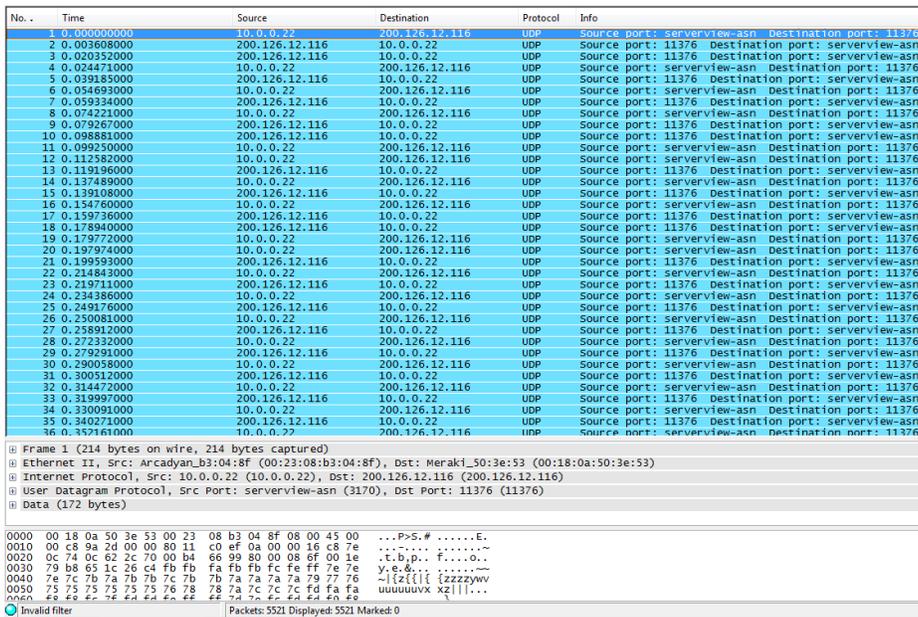


Figura 4.27: Captura de paquetes del cliente 2 en Zona 3 (Roofnet)

Zona 4:

a) Cliente softphone en PC de escritorio:

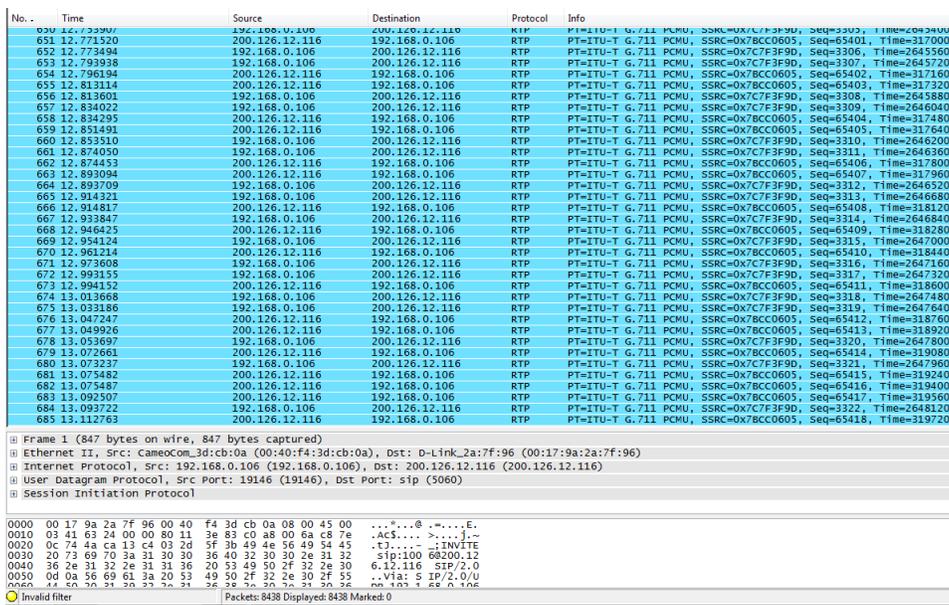


Figura 4.28: Captura de paquetes del cliente 1 en Zona 4 (Roofnet)

b) Cliente softphone en laptop:

No. v.	Time	Source	Destination	Protocol	Info
530	12.723907	192.168.0.106	200.126.12.116	KMP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=5302, Time=2649400
531	12.7271520	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65401, Time=317000
532	12.773494	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3306, Time=2645560
533	12.793938	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3307, Time=2645720
534	12.796194	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65402, Time=317160
535	12.813114	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65403, Time=317320
536	12.813601	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3308, Time=2645880
537	12.834022	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3309, Time=2646040
538	12.834295	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65404, Time=317480
539	12.851491	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65405, Time=317640
560	12.853510	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3310, Time=2646200
561	12.874050	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3311, Time=2646360
562	12.874453	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65406, Time=317800
563	12.893094	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65407, Time=317960
564	12.893709	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3312, Time=2646520
565	12.914321	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3313, Time=2646680
566	12.914817	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65408, Time=318120
567	12.933847	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3314, Time=2646840
568	12.946425	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65409, Time=318280
569	12.954124	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3315, Time=2647000
570	12.961214	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65410, Time=318440
571	12.973608	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3316, Time=2647160
572	12.993155	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3317, Time=2647320
573	12.994152	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65411, Time=318600
574	13.013668	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3318, Time=2647480
575	13.033186	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3319, Time=2647640
576	13.047247	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65412, Time=318760
577	13.049926	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65413, Time=318920
578	13.053697	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3320, Time=2647800
579	13.072661	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65414, Time=319080
580	13.073237	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3321, Time=2647960
581	13.075482	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65415, Time=319240
582	13.075487	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65416, Time=319400
583	13.092507	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65417, Time=319560
584	13.093722	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7c7f3f9d, Seq=3322, Time=2648120
585	13.112763	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x78cc0605, Seq=65418, Time=319720

☐ Frame 1 (847 bytes on wire, 847 bytes captured)  
 ☐ Ethernet II, Src: CameoCom\_3d:cb:0a (00:40:f4:3d:cb:0a), Dst: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96)  
 ☐ Internet Protocol, Src: 192.168.0.106 (192.168.0.106), Dst: 200.126.12.116 (200.126.12.116)  
 ☐ User Datagram Protocol, Src Port: 19146 (19146), Dst Port: sip (5060)  
 ☐ Session Initiation Protocol

```

0000 00 17 9a 2a 7f 96 00 40 f4 3d cb 0a 08 00 45 00  ...*..@.-...E.
0010 03 41 63 24 00 00 80 11 3e 83 c0 a8 00 6a c8 7e  .Ac3....>...j~
0020 0c 74 4a c4 13 c4 03 2d 3f 3b 45 4a 36 49 54 45  .?.....HWITE
0030 20 73 69 70 3a 31 30 30 36 40 32 30 30 2e 31 32  sip:100 68200,12
0040 86 2e 31 32 2e 31 31 36 20 53 49 50 2f 32 2e 30  6.12.116 SIP/2.0
0050 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 53  --Via: SIP/2.0/U
0060 11 50 70 31 20 27 7a 31 26 2e 7a 70 7a 31 7a 56  oo 103 1 68 0 106
  
```

Invalid filter      Packets: 8438 Displayed: 8438 Marked: 0

**Figura 4.29: Captura de paquetes del cliente 2 en Zona 4 (Roofnet)**

### 4.3. Pruebas Empleando Wing como Protocolo De Enrutamiento Inalámbrico Mesh

En esta sección se detallan las pruebas llevadas a cabo en la red inalámbrica mallada empleando el protocolo de enrutamiento W.I.N.G.

#### 4.3.1. Pérdida de Paquetes, Jitter, Ancho De Banda, Retardo

Se realizaron las pruebas en cada zona, usando el protocolo de enrutamiento WING, realizando llamadas telefónicas y capturando los paquetes que viajaban en la red usando la herramienta de

captura de paquetes Wireshark. Los detalles se muestran a continuación:

**Zona 1:**

a) Enrutador 1:

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.1	10.0.1.20	SSH	Encrypted response packet len=132
2	0.004139	10.0.1.20	10.0.1.1	TCP	7564 > ssh [ACK] Seq=1 Ack=133 win=32745 Len=0
3	1.974804	10.0.1.20	41.201.106.249	TCP	7692 > google[1]a-svc [SYN] Seq=0 win=0 len=0 MSS=1460 ws=3 TSV=0 TSEQ=0
4	2.936833	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
5	3.013223	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
6	3.028908	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
7	3.039681	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
8	3.047930	10.0.1.20	200.126.12.116	SIP	Status: 200 OK [packet size limited during capture]
9	3.048784	200.126.12.116	10.0.1.20	UDP	Source port: 53100 Destination port: 25482
10	3.061627	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
11	3.080650	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
12	3.100245	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
13	3.120811	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
14	3.141027	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
15	3.144132	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
16	3.143004	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
17	3.160267	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
18	3.162408	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
19	3.170063	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
20	3.183654	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
21	3.208382	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
22	3.205002	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
23	3.210191	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
24	3.222961	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
25	3.230565	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
26	3.240986	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
27	3.250236	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
28	3.261165	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
29	3.270618	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
30	3.280361	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
31	3.293513	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
32	3.302716	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
33	3.310885	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
34	3.321028	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334
35	3.330156	200.126.12.116	10.0.1.20	UDP	Source port: 16334 Destination port: 53100
36	3.343386	10.0.1.20	200.126.12.116	UDP	Source port: 53100 Destination port: 16334

[Frame 1 (186 bytes on wire, 90 bytes captured)]  
 Ethernet II, Src: Camecom\_f8:67:1d (00:18:e7:f8:67:1d), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.1.20 (10.0.1.20)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: 7564 (7564), Seq: 1, Ack: 1, Len: 132  
 SSH Protocol  
 [packet size limited during capture: ssh truncated]

```

0000 00 23 08 b3 04 8f 00 18 e7 f8 67 1d 08 00 45 10  .#. .... .g...E.
0010 00 ac 0a 4a 40 00 40 06 19 de 0a 00 01 01 0a 00  ...30.8. ....
0020 01 14 00 16 1d 8c 34 18 1a ba 57 fe 93 55 90 18  .... . .w.uP.
0030 10 ee ed 15 00 00 00 81 c5 ed dd b3 4d f9 79 68  .... . .M.yh
0040 16 00 58 86 ee 8c bc 2d 38 df 8a c5 09 1d 45 78  .].....8.....Ex
0050 06 1a c8 c5 09 99 90 c7 89 6f                    .].....8.....
  
```

**Figura 4.30: Captura de paquetes del enrutador 1 en Zona 1(Wing)**

b) Enrutador 2:

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.2	10.0.1.20	SSH	Encrypted response packet len=132
2	0.001666	10.0.1.20	10.0.1.2	TCP	7569 > ssh [ACK] Seq=1 Ack=133 win=32590 Len=0
3	74.152823	10.0.1.20	10.0.1.2	SSH	Encrypted request packet len=52

[Frame 1 (186 bytes on wire, 90 bytes captured)]  
 Ethernet II, Src: Camecom\_fa:2d:c1 (00:18:e7:fa:2d:c1), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.20 (10.0.1.20)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: 7569 (7569), Seq: 1, Ack: 1, Len: 132

**Figura 4.31: Captura de paquetes del enrutador 2 en Zona 1(Wing)**

## c) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.106	200.126.12.116	UDP	Source port: 59108 Destination port: 510
2	4.606134	200.126.12.116	192.168.0.106	SIP/SDP	Status: 200 OK, with session description
3	4.618066	192.168.0.106	200.126.12.116	RTCP	Receiver Report source description
4	4.696472	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6447, Time=1847700, Mark
5	4.696733	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6448, Time=1847860
6	4.719862	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6449, Time=1848020
7	4.725628	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6450, Time=1848180
8	4.733831	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24292, Time=2031920
9	4.733837	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24293, Time=2032080
10	4.752928	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24294, Time=2032240
11	4.759995	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6451, Time=1848340
12	4.762249	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24295, Time=2032400
13	4.765748	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6452, Time=1848500
14	4.786137	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6453, Time=1848660
15	4.789997	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24296, Time=2032560
16	4.805796	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6454, Time=1848820
17	4.807324	192.168.0.106	200.126.12.116	SIP	Request: ACK sip:1007@200.126.12.116
18	4.813741	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24297, Time=2032720
19	4.819721	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24298, Time=2032880
20	4.826193	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6455, Time=1848980
21	4.838677	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24299, Time=2033040
22	4.849095	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6456, Time=1849140
23	4.859528	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24300, Time=2033200
24	4.866260	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6457, Time=1849300
25	4.885731	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6458, Time=1849460
26	4.905235	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6459, Time=1849620
27	4.925799	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6460, Time=1849780
28	4.933088	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24301, Time=2033360
29	4.933096	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24302, Time=2033520
30	4.933098	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24303, Time=2033680
31	4.939783	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24304, Time=2033840
32	4.950041	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6461, Time=1849940
33	4.975681	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6462, Time=1850100
34	4.987356	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24305, Time=2034000
35	4.987364	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17581154, Seq=24306, Time=2034160
36	4.986070	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x17f5f58a, Seq=6463, Time=1850260

Frame 1 (46 bytes on wire, 46 bytes captured)  
 Ethernet II, Src: ciscocon\_3d:cb:0a (00:40:f4:3d:cb:0a), Dst: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96)  
 Internet Protocol, Src: 192.168.0.106 (192.168.0.106), Dst: 200.126.12.116 (200.126.12.116)  
 User Datagram Protocol, Src Port: 59108 (59108), Dst Port: 510 (5060)  
 data (4 bytes)

0000 00 17 9a 2a 7f 96 00 40 f4 3d cb 0a 08 00 45 00 ...\*..@ \_-...E.  
 0010 00 20 4b 0a 00 00 80 11 59 be c0 a8 00 6a c8 7e .K.....Y....]-  
 0020 0c 74 e6 e4 13 c4 00 0c 55 14 0d 0a 0d 0a .....U.....

File: "C:\Users\joedward\espof\PROYECTO ... Packets: 6261 Displayed: 6261 Marked: 0

Figura 4.32: Captura de paquetes del cliente 1 en Zona 1(Wing)

Wireshark: RTP Stream Analysis

Forward Direction Reversed Direction

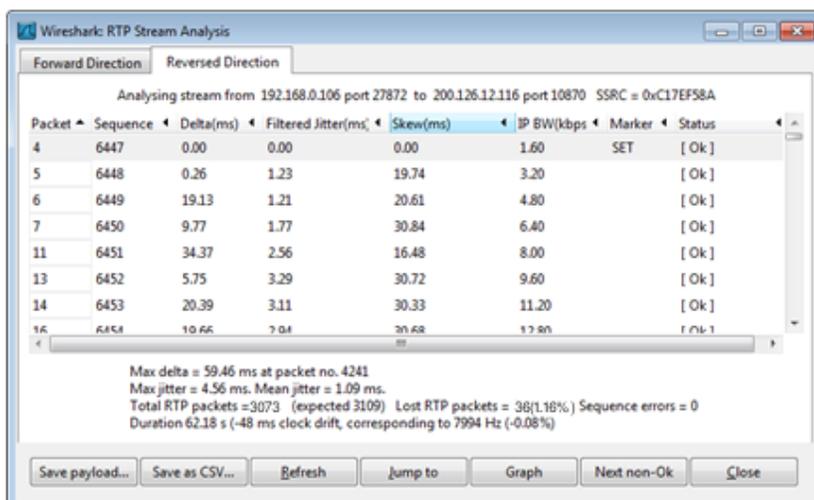
Analysing stream from 200.126.12.116 port 10870 to 192.168.0.106 port 27872 SSRC = 0x17581154

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
8	24292	0.00	0.00	0.00	1.60		[ Ok ]
9	24293	0.01	1.25	19.99	3.20		[ Ok ]
10	24294	19.09	1.23	20.90	4.80		[ Ok ]
12	24295	9.32	1.82	31.58	6.40		[ Ok ]
15	24296	27.45	2.17	24.13	8.00		[ Ok ]
18	24297	24.04	2.29	20.09	9.60		[ Ok ]
19	24298	5.98	3.02	34.11	11.20		[ Ok ]

Max delta = 779.54 ms at packet no. 5245  
 Max jitter = 52.78 ms. Mean jitter = 12.48 ms.  
 Max skew = -1031.75 ms.  
 Total RTP packets = 3022 (expected 3022) Lost RTP packets = 0 (0.00%) Sequence errors = 0  
 Duration 62.13 s (-324 ms clock drift, corresponding to 7958 Hz (-0.52%))

Save payload... Save as CSV... Refresh Jump to Graph Next non-Ok Close

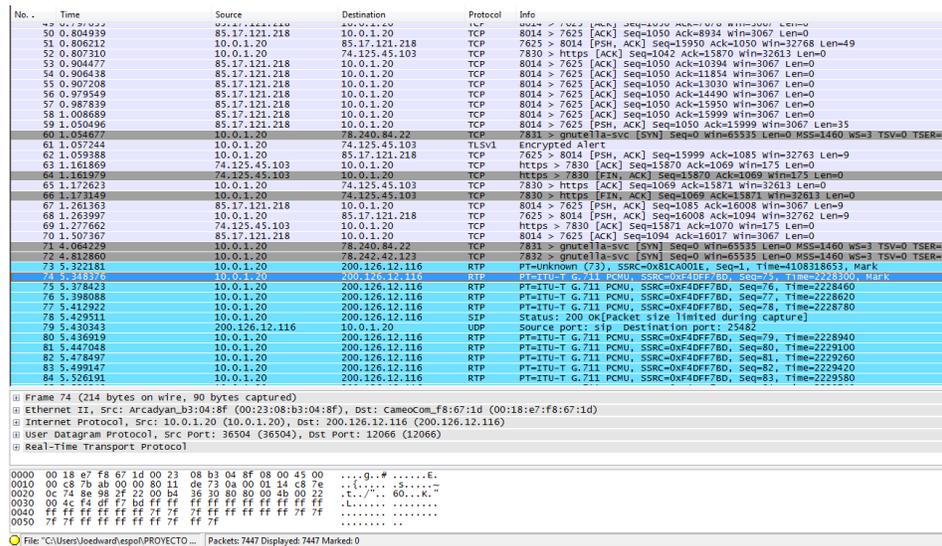
Figura 4.33: Steam RTP en el cliente en la dirección de avance en Zona 1(Wing)



**Figura 4.34: Steam RTP en el cliente en la dirección de reversa en Zona 1(Wing)**

**Zona 2:**

**a) Enrutador 1:**



**Figura 4.35: Captura de paquetes del enrutador 1 en Zona 2 (Wing)**

## b) Enrutador 2:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.2	10.0.1.20	SSH	Encrypted response packet len=132
2	0.033870	10.0.1.20	10.0.1.2	TCP	7569 > ssh [ACK] Seq=1 Ack=133 Win=32768 Len=0
3	63.323050	10.0.1.20	10.0.1.2	SSH	Encrypted request packet len=52

Frame 1 (186 bytes on wire, 90 bytes captured)  
 Ethernet II, Src: cameoCom\_fa:2d:c1 (00:18:e7:fa:2d:c1), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.20 (10.0.1.20)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: 7569 (7569), Seq: 1, Ack: 1, Len: 132  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000  00 23 08 b3 04 8f 00 18 e7 fa 2d c1 08 00 45 10  .#. . . . .;@..E.
0010  00 ac 28 f2 40 00 40 06 fb 34 0a 00 01 02 0a 00  ..E@. @. . . . .
0020  01 14 00 16 1d 91 19 fb 3b 59 1e 08 c8 93 50 18  . . . . .f..ayP.
0030  0e d6 62 76 00 00 c8 a7 9f 3b a4 3d ab 11 73 c8  . .bv. . . . .;S.
0040  88 65 3e ab 6a 71 83 b1 4d 05 ae f2 44 68 63 09  .e>.jq. M..Dhc.
0050  5c c2 5c 30 7e b1 ff fe 07 cc                    \..0-....
  
```

**Figura 4.36: Captura de paquetes del enrutador 2 en Zona 2 (Wing)**

## c) Enrutador 3:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.20	SSH	Encrypted response packet len=132
2	0.002628	10.0.1.20	10.0.1.3	TCP	a1agent > ssh [ACK] Seq=1 Ack=133 Win=32691 Len=0
3	67.196532	10.0.1.20	10.0.1.3	SSH	Encrypted request packet len=52

Frame 1 (186 bytes on wire, 90 bytes captured)  
 Ethernet II, Src: cameoCom\_f8:3b:40 (00:18:e7:f8:3b:40), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.20 (10.0.1.20)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: a1agent (7738), Seq: 1, Ack: 1, Len: 132  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000  00 23 08 b3 04 8f 00 18 e7 f8 3b 40 08 00 45 10  .#. . . . .;@..E.
0010  00 ac a8 45 40 00 40 06 7b e0 0a 00 01 03 0a 00  ..E@. @. . . . .
0020  01 14 00 16 1e 3a b2 9b 66 94 d5 61 79 96 50 18  . . . . .f..ayP.
0030  0e d6 62 76 00 00 c8 a7 9f 3b a4 3d ab 11 73 c8  . .bv. . . . .;S.
0040  88 65 3e ab 6a 71 83 b1 4d 05 ae f2 44 68 63 09  .e>.jq. M..Dhc.
0050  5c c2 5c 30 7e b1 ff fe 07 cc                    \..0-....
  
```

File: "C:\Users\Joedward\espo\PROYECTO ..." Packets: 3 Displayed: 3 Marked: 0

**Figura 4.37: Captura de paquetes del enrutador 3 en Zona 2 (Wing)**

e) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
2	0.000012	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
3	0.000014	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
4	0.000017	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
5	0.000020	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
6	0.000024	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
7	0.000029	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
8	0.001324	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
9	0.001329	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
10	0.002321	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	0.003484	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
12	0.003827	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
13	0.009727	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
14	2.752890	200.75.202.236	192.168.0.106	HTTP	HTTP/1.1 200 OK (application/octet-stream)
15	2.756912	192.168.0.106	200.75.202.236	HTTP	GET /dln_aspx?e=10000101&id=69418446&c?ient=dyngate&p=10000214 HTTP/1.1
16	3.142378	200.75.202.236	192.168.0.106	TCP	http > 50188 [ACK] Seq=133 Ack=218 win=65101 Len=0
17	4.540972	200.126.12.116	192.168.0.106	STP/SDP	Status: 200 OK, with session description
18	4.550948	192.168.0.106	200.126.12.116	RTP	Receiver Report source description
19	4.657164	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1144, Time=68000, Mark
20	4.665282	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1145, Time=68160
21	4.665531	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1146, Time=68320
22	4.668214	192.168.0.106	200.126.12.116	SIP	Request: ACK sip:1007@200.126.12.116
23	4.674699	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1147, Time=68480
24	4.683098	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48378, Time=229896
25	4.690194	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48379, Time=2230056
26	4.694316	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1148, Time=68640
27	4.714698	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1149, Time=68800
28	4.734373	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1150, Time=68960
29	4.755074	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1151, Time=69120
30	4.761135	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48380, Time=2230216
31	4.761140	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48381, Time=2230376
32	4.761143	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48382, Time=2230536
33	4.761145	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48383, Time=2230696
34	4.774426	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xE8F8DF21F, Seq=1152, Time=69280
35	4.804099	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48384, Time=2230856
36	4.804105	200.126.12.116	192.168.0.106	RTP	PT=ITU-T G.711 PCMU, SSRC=0x2898CB3, Seq=48385, Time=2231016

Frame 1 (294 bytes on wire, 294 bytes captured)  
 Ethernet II, Src: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 239.255.255.250 (239.255.255.250)  
 User Datagram Protocol, Src Port: sdp (1900), Dst Port: sdp (1900)  
 Hypertext Transfer Protocol

```

0000 ff ff ff ff ff 00 17 9a 2a 7f 96 08 00 45 00 .....*.....E.
0010 01 18 da e8 00 00 7f 11 af 48 c0 a8 00 01 ef ff .....H.....
0020 ff fa 07 6c 07 6c 01 04 bc 26 4e 4f 54 49 46 99 .....NOTIFY
0030 20 2a 20 48 34 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/1.1..POS
0040 54 3a 32 33 39 2e 32 35 35 2e 32 35 2e 32 35 T:239.255.255.25
0050 30 3a 31 39 30 30 0d 0a 23 41 43 48 45 2d 43 4f 0:1900..G:40E-CO
0060 2a 4f c9 4f 4f 92 6d 61 78 94 67 67 66 34 31 37 .....m...v...
    
```

File: C:\Users\leedward\esoph\PROJECTO... Packets: 6481 Displayed: 6481 Marked: 0

Figura 4.38: Captura de paquetes del cliente 1 en Zona 2 (Wing)

Wireshark: RTP Stream Analysis

Analysing stream from 192.168.0.106 port 3266 to 200.126.12.116 port 14194 SSRC = 0xE8F8DF21F

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
19	1144	0.00	0.00	0.00	1.60	SET	[Ok]
20	1145	8.12	0.74	11.88	3.20		[Ok]
21	1146	0.25	1.93	31.63	4.80		[Ok]
23	1147	9.17	2.49	42.47	6.40		[Ok]
26	1148	19.62	2.36	42.85	8.00		[Ok]
27	1149	20.38	2.23	42.47	9.60		[Ok]
28	1150	19.67	2.11	42.79	11.20		[Ok]

Max delta = 92.71 ms at packet no. 414  
 Max jitter = 8.98 ms. Mean jitter = 0.96 ms.  
 Max skew = -46.83 ms.  
 Total RTP packets = 3206 (expected 3206) Lost RTP packets = 0 (0.00%) Sequence errors = 0  
 Duration 64.11 s (-44 ms clock drift, corresponding to 7994 Hz (-0.07%))

Buttons: Save payload... Save as CSV... Refresh Jump to Graph Next non-Ok Close

Figura 4.39: Steam RTP en el cliente en la dirección de avance en Zona 2 (Wing)



b) Enrutador 2:

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.2	TCP	37267 > ssh [ACK] seq=1 Ack=1 win=4034 Len=0
2	0.006903	10.0.1.2	10.0.1.3	SSH	Encrypted response packet len=132
3	0.009661	10.0.1.3	10.0.1.2	TCP	37267 > ssh [ACK] seq=1 Ack=133 win=4034 Len=0
4	66.197527	10.0.1.3	10.0.1.2	SSH	Encrypted request packet len=52

[Frame 1 (54 bytes on wire, 54 bytes captured)]  
 [Ethernet II, Src: Cameocom\_f8:3b:40 (00:18:e7:f8:3b:40), Dst: Cameocom\_fa:2d:c1 (00:18:e7:fa:2d:c1)]  
 [Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.2 (10.0.1.2)]  
 [Transmission Control Protocol, Src Port: 37267 (37267), Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 0]

```

0000 00 18 e7 fa 2d c1 00 18 e7 f8 3b 40 08 00 45 10  ...:..:;@..E.
0010 00 28 ae 1c 40 00 40 06 76 9f 0a 00 01 03 0a 00  ...:..@.Y.....
0020 01 02 91 93 00 16 21 f1 b4 94 fc e4 90 58 50 10  .....:..:..XP.
0030 0f c2 94 a1 00 00  .....
  
```

File: "C:\Users\Joedward\espol\PROYECTO..." Packets: 4 Displayed: 4 Marked: 0

Figura 4.42: Captura de paquetes del enrutador 1 en Zona 3 (Wing)

c) Enrutador 3:

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.20	SSH	Encrypted response packet len=132
2	0.001008	10.0.1.20	10.0.1.3	TCP	atagent > ssh [ACK] seq=1 Ack=133 win=32661 Len=0
3	64.473361	10.0.1.20	10.0.1.3	SSH	Encrypted request packet len=52
4	64.473491	10.0.1.3	10.0.1.20	TCP	ssh > 8248 [ACK] seq=1 Ack=53 win=3798 Len=0
5	64.489956	10.0.1.3	10.0.1.2	SSH	Encrypted request packet len=52
6	64.512582	10.0.1.2	10.0.1.3	SSH	Encrypted response packet len=148
7	64.512707	10.0.1.3	10.0.1.2	TCP	37267 > ssh [ACK] seq=53 Ack=149 win=4034 Len=0
8	64.519975	10.0.1.3	10.0.1.20	SSH	Encrypted response packet len=148
9	64.712133	10.0.1.20	10.0.1.3	TCP	8248 > ssh [ACK] seq=53 Ack=149 win=32768 Len=0
10	68.789336	10.0.1.20	10.0.1.3	SSH	Encrypted request packet len=52

[Frame 1 (186 bytes on wire, 90 bytes captured)]  
 [Ethernet II, Src: cameocom\_f8:3b:40 (00:18:e7:f8:3b:40), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)]  
 [Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.20 (10.0.1.20)]  
 [Transmission Control Protocol, Src Port: ssh (22), Dst Port: atagent (7738), Seq: 1, Ack: 1, Len: 132]  
 [SSH Protocol]  
 [packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 00 18 e7 f8 3b 40 08 00 45 10  .#. ....:;@..E.
0010 00 ac aa 3a 40 00 40 06 79 eb 0a 00 01 03 0a 00  ...:..@.Y.....
0020 01 14 00 16 1e 3a b2 9c 18 24 d5 61 7f e2 50 18  .....:..:..:..P.
0030 0e 06 bf b5 00 00 81 cf e7 81 54 ac 41 a8 df  .....:..:..T.A..
0040 33 1e 32 5e 57 6d 20 ca 31 df 9a 5f 20 57 dc f0  3.2*wm . 1. . W..
0050 69 ec e4 77 6d 21 a3 53 61 87 1. .wm1. S a.
  
```

File: "C:\Users\Joedward\espol\PROYECTO..." Packets: 10 Displayed: 10 Marked: 0

Figura 4.43: Captura de paquetes del enrutador 3 en Zona 3 (Wing)

d) Enrutador 4:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.4	10.0.1.20	SSH	Encrypted response packet len=132
2	0.000880	10.0.1.20	10.0.1.4	TCP	8236 > ssh [ACK] Seq=1 Ack=133 win=32637 Len=0
3	61.841034	10.0.1.20	10.0.1.4	SSH	Encrypted request packet len=52

Frame 1 (186 bytes on wire, 90 bytes captured)

Ethernet II, Src: CamecoCom\_F8:94:29 (00:18:e7:f8:94:29), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)

Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.20 (10.0.1.20)

Transmission Control Protocol, Src Port: ssh (22), Dst Port: 8236 (8236), Seq: 1, Ack: 1, Len: 132

SSH Protocol

[Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 00 18 e7 f8 94 29 08 00 45 10  .#. . . . .E.
0010 00 ac 3f 18 40 00 04 06 e5 0c 0a 00 01 04 0a 00  .?.@. . . . .
0020 01 14 00 16 20 2c d8 4e a7 f4 a1 d2 4a 59 50 18  . . . . .N . . . . .JYP.
0030 0e d6 ab 8b 00 00 2e db c0 4e 30 40 fe e1 67 e2  . . . . .N08.g.
0040 88 8b af 1a 30 b3 a0 14 67 01 63 ee e2 0f 99 af  . . . . .g.C. . . . .
0050 c1 27 f7 89 af bd 0d 39 f0 e8  . . . . .9 . . . . .
    
```

File: "C:\Users\joedward\espo\PROYECTO..." Packets: 3 Displayed: 3 Marked: 0

Figura 4.44: Captura de paquetes del enrutador 4 en Zona 3 (Wing)

e) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.106	192.168.0.255	BROWSER	Host Announcement COMMOV, workstation, Server, NT workstation
2	4.352340	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
3	4.352345	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
4	4.352347	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
5	4.357115	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
6	4.357119	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
7	4.357122	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
8	4.357124	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
9	4.357127	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
10	4.357129	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	4.358005	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
12	4.361473	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
13	4.361485	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
14	4.361492	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
15	9.093657	192.168.0.106	200.126.12.116	UDP	Source port: 46052 Destination port: sip
16	9.455573	200.126.12.116	192.168.0.106	SIP	Request: OPTIONS sip:10108200.126.12.109:60541;instance=080ed536b30071dc
17	9.646634	192.168.0.106	200.126.12.116	SIP	Status: 200 OK
18	16.038443	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
19	16.038869	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
20	16.040929	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
21	16.041363	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
22	19.039322	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
23	19.039590	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
24	19.042108	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
25	19.042735	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
26	19.364841	200.75.202.236	192.168.0.106	HTTP	HTTP/1.1 200 OK (application/octet-stream)
27	19.380956	192.168.0.106	200.75.202.236	HTTP	GET /din.aspx?S=10000101&id=694184466&client=Byngate&P=10000230 HTTP/1.1
28	19.722593	200.75.202.236	192.168.0.106	TCP	http > 50188 [ACK] Seq=133 Ack=218 win=64667 Len=0
29	22.040204	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
30	22.040810	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
31	22.042939	fe80::20b3:ddc1:7f31::ff02::c	ff02::c	SSDP	M-SEARCH * HTTP/1.1
32	22.043206	192.168.0.106	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
33	23.237466	200.126.12.116	192.168.0.106	SIP/SDP	Status: 200 OK, with session description
34	23.249442	192.168.0.106	200.126.12.116	RTCP	Receiver Report source description
35	23.348488	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4e54070e, Seq=5602, Time=524400, Mark
36	23.348907	192.168.0.106	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x4e54070e, Seq=5603, Time=524560

Frame 1 (243 bytes on wire, 243 bytes captured)

Ethernet II, Src: CamecoCom\_3d:cb:0a (00:40:f4:3d:cb:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol, Src: 192.168.0.106 (192.168.0.106), Dst: 192.168.0.255 (192.168.0.255)

User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)

NetBIOS Datagram Service

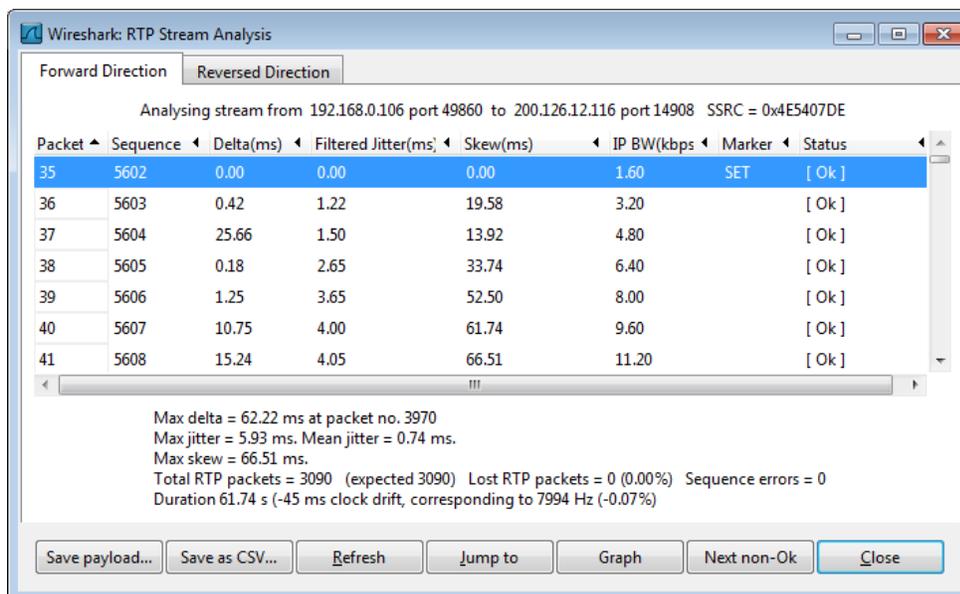
SMB (Server Message Block Protocol)

```

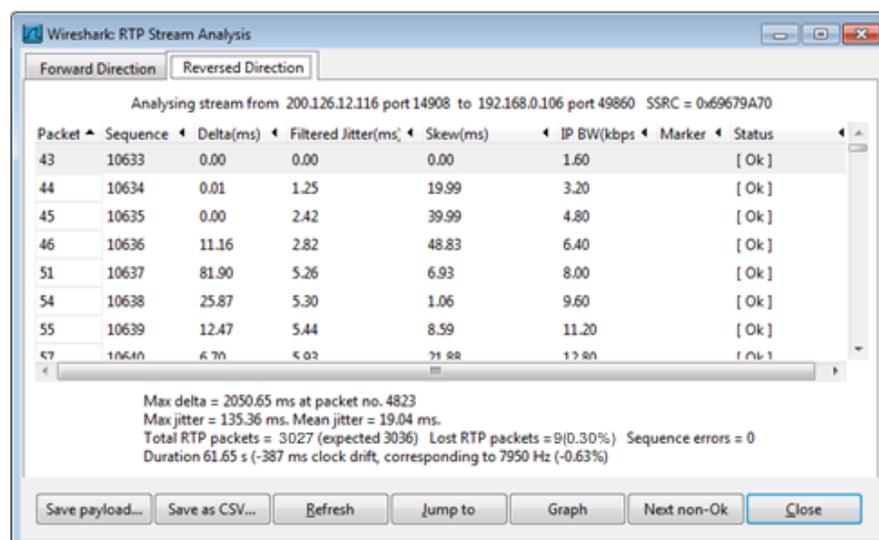
0000 ff ff ff ff ff 00 40 f4 3d cb 0a 08 00 45 00  . . . . .@ . . . . .E.
0010 00 e5 e2 00 00 80 11 54 89 c0 a8 b1 00 00 00  . . . . .T. . . . .
0020 00 ff 00 8a 00 8a 00 01 e1 f1 11 02 e9 3c c0 a8  . . . . . . . . . .
0030 00 6a 00 8a 00 bb 00 00 20 45 44 45 50 45 4e 45  . . . . .EDEPENE
0040 4e 45 50 46 47 43 41 43 41 43 41 43 41 43 41 43  . . . . .NEPPECAC ACACACAC
0050 41 43 41 43 41 43 41 43 41 00 20 46 48 45 50 46  . . . . .ACACACAC A. FHEPP
0060 4e 45 50 46 47 43 41 43 41 43 41 43 41 43 41 43  . . . . .NEPPEPPCACACACACAC
    
```

File: "C:\Users\joedward\espo\PROYECTO..." Packets: 62/2 Displayed: 62/2 Marked: 0

Figura 4.45: Captura de paquetes del cliente en Zona 3 (Wing)

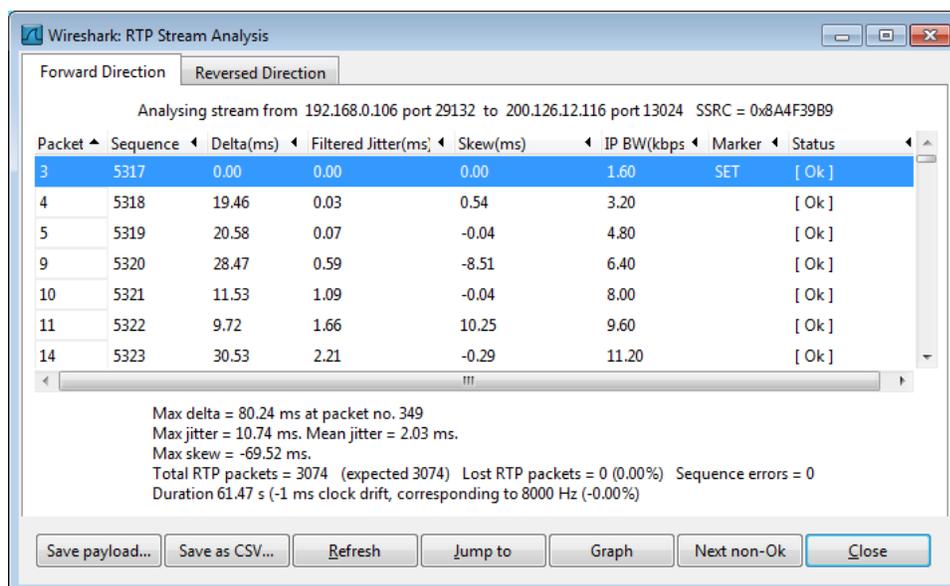


**Figura 4.46: Steam RTP en el cliente en la dirección de avance en Zona 3 (Wing)**

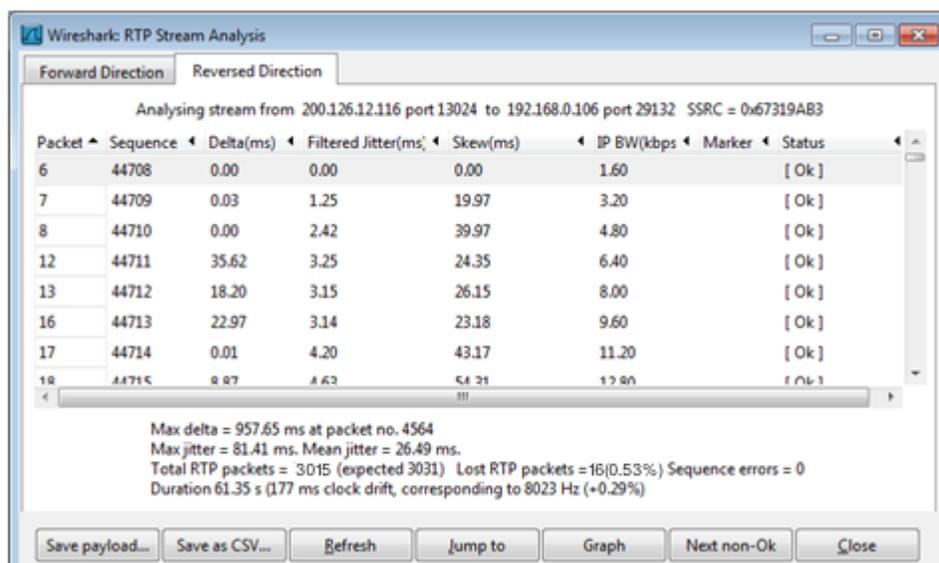


**Figura 4.47: Steam RTP en el cliente en la dirección de reversa en Zona 3 (Wing)**





**Figura 4.50: Steam RTP en el cliente en la dirección de avance en Zona 4 (Wing)**



**Figura 4.51: Steam RTP en el cliente en la dirección de reversa en Zona 4 (Wing)**

## 4.4. Pruebas Empleando OLSR como Protocolo de Enrutamiento Inalámbrico Mesh

En esta sección se detallan las pruebas llevadas a cabo en la red inalámbrica mallada empleando el protocolo de enrutamiento O.L.S.R.x

### 4.4.1. Pérdida de Paquetes, Jitter, Ancho De Banda, Retardo

Se realizaron las pruebas en cada zona, usando el protocolo de enrutamiento OLSR, realizando llamadas telefónicas y capturando los paquetes que viajaban en la red usando la herramienta de captura de paquetes Wireshark. Los detalles se muestran a continuación:

#### Zona 1:

##### a) Enrutador 1:

No. -	Time	Source	Destination	Protocol	Info
607	8.901810	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
608	8.912362	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
609	8.924228	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
610	8.932246	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
611	8.933501	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
612	8.934068	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
613	8.934637	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
614	8.944782	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
615	8.952382	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
616	8.959526	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
617	8.972416	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
618	8.980056	10.0.1.2	10.0.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes
619	8.982014	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
620	8.982593	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
621	8.984909	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
622	8.986600	10.0.1.3	10.0.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 28 Bytes
623	8.992137	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
624	8.999912	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 28 Bytes
625	9.012667	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
626	9.014430	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
627	9.023158	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
628	9.029106	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
629	9.029742	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
630	9.030332	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
631	9.031997	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
632	9.039642	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
633	9.062549	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
634	9.063874	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
635	9.077714	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
636	9.078286	10.0.0.70	200.126.12.116	UDP	Source port: 10606 Destination port: 10656
637	9.082706	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
638	9.092161	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
639	9.094531	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276
640	9.112713	200.126.12.116	10.0.0.70	UDP	Source port: 17276 Destination port: 38052
641	9.120008	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 Bytes
642	9.120481	10.0.0.70	200.126.12.116	UDP	Source port: 38052 Destination port: 17276

[Frame 1 (106 bytes on wire, 96 bytes captured)]  
 [Ethernet II, Src: Cisco-Li-27:b8:3f (68:7f:74:27:b8:3f), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)]  
 [Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.0.70 (10.0.0.70)]  
 [Transmission Control Protocol, Src Port: ssh (22), Dst Port: lontalk-urgent (1629), Seq: 1, Ack: 1, Len: 52]  
 [SSH Protocol]  
 [packet size limited during capture: SSH truncated]

```

0000  00 23 08 b3 04 8f 68 7f 74 27 b8 3f 08 00 45 10  .h.t?..E.
0010  00 5c 21 d3 40 00 40 06 03 73 0a 00 01 01 0a 00  .!..h..s...p.
0020  00 46 00 16 06 5d bb 9d 04 ea 93 e3 00 c6 50 18  .P...].
0030  19 20 02 91 00 00 51 7b 55 48 61 c5 d7 9a 41 98  .)  Uha...A.
0040  4e da 29 60 3a 20 96 c8 74 33 77 5b 3a aa 03 ef  .)  t3w[0...
0050  e8 70 a3 a1 87 af 49 04 87 a5 25 e8 ad d6 85 8e  .p...i...w.....
  
```

File: "C:\Users\Joedwari\esp\PROYECTO... Packets: 31934 Displayed: 31934 Marked: 0

Figura 4.52: Captura de paquetes del enrutador 1 en Zona 1 (OLSR)

b) Enrutador 2:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
2	0.000868	10.0.0.70	10.0.1.2	TCP	oraclenet8cman > ssh [ACK] Seq=1 Ack=53 win=32638 Len=0
3	0.001459	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
4	0.002591	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
5	0.003408	10.0.0.70	10.0.1.2	TCP	oraclenet8cman > ssh [ACK] Seq=1 Ack=157 win=32625 Len=0
6	0.003951	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
7	0.005590	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
8	0.006585	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=52
9	0.012899	10.0.0.70	10.0.1.2	TCP	oraclenet8cman > ssh [ACK] Seq=1 Ack=261 win=32612 Len=0
10	0.013252	10.0.1.2	10.0.0.70	SSH	Encrypted response packet len=276
11	0.016656	10.0.0.70	10.0.1.2	TCP	oraclenet8cman > ssh [ACK] Seq=1 Ack=589 win=32768 Len=0
12	0.024927	10.0.1.2	255.255.255.255	OLSR V1	OLSR (IPv4) Packet, Length: 28 Bytes
13	0.131107	10.0.1.4	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 24 Bytes
14	0.192257	10.0.1.3	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 96 Bytes (not enough data in packet)
15	0.235377	10.0.1.4	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 44 Bytes
16	0.294493	10.0.1.1	255.255.255.255	UDP	OLSR Packet, Length: 56 Bytes (not enough data in packet)
17	0.464947	200.126.12.116	10.0.0.70	ICMP	Destination unreachable (port unreachable)
18	0.725018	10.0.1.2	255.255.255.255	OLSR V1	OLSR (IPv4) Packet, Length: 32 Bytes
19	0.725018	10.0.1.2	10.0.1.255	UDP	OLSR Packet, Length: 84 Bytes (not enough data in packet)
20	1.378210	200.126.12.116	10.0.0.70	ICMP	Destination unreachable (port unreachable)
21	1.392474	10.0.1.3	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 32 Bytes
22	1.855551	10.0.1.3	10.0.1.255	UDP	OLSR Packet, Length: 68 Bytes (not enough data in packet)
23	1.874733	10.0.1.1	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 44 Bytes
24	1.934956	10.0.1.1	255.255.255.255	OLSR V1	OLSR (IPv4) Packet, Length: 32 Bytes
25	1.534205	10.0.1.1	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 28 Bytes
26	2.383109	200.126.12.116	10.0.0.70	ICMP	Destination unreachable (port unreachable)
27	2.424961	10.0.1.2	255.255.255.255	OLSR V1	OLSR (IPv4) Packet, Length: 32 Bytes
28	2.705138	10.0.1.2	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 36 Bytes
29	2.712837	10.0.1.3	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 28 Bytes
30	2.434347	10.0.1.1	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 24 Bytes
31	3.612733	10.0.1.3	10.0.1.255	UDP	OLSR Packet, Length: 56 Bytes (not enough data in packet)
32	3.674387	10.0.1.1	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 44 Bytes
33	3.716197	10.0.1.4	10.0.1.255	OLSR V1	OLSR (IPv4) Packet, Length: 44 Bytes
34	3.814322	10.0.1.1	255.255.255.255	OLSR V1	OLSR (IPv4) Packet, Length: 32 Bytes
35	4.144960	10.0.1.2	255.255.255.255	UDP	OLSR Packet, Length: 56 Bytes (not enough data in packet)
36	4.505145	10.0.1.2	10.0.1.255	UDP	OLSR Packet, Length: 64 Bytes (not enough data in packet)

[Frame 1 (106 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-Li\_27:ac:78 (68:f7:74:27:ac:78), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.0.70 (10.0.0.70)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: oraclenet8cman (1630), Seq: 1, Ack: 1, Len: 52  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 68 f7 74 27 ac 78 08 00 45 10 .#. . . . . h . t . x . . E .
0010 00 5c a3 32 40 00 40 06 82 12 00 00 02 08 00 . \ . p . . . . . . . . . . . . . . .
0020 00 46 00 16 06 5e 9a e7 b9 8a 2b 60 e1 22 50 18 F . . . . . . . . . . . . . . .
0030 19 20 cb fd 00 00 de 9f 9e 45 83 5a c6 98 c9 6a . . . . . . . . . . . E . Z . . . . j
0040 44 66 c0 de 17 44 e2 c6 b7 33 61 46 e1 dc 23 df . . . . . . . . . . . . . . . . . . . #
0050 e9 fe 06 1b ee 28 79 63 cf f8 3d 60 bd 03 44 . . . . . . . . . . . . . . . . . . . . D
  
```

File: C:\Users\Joedward\espol\PROYECTO... Packets: 7041 Displayed: 7041 Marked: 0

Figura 4.53: Captura de paquetes del enrutador 2 en Zona 1 (OLSR)

c) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2502, Time=1731200
2	0.003166000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15632, Time=3076096
3	0.011576000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15633, Time=3076256
4	0.019204000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2503, Time=1731360
5	0.028184000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15634, Time=3076416
6	0.049454000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2504, Time=1731520
7	0.051338000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15635, Time=3076576
8	0.068900000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2505, Time=1731680
9	0.080090000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2506, Time=1731840
10	0.083274000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15636, Time=3076736
11	0.099274000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15637, Time=3076896
12	0.099531000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2507, Time=1732000
13	0.119760000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2508, Time=1732160
14	0.122984000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15638, Time=3077056
15	0.139060000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15639, Time=3077216
16	0.139627000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2509, Time=1732320
17	0.159863000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2510, Time=1732480
18	0.163649000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15640, Time=3077376
19	0.170444000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15641, Time=3077536
20	0.179337000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2511, Time=1732640
21	0.188687000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15642, Time=3077696
22	0.200206000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2512, Time=1732800
23	0.219680000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15643, Time=3077856
24	0.219687000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2513, Time=1732960
25	0.238226000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15644, Time=3078016
26	0.238534000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2514, Time=1733120
27	0.252925000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15645, Time=3078176
28	0.259429000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2515, Time=1733280
29	0.268588000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15646, Time=3078336
30	0.289784000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2516, Time=1733440
31	0.291155000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15647, Time=3078496
32	0.309045000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2517, Time=1733600
33	0.319004000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15648, Time=3078556
34	0.319273000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2518, Time=1733760
35	0.338828000	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C0592A4, Seq=15649, Time=3078816
36	0.339265000	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8E7E1015, Seq=2519, Time=1733920

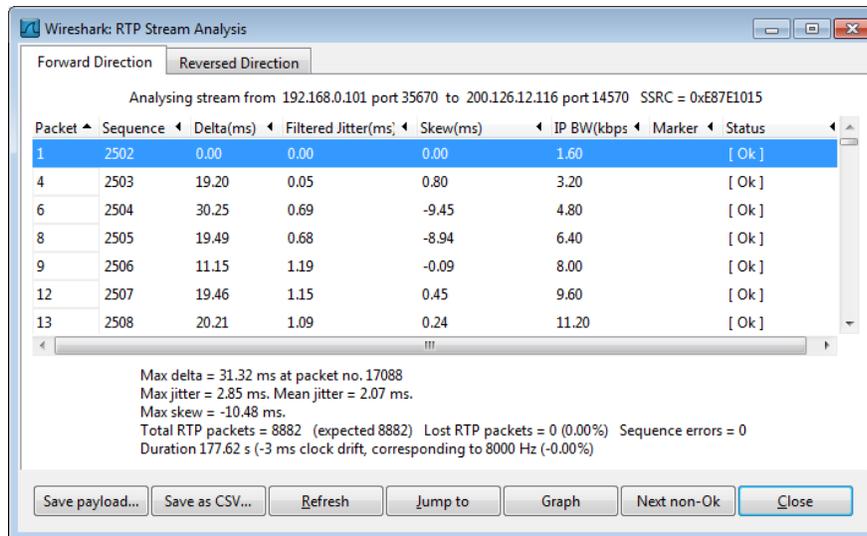
[Frame 1 (214 bytes on wire, 214 bytes captured)  
 Ethernet II, Src: IntelCor\_54:2d:35 (00:1c:0c:54:2d:35), Dst: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96)  
 Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 200.126.12.116 (200.126.12.116)  
 User Datagram Protocol, Src Port: 35670 (35670), Dst Port: 14570 (14570)  
 Real-Time Transport Protocol

```

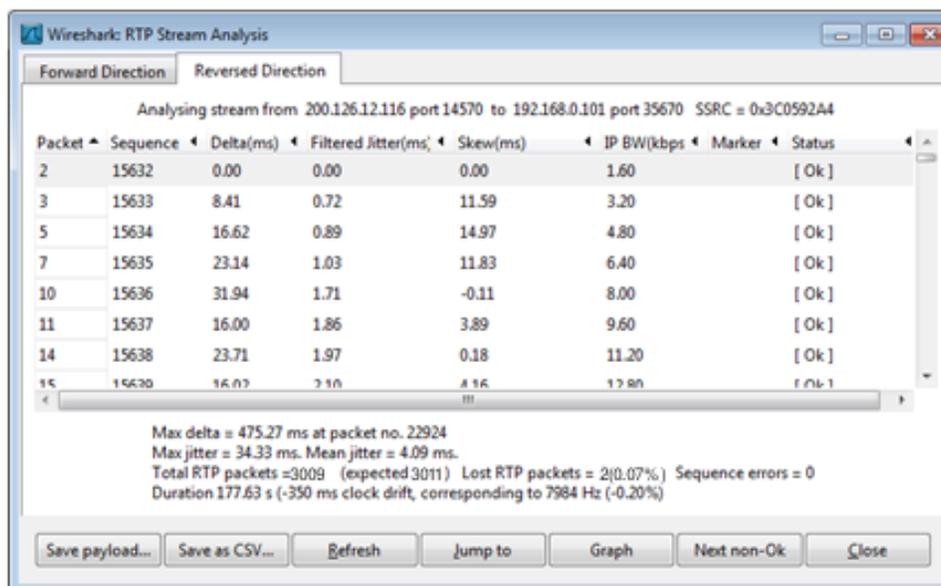
0000 00 17 9a 2a 7f 96 00 1c c0 54 2d 35 08 00 45 00 . . . . . T . S . . E .
0010 00 c8 70 c8 00 00 80 11 33 5d c0 a8 00 65 c8 7e . . . . . j . . . . . ~
0020 0c 74 8b 56 38 ea 00 b4 e0 09 80 00 09 c8 00 1a . . . . . . . . . . . . . . .
0030 6a 80 e8 7e 10 15 7b 79 7b 7a 7d f8 f9 f8 f8 fb j . . . . . [ y ] . . . .
0040 fe 7c 7e 73 75 76 7a 7d fd fa 7f f5 fc 7c fe fd . [vsuvz] . . . . .
0050 fa ff fa ff fd fe 7e 7c 76 75 71 72 7a 7a 7a . . . . . [vsuvz] . . . . .
0060 7b 7a 7c 7b 7a 76 77 76 55 70 7c 7a 6f 6e 6a . . . . . [vsuvz] . . . . .
  
```

File: C:\Users\Joedward\espol\PROYECTO... Packets: 27516 Displayed: 27516 Marked: 0

Figura 4.54: Captura de paquetes del cliente en Zona 1 (OLSR)



**Figura 4.55: Steam RTP en el cliente en la dirección de avance en Zona 1(OLSR)**



**Figura 4.56: Steam RTP en el cliente en la dirección de reversa**

Zona 2:

a) Enrutador 1:

No.	Time	Source	Destination	Protocol	Info
876	13.292264	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
877	13.439336	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
878	13.449155	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
879	13.470197	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
880	13.488869	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
881	13.502691	10.0.0.70	200.126.12.116	SIP	Status: 200 OK(Packet size limited during capture)
882	13.504224	200.126.12.116	10.0.0.70	UDP	Source port: sip Destination port: 9880
883	13.520969	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
884	13.523131	65.54.81.90	10.0.1.2	TCP	http > 50794 [ACK] Seq=178 Ack=263 Win=65696 Len=0
885	13.524626	65.54.81.90	10.0.1.90	TCP	http > 50794 [ACK] Seq=178 Ack=263 Win=65696 Len=0
886	13.531034	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
887	13.531940	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
888	13.556403	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
889	13.564137	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
890	13.568178	10.0.1.1	10.0.1.255	UDP	OLSR Packet, Length: 80 bytes (not enough data in packet)
891	13.575974	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
892	13.588200	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
893	13.596341	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
894	13.599236	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
895	13.607054	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
896	13.616018	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
897	13.629757	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
898	13.636475	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
899	13.653556	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
900	13.655962	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
901	13.671157	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
902	13.676426	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
903	13.690604	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
904	13.696183	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
905	13.712197	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
906	13.716488	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
907	13.728850	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
908	13.738123	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
909	13.756705	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
910	13.768333	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
911	13.780440	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256

Frame 1 (106 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:b8:3f (68:7f:74:27:b8:3f), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.1 (10.0.1.1), Dst: 10.0.0.70 (10.0.0.70)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: gsigatekeeper (2119), Seq: 1, Ack: 1, Len: 52  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]  
 0000 00 23 08 b3 04 8f 68 7f 74 27 b8 3f 08 00 45 10 .#...h.t'.x..E.  
 0010 00 5c 3a c0 40 00 06 ea 85 0a 00 01 01 0a 00 .[.S.@.....  
 0020 00 46 00 16 08 47 58 90 89 df f2 ce 43 ef 50 18 .F...G...COP.  
 0030 19 20 bc 84 00 00 38 90 4b 49 79 4c 39 5e 4b 1e ....8.4X...  
 0040 9a fe 64 ee f7 5f af c7 c3 83 ce fb e7 f6 21 27 .[.S.W.:c[...]  
 0050 e5 06 14 ab c9 1a 46 53 9a 6b ba f4 5d d3 .[T.:.F.S...].  
 File: C:\Users\joedward\espoh\PROYECTO... Packets: 31806 Displayed: 31806 Marked: 0

Figura 4.57: Captura de paquetes del enrutador 1 en Zona 2 (OLSR)

b) Enrutador 2:

No.	Time	Source	Destination	Protocol	Info
496	9.244255	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
497	9.250170	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
498	9.263702	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
499	9.269822	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
500	9.283074	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
501	9.291286	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
502	9.301960	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
503	9.309888	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
504	9.330455	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
505	9.332018	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
506	9.351833	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
507	9.360366	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
508	9.389832	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
509	9.409378	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
510	9.429936	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
511	9.449423	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
512	9.469981	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
513	9.494421	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
514	9.509988	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
515	9.529460	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
516	9.550729	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
517	9.569519	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
518	9.572529	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 28 Bytes
519	9.589062	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
520	9.609526	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
521	9.632618	10.0.1.1	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 Bytes
522	9.629992	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
523	9.649716	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
524	9.670220	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
525	9.689810	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
526	9.692579	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 Bytes
527	9.710275	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
528	9.731968	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
529	9.750068	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
530	9.769912	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
531	9.774366	10.0.1.0	192.87.183.138	HTTP	GET /ecm/brand/ndata/ndfwpars/can/0011/ Toas...

Frame 1 (106 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:ac:78 (68:7f:74:27:ac:78), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.0.70 (10.0.0.70)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: caupc-remote (2122), Seq: 1, Ack: 1, Len: 52  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]  
 0000 00 23 08 b3 04 8f 68 7f 74 27 ac 78 08 00 45 10 .#...h.t'.x..E.  
 0010 00 5c e9 a3 40 00 06 3b a1 0a 90 01 02 0a 00 .[.S.@.....  
 0020 00 46 00 16 08 4a 20 f1 30 c0 03 a3 83 f3 50 18 .F... .O...P.  
 0030 19 20 73 df 00 00 84 76 e2 79 8d 10 4a e0 83 . .S...V.y..@...  
 0040 cf b1 89 04 03 6d fb 86 e2 8c 60 56 06 0c 85 .[.S...F..V...  
 0050 d2 28 f4 6a 73 53 af 5f d1 b5 a6 0c 7a 46 58 b1 .[.S...].....FX.  
 File: C:\Users\joedward\espoh\PROYECTO... Packets: 29793 Displayed: 29793 Marked: 0

Figura 4.58: Captura de paquetes del enrutador 2 en Zona 2 (OLSR)

c) Enrutador 3:

No.	Time	Source	Destination	Protocol	Info
470	7.222904	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
471	7.225105	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
472	7.227488	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
473	7.230950	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
474	7.231941	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
475	7.237337	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
476	7.259935	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
477	7.275648	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
478	7.276346	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
479	7.279491	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=970 ack=105314 win=27375 Len=0
480	7.285001	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
481	7.288929	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
482	7.305733	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
483	7.308971	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
484	7.325122	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
485	7.330947	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
486	7.345794	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
487	7.350192	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
488	7.365112	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
489	7.381618	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
490	7.386058	10.0.1.1	10.0.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes
491	7.387341	198.87.182.138	10.0.1.2	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
492	7.388592	198.87.182.138	10.0.1.255	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
493	7.389208	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
494	7.395897	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
495	7.402686	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
496	7.403136	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
497	7.405353	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
498	7.406038	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=970 ack=108234 win=26645 Len=0
499	7.419591	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
500	7.425985	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
501	7.429122	10.0.0.70	8.8.8.8	DNS	Standard query A 8.8.8.8
502	7.440964	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
503	7.445300	200.126.12.116	10.0.0.70	UDP	Source port: 15848 Destination port: 22256
504	7.448713	198.87.182.138	10.0.1.2	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
505	7.451115	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)

Frame 1 (106 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:b6:23 (68:7f:74:27:b6:23), Dst: Arcadyan\_b3:04:8f (00:23:08:b3:04:8f)  
 Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.0.70 (10.0.0.70)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: gtp-control (2123), Seq: 1, Ack: 1, Len: 52  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000 00 23 08 b3 04 8f 68 7f 74 27 b6 23 08 00 45 10  .#...h.t'..E.
0010 00 5c 44 30 40 00 40 06 e1 08 0a 00 01 03 0a 00  \08.8.....
0020 00 46 00 16 08 4b 4f 77 6f 6d 64 4f 78 80 18   .F...KMD..P.
0030 19 20 0f 8d 00 00 04 3e be 9e cb 73 09 e9 30    .....>..SP.0
0040 71 9a 76 06 05 5b a6 2b df 48 66 8d 4b f9 df f7  0...|..HF...
0050 08 f5 c2 80 9f 0e 71 a9 04 73 0e 41 81 75 25   ..A.Au4u5
    
```

File: C:\Users\Joedward\esp\PROYECTO... Packets: 28032 Displayed: 28032 Marked: 0

Figura 4.59: Captura de paquetes del enrutador 3 en Zona 2 (OLSR)

d) Enrutador 4:

No.	Time	Source	Destination	Protocol	Info
100	5.058303	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 28 Bytes
101	5.116123	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
102	5.122981	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
103	5.133971	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
104	5.142722	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
105	5.148475	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=647 ack=53853 win=25185 Len=0
106	5.219677	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
107	5.290112	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
108	5.310494	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
109	5.337357	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
110	5.345593	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
111	5.346948	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=647 ack=59495 win=25915 Len=0
112	5.353882	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
113	5.403149	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
114	5.411256	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=647 ack=62415 win=25185 Len=0
115	5.463020	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
116	5.470256	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
117	5.479277	10.0.1.2	10.0.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 24 Bytes
118	5.487545	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
119	5.509779	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
120	5.511090	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
121	5.609465	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=647 ack=63875 win=25185 Len=0
122	5.617225	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
123	5.642404	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
124	5.649461	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
125	5.652300	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
126	5.652300	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
127	5.664229	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic(Packet size limited during capture)
128	5.664796	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] seq=647 ack=66795 win=25185 Len=0
129	5.692297	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
130	5.696655	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
131	5.707246	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
132	5.709404	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
133	5.710340	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
134	5.710596	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
135	5.744976	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 Bytes

Frame 1 (98 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:b4:7f (68:7f:74:27:b4:7f), Dst: Cisco-L1\_27:b6:23 (68:7f:74:27:b6:23)  
 Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.3 (10.0.1.3)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: clearvisn (2052), Seq: 1, Ack: 1, Len: 44  
 SSH Protocol  
 [Packet size limited during capture: SSH truncated]

```

0000 68 7f 74 27 b6 23 68 7f 74 27 b4 7f 08 00 45 10  h.t'.#h.t'...E.
0010 00 54 0b 9e 4b 00 40 06 48 ef 0a 00 01 04 0a 00  .t..8.h.....
0020 01 03 00 16 08 04 39 8d 68 2c 52 1f 99 76 50 18  ..r..8.h.r..P.
0030 16 80 76 99 00 00 41 88 c9 29 89 76 f0 b6 8e a1  .:..A..j.V...
0040 ca ac 9a 8c e7 e7 60 19 57 27 a8 39 63 8a e1 71  ..Oz..T.I.....
0050 b0 fa 4f 7a 22 6c b2 54 49 86 81 f8 f5 06 09 45   ..
    
```

File: C:\Users\Joedward\esp\PROYECTO... Packets: 6832 Displayed: 6832 Marked: 0

Figura 4.60: Captura de paquetes del enrutador 4 en Zona 2 (OLSR)

e) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
100	4.937547	10.0.1.2	198.87.182.138	TCP	TCP Previous segment lost, 50636 > http [ACK] Seq=647 Ack=30735 Win=0
101	5.058203	10.0.1.1	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 28 bytes
102	5.116123	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
103	5.122961	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
104	5.133971	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
105	5.142722	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
106	5.146475	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] Seq=647 Ack=3655 Win=25185 Len=0
107	5.219677	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
108	5.290112	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
109	5.330494	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
110	5.337357	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
111	5.343553	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
112	5.346948	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] Seq=647 Ack=59495 Win=25915 Len=0
113	5.353882	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
114	5.403149	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
115	5.411256	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] Seq=647 Ack=62415 Win=25185 Len=0
116	5.463020	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
117	5.470256	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
118	5.479277	10.0.1.2	198.87.182.138	OLSR v1	OLSR (IPv4) Packet, Length: 24 bytes
119	5.487545	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
120	5.509779	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
121	5.511690	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
122	5.609465	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] Seq=647 Ack=63875 Win=25185 Len=0
123	5.617225	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
124	5.642404	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
125	5.649461	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
126	5.652200	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
127	5.664229	198.87.182.138	10.0.1.90	HTTP	Continuation or non-HTTP traffic [packet size limited during capture]
128	5.664796	10.0.1.2	198.87.182.138	TCP	50636 > http [ACK] Seq=647 Ack=66795 Win=25185 Len=0
129	5.692297	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
130	5.696655	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
131	5.707246	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
132	5.709404	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
133	5.710140	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
134	5.710506	10.0.0.70	200.126.12.116	UDP	Source port: 22256 Destination port: 15848
135	5.720276	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 22 bytes

[Frame 1 (98 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-Li\_27:b4:7f (68:7f:74:27:b4:7f), Dst: Cisco-Li\_27:b6:23 (68:7f:74:27:b6:23)  
 Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.3 (10.0.1.3)  
 Transmission Control Protocol, Src Port: ssh (22), Dst Port: clearvisn (2052), Seq: 1, Ack: 1, Len: 44  
 SSH Protocol  
 [packet size limited during capture: SSH truncated]

```

0000 68 7f 74 27 b6 23 68 7f 74 27 b4 7f 08 00 45 10  h.t'.#h. t'....E.
0010 00 54 db 9e 40 00 40 06 48 ef 0a 00 01 04 0a 00  .T..8..H.....
0020 01 03 00 16 08 04 39 8d 68 2c 52 1f 99 76 50 18  .....9..R..VP.
0030 16 40 7d 99 00 00 41 88 c9 29 89 76 f0 b6 8e a1  .:)...A..:).V...
0040 ca ac 9a ac e7 e7 e0 19 57 27 ae 39 d3 5a e1 71  .....W.9.Z.q
0050 b0 ff 4f 7a 23 6c b2 54 49 86 81 f8 f5 06 09 45  ..o2'.T I.....E
  
```

File: C:\Users\loedward\esp\PROYECTO... Packets: 6832 Displayed: 6832 Marked: 0

Figura 4.61: Captura de paquetes del cliente en Zona 2 (OLSR)

Packet	Sequence	Delta	Filtered Jitter	Skew	IP BW	Marker	Status
22	3711	0.00	0.00	0.00	1.60	SET	[Ok]
25	3712	20.55	0.03	-0.55	3.20		[Ok]
27	3713	19.55	0.06	-0.11	4.80		[Ok]
29	3714	20.40	0.08	-0.50	6.40		[Ok]
33	3715	19.63	0.10	-0.14	8.00		[Ok]
35	3716	20.47	0.12	-0.61	9.60		[Ok]
37	3717	19.51	0.15	-0.12	11.20		[Ok]

Max delta = 39.97 ms at packet no. 9554  
 Max jitter = 6.23 ms, Mean jitter = 2.59 ms.  
 Max skew = -29.66 ms.  
 Total RTP packets = 8569 (expected 8569) Lost RTP packets = 0 (0.00%) Sequence errors = 0  
 Duration 171.37 s (-23 ms clock drift, corresponding to 7999 Hz (-0.01%))

Figura 4.62: Steam RTP en el cliente en la dirección de avance en Zona 2 (OLSR)

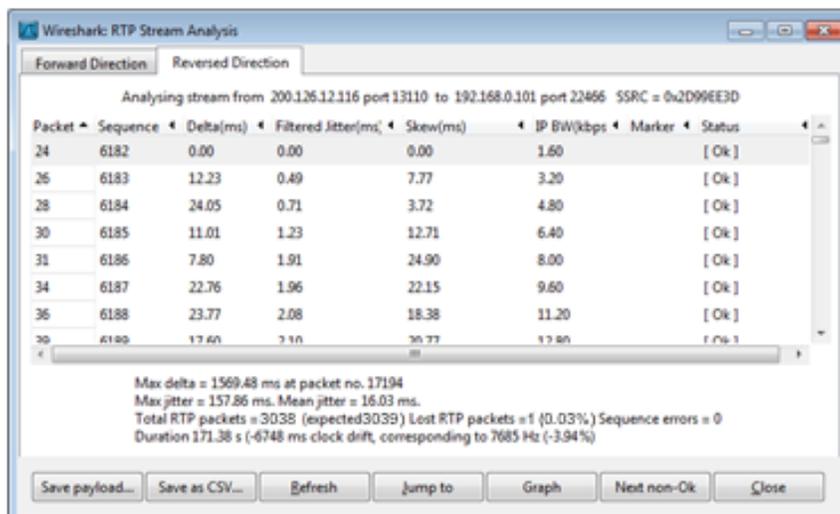


Figura 4.63: Steam RTP en el cliente en la dirección de reversa

### Zona 3:

#### a) Enrutador 1:

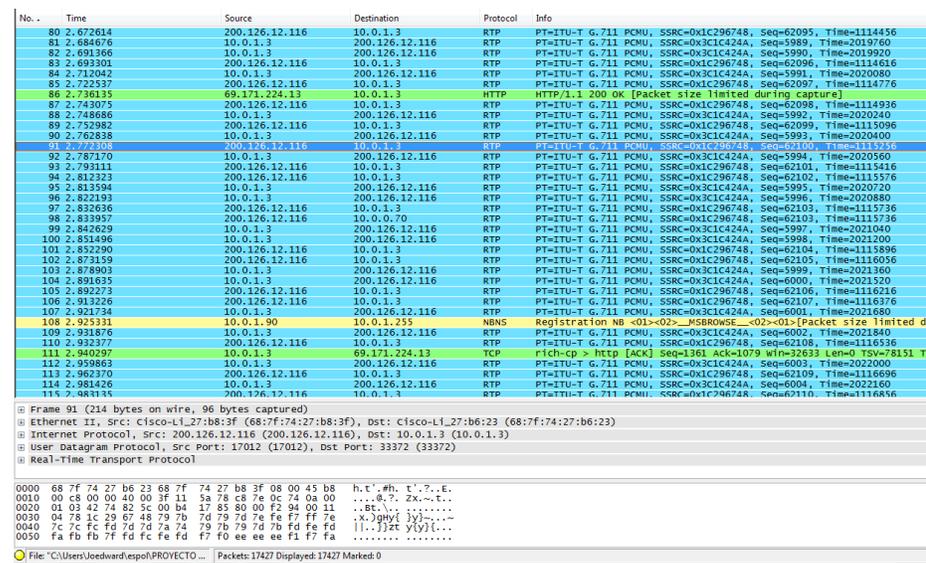


Figura 4.64: Captura de paquetes del enrutador 1 en Zona 3 (OLSR)

b) Enrutador 2:

No.	Time	Source	Destination	Protocol	Info
45	1.769855	10.0.1.3	10.0.1.1	TCP	epnsdp > ssh [ACK] Seq=45 Ack=221 win=7560 Len=0
46	1.770495	10.0.1.1	10.0.1.3	SSH	Encrypted response packet len=280
47	1.771999	10.0.1.3	10.0.1.1	TCP	epnsdp > ssh [ACK] Seq=45 Ack=265 win=7560 Len=0
48	1.772699	10.0.1.3	10.0.0.70	SSH	Encrypted response packet len=68
49	1.774777	10.0.1.3	10.0.0.70	SSH	Encrypted response packet len=52
50	1.776655	10.0.1.3	10.0.1.1	TCP	epnsdp > ssh [ACK] Seq=45 Ack=545 win=7560 Len=0
51	1.780494	10.0.1.3	10.0.0.70	SSH	Encrypted response packet len=84
52	1.878086	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 bytes
53	2.430452	10.0.1.90	10.0.1.255	NBNS	Registration NB WORKGROUP-ID (Packet size limited during capture)
54	2.455198	10.0.1.4	10.0.1.255	UDP	OLSR Packet, Length: 68 bytes (not enough data in packet)
55	2.879662	10.0.1.1	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 bytes
56	2.918266	10.0.1.1	10.0.1.255	UDP	OLSR Packet, Length: 68 bytes (not enough data in packet)
57	3.180495	10.0.1.90	10.0.1.255	NBNS	Registration NB WORKGROUP-ID (Packet size limited during capture)
58	3.515894	10.0.1.3	10.0.1.255	UDP	OLSR Packet, Length: 132 bytes (not enough data in packet)
59	3.558649	10.0.1.2	10.0.1.255	UDP	OLSR Packet, Length: 84 bytes (not enough data in packet)
60	3.678094	10.0.1.2	255.255.255.255	UDP	OLSR Packet, Length: 56 bytes (not enough data in packet)
61	3.782442	10.0.1.3	200.126.12.116	UDP	Source port: 33373 Destination port: 17013
62	3.826472	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5958, Time=2014800, Mark
63	3.839905	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5959, Time=2014960
64	3.839927	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5960, Time=2015120
65	3.869922	10.0.1.3	200.126.12.116	SIP	Status: 200 OK [Packet size limited during capture]
66	3.875215	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5961, Time=2015280
67	3.885614	200.126.12.116	10.0.1.3	UDP	Source port: sfp Destination port: 9880
68	3.886553	200.126.12.116	10.0.0.70	UDP	Source port: sfp Destination port: 9880
69	3.889608	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5962, Time=2015440
70	3.911115	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5963, Time=2015600
71	3.911629	200.126.12.116	10.0.1.3	UDP	Source port: sfp Destination port: 9880
72	3.913903	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62069, Time=1110296, Mark
73	3.929535	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5964, Time=2015760
74	3.931027	200.126.12.116	10.0.1.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62070, Time=1110456
75	3.931806	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62071, Time=1110616
76	3.955652	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5965, Time=2015920
77	3.959782	200.126.12.116	10.0.1.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62071, Time=1110616
78	3.962200	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5966, Time=2016080
79	3.970180	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5966, Time=2016080
80	3.971927	200.126.12.116	10.0.1.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62072, Time=1110776
Frame 568 (214 bytes on wire, 96 bytes captured)					
Ethernet II, Src: Cisco-Li_27:b8:3f (68:f7:74:27:b8:3f), Dst: Cisco-Li_27:b6:23 (68:f7:74:27:b6:23)					
Internet Protocol, Src: 200.126.12.116 (200.126.12.116), Dst: 10.0.1.3 (10.0.1.3)					
User Datagram Protocol, Src Port: 17012 (17012), Dst Port: 33372 (33372)					
Real-Time Transport Protocol					
h.t'.#h. t'.?..E. ...0.?. Zx...E. ...0.?. JA... [8 JgHz] wzwyyw  [...jy XyX ... ]zW(-...- ...]					

Figura 4.65: Captura de paquetes del enrutador 2 en zona 3(OLSR)

c) Enrutador 3:

No.	Time	Source	Destination	Protocol	Info
93	3.564893	10.0.1.3	10.0.0.70	SSH	Encrypted response packet len=52
94	3.567381	10.0.1.1	10.0.1.3	SSH	Encrypted response packet len=280
95	3.567709	10.0.1.3	10.0.1.1	TCP	epnsdp > ssh [ACK] Seq=45 Ack=545 win=7560 Len=0
96	3.571458	10.0.1.3	10.0.0.70	SSH	Encrypted response packet len=84
97	3.572395	10.0.0.70	10.0.1.3	TCP	netmout > ssh [ACK] Seq=89 Ack=309 win=32651 Len=0
98	3.678084	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 bytes
99	4.221953	10.0.1.90	10.0.1.255	NBNS	Registration NB WORKGROUP-ID (Packet size limited during capture)
100	4.246694	10.0.1.4	10.0.1.255	UDP	OLSR Packet, Length: 68 bytes (not enough data in packet)
101	4.671188	10.0.1.1	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 bytes
102	4.708799	10.0.1.1	10.0.1.255	UDP	OLSR Packet, Length: 68 bytes (not enough data in packet)
103	4.972021	10.0.1.90	10.0.1.255	NBNS	Registration NB WORKGROUP-ID (Packet size limited during capture)
104	5.305330	10.0.1.3	10.0.1.255	UDP	OLSR Packet, Length: 132 bytes (not enough data in packet)
105	5.332038	10.0.1.2	10.0.1.255	UDP	OLSR Packet, Length: 84 bytes (not enough data in packet)
106	5.471061	10.0.1.2	255.255.255.255	UDP	OLSR Packet, Length: 56 bytes (not enough data in packet)
107	5.572805	10.0.0.70	200.126.12.116	UDP	Source port: 33373 Destination port: 17013
108	5.573336	10.0.1.3	200.126.12.116	UDP	Source port: 33373 Destination port: 17013
109	5.610295	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5958, Time=2014800, Mark
110	5.610694	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5958, Time=2014800, Mark
111	5.630469	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5959, Time=2014960
112	5.630833	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5959, Time=2014960
113	5.650557	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5960, Time=2015120
114	5.650837	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5960, Time=2015120
115	5.659141	10.0.0.70	200.126.12.116	SIP	Status: 200 OK [Packet size limited during capture]
116	5.659407	10.0.1.3	200.126.12.116	SIP	Status: 200 OK [Packet size limited during capture]
117	5.665844	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5961, Time=2015280
118	5.666127	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5961, Time=2015280
119	5.677140	200.126.12.116	10.0.1.3	UDP	Source port: sfp Destination port: 9880
120	5.677476	200.126.12.116	10.0.0.70	UDP	Source port: sfp Destination port: 9880
121	5.680282	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5962, Time=2015440
122	5.680560	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5962, Time=2015440
123	5.700990	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5963, Time=2015600
124	5.701271	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5963, Time=2015600
125	5.703159	200.126.12.116	10.0.1.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62069, Time=1110296, Mark
126	5.703482	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62069, Time=1110296, Mark
127	5.720205	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5964, Time=2015760
128	5.720464	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C424A, Seq=5964, Time=2015760
Frame 141 (214 bytes on wire, 96 bytes captured)					
Ethernet II, Src: Cisco-Li_27:b8:3f (68:f7:74:27:b8:3f), Dst: Cisco-Li_27:b6:23 (68:f7:74:27:b6:23)					
Internet Protocol, Src: 200.126.12.116 (200.126.12.116), Dst: 10.0.1.3 (10.0.1.3)					
User Datagram Protocol, Src Port: 17012 (17012), Dst Port: 33372 (33372)					
Real-Time Transport Protocol					
h.t'.#h. t'.?..E. ...0.?. Zx...E. ...0.?. JA... [8 JgHz] wzwyyw  [...jy XyX ... ]zW(-...- ...]					

Figura 4.66: Captura de paquetes del enrutador 3 en zona 3 (OLSR)

d) Enrutador 4:

No.	Time	Source	Destination	Protocol	Info
109	3.33062	10.0.0.70	10.0.1.1	SSH	encrypted response packet r6mos
110	3.330430	10.0.0.70	10.0.1.1	TCP	netshout > ssh [ACK] Seq=89 Ack=309 Win=32655 Len=0
111	5.628889	10.0.1.2	255.255.255.255	OLSR v1	OLSR (IPv4) Packet, Length: 32 Bytes
112	6.203194	10.0.1.4	10.0.1.255	UDP	OLSR Packet, Length: 88 Bytes (not enough data in packet)
113	7.285421	10.0.1.3	10.0.1.255	UDP	OLSR Packet, Length: 132 Bytes (not enough data in packet)
114	7.319043	10.0.1.2	10.0.1.255	UDP	OLSR Packet, Length: 84 Bytes (not enough data in packet)
115	7.429054	10.0.1.2	255.255.255.255	UDP	OLSR Packet, Length: 56 Bytes (not enough data in packet)
116	7.530810	10.0.0.70	200.126.12.116	UDP	Source port: 33373 Destination port: 17013
117	7.531970	10.0.1.3	200.126.12.116	UDP	Source port: 33373 Destination port: 17013
118	7.588254	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5958, Time=2014800, Mark
119	7.589730	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5958, Time=2014800, Mark
120	7.588466	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5959, Time=2014960
121	7.589444	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5959, Time=2014960
122	7.608541	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5960, Time=2015120
123	7.609448	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5960, Time=2015120
124	7.617153	10.0.0.70	200.126.12.116	SIP	Status: 200 OK[Packet size limited during capture]
125	7.618823	10.0.1.3	200.126.12.116	SIP	Status: 200 OK[Packet size limited during capture]
126	7.623806	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5961, Time=2015280
127	7.624768	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5961, Time=2015280
128	7.630361	200.126.12.116	10.0.0.70	UDP	Source port: 519 Destination port: 9880
129	7.638273	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5962, Time=2015440
130	7.639152	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5962, Time=2015440
131	7.639883	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5963, Time=2015600
132	7.663418	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62089, Time=1102096, Mark
133	7.678195	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5964, Time=2015760
134	7.679052	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5964, Time=2015760
135	7.681300	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62070, Time=110456
136	7.704103	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5965, Time=2015920
137	7.705183	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5965, Time=2015920
138	7.717218	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62071, Time=110616
139	7.718645	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5966, Time=2016080
140	7.719704	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5966, Time=2016080
141	7.721480	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62072, Time=110776
142	7.737648	10.0.0.70	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5967, Time=2016240
143	7.738489	10.0.1.3	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3C1C4244, Seq=5967, Time=2016240
144	7.751563	200.126.12.116	10.0.0.70	RTP	PT=ITU-T G.711 PCMU, SSRC=0x1C296748, Seq=62073, Time=110936

Frame 36 (98 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-Li-27:b6:23 (68:7f:74:27:b6:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Internet Protocol, Src: 10.0.1.3 (10.0.1.3), Dst: 10.0.1.255 (10.0.1.255)  
 User Datagram Protocol, Src Port: olsr (698), Dst Port: olsr (698)  
 Data (54 bytes)

```

0000 ff ff ff ff ff ff 68 7f 74 27 b6 23 08 00 45 10 .....h. t. #. .E.
0010 00 54 00 00 00 40 11 23 88 0a 00 03 0a 00 .....T.8. .m. .t.
0020 01 ff 02 ba 02 ba 00 40 77 97 00 38 cf 38 04 e7 .....0 w. .8. .8.
0030 00 14 0a 00 01 02 fe 01 3c e4 6d 01 60 ff ff ..... . . . . .
0040 ff 00 01 86 00 20 0a 00 01 03 01 00 0d 49 00 00 ..... . . . . .
0050 05 03 06 00 00 10 0a 00 01 02 0a 00 01 04 0a 00 ..... . . . . .
    
```

Figura 4.67: Captura de paquetes del enrutador 4 en zona 3 (OLSR)

e) Cliente softphone:

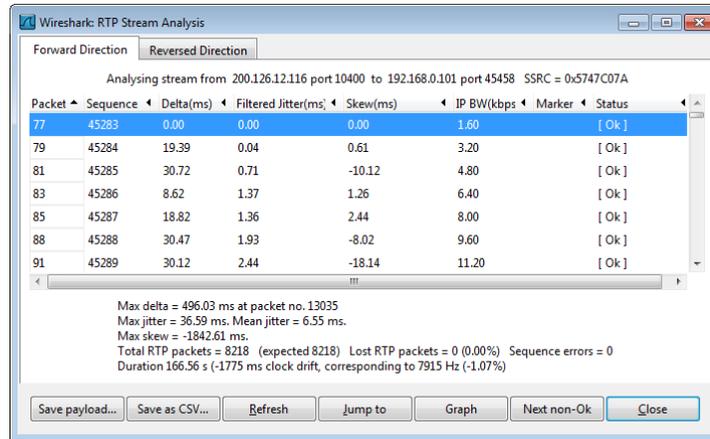
No.	Time	Source	Destination	Protocol	Info
46	3.955849	192.168.0.101	200.126.12.116	SIP/SDP	Request: INVITE sip:10068200.126.12.116, with session description
47	3.955989	200.126.12.116	192.168.0.101	SIP	Status: 100 trying
48	4.293318	200.126.12.116	192.168.0.101	SIP	Status: 180 Ringing
49	5.024873	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
50	5.024107	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
51	5.024366	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
52	5.025297	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
53	5.026487	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
54	5.026731	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
55	5.027668	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
56	5.028889	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
57	5.029140	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
58	5.030607	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
59	5.031251	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
60	5.031488	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
61	5.032421	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
62	6.393813	74.125.229.55	192.168.0.101	TCP	[TCP segment of a reassembled PDU]
63	6.544794	192.168.0.101	74.125.229.55	TCP	autonoc > http [ACK] Seq=1820 Ack=701 Win=65187 Len=0
64	9.918461	192.168.0.101	69.4.231.53	TCP	elfrq-repl > http [FIN, ACK] Seq=1 Ack=2 Win=6535 Len=0
65	9.919230	192.168.0.101	69.4.231.53	TCP	unizonus > http [FIN, ACK] Seq=1 Ack=2 Win=6535 Len=0
66	9.919538	192.168.0.101	69.4.231.53	TCP	blaze > http [FIN, ACK] Seq=1 Ack=2 Win=6535 Len=0
67	9.920246	192.168.0.101	69.4.231.53	TCP	winspans > http [FIN, ACK] Seq=1 Ack=2 Win=6535 Len=0
68	9.920522	192.168.0.101	69.4.231.53	TCP	fuscript > http [FIN, ACK] Seq=1 Ack=2 Win=6535 Len=0
69	10.040104	69.4.231.53	192.168.0.101	TCP	http > elfrq-repl [ACK] Seq=2 Ack=2 Win=8140 Len=0
70	10.040681	69.4.231.53	192.168.0.101	TCP	http > winspans [ACK] Seq=2 Ack=2 Win=7106 Len=0
71	10.040746	69.4.231.53	192.168.0.101	TCP	http > unizonus [ACK] Seq=2 Ack=2 Win=7051 Len=0
72	10.040845	69.4.231.53	192.168.0.101	TCP	http > blaze [ACK] Seq=2 Ack=2 Win=7063 Len=0
73	10.041215	69.4.231.53	192.168.0.101	TCP	http > fuscript [ACK] Seq=2 Ack=2 Win=9436 Len=0
74	13.447069	200.126.12.116	192.168.0.101	SIP/SDP	Status: 200 OK, with session description
75	13.451008	192.168.0.101	200.126.12.116	RTP	Receiver Report source description
76	13.481658	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xc886e186, Seq=395, Time=110300, Mark
77	13.483852	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3747c07a, Seq=4283, Time=2015600
78	13.501276	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xc886e186, Seq=396, Time=110460
79	13.503245	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3747c07a, Seq=4284, Time=2015760
80	13.521940	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0xc886e186, Seq=397, Time=110620
81	13.523668	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x3747c07a, Seq=4285, Time=2015800

Frame 501 (214 bytes on wire, 214 bytes captured)  
 Ethernet II, Src: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96), Dst: Intelcor\_34:26:35 (00:1c:c0:34:26:35)  
 Internet Protocol, Src: 200.126.12.116 (200.126.12.116), Dst: 192.168.0.101 (192.168.0.101)  
 User Datagram Protocol, Src Port: 10400 (10400), Dst Port: 45458 (45458)  
 Real-Time Transport Protocol

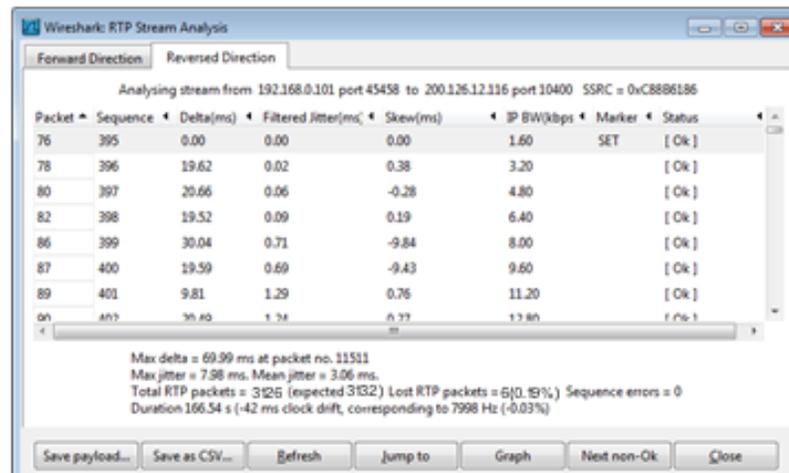
```

0000 00 1c c0 34 2d 35 00 17 9a 2a 7f 96 08 00 45 b8 ...T.S. .#.. .E.
0010 00 c8 00 00 40 00 3f 11 a4 6d c8 7e 0c 74 c0 a8 ..... .m. .t.
0020 00 65 28 a0 b1 92 00 b4 03 72 80 00 b1 b6 00 ff ..C....f.....f
0030 43 50 57 c0 7a f7 f5 7d 7d 6a c8 68 67 67 .....E.....jvJfJg
0040 6d 6d 6d 73 7b 7f fe f7 ff ee ef ed ed f0 f7 mkmks{.....
0050 fc fa fa 74 71 6f fe 6e 70 73 73 72 77 7c .....-wqon npstsrw|
0060 7c fa fa fe ..C....f.....f
    
```

Figura 4.68: Captura de paquetes del cliente en zona 3 (OLSR)



**Figura 4.69: Steam RTP en el cliente en la dirección de avance en Zona 3 (OLSR)**



**Figura 4.70: Steam RTP en el cliente en la dirección de reversa en Zona 3 (OLSR)**

Zona 4:

a) Enrutador 1:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
2	0.000234	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
3	0.015170	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
4	0.032019	10.0.1.1	10.0.0.70	SSH	Encrypted response packet len=52
5	0.033154	10.0.1.1	10.0.0.70	SSH	Encrypted response packet len=52
6	0.047905	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
7	0.048309	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
8	0.048529	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
9	0.062374	10.0.0.70	200.126.12.116	UDP	Source port: 10600 Destination port: 16308
10	0.086149	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
11	0.085970	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
12	0.086280	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
13	0.144003	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
14	0.144352	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
15	0.144566	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
16	0.145058	10.0.0.70	200.126.12.116	UDP	Source port: 10600 Destination port: 16308
17	0.149008	10.0.0.70	200.126.12.116	UDP	Source port: 10600 Destination port: 16308
18	0.152858	10.0.0.70	200.126.12.116	UDP	Source port: 10600 Destination port: 16308
19	0.191175	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
20	0.192103	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
21	0.192400	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
22	0.227977	10.0.1.1	10.0.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 44 Bytes
23	0.236881	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
24	0.239447	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
25	0.240044	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
26	0.240341	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
27	0.246811	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
28	0.270057	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
29	0.272734	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
30	0.275255	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
31	0.281184	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
32	0.283711	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600
33	0.287972	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
34	0.288316	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
35	0.288530	200.126.12.116	10.0.1.3	UDP	Source port: 16308 Destination port: 10600
36	0.305041	200.126.12.116	10.0.0.70	UDP	Source port: 16308 Destination port: 10600

Frame 1 (214 bytes on wire, 96 bytes captured)  
 Ethernet II, Src: Cisco-L1\_27:b8:3f (68:7f:74:27:b8:3f), Dst: Cisco-L1\_27:b6:23 (68:7f:74:27:b6:23)  
 Internet Protocol, Src: 200.126.12.116 (200.126.12.116), Dst: 10.0.1.3 (10.0.1.3)  
 User Datagram Protocol, Src Port: 16308 (16308), Dst Port: 10600 (10600)  
 Data (54 bytes)

```

0000 68 7f 74 27 b6 23 68 7f 74 27 b8 3f 08 00 45 b8 h.t'.#h.t'.P..E.
0010 00 c8 00 00 40 00 3f 11 5a 78 c8 7e 0c 74 0a 00 ...0.?.Zx...t...
0020 01 03 3f b4 29 68 00 b4 36 63 80 00 40 81 00 02 ...?..h..6c..0...
0030 15 c0 50 91 a1 8c 7f ff 7e fd fd fd fe fe fe fe P.....
0040 fd fe 7f ff 7f 7e fd fd fd fe fe fe 7f ff fd fe .....
0050 fe fe fd fe ff ff ff ff ff fe ff 7e ff 7d 7e 7f .....]...
  
```

File: C:\Users\joedward\espo\PROYECTO... | Packets: 17996 Displayed: 17996 Marked: 0

Figura 4.71: Captura de paquetes del enrutador 1 en Zona 4 (OLSR)

b) Cliente softphone:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.101	204.2.241.145	TCP	dab-st1-c > http [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
2	0.092746	204.2.241.145	192.168.0.101	TCP	http > dab-st1-c [FIN, ACK] Seq=1 Ack=2 Win=770 Len=0
3	0.092816	192.168.0.101	204.2.241.145	TCP	dab-st1-c > http [ACK] Seq=2 Ack=2 Win=65535 Len=0
4	1.239408	192.168.0.101	200.126.12.116	SIP/SDP	Request: INVITE sip:10068200.126.12.116, with session description
5	1.240998	200.126.12.116	192.168.0.101	SIP	Status: 407 Proxy Authentication Required
6	1.241642	192.168.0.101	200.126.12.116	SIP	Request: ACK sip:10068200.126.12.116
7	1.241976	192.168.0.101	200.126.12.116	SIP/SDP	Request: INVITE sip:10068200.126.12.116, with session description
8	1.244335	200.126.12.116	192.168.0.101	SIP	Status: 100 Trying
9	1.571041	200.126.12.116	192.168.0.101	SIP	Status: 180 Ringing
10	4.638692	192.168.0.101	74.125.229.54	TCP	[TCP segment of a reassembled PDU]
11	4.658715	192.168.0.101	74.125.229.54	HTTP	POST /mail/?ui=2&k=3c5489143&rid=b4cc...&view=1&start=0&num=70&hlo
12	4.731198	74.125.229.54	192.168.0.101	TCP	http > 4910 [ACK] Seq=1 Ack=2006 Win=62328 Len=0
13	4.909518	192.168.0.101	74.125.229.54	TCP	HTTP/1.1 200 OK (text/javascript)
14	5.071860	192.168.0.101	74.125.229.54	TCP	4910 > http [ACK] Seq=2006 Ack=1370 Win=64132 Len=0
15	6.759351	200.126.12.116	192.168.0.101	SIP/SDP	Status: 200 OK, with session description
16	6.763637	192.168.0.101	200.126.12.116	RTCP	Receiver Report Source description
17	6.790528	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=2921, Time=16100, Mark
18	6.795466	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38404, Time=2964136
19	6.803064	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38405, Time=2964296
20	6.809987	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2922, Time=16260
21	6.823497	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38406, Time=2964456
22	6.830723	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2923, Time=16420
23	6.845146	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38407, Time=2964616
24	6.850154	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2924, Time=16580
25	6.864350	192.168.0.101	200.126.12.116	SIP	Request: ACK sip:10068200.126.12.116
26	6.868350	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38408, Time=2964776
27	6.870653	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2925, Time=16740
28	6.886253	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38409, Time=2964936
29	6.890144	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2926, Time=16900
30	6.904680	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38410, Time=2965096
31	6.910754	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2927, Time=17060
32	6.924994	200.126.12.116	192.168.0.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x444f4852c, Seq=38411, Time=2965256
33	6.930195	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2928, Time=17220
34	6.939460	192.168.0.101	200.126.12.116	RTP	PT=ITU-T G.711 PCMU, SSRC=0x6902e8ec, Seq=2929, Time=17380
35	6.940529	192.168.0.101	200.9.176.5	DNS	standard query A mobile.google.com
36	6.943013	192.168.0.101	200.9.176.5	DNS	standard query A www.google.com

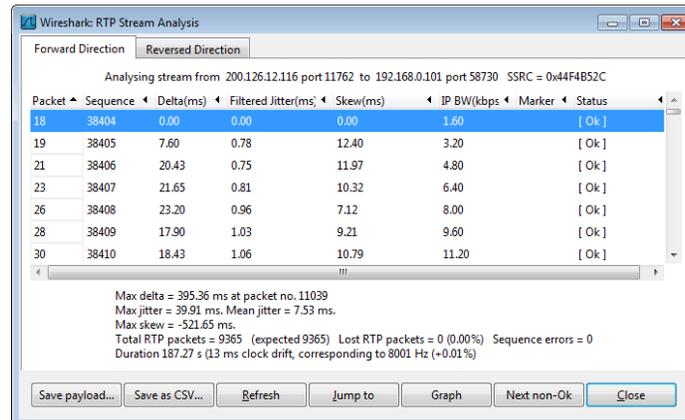
Frame 1 (54 bytes on wire, 54 bytes captured)  
 Ethernet II, Src: IntelCor\_54:2d:35 (00:1c:c0:54:2d:35), Dst: D-Link\_2a:7f:96 (00:17:9a:2a:7f:96)  
 Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 204.2.241.145 (204.2.241.145)  
 Transmission Control Protocol, Src Port: dab-st1-c (1076), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

```

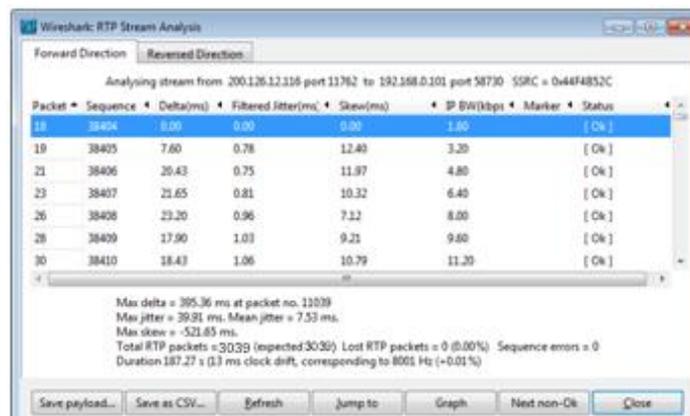
0000 00 17 9a 2a 7f 96 00 1c c0 54 2d 35 08 00 45 00 ...*.T-.E.
0010 00 28 f5 5c 40 00 80 06 86 d1 c0 a8 05 6c c0 02 ...(\@...e..
0020 f1 91 04 34 00 50 ce 01 b7 17 71 6d f8 be 50 11 ...4.P...qm.P.
0030 ff ff 7e bc 00 00 .....
  
```

File: C:\Users\joedward\espo\PROYECTO... | Packets: 20774 Displayed: 20774 Marked: 0

Figura 4.72: Captura de paquetes del cliente en Zona 4 (OLSR)

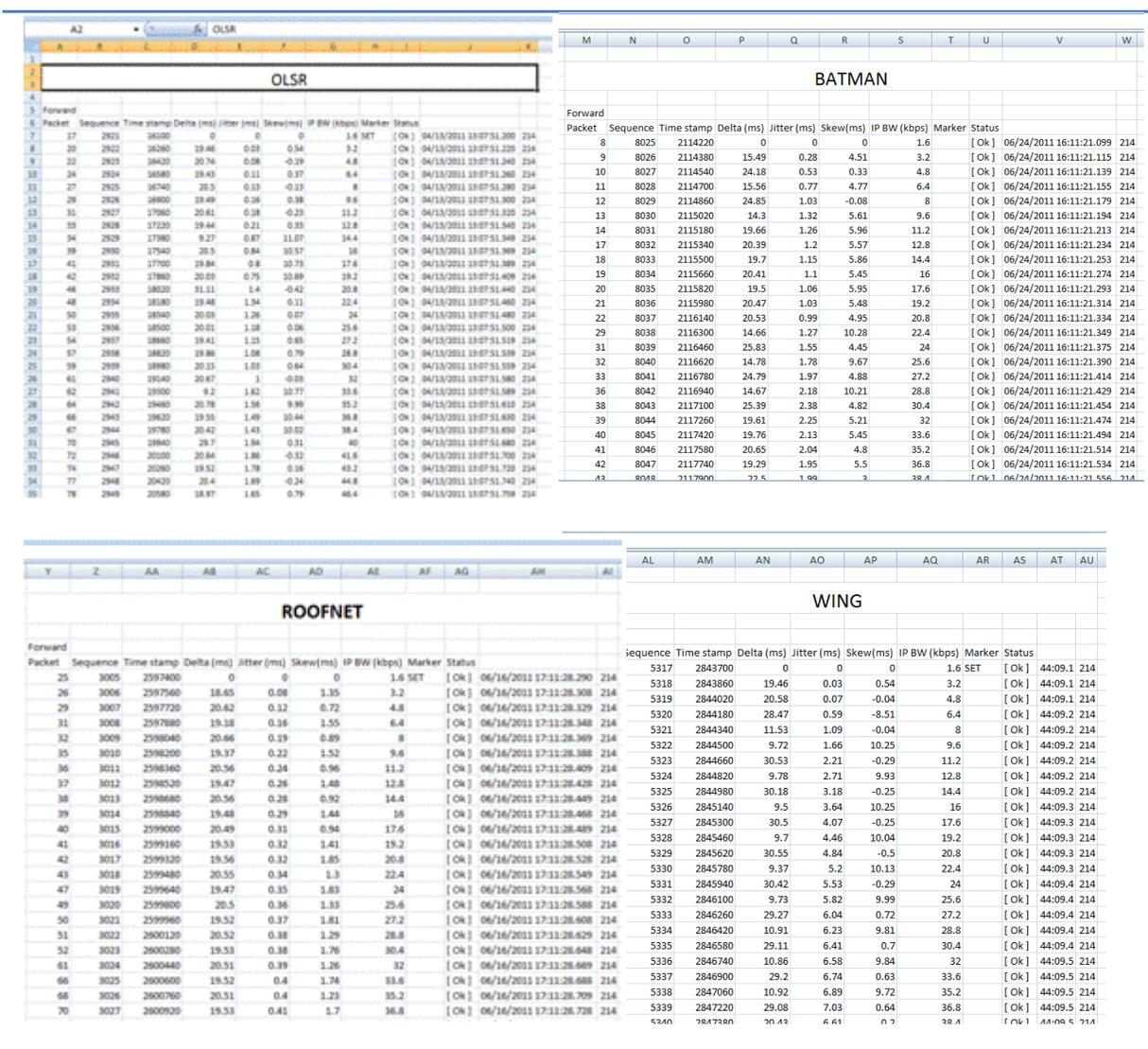


**Figura 4.73: Steam RTP en el cliente en la dirección de avance en Zona 4 (OLSR)**



**Figura 4.74: Steam RTP en el cliente en la dirección de reversa en Zona 4 (OLSR)**

Con estas capturas se procedió a realizar un análisis de ancho de banda, jitter y retardo en función del tiempo. Dado que la cantidad de paquetes es muy grande se promediaron los valores cada 4 segundos, esto da aproximadamente unos 15 puntos, dado que son alrededor de 60 minutos de duración de llamadas. Para ello, en primer lugar, se exportaron los datos capturados a Excel, como se muestra a continuación:



**Figura 4.75: Exportación a Excel de los paquetes de cada protocolo de enrutamiento capturados con Wireshark**

Posteriormente, estos valores fueron exportados a Matlab, donde mediante el código de programa se calcularon los valores promedios de ancho de banda, retardo y jitter.

Las gráficas obtenidas se muestran y se analizan en el capítulo siguiente. Con ellos se procedió a hacer el análisis respectivo de cada protocolo para determinar cuál de ellos es más eficiente.

A continuación se detalla el análisis estadístico de los datos que se capturaron en Wireshark en el softphone instalado en la computadora de escritorio. Para ello, se hizo uso de la herramienta de análisis estadístico MINITAB, donde se procedió a ingresar los valores de retardo, jitter y delay para cada protocolo en cada una de las zonas definidas. Se obtuvo para cada parámetro sus respectivos valores de desviación estándar y media para usarlos en el análisis de los intervalos de confianza. Luego se muestra un histograma que representa la frecuencia con la que se presentaron los valores. Finalmente, se presenta el respectivo análisis de intervalos de confianza para la media poblacional, con los datos que se obtuvieron.

## a. Zona 1:

## OLSR

## Descriptive Statistics: RETARDO OZ1; JITTER OZ1; BW OZ1

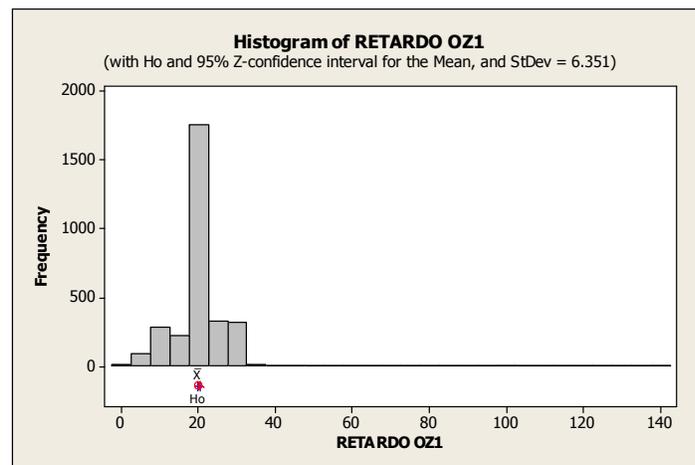
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median	Q3
RETARDO OZ1	3038	0	20.016	0.115	6.351	0.500	18.800	20.235	22.040
JITTER OZ1	3038	0	3.8770	0.0279	1.5404	0.7200	2.9500	3.3700	4.6300
BW OZ1	3038	0	80.068	0.106	5.826	3.200	80.000	80.000	81.600

Variable	Maximum
RETARDO OZ1	141.170
JITTER OZ1	17.3100
BW OZ1	94.400

**Figura 4.76: Información de estadística descriptiva para OLSR en la zona 1**

Retardo:



**Figura 4.77: Histograma de frecuencias para el retardo de OLSR en la zona 1**

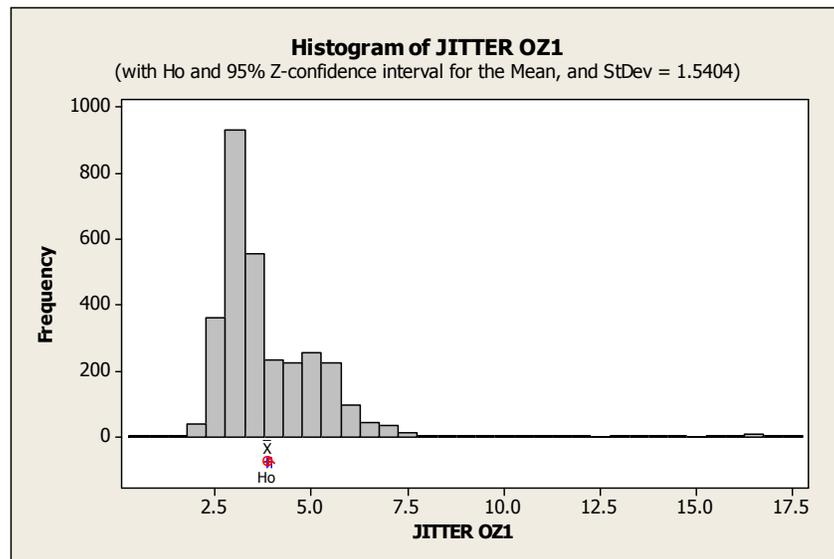
### One-Sample Z: RETARDO OZ1

Test of  $\mu = 20.016$  vs not = 20.016  
 The assumed standard deviation = 6.351

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO OZ1	3038	20.0155	6.3510	0.1152	(19.7897; 20.2414)	-0.00	0.997

**Figura 4.78: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 1**

Jitter:



**Figura 4.79: Histograma de frecuencias para el jitter de OLSR en la zona 1**

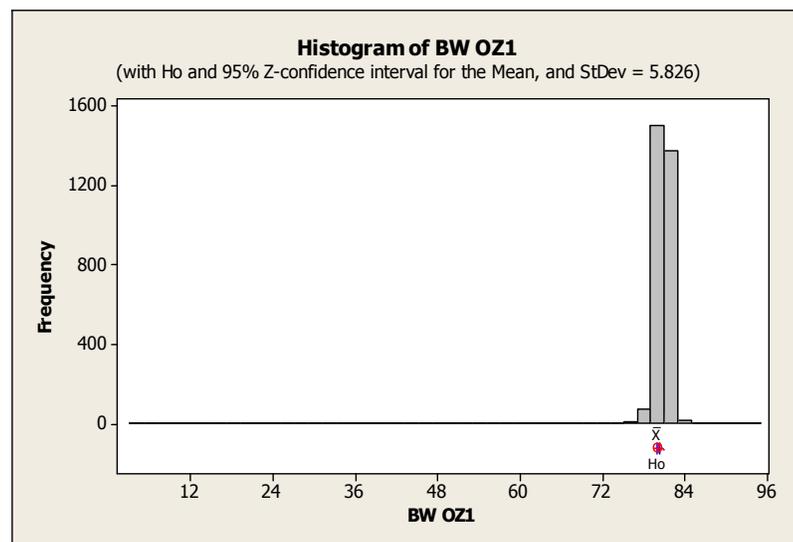
**One-Sample Z: JITTER OZ1**

Test of  $\mu = 3.877$  vs not = 3.877  
 The assumed standard deviation = 1.5404

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER OZ1	3038	3.87702	1.54037	0.02795	(3.82224; 3.93179)	0.00	0.999

**Figura 4.80: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 1**

Ancho de Banda:



**Figura 4.81: Histograma de frecuencias para el ancho de banda de OLSR en la zona 1**

### One-Sample Z: BW OZ1

Test of mu = 80.068 vs not = 80.068  
The assumed standard deviation = 5.826

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW OZ1	3038	80.0685	5.8263	0.1057	(79.8613; 80.2756)	0.00	0.996

**Figura 4.82: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 1**

### BATMAN

#### Descriptive Statistics: RETARDO BZ1; JITTER BZ1; BW BZ1

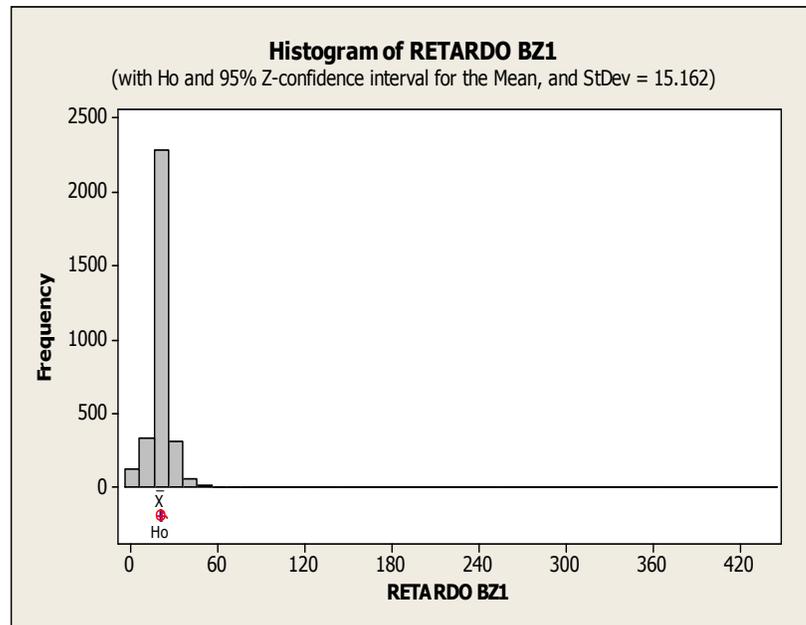
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO BZ1	3134	0	20.264	0.271	15.162	0.000000000	17.490	19.960
JITTER BZ1	3134	0	4.9808	0.0718	4.0178	0.2100	2.8200	3.8800
BW BZ1	3134	0	79.316	0.140	7.864	3.200	80.000	80.000

Variable	Q3	Maximum
RETARDO BZ1	22.143	439.220
JITTER BZ1	5.9000	31.8900
BW BZ1	81.600	110.400

**Figura 4.83: Información de estadística descriptiva para BATMAN en la zona 1**

Retardo:



**Figura 4.84: Histograma de frecuencias para el retardo de BATMAN en la zona 1**

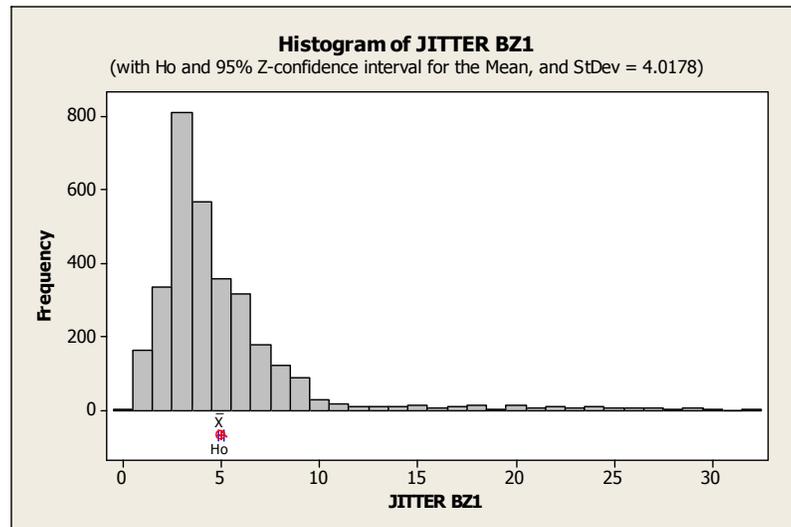
**One-Sample Z: RETARDO BZ1**

Test of  $\mu = 20.264$  vs not = 20.264  
The assumed standard deviation = 15.162

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO BZ1	3134	20.2644	15.1623	0.2708	(19.7336; 20.7952)	0.00	0.999

**Figura 4.85: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 1**

Jitter:



**Figura 4.86: Histograma de frecuencias para el jitter de BATMAN en la zona 1**

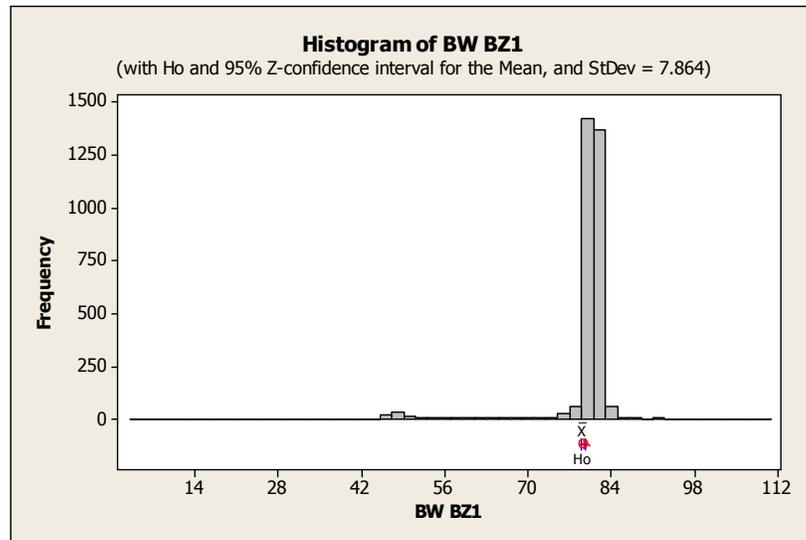
#### One-Sample Z: JITTER BZ1

Test of  $\mu = 4.9808$  vs not = 4.9808  
The assumed standard deviation = 4.0178

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER BZ1	3134	4.98075	4.01775	0.07177	(4.84009; 5.12142)	-0.00	0.999

**Figura 4.87: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 1**

Ancho De Banda:



**Figura 4.88: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 1**

#### One-Sample Z: BW BZ1

Test of  $\mu = 79.316$  vs not = 79.316  
The assumed standard deviation = 7.864

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW BZ1	3134	79.3159	7.8640	0.1405	(79.0406; 79.5912)	-0.00	0.999

**Figura 4.89: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 1**

## ROOFNET

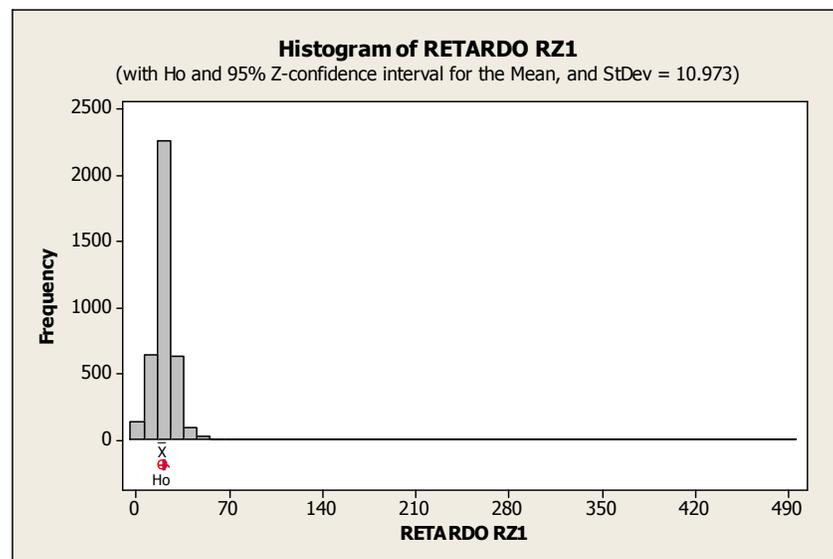
### Descriptive Statistics: RETARDO RZ1; JITTER RZ1; BW RZ1

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO RZ1	3805	0	20.110	0.178	10.973	0.000000000	16.115	19.960
JITTER RZ1	3805	0	5.7125	0.0367	2.2637	0.4300	4.2450	5.3700
BW RZ1	3805	0	79.963	0.0993	6.127	3.200	80.000	80.000

Variable	Q3	Maximum
RETARDO RZ1	23.820	494.260
JITTER RZ1	6.7600	36.6700
BW RZ1	81.600	84.800

**Figura 4.90: Información de estadística descriptiva para ROOFNET en la zona 1**

Retardo:



**Figura 4.91: Histograma de frecuencias para el retardo de ROOFNET en la zona 1**

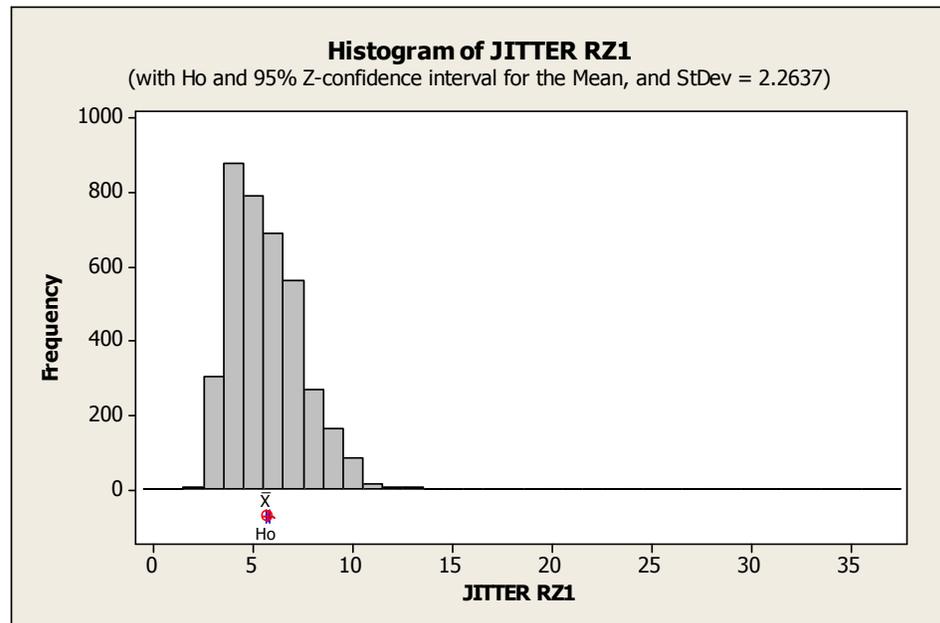
**One-Sample Z: RETARDO RZ1**

Test of  $\mu = 20.11$  vs not = 20.11  
 The assumed standard deviation = 10.973

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO RZ1	3805	20.1095	10.9732	0.1779	(19.7609; 20.4582)	-0.00	0.998

**Figura 4.92: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 1**

Jitter:



**Figura 4.93: Histograma de frecuencias para el jitter de ROOFNET en la zona 1**

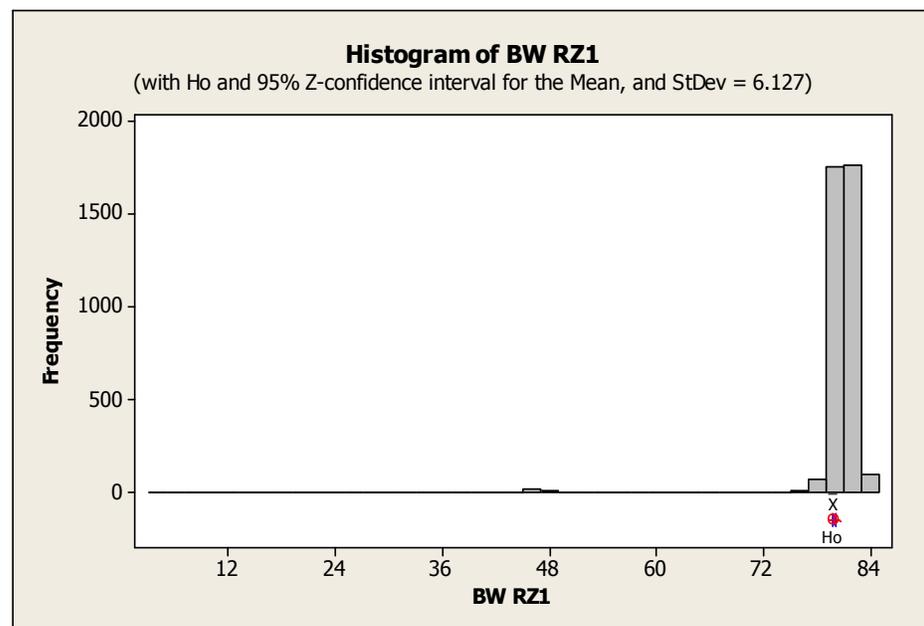
### One-Sample Z: JITTER RZ1

Test of  $\mu = 5.7125$  vs not = 5.7125  
 The assumed standard deviation = 2.2637

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER RZ1	3805	5.71248	2.26374	0.03670	(5.64055; 5.78441)	-0.00	1.000

**Figura 4.94: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 1**

Ancho De Banda:



**Figura 4.95: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 1**

**One-Sample Z: BW RZ1**

Test of  $\mu = 79.963$  vs not = 79.963  
 The assumed standard deviation = 6.127

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW RZ1	3805	79.9634	6.1271	0.0993	(79.7687; 80.1581)	0.00	0.997

**Figura 4.96: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 1**

**WING****Descriptive Statistics: RETARDO WZ1; JITTER WZ1; BW WZ1**

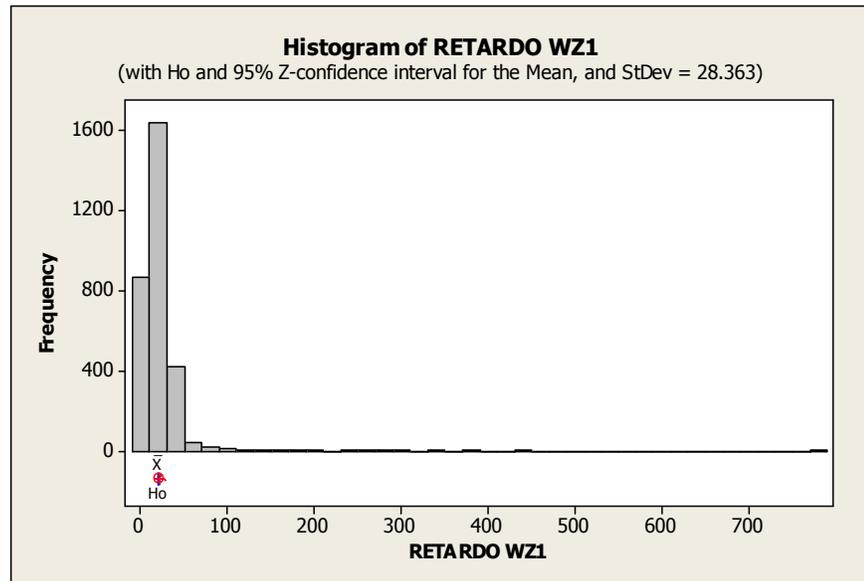
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO WZ1	3021	0	20.566	0.516	28.363	0.000000000	5.490	19.290
JITTER WZ1	3021	0	12.429	0.101	5.568	1.230	8.685	11.300
BW WZ1	3021	0	78.247	0.185	10.145	3.200	78.400	80.000

Variable	Q3	Maximum
RETARDO WZ1	24.110	779.540
JITTER WZ1	14.730	52.780
BW WZ1	81.600	129.600

**Figura 4.97: Información de estadística descriptiva para WING en la zona 1**

Retardo:



**Figura 4.98: Histograma de frecuencias para el retardo de WING en la zona 1**

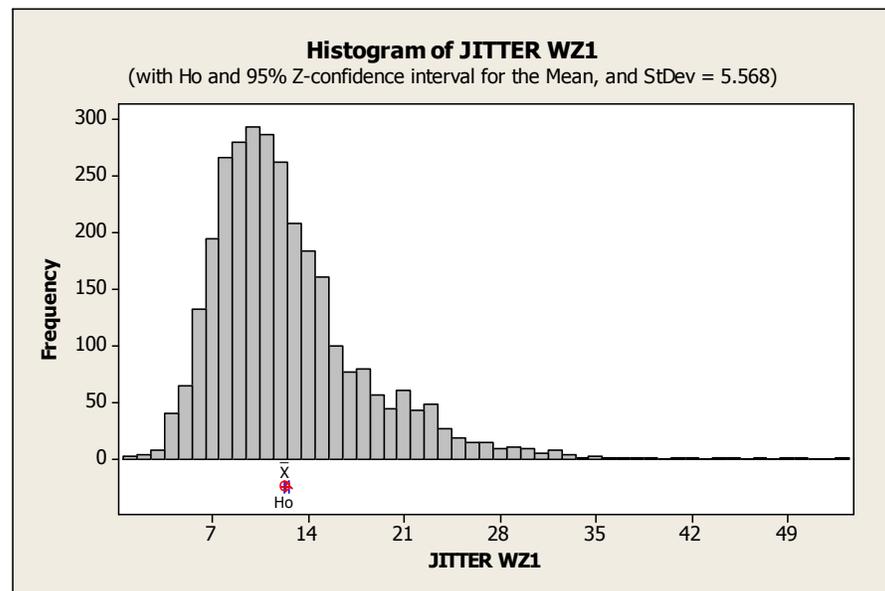
**One-Sample Z: RETARDO WZ1**

Test of  $\mu = 20.566$  vs not = 20.566  
The assumed standard deviation = 28.363

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO WZ1	3021	20.5657	28.3633	0.5160	(19.5543; 21.5771)	-0.00	1.000

**Figura 4.99: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 1**

Jitter:



**Figura 4.100: Histograma de frecuencias para el jitter de WING en la zona 1**

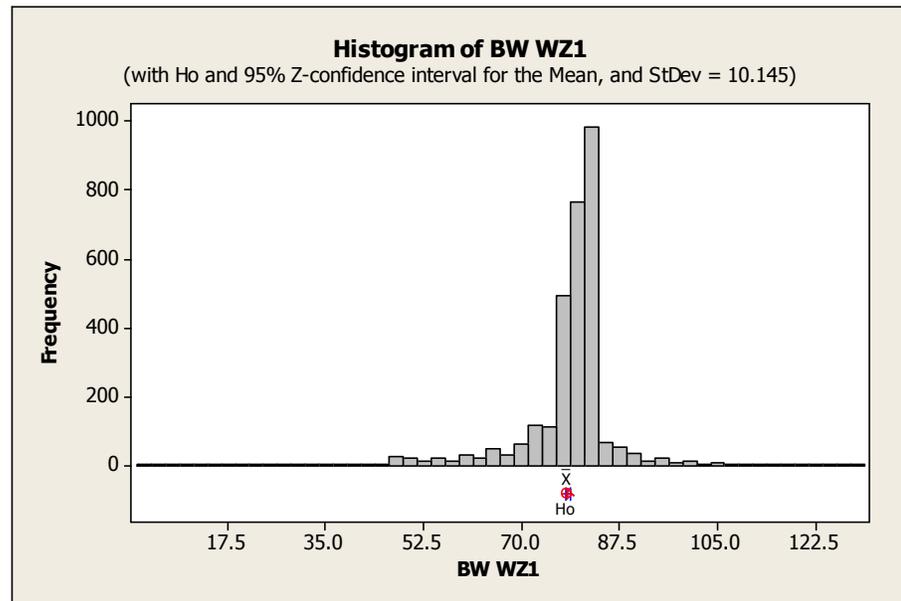
**One-Sample Z: JITTER WZ1**

Test of  $\mu = 12.429$  vs not = 12.429  
The assumed standard deviation = 5.568

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER WZ1	3021	12.4290	5.5684	0.1013	(12.2304; 12.6275)	-0.00	1.000

**Figura 4.101: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 1**

Ancho De Banda:



**Figura 4.102: Histograma de frecuencias para el ancho de banda de WING en la zona 1**

**One-Sample Z: BW WZ1**

Test of  $\mu = 78.247$  vs not = 78.247  
The assumed standard deviation = 10.145

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW WZ1	3021	78.2469	10.1452	0.1846	(77.8852; 78.6087)	-0.00	1.000

**Figura 4.103: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 1**

## b. Zona 2:

## OLSR

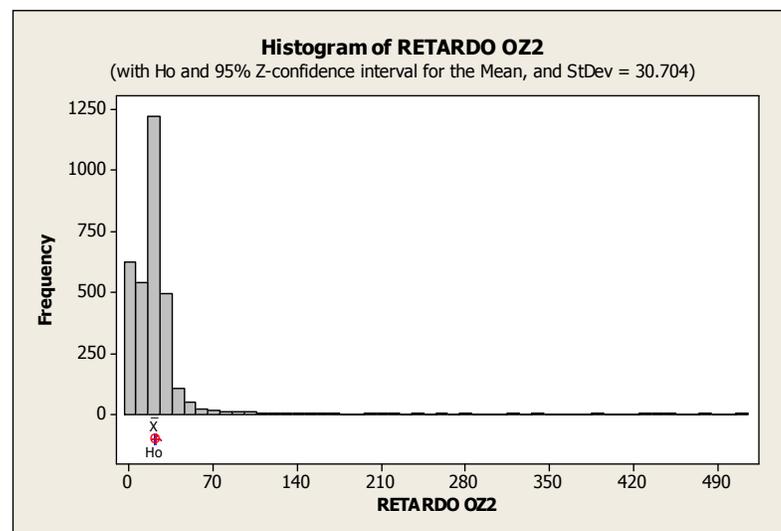
## Descriptive Statistics: RETARDO OZ2; JITTER OZ2; BW OZ2

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median	Q3
RETARDO OZ2	3131	0	20.990	0.549	30.704	0.0300	8.280	18.810	24.610
JITTER OZ2	3131	0	12.294	0.116	6.513	0.490	7.720	10.320	15.300
BW OZ2	3131	0	77.935	0.198	11.068	3.200	78.400	80.000	81.600

Variable	Maximum
RETARDO OZ2	514.230
JITTER OZ2	48.120
BW OZ2	110.400

**Figura 4.104: Información de estadística descriptiva para OLSR en la zona 2**

Retardo:



**Figura 4.105: Histograma de frecuencias para el retardo de OLSR en la zona 2**

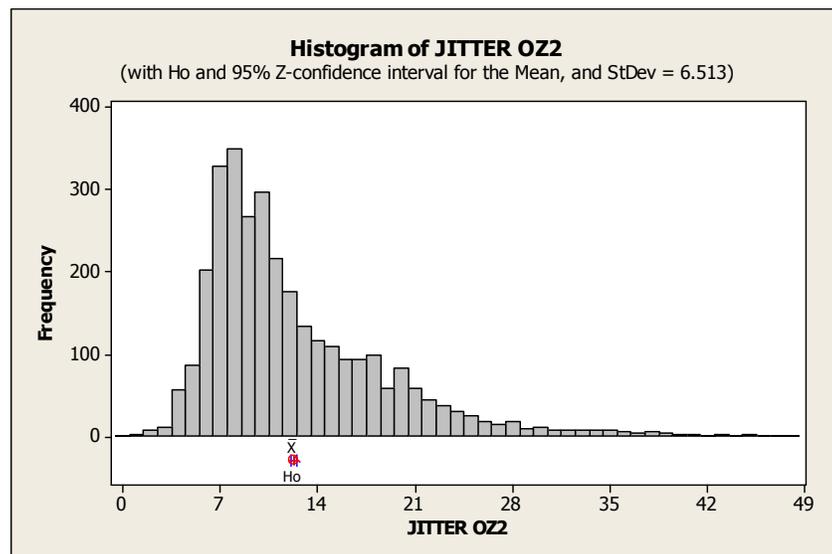
### One-Sample Z: RETARDO OZ2

Test of  $\mu = 20.99$  vs not = 20.99  
 The assumed standard deviation = 30.704

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO OZ2	3131	20.9904	30.7041	0.5487	(19.9149; 22.0658)	0.00	0.999

**Figura 4.106: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 2**

Jitter:



**Figura 4.107: Histograma de frecuencias para el jitter de OLSR en la zona 2**

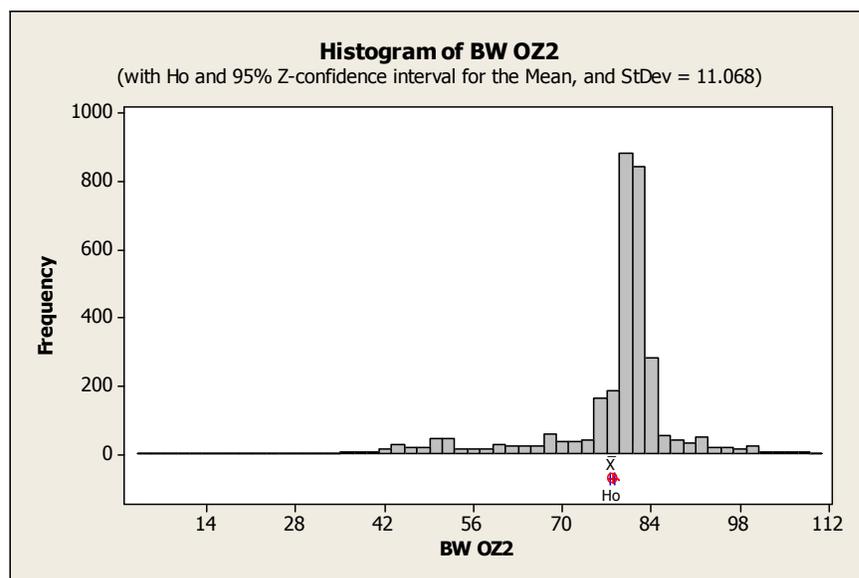
**One-Sample Z: JITTER OZ2**

Test of  $\mu = 12.294$  vs not = 12.294  
 The assumed standard deviation = 6.513

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER OZ2	3131	12.2936	6.5127	0.1164	(12.0655; 12.5218)	-0.00	0.998

**Figura 4.108: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 2**

Ancho De Banda:



**Figura 4.109: Histograma de frecuencias para el ancho de banda de OLSR en la zona 2**

**One-Sample Z: BW OZ2**

Test of mu = 77.935 vs not = 77.935  
 The assumed standard deviation = 11.068

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW OZ2	3131	77.9350	11.0683	0.1978	(77.5473; 78.3227)	-0.00	1.000

**Figura 4.110: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 2**

**BATMAN****Descriptive Statistics: RETARDO BZ2; JITTER BZ2; BW BZ2**

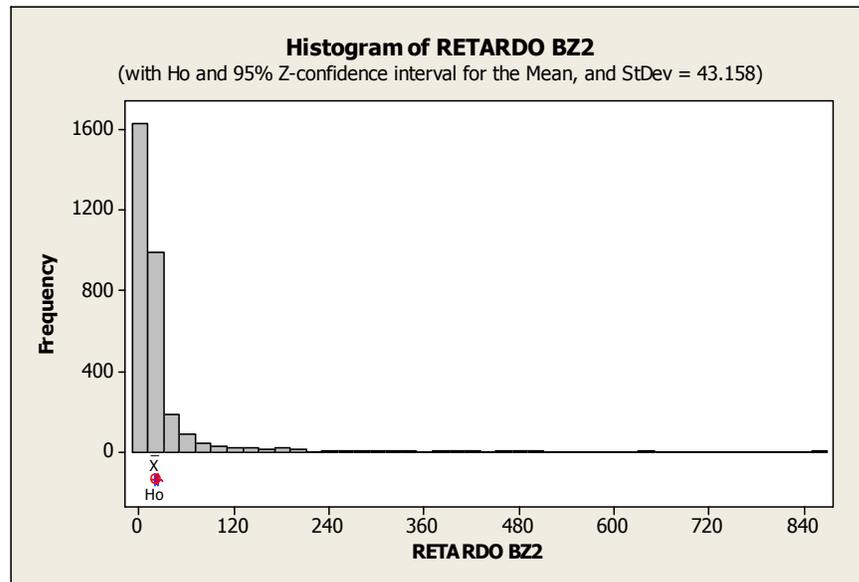
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO BZ2	3045	0	20.221	0.782	43.158	0.0000000000	2.485	8.340
JITTER BZ2	3045	0	19.288	0.210	11.574	1.250	12.850	18.410
BW BZ2	3045	0	85.855	0.562	31.021	3.200	75.200	80.000

Variable	Q3	Maximum
RETARDO BZ2	21.055	857.970
JITTER BZ2	23.370	132.470
BW BZ2	89.600	227.200

**Figura 4.111: Información de estadística descriptiva para BATMAN en la zona 2**

Retardo:



**Figura 4.112: Histograma de frecuencias para el retardo de BATMAN en la zona 2**

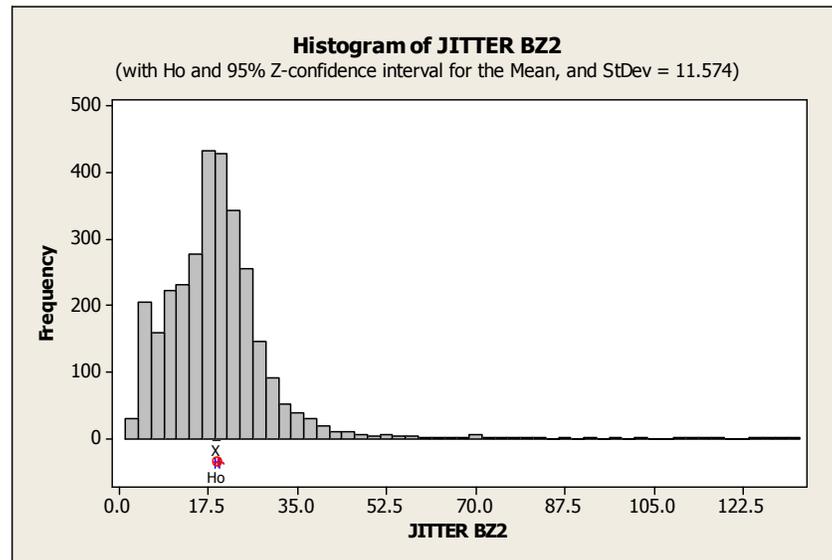
**One-Sample Z: RETARDO BZ2**

Test of  $\mu = 20.221$  vs not = 20.221  
The assumed standard deviation = 43.158

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO BZ2	3045	20.2205	43.1583	0.7821	(18.6876; 21.7534)	-0.00	0.999

**Figura 4.113: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 2**

Jitter:



**Figura 4.114: Histograma de frecuencias para el jitter de BATMAN en la zona 2**

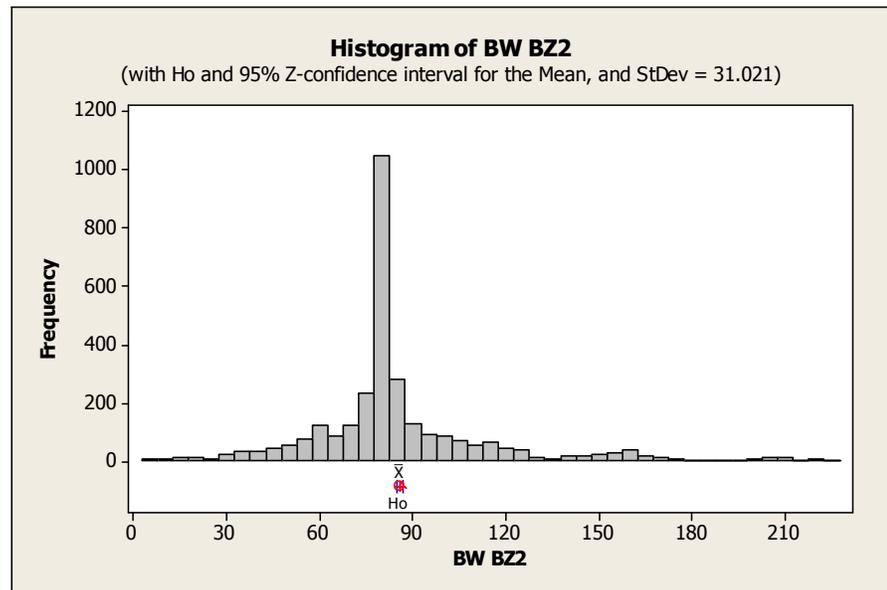
#### One-Sample Z: JITTER BZ2

Test of  $\mu = 19.288$  vs not = 19.288  
The assumed standard deviation = 11.574

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER BZ2	3045	19.2885	11.5743	0.2097	(18.8774; 19.6995)	0.00	0.998

**Figura 4.115: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 2**

Ancho De Banda:



**Figura 4.116: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 2**

**One-Sample Z: BW BZ2**

Test of  $\mu = 85.855$  vs not = 85.855  
The assumed standard deviation = 31.021

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW BZ2	3045	85.8546	31.0205	0.5622	(84.7528; 86.9564)	-0.00	0.999

**Figura 4.117: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 2**

## ROOFNET

### Descriptive Statistics: RETARDO RZ2; JITTER RZ2; BW RZ2

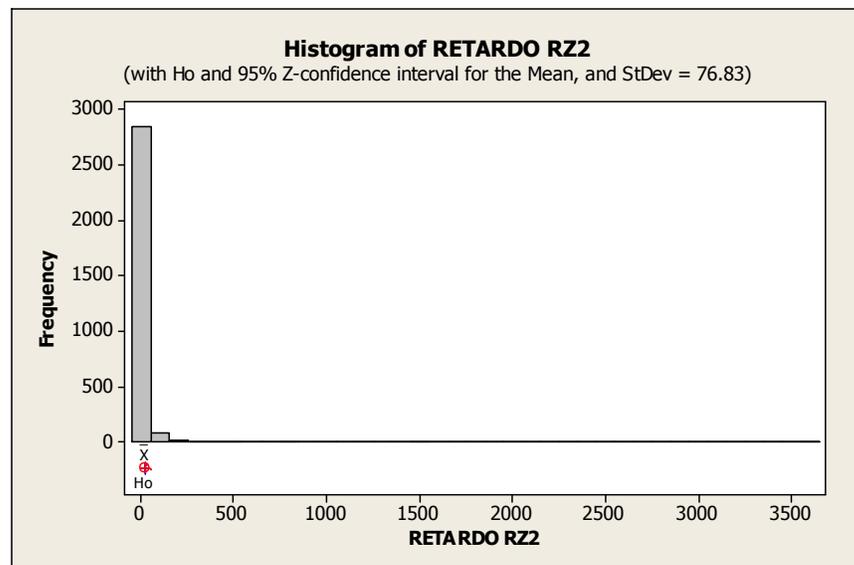
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO RZ2	2942	0	20.76	1.42	76.83	0.000000000	7.09	17.03
JITTER RZ2	2942	0	13.592	0.285	15.461	0.580	7.860	10.610
BW RZ2	2942	0	89.623	0.912	49.458	1.600	78.400	80.000

Variable	Q3	Maximum
RETARDO RZ2	24.11	3588.68
JITTER RZ2	15.525	273.310
BW RZ2	83.200	371.200

**Figura 4.118: Información de estadística descriptiva para ROOFNET en la zona 2**

Retardo:



**Figura 4.119: Histograma de frecuencias para el retardo de ROOFNET en la zona 2**

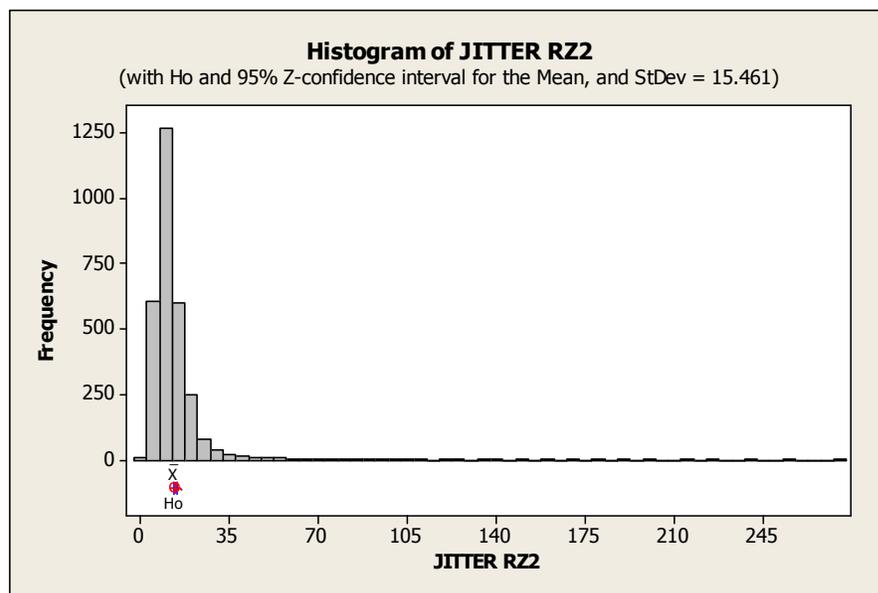
### One-Sample Z: RETARDO RZ2

Test of  $\mu = 20.76$  vs not = 20.76  
 The assumed standard deviation = 76.83

Variable	N	Mean	StDev	SE Mean	95% CI	Z
RETARDO RZ2	2942	20.7568	76.8271	1.4165	(17.9805; 23.5330)	-0.00 0.9

**Figura 4.120: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 2**

Jitter:



**Figura 4.121: Histograma de frecuencias para el jitter de ROOFNET en la zona 2**

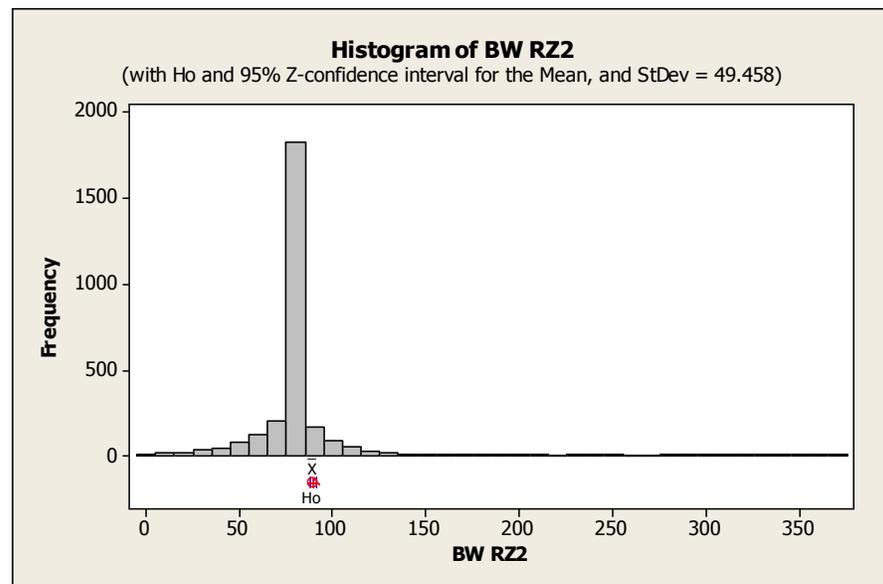
### One-Sample Z: JITTER RZ2

Test of  $\mu = 13.592$  vs not = 13.592  
 The assumed standard deviation = 15.461

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER RZ2	2942	13.5923	15.4609	0.2850	(13.0336; 14.1509)	0.00	0.999

**Figura 4.122: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 2**

Ancho De Banda:



**Figura 4.123: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 2**

### One-Sample Z: BW RZ2

Test of mu = 89.623 vs not = 89.623  
The assumed standard deviation = 49.458

Variable	N	Mean	StDev	SE Mean	95% CI	Z
BW RZ2	2942	89.6234	49.4580	0.9118	(87.8362; 91.4105)	0.00

**Figura 4.124: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 2**

### WING

#### Descriptive Statistics: RETARDO WZ2; JITTER WZ2; BW WZ2

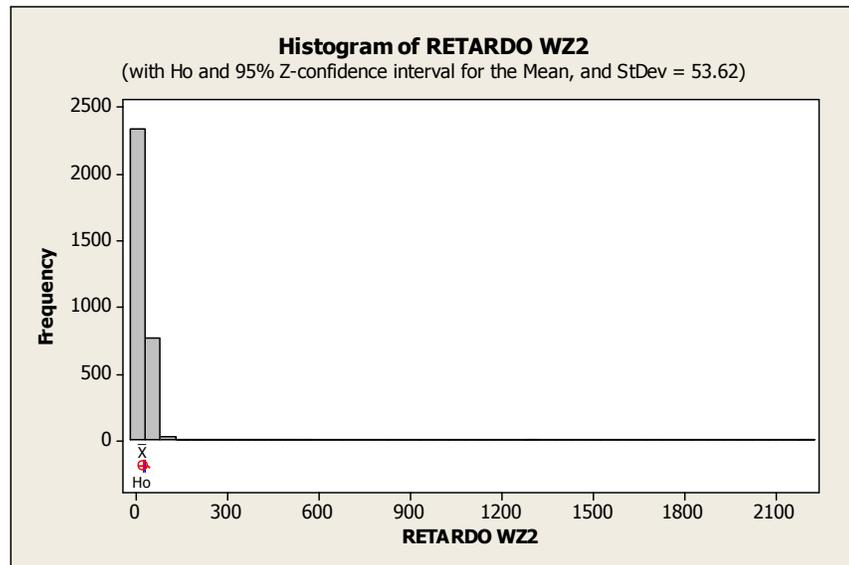
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO WZ2	3154	0	20.31	0.955	53.62	0.000000000	0.828	16.58
JITTER WZ2	3154	0	15.898	0.201	11.268	0.810	10.745	14.010
BW WZ2	3154	0	86.551	0.705	39.610	1.600	78.400	80.000

Variable	Q3	Maximum
RETARDO WZ2	25.59	2188.39
JITTER WZ2	18.578	195.030
BW WZ2	83.200	321.600

**Figura 4.125: Información de estadística descriptiva para WING en la zona 2**

Retardo:



**Figura 4.126: Histograma de frecuencias para el retardo de WING en la zona 2**

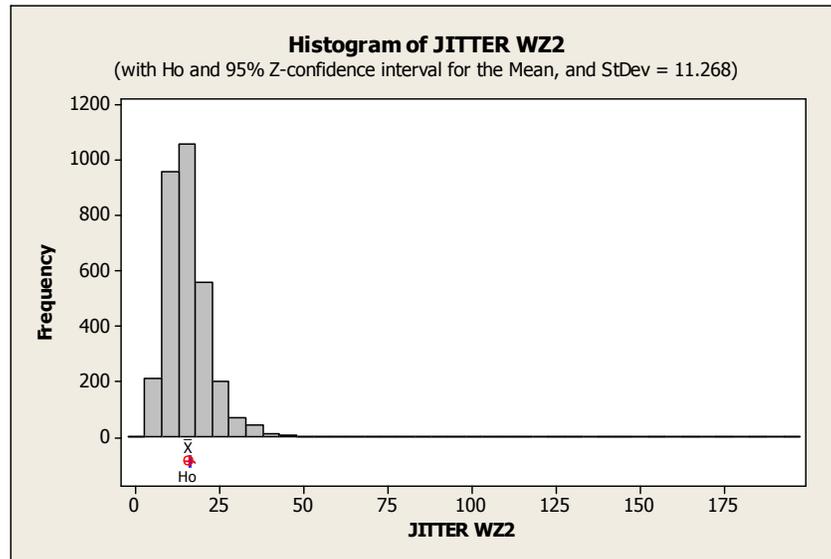
#### One-Sample Z: RETARDO WZ2

Test of  $\mu = 20.31$  vs not = 20.31  
The assumed standard deviation = 53.62

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO WZ2	3154	20.3135	53.6234	0.9548	(18.4422; 22.1848)	0.00	0.997

**Figura 4.127: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 2**

Jitter:



**Figura 4.128: Histograma de frecuencias para el jitter de WING en la zona 2**

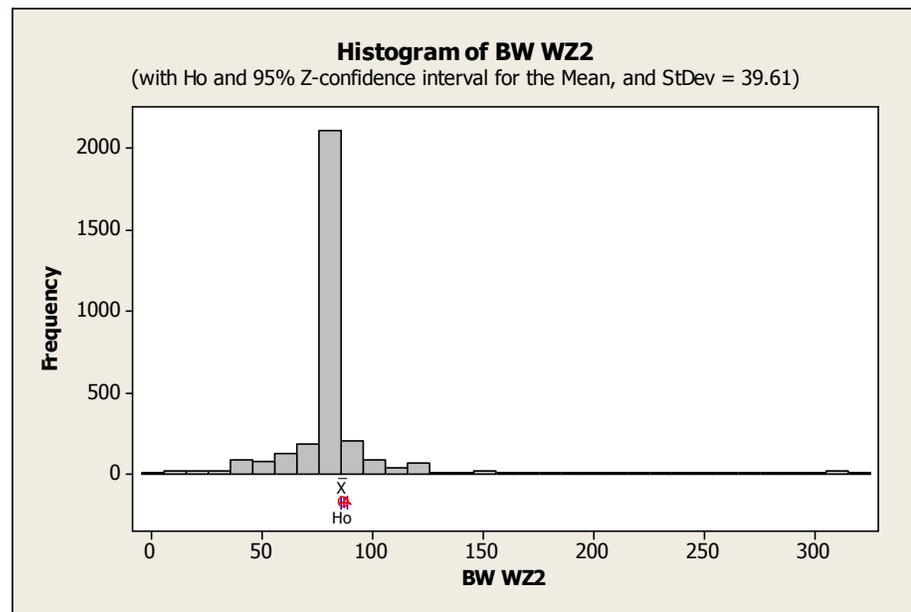
#### One-Sample Z: JITTER WZ2

Test of  $\mu = 15.898$  vs not = 15.898  
The assumed standard deviation = 11.268

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER WZ2	3154	15.8984	11.2685	0.2006	(15.5051; 16.2916)	0.00	0.999

**Figura 4.129: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 2**

Ancho de Banda:



**Figura 4.130: Histograma de frecuencias para el ancho de banda de WING en la zona 2**

**One-Sample Z: BW WZ2**

Test of  $\mu = 86.551$  vs not = 86.551  
The assumed standard deviation = 39.61

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW WZ2	3154	86.5507	39.6101	0.7053	(85.1683; 87.9330)	-0.00	1.000

**Figura 4.131: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 2**

## c. Zona 3:

## OLSR

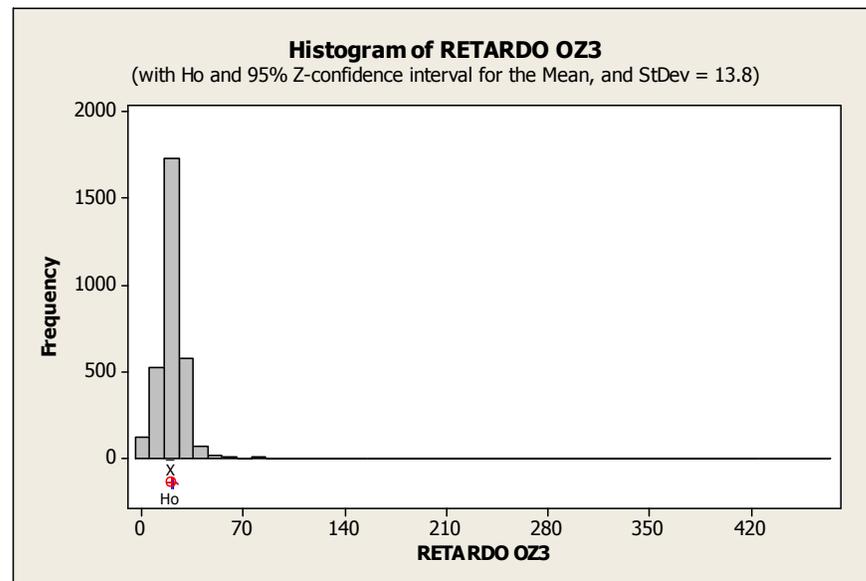
## Descriptive Statistics: RETARDO BZ3; JITTER BZ3; BW BZ3

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO BZ3	3012	0	20.124	0.215	11.775	0.000000000	17.563	20.010
JITTER BZ3	3012	0	5.3705	0.0722	3.9612	0.4400	2.8100	4.3500
BW BZ3	3012	0	79.788	0.123	6.723	3.200	80.000	80.000

Variable	Q3	Maximum
RETARDO BZ3	22.838	410.090
JITTER BZ3	6.4100	29.4900
BW BZ3	81.600	96.000

**Figura 4.132: Información de estadística descriptiva para OLSR en la zona 3**

Retardo:



**Figura 4.133: Histograma de frecuencias para el retardo de OLSR en la zona 3**

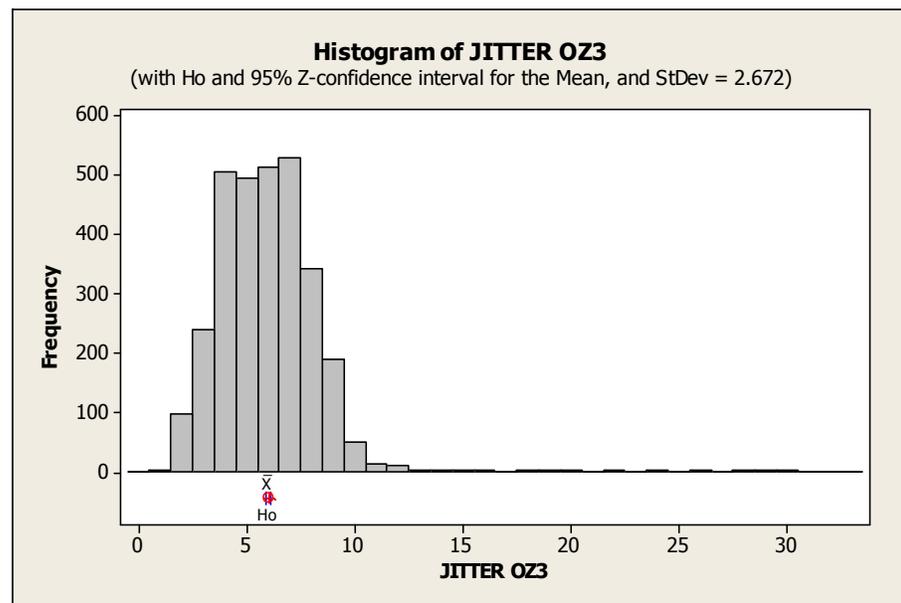
### One-Sample Z: RETARDO OZ3

Test of  $\mu = 20.283$  vs not = 20.283  
 The assumed standard deviation = 13.8

Variable	N	Mean	StDev	SE Mean	95% CI	Z
RETARDO OZ3	3038	20.2826	13.7996	0.2504	(19.7918; 20.7733)	-0.00

**Figura 4.134: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 3**

Jitter:



**Figura 4.135: Histograma de frecuencias para el jitter de OLSR en la zona 3**

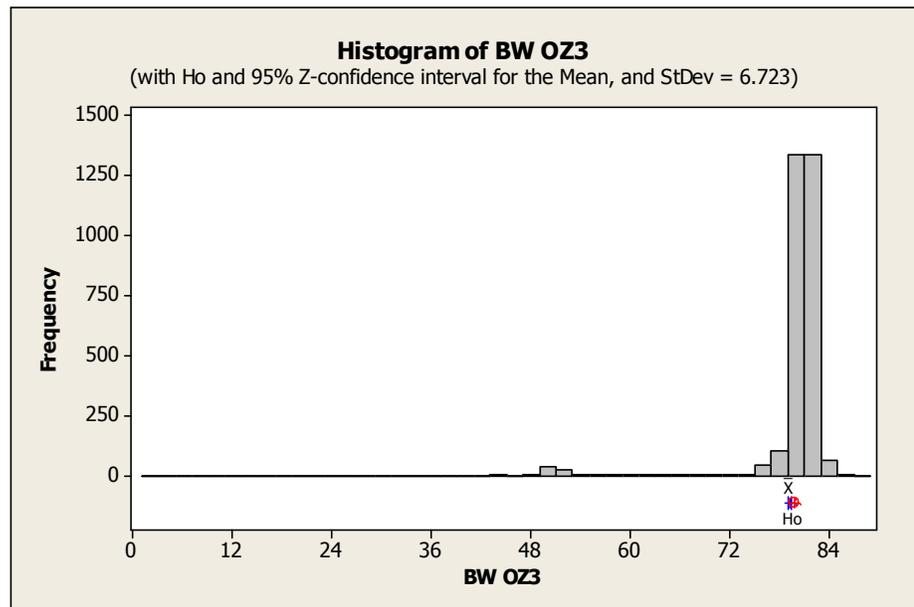
**One-Sample Z: JITTER OZ3**

Test of  $\mu = 6.0134$  vs not = 6.0134  
 The assumed standard deviation = 2.672

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER OZ3	3038	6.01342	2.67200	0.04848	(5.91841; 6.10843)	0.00	1.000

**Figura 4.136: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 3**

Ancho de Banda:



**Figura 4.137: Histograma de frecuencias para el ancho de banda de OLSR en la zona 3**

**One-Sample Z: BW OZ3**

Test of mu = 79.788 vs not = 79.788  
 The assumed standard deviation = 6.723

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW OZ3	3039	79.2376	7.5707	0.1220	(78.9986; 79.4767)	-4.51	0.000

**Figura 4.138: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 3**

**BATMAN****Descriptive Statistics: RETARDO BZ3; JITTER BZ3; BW BZ3**

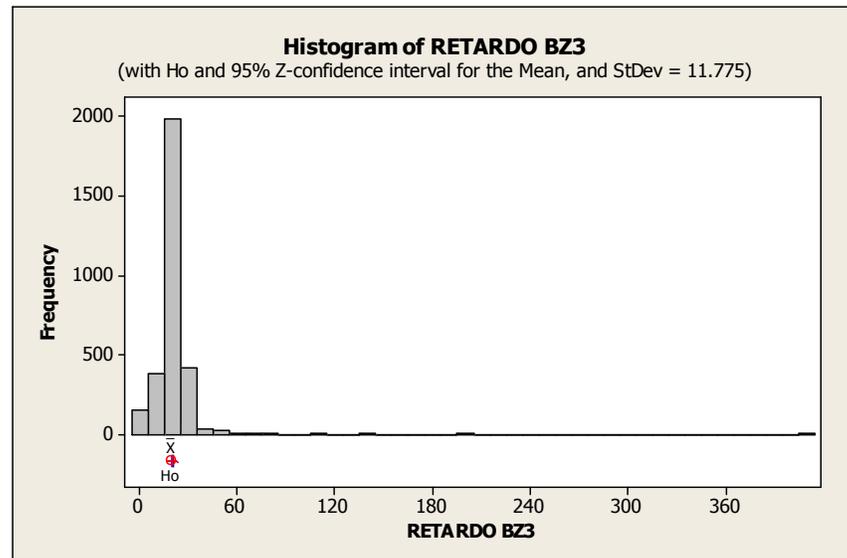
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO BZ3	3012	0	20.124	0.215	11.775	0.000000000	17.563	20.010
JITTER BZ3	3012	0	5.3705	0.0722	3.9612	0.4400	2.8100	4.3500
BW BZ3	3012	0	79.788	0.123	6.723	3.200	80.000	80.000

Variable	Q3	Maximum
RETARDO BZ3	22.838	410.090
JITTER BZ3	6.4100	29.4900
BW BZ3	81.600	96.000

**Figura 4.139: Información de estadística descriptiva para BATMAN en la zona 3**

Retardo:



**Figura 4.140: Histograma de frecuencias para el retardo de BATMAN en la zona 3**

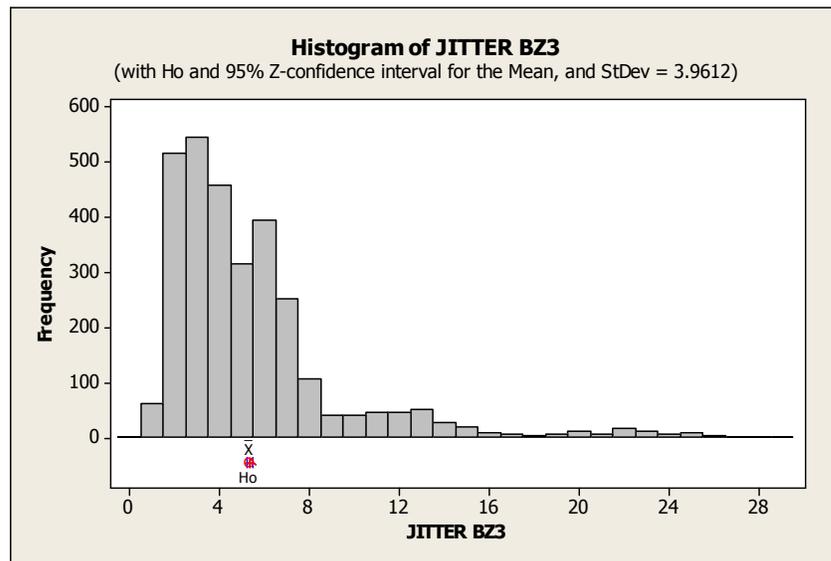
#### One-Sample Z: RETARDO BZ3

Test of  $\mu = 20.124$  vs not = 20.124  
The assumed standard deviation = 11.775

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO BZ3	3012	20.1241	11.7753	0.2146	(19.7036; 20.5446)	0.00	1.000

**Figura 4.141: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 3**

Jitter:



**Figura 4.142: Histograma de frecuencias para el jitter de BATMAN en la zona 3**

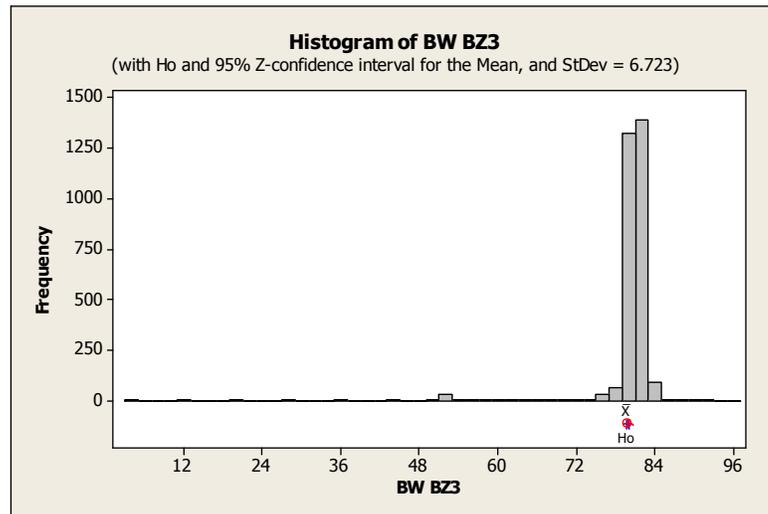
#### One-Sample Z: JITTER BZ3

Test of  $\mu = 5.3705$  vs not = 5.3705  
The assumed standard deviation = 3.9612

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER BZ3	3012	5.37052	3.96119	0.07218	(5.22906; 5.51199)	0.00	1.000

**Figura 4.143: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 3**

Ancho de Banda:



**Figura 4.144: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 3**

#### One-Sample Z: BW BZ3

Test of  $\mu = 79.788$  vs not = 79.788  
The assumed standard deviation = 6.723

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW BZ3	3012	79.7880	6.7230	0.1225	(79.5480; 80.0281)	0.00	1.000

**Figura 4.145: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 3**

## ROOFNET

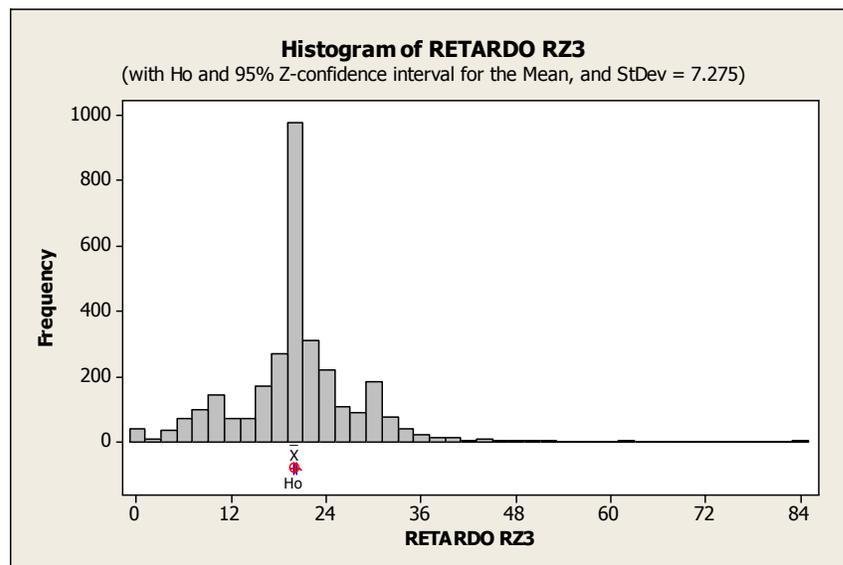
### Descriptive Statistics: RETARDO RZ3; JITTER RZ3; BW RZ3

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO RZ3	3024	0	19.998	0.132	7.275	0.000000000	17.453	20.050
JITTER RZ3	3024	0	4.9118	0.0236	1.2982	0.1300	3.9700	4.8000
BW RZ3	3024	0	80.156	0.106	5.808	3.200	80.000	80.000

Variable	Q3	Maximum
RETARDO RZ3	23.095	84.670
JITTER RZ3	5.7475	10.0500
BW RZ3	81.600	84.800

**Figura 4.146: Información de estadística descriptiva para ROOFNET en la zona 3**

Retardo:



**Figura 4.147: Histograma de frecuencias para el retardo de ROOFNET en la zona 3**

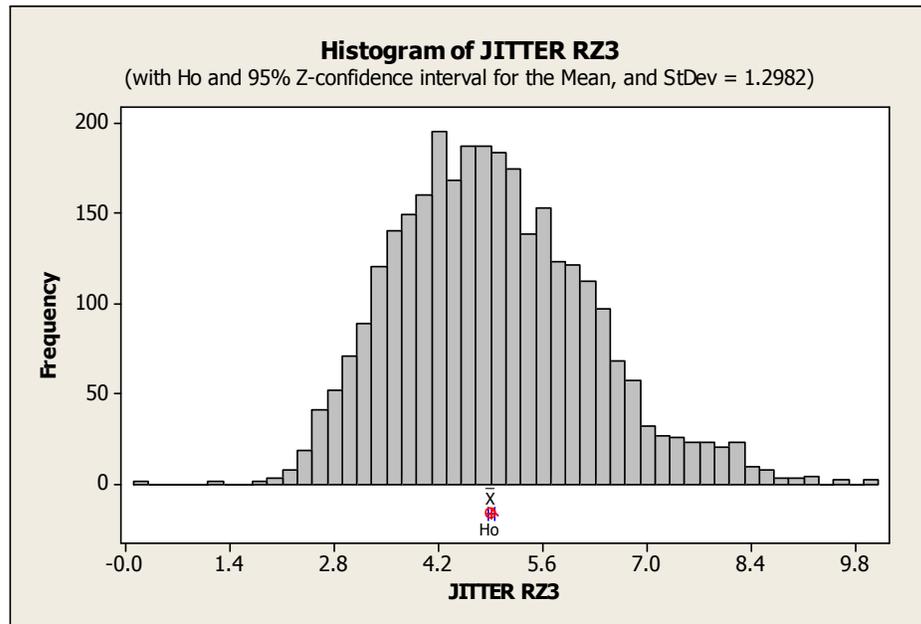
**One-Sample Z: RETARDO RZ3**

Test of  $\mu = 19.998$  vs not = 19.998  
 The assumed standard deviation = 7.275

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO RZ3	3024	19.9977	7.2754	0.1323	(19.7384; 20.2570)	-0.00	0.998

**Figura 4.148: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 3**

Jitter:



**Figura 4.149: Histograma de frecuencias para el jitter de ROOFNET en la zona 3**

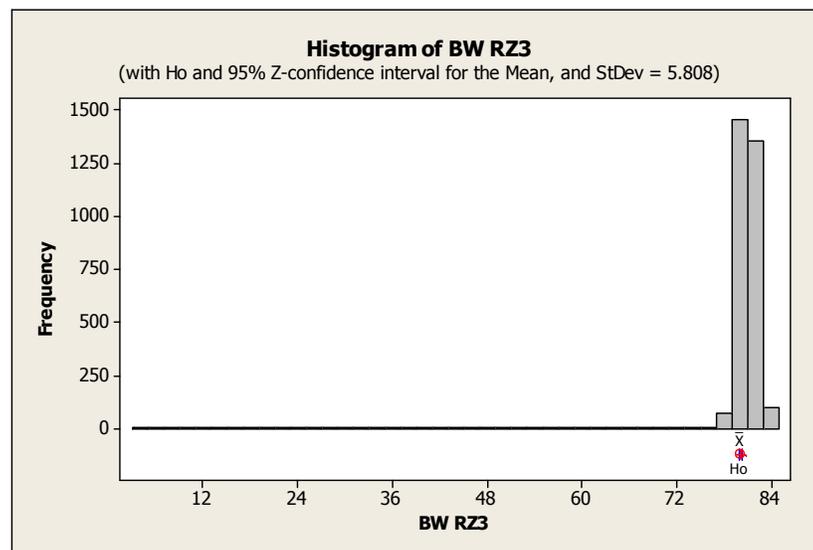
### One-Sample Z: JITTER RZ3

Test of  $\mu = 4.9118$  vs not = 4.9118  
 The assumed standard deviation = 1.2982

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER RZ3	3024	4.91182	1.29822	0.02361	(4.86555; 4.95809)	0.00	0.999

**Figura 4.150: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 3**

Ancho de Banda:



**Figura 4.151: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 3**

**One-Sample Z: BW RZ3**

Test of mu = 80.156 vs not = 80.156  
 The assumed standard deviation = 5.808

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW RZ3	3024	80.1556	5.8081	0.1056	(79.9485; 80.3626)	-0.00	0.997

**Figura 4.152: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 3**

**WING****Descriptive Statistics: RETARDO WZ3; JITTER WZ3; BW WZ3**

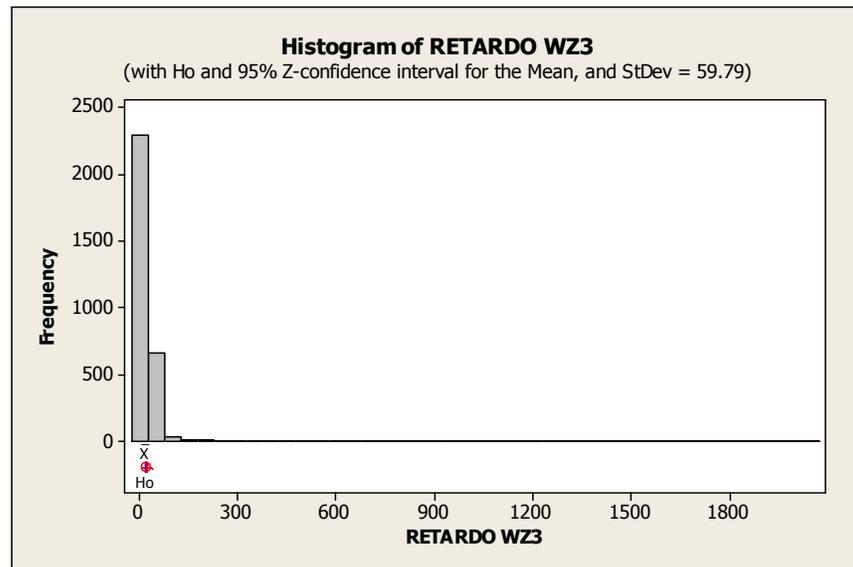
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO WZ3	3035	0	20.31	1.09	59.79	0.000000000	0.0100	11.84
JITTER WZ3	3035	0	18.979	0.211	11.612	1.250	12.870	16.480
BW WZ3	3035	0	85.338	0.575	31.690	1.600	76.800	80.000

Variable	Q3	Maximum
RETARDO WZ3	24.51	2050.66
JITTER WZ3	21.470	135.360
BW WZ3	84.800	244.800

**Figura 4.153: Información de estadística descriptiva para WING en la zona 3**

Retardo:



**Figura 4.154: Histograma de frecuencias para el retardo de WING en la zona 3**

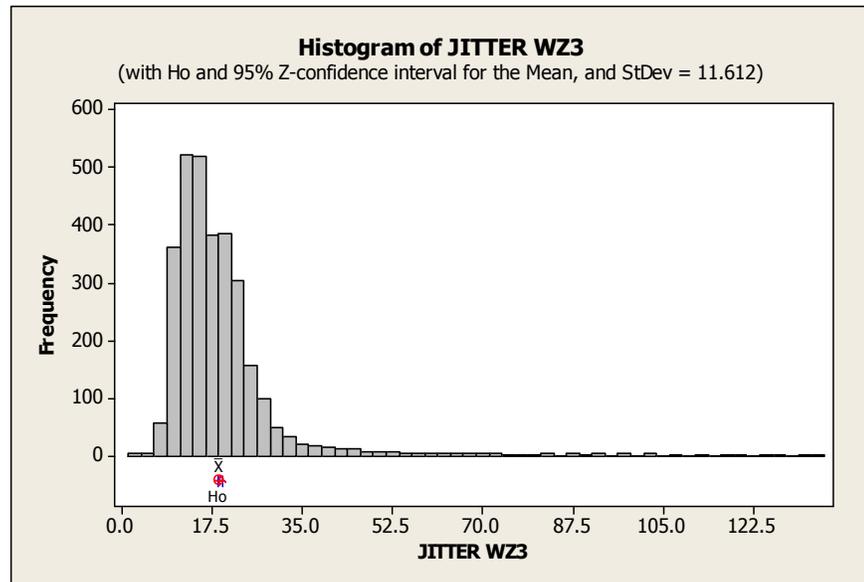
#### One-Sample Z: RETARDO WZ3

Test of  $\mu = 20.31$  vs not = 20.31  
The assumed standard deviation = 59.79

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO WZ3	3035	20.3121	59.7862	1.0853	(18.1850; 22.4393)	0.00	0.998

**Figura 4.155: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 3**

Jitter:



**Figura 4.156: Histograma de frecuencias para el jitter de WING en la zona 3**

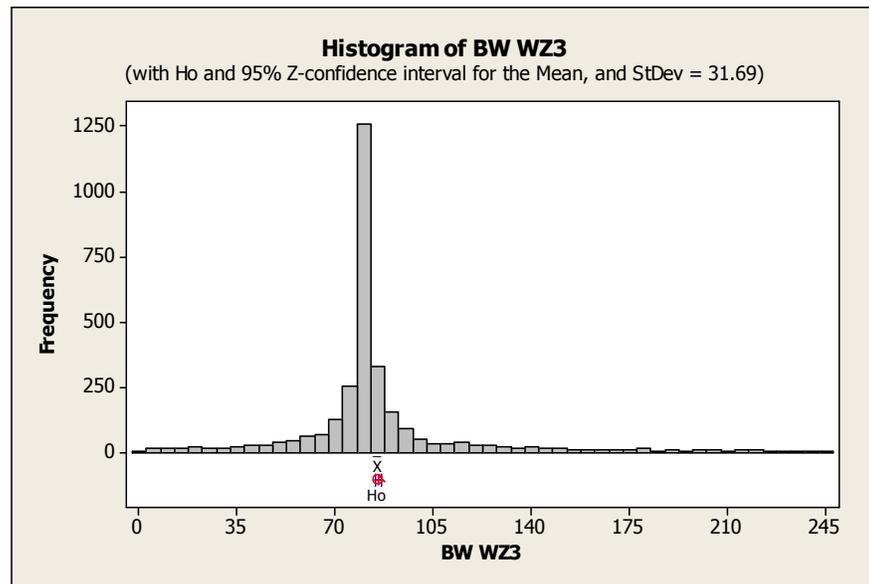
#### One-Sample Z: JITTER WZ3

Test of  $\mu = 18.979$  vs not = 18.979  
The assumed standard deviation = 11.612

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER WZ3	3035	18.9786	11.6115	0.2108	(18.5655; 19.3918)	-0.00	0.999

**Figura 4.157: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 3**

Ancho de Banda:



**Figura 4.158: Histograma de frecuencias para el ancho de banda de WING en la zona 3**

#### One-Sample Z: BW WZ3

Test of  $\mu = 85.338$  vs not = 85.338  
The assumed standard deviation = 31.69

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW WZ3	3035	85.3383	31.6898	0.5752	(84.2108; 86.4657)	0.00	1.000

**Figura 4.159: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 3**

## d. Zona 4:

## OLSR

## Descriptive Statistics: JITTER OZ4; BW OZ4; RETARDO BZ4

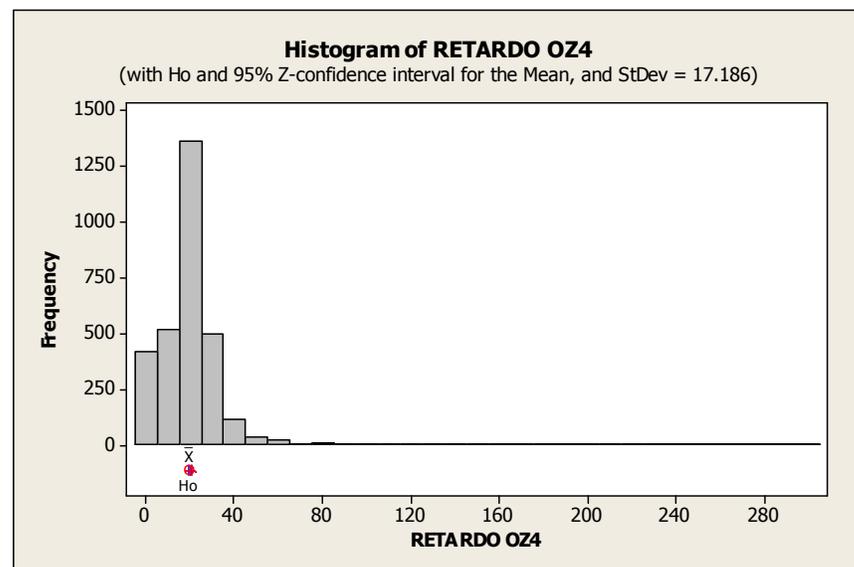
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
JITTER OZ4	3010	0	9.3241	0.0896	4.9182	0.7500	6.0800	7.9700
BW OZ4	3010	0	80.135	0.133	7.308	3.200	80.000	80.000
RETARDO BZ4	3001	0	20.115	0.506	27.744	0.000000000	7.360	18.620

Variable	Q3	Maximum
JITTER OZ4	10.9800	39.9100
BW OZ4	81.600	121.600
RETARDO BZ4	24.550	545.430

**Figura 4.160: Información de estadística descriptiva para OLSR en la zona 4**

Retardo:



**Figura 4.161: Histograma de frecuencias para el retardo de OLSR en la zona 4**

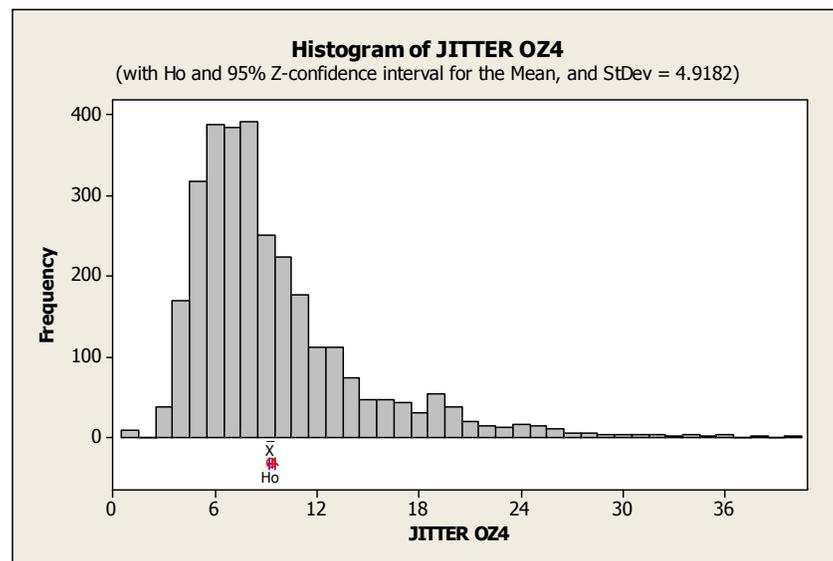
**One-Sample Z: RETARDO OZ4**

Test of  $\mu = 20.001$  vs not = 20.001  
 The assumed standard deviation = 17.186

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO OZ4	3010	20.0008	17.1858	0.3133	(19.3868; 20.6148)	-0.00	0.999

**Figura 4.162: Resultado de prueba de intervalos de confianza para el retardo de OLSR en la zona 4**

Jitter:



**Figura 4.163: Histograma de frecuencias para el jitter de OLSR en la zona 4**

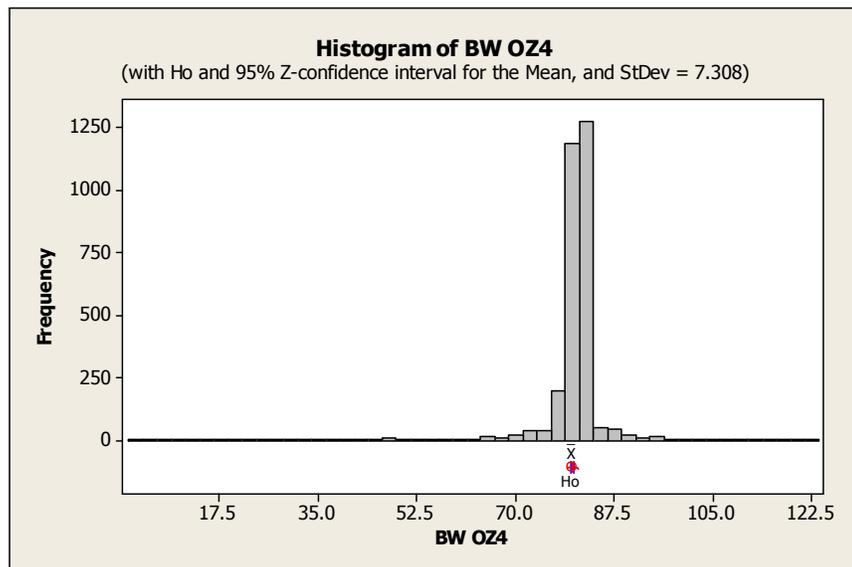
### One-Sample Z: JITTER OZ4

Test of  $\mu = 9.3241$  vs not = 9.3241  
 The assumed standard deviation = 4.9182

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER OZ4	3010	9.32409	4.91822	0.08964	(9.14839; 9.49979)	-0.00	1.000

**Figura 4.164: Resultado de prueba de intervalos de confianza para el jitter de OLSR en la zona 4**

Ancho de Banda:



**Figura 4.165: Histograma de frecuencias para el ancho de banda de OLSR en la zona 4**

**One-Sample Z: BW OZ4**

Test of mu = 80.135 vs not = 80.135  
 The assumed standard deviation = 7.308

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW OZ4	3010	80.1350	7.3079	0.1332	(79.8739; 80.3961)	0.00	1.000

**Figura 4.166: Resultado de prueba de intervalos de confianza para el ancho de banda de OLSR en la zona 4**

**BATMAN****Descriptive Statistics: RETARDO BZ4; JITTER BZ4; BW BZ4**

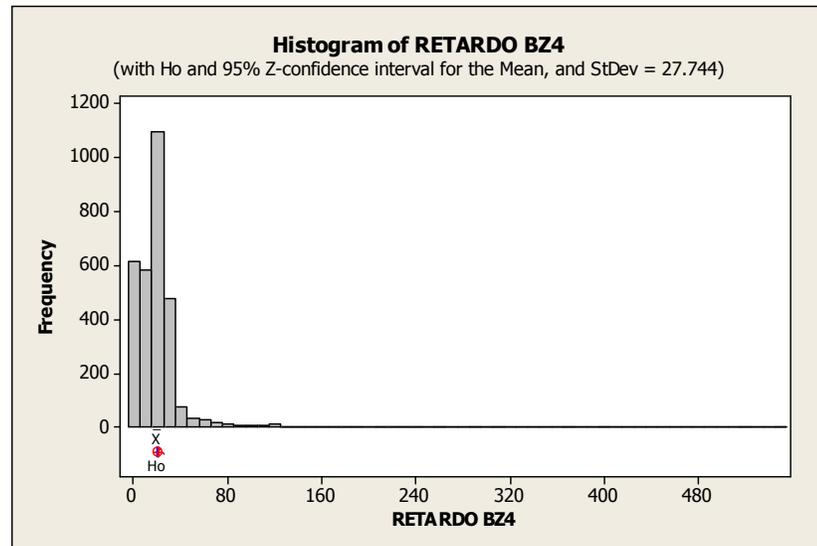
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO BZ4	3001	0	20.115	0.506	27.744	0.000000000	7.360	18.620
JITTER BZ4	3001	0	12.401	0.130	7.114	0.760	7.780	10.450
BW BZ4	3001	0	81.615	0.329	18.010	3.200	80.000	81.600

Variable	Q3	Maximum
RETARDO BZ4	24.550	545.430
JITTER BZ4	15.375	67.130
BW BZ4	81.600	188.800

**Figura 4.167: Información de estadística descriptiva para BATMAN en la zona 4**

Retardo:



**Figura 4.168: Histograma de frecuencias para el retardo de BATMAN en la zona 4**

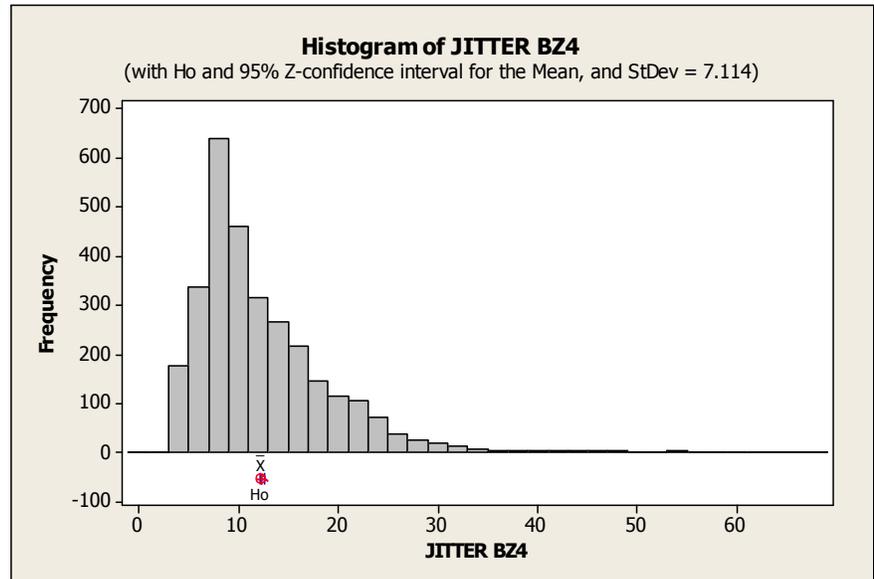
#### One-Sample Z: RETARDO BZ4

Test of  $\mu = 20.115$  vs not = 20.115  
The assumed standard deviation = 27.744

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO BZ4	3001	20.1147	27.7437	0.5064	(19.1221; 21.1073)	-0.00	1.000

**Figura 4.169: Resultado de prueba de intervalos de confianza para el retardo de BATMAN en la zona 4**

Jitter:



**Figura 4.170: Histograma de frecuencias para el jitter de BATMAN en la zona 4**

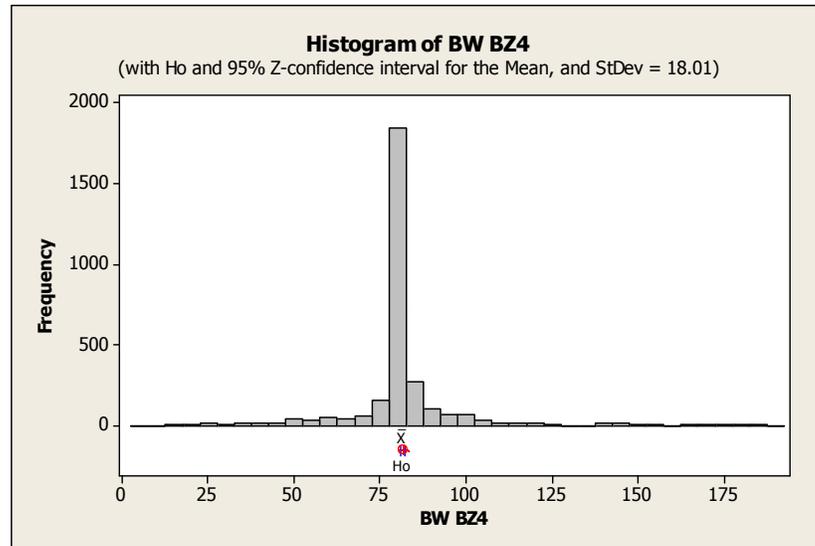
#### One-Sample Z: JITTER BZ4

Test of  $\mu = 12.401$  vs not = 12.401  
The assumed standard deviation = 7.114

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER BZ4	3001	12.4012	7.1137	0.1299	(12.1467; 12.6557)	0.00	0.999

**Figura 4.171: Resultado de prueba de intervalos de confianza para el jitter de BATMAN en la zona 4**

Ancho de Banda:



**Figura 4.172: Histograma de frecuencias para el ancho de banda de BATMAN en la zona 4**

#### One-Sample Z: BW BZ4

Test of  $\mu = 81.615$  vs not = 81.615  
The assumed standard deviation = 18.01

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW BZ4	3001	81.6155	18.0100	0.3288	(80.9711; 82.2598)	0.00	0.999

**Figura 4.173: Resultado de prueba de intervalos de confianza para el ancho de banda de BATMAN en la zona 4**

## ROOFNET

### Descriptive Statistics: RETARDO RZ4; JITTER RZ4; BW RZ4

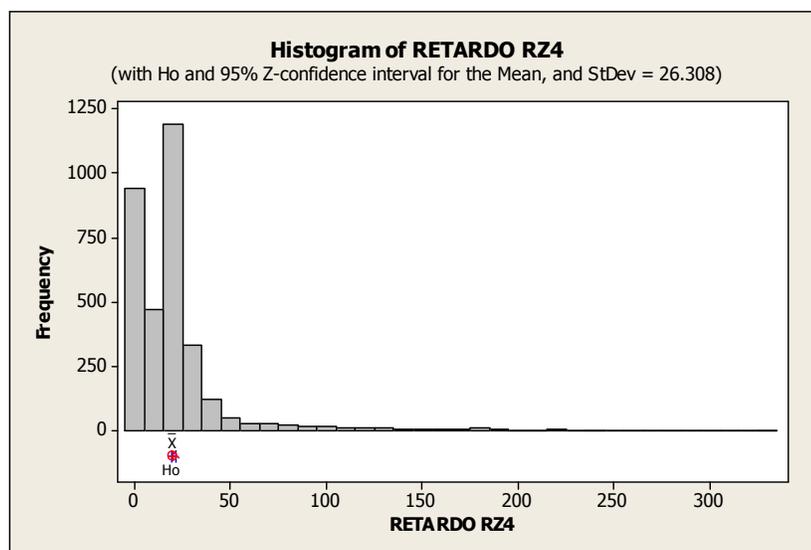
Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median
RETARDO RZ4	3279	0	20.060	0.459	26.308	0.000000000	2.870	17.230
JITTER RZ4	3279	0	14.311	0.0871	4.986	0.890	10.690	14.120
BW RZ4	3279	0	80.099	0.143	8.197	3.200	78.400	80.000

Variable	Q3	Maximum
RETARDO RZ4	23.440	334.130
JITTER RZ4	17.290	35.160
BW RZ4	81.600	108.800

**Figura 4.174: Información de estadística descriptiva para ROOFNET en la zona 4**

Retardo:



**Figura 4.175: Histograma de frecuencias para el retardo de ROOFNET en la zona 4**

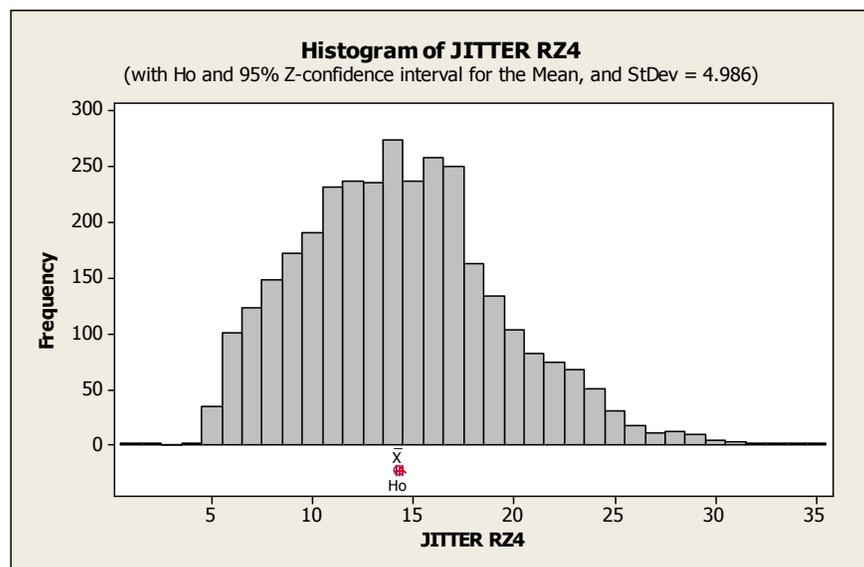
**One-Sample Z: RETARDO RZ4**

Test of  $\mu = 20.06$  vs not = 20.06  
 The assumed standard deviation = 26.308

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO RZ4	3279	20.0600	26.3085	0.4594	(19.1595; 20.9604)	-0.00	1.000

**Figura 4.176: Resultado de prueba de intervalos de confianza para el retardo de ROOFNET en la zona 4**

Jitter:



**Figura 4.177: Histograma de frecuencias para el jitter de ROOFNET en la zona 4**

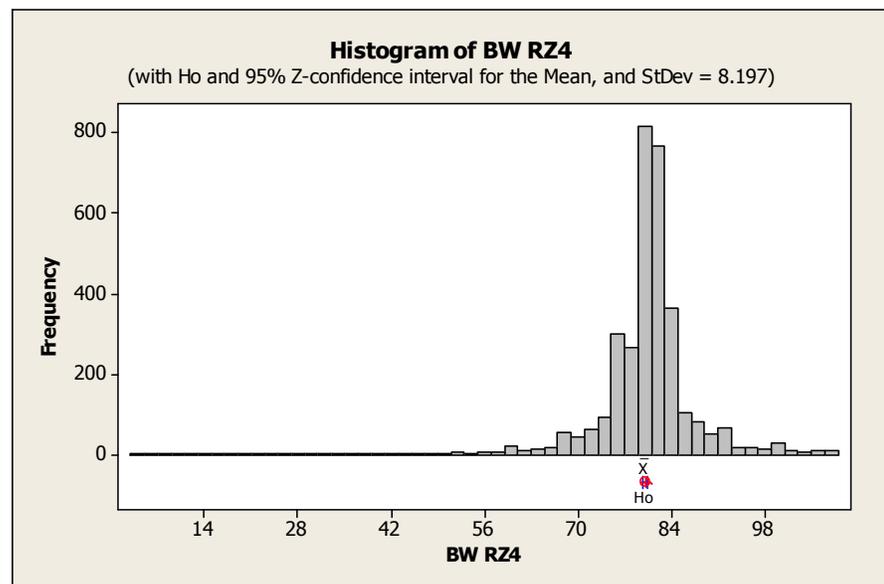
### One-Sample Z: JITTER RZ4

Test of  $\mu = 14.311$  vs not = 14.311  
 The assumed standard deviation = 4.986

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER RZ4	3279	14.3107	4.9857	0.0871	(14.1400; 14.4813)	-0.00	0.997

**Figura 4.178: Resultado de prueba de intervalos de confianza para el jitter de ROOFNET en la zona 4**

Ancho De Banda:



**Figura 4.179: Histograma de frecuencias para el ancho de banda de ROOFNET en la zona 4**

**One-Sample Z: BW RZ4**

Test of mu = 80.099 vs not = 80.099  
 The assumed standard deviation = 8.197

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW RZ4	3279	80.0986	8.1970	0.1431	(79.8180; 80.3791)	-0.00	0.998

**Figura 4.180: Resultado de prueba de intervalos de confianza para el ancho de banda de ROOFNET en la zona 4**

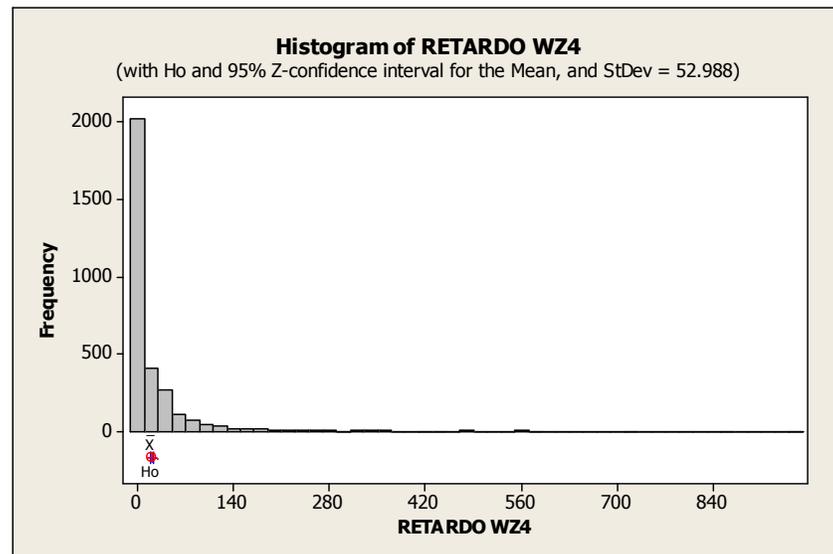
**WING****Descriptive Statistics: RETARDO WZ4; JITTER WZ4; BW WZ4**

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1
RETARDO WZ4	3030	0	20.245	0.963	52.988	0.0000000000	0.0000000000
JITTER WZ4	3030	0	26.387	0.166	9.161	1.250	20.348
BW WZ4	3030	0	85.357	0.630	34.660	3.200	65.600

Variable	Median	Q3	Maximum
RETARDO WZ4	0.0100	21.440	957.650
JITTER WZ4	23.900	29.890	81.410
BW WZ4	80.000	100.800	198.400

**Figura 4.181: Información de estadística descriptiva para WING en la zona 4**

Retardo:



**Figura 4.182: Histograma de frecuencias para el retardo de WING en la zona 4**

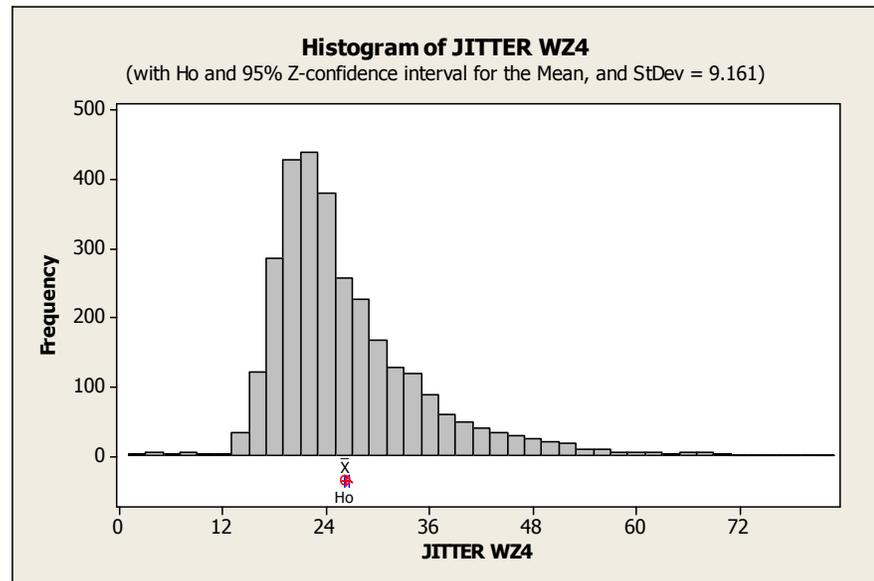
#### One-Sample Z: RETARDO WZ4

Test of  $\mu = 20.245$  vs not = 20.245  
The assumed standard deviation = 52.988

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
RETARDO WZ4	3030	20.2451	52.9883	0.9626	(18.3584; 22.1318)	0.00	1.000

**Figura 4.183: Resultado de prueba de intervalos de confianza para el retardo de WING en la zona 4**

Jitter:



**Figura 4.184: Histograma de frecuencias para el jitter de WING en la zona 4**

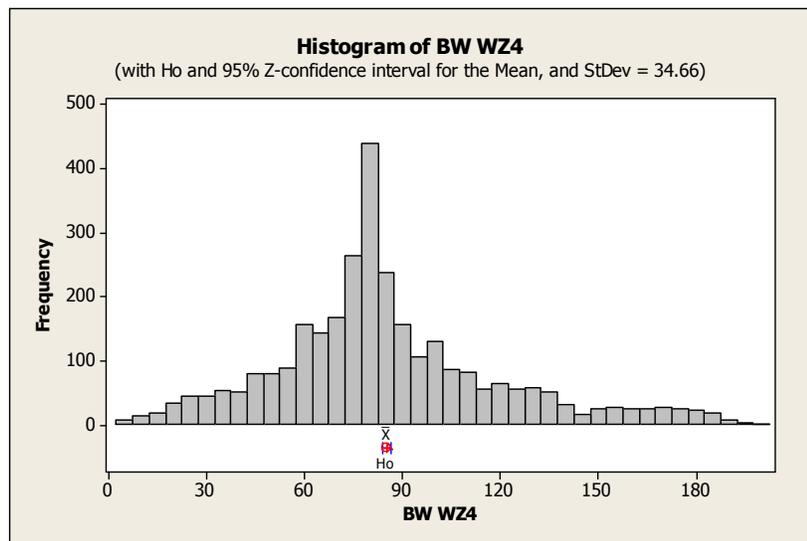
#### One-Sample Z: JITTER WZ4

Test of  $\mu = 26.387$  vs not = 26.387  
The assumed standard deviation = 9.161

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
JITTER WZ4	3030	26.3869	9.1612	0.1664	(26.0607; 26.7131)	-0.00	1.000

**Figura 4.185: Resultado de prueba de intervalos de confianza para el jitter de WING en la zona 4**

Ancho de Banda:



**Figura 4.186: Histograma de frecuencias para el ancho de banda de WING en la zona 4**

**One-Sample Z: BW WZ4**

Test of  $\mu = 85.357$  vs not = 85.357  
The assumed standard deviation = 34.66

Variable	N	Mean	StDev	SE Mean	95% CI	Z	P
BW WZ4	3030	85.3566	34.6598	0.6297	(84.1225; 86.5907)	-0.00	0.999

**Figura 4.187: Resultado de prueba de intervalos de confianza para el ancho de banda de WING en la zona 4**

# CAPITULO 5

## 5. ANÁLISIS DE LOS RESULTADOS

Del análisis estadístico de los datos capturados, se puede afirmar, con un 95% de nivel de confianza, que en la zona 1, la media poblacional de cada protocolo para cada parámetro se encuentra en los siguientes intervalos de confianza:

Retardo:

- OLSR: Entre 19.7897 ms y 20.2414 ms
- B.A.T.M.A.N.: Entre 19.7336 ms y 20.7952 ms
- Roofnet: Entre 19.7609 ms y 20.4582 ms
- W.I.N.G.: Entre 19.5543 ms y 21.5771 ms

**Jitter:**

- OLSR: Entre 3.82224 ms y 3.93179 ms
- B.A.T.M.A.N.: Entre 4.84009 ms y 5.12142 ms
- Roofnet: Entre 5.64055 ms y 5.78441 ms
- W.I.N.G.: Entre 12.2304 ms y 12.6275 ms

**Ancho de Banda:**

- OLSR: Entre 79.8613 Kbps y 80.2756 Kbps
- B.A.T.M.A.N.: Entre 79.0406 Kbps y 79.5912 Kbps
- Roofnet: Entre 79.7687 Kbps y 80.1581 Kbps
- W.I.N.G.: Entre 77.8852 Kbps y 78.6087 Kbps

De igual manera, en la zona 2 se puede afirmar con un 95% de certeza que los valores para la media poblacional de cada parámetro están en los siguientes intervalos de confianza:

**Retardo:**

- OLSR: Entre 19.9149 ms y 22.0658 ms

- B.A.T.M.A.N.: Entre 18.6876 ms y 21.7534 ms
- Roofnet: Entre 17.9805 ms y 23.5330 ms
- W.I.N.G.: Entre 18.4422 ms y 22.1848 ms

Jitter:

- OLSR: Entre 12.0655 ms y 12.5218 ms
- B.A.T.M.A.N.: Entre 18.8774 ms y 19.6995 ms
- Roofnet: Entre 13.0336 ms y 14.1509 ms
- W.I.N.G.: Entre 15.5051 ms y 16.2916 ms

Ancho de Banda:

- OLSR: Entre 77.5473 Kbps y 78.3227 Kbps
- B.A.T.M.A.N.: Entre 84.7528 Kbps y 86.9564 Kbps
- Roofnet: Entre 87.8362 Kbps y 91.4105 Kbps
- W.I.N.G.: Entre 85.1683 Kbps y 87.9330 Kbps

En la zona 3, con el mismo 95% de certeza, los valores de las medias poblacionales se encuentran en los siguientes intervalos de confianza:

Retardo:

- OLSR: Entre 19.7918 ms y 20.7733 ms
- B.A.T.M.A.N.: Entre 19.7036 ms y 20.5446 ms
- Roofnet: Entre 19.7384 ms y 20.2570 ms
- W.I.N.G.: Entre 18.1850 ms y 22.4393 ms

Jitter:

- OLSR: Entre 5.91841 ms y 6.10843 ms
- B.A.T.M.A.N.: Entre 5.22906 ms y 5.51199 ms
- Roofnet: Entre 4.86555 ms y 4.95809 ms
- W.I.N.G.: Entre 18.5655 ms y 19.3918 ms

Ancho de Banda:

- OLSR: Entre 78.9986 Kbps y 79.4767 Kbps
- B.A.T.M.A.N.: Entre 79.5480 Kbps y 80.0281 Kbps
- Roofnet: Entre 79.9485 Kbps y 80.3626 Kbps
- W.I.N.G.: Entre 84.2108 Kbps y 86.4657 Kbps

Finalmente, con un 95% de certeza, en la zona 4 los valores de la media poblacional de cada parámetro, se ubican en los siguientes intervalos de confianza:

Retardo:

- OLSR: Entre 19.3868 ms y 20.6148 ms
- B.A.T.M.A.N.: Entre 19.1221 ms y 21.1073 ms
- Roofnet: Entre 19.1595 ms y 20.9604 ms
- W.I.N.G.: Entre 18.3584 ms y 22.1318ms

Jitter:

- OLSR: Entre 9.14839 ms y 9.49979 ms
- B.A.T.M.A.N.: Entre 12.1467 ms y 12.6557 ms
- Roofnet: Entre 14.1400 ms y 14.4813 ms
- W.I.N.G.: Entre 26.0607 ms y 26.7131 ms

Ancho de Banda:

- OLSR: Entre 79.8739 Kbps y 80.3961 Kbps
- B.A.T.M.A.N.: Entre 80.9711 Kbps y 82.2598 Kbps

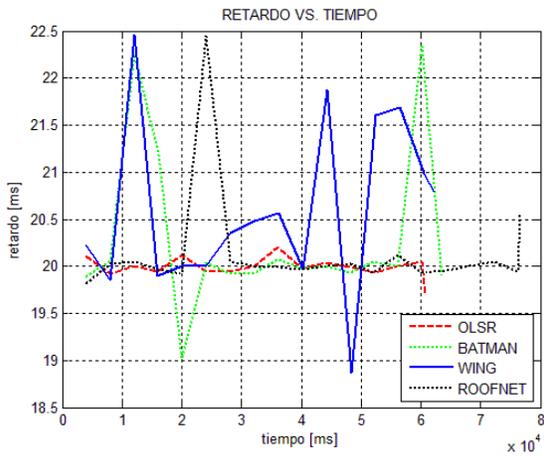
- Roofnet: Entre 79.8180 Kbps y 80.3791 Kbps
- W.I.N.G.: Entre 84.1225 Kbps y 86.5907 Kbps

Este análisis estadístico de intervalos de confianza para la estimación de la media poblacional a partir de los datos extraídos de una muestra (los datos que se capturaron con Wireshark) se realizó con ayuda de la herramienta MINITAB, tal como se muestra a detalle en el capítulo anterior en las figuras 4.76 a 4.187.

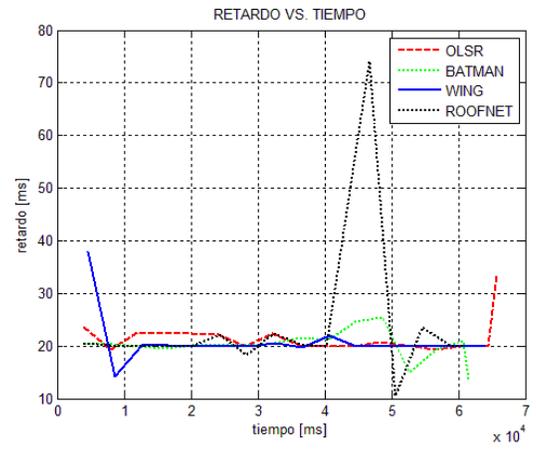
### **5.1 Análisis comparativo de los protocolos proactivos y reactivos en la red implementada**

A continuación se detalla el análisis de los parámetros jitter, ancho de banda, retardo y pérdida de paquetes para determinar cuál es el protocolo más eficiente. Para ello, se elaboraron gráficas y tablas que permiten visualizar estos resultados :

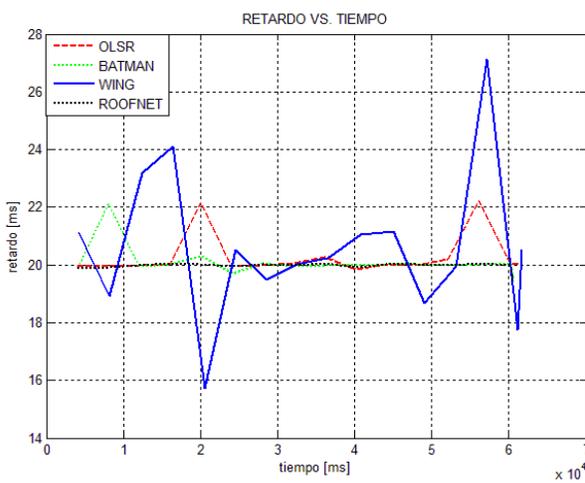
**Retardo:**



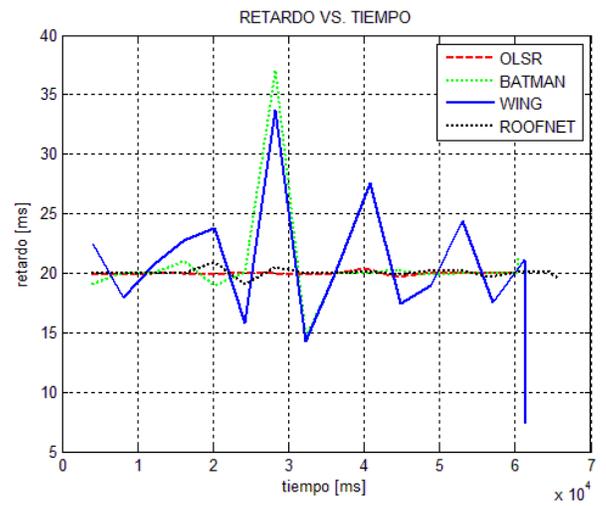
**Figura 5.1: Retardo en Zona 1**



**Figura 5.2: Retardo en Zona 2**



**Figura 5.3: Retardo en Zona 3**



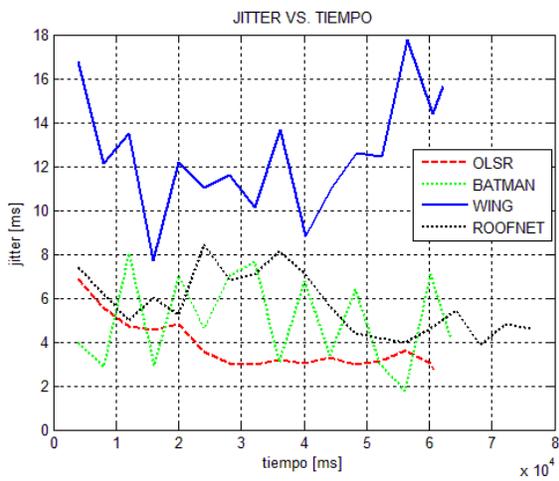
**Figura 5.4: Retardo en Zona 4**

Como se puede apreciar en las Figuras 5.1, 5.2, 5.3 y 5.4, OLSR tiene valores de retardo más estables, estando los mismos en valores muy próximos a 20ms en cada zona. Roofnet presenta valores de retardo muy estables y similares a los obtenidos con OLSR en las zonas 3 (Figura 5.3) y zona 4 (Figura 5.4), pero no así en las zonas 1 (Figura 5.1) y zona 2 (Figura 5.2) donde hay momentos en que esto cambia más notoriamente.

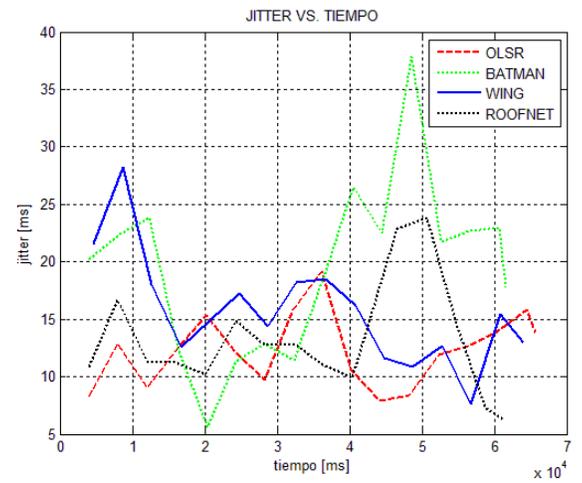
WING en casi todas las zonas muestra valores cambiantes de retardo, desde casi 16ms hasta aproximadamente 27ms, dependiendo de la zona observada; únicamente en la zona 2 (Figura 5.2) muestra retardo estable.

BATMAN, finalmente, tiene pocos picos de retardo y, en promedio, muestra niveles bajos en cada zona, pero aún así no llega a los valores que se muestran con OLSR. En términos generales, y obviando ciertos valores que pueden ser considerados como datos aberrantes, como por ejemplo el punto de Roofnet entre los 4 y los 5 segundos de llamada en la zona 2 (Figura 5.2), cada protocolo se maneja con valores bastante aceptables de retardo, recordando que se recomienda que para aplicaciones de VoIP estos valores sean menores a los 150 ms.

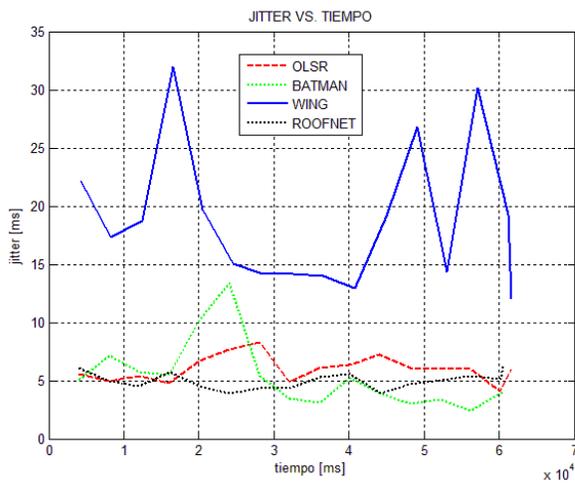
**Jitter:**



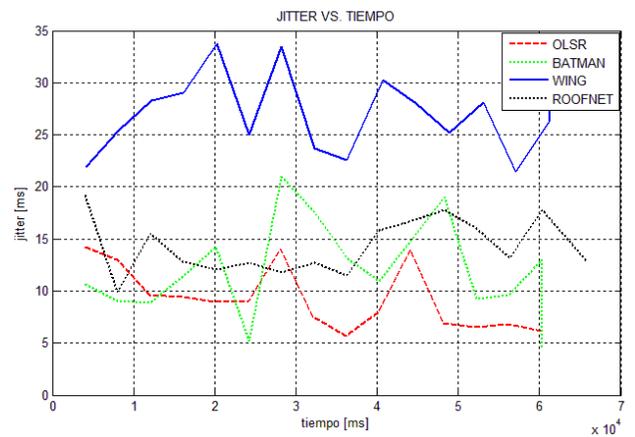
**Figura 5.5: Jitter en Zona 1**



**Figura 5.6: Jitter en Zona 2**



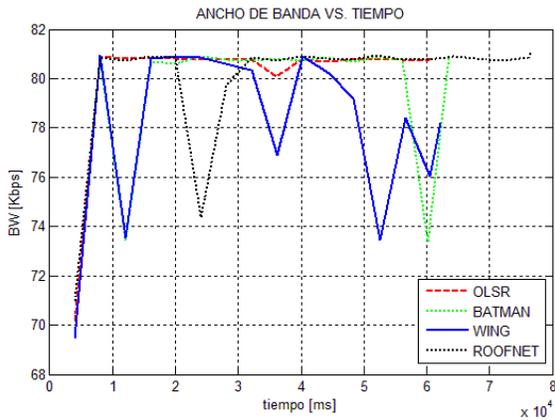
**Figura 5.7: Jitter en Zona 3**



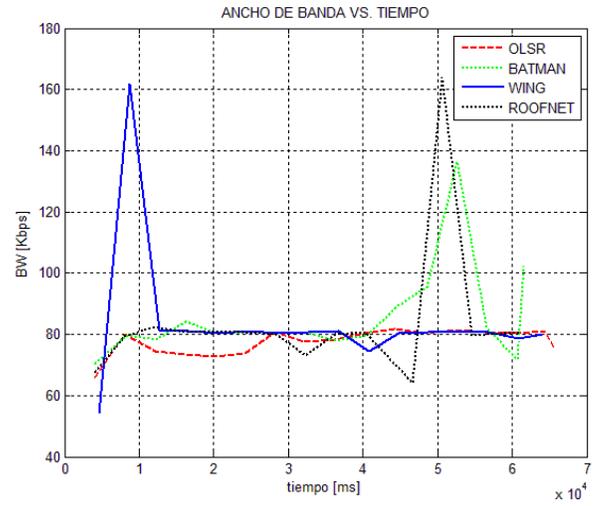
**Figura 5.8: Jitter en Zona 4**

Los valores de jitter, como se puede apreciar en las figuras 5.5, 5.6, 5.7 y 5.8, son más bien variantes en todos los protocolos. En el caso de OLSR, donde mejores valores muestra es en la zona 1 (Fig. 5.5) donde toma valores de entre 3 ms y 7 ms aproximadamente; su pico más notorio está en la zona 2 (Figura 5.6) entre los 30 y 40 s de llamada, donde alcanza un valor cercano a los 20 ms. WING, por otro lado presenta los valores más altos de jitter, especialmente en las zonas 3 y 4 (Fig. 5.7 y 5.8 respectivamente) donde alcanza valores de hasta entre 30 y 35 ms. BATMAN, en cambio, muestra valores muy aproximados a OLSR, pero aún así no lo supera, puesto que presenta unos pocos valores muy variantes, siendo el más notorio en la zona 2 (Fig. 5.6) entre los 40 y los 50 s. ROOFNET presenta también valores de jitter cercanos a OLSR. Su pico más alto lo presenta en la zona 2 (Fig. 5.6) entre 40 y 50 s de llamada, donde llega a casi 25 ms. De manera general, todos los protocolos presentan buenos valores de jitter, puesto que se recomienda que estos valores sean inferiores a los 100 ms entre el punto inicial y el punto final de la comunicación. No obstante, OLSR es el que presenta los valores más bajos.

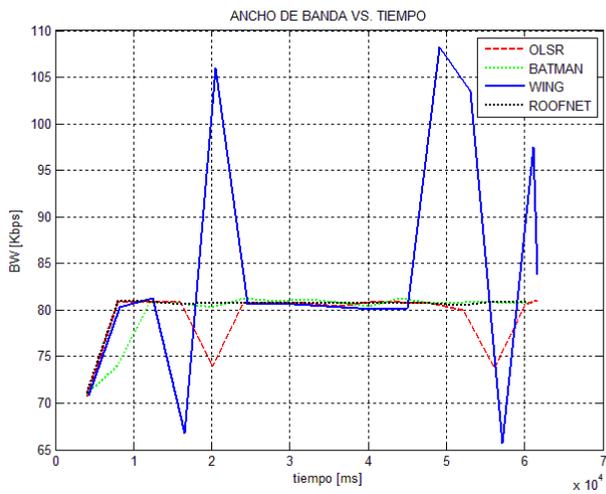
**Ancho de Banda:**



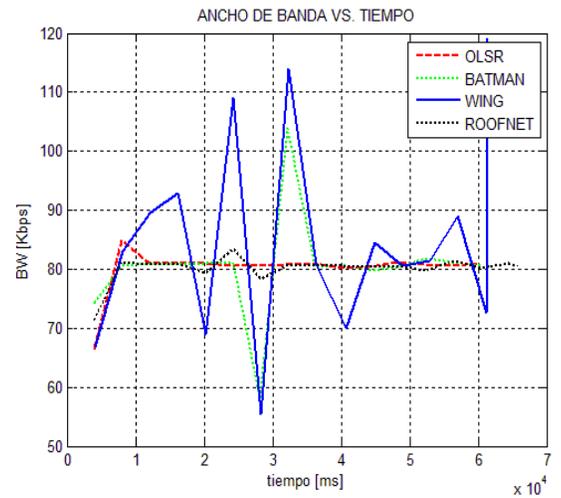
**Figura 5.9: Ancho de Banda consumido en Zona 1**



**Figura 5.10: Ancho de Banda consumido en Zona 2**



**Figura 5.11: Ancho de Banda consumido en Zona 3**



**Figura 5.12: Ancho de Banda consumido en Zona 4**

En las figuras 5.9, 5.10, 5.11, 5.12, e indiferentemente del protocolo, se puede apreciar claramente el impacto que produce el ancho de banda en el retardo de los paquetes. Es así, que cuando aumenta el valor del ancho de banda, el valor del retardo disminuye; y, cuando el valor del ancho de banda disminuye, el valor del retardo aumenta. WING, seguido por BATMAN, muestran valores cambiantes de ancho de banda, lo cual se ve puede ver reflejado en el retardo. Especialmente, en el caso de WING que durante ciertos momentos cambia drásticamente estos valores, los cuales pueden llegar desde los 60 Kbps hasta los 160 Kbps, como se muestra en la figura 5.10, durante los 10 primeros segundos de llamada; mientras que BATMAN, un poco más estable que WING, presenta valores que, en su mayoría, están alrededor de 80 Kbps, con picos de entre 60 y 105 Kbps en la zona 4 (Figura 5.12) entre los 20 y los 40 s. OLSR y Roofnet muestran valores más estables, que están alrededor de 80Kbps. OLSR tiene muy pocas variaciones en sus valores de ancho de banda, siendo la más notoria la que presenta en la zona 3 (Figura 5.11), con dos decrementos a 75 Kbps a los 20 s y entre los 50 y los 60 s. ROOFNET, en cambio, presenta ligeramente más cambios, como los que muestra en la zona 1 (Figura 5.9) donde baja hasta a 75 Kbps entre los 20 y los 30 s, y en la zona 2 (Figura 5.10) donde hay un pico a casi 160 Kbps alrededor del segundo 50; pero, no obstante, el resto

del tiempo en cada zona, ROOFNET se mantiene en aproximadamente 80 Kpbs.

Para poder observar el desempeño de cada protocolo en la zona respectiva se detallará en tablas el funcionamiento con los valores reales obtenidos:

- Retardo

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Retardo [ms]						
4002	20,1102	4017	19,8855	4004	20,2197	4003	19,8187
8026	19,9214	8049	20,0596	8014	19,8520	8010	20,0316
12026	20,0005	12053	22,2443	12034	22,4599	12019	20,0442
16036	19,9490	16058	21,1899	16034	19,9008	16033	19,9721
20059	20,1143	20072	19,0261	20034	20,0003	20037	19,9226
24088	19,9446	24080	20,0413	24053	19,9973	24055	22,4456
28096	19,9415	28105	19,9216	28063	20,3529	28065	20,0509
32098	20,0086	32111	19,9333	32159	20,4802	32086	20,0009
36117	20,1975	36127	20,0780	36210	20,5653	36104	19,9911
40132	19,9779	40142	19,9776	40224	19,9656	40118	19,9701
44140	20,0406	44143	20,0016	44403	21,8798	44118	20,0029
48159	19,9949	48149	19,9308	48403	18,8685	48143	20,0247
52167	19,9358	52160	20,0552	52529	21,6037	52149	19,9279
56167	20,0002	56161	20,0075	56541	21,6844	56153	20,1208
60177	20,0534	60185	22,3543	60549	20,9860	60159	19,9307
60807	19,6841	63509	19,9018	62129	20,7918	64169	19,9509
---	---	---	---	---	---	68171	20,0078
---	---	---	---	---	---	72180	20,0460
---	---	---	---	---	---	76188	19,9400
---	---	---	---	---	---	76517	20,5675

**Tabla VIII - Zona 1-Valores obtenidos de Retardo**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Retardo [ms]						
4007	23,5683	4071	20,4581	4662	37.8987	4012	20,5721
8014	19,2657	8257	20,4186	8665	14.0980	8013	20,1096
12087	22,5029	12286	19,8480	12679	20.0664	12019	20,0268
16142	22,4033	16303	19,5961	16690	20.0580	16055	20,1823
20155	22,2936	20305	20,1101	20698	19.8393	20063	19,8394
24160	22,1305	24313	20,0403	24709	20.0572	24262	22,1007
28183	20,0139	28323	20,1509	28711	20.0098	28290	18,3107
32189	22,3812	32370	20,5426	32717	20.5415	32303	22,2906
36207	20,0894	36442	21,6588	36738	19.8112	36306	20,3210
40210	19,9164	40523	21,1422	40759	21.9689	40311	19,9257
44225	19,8736	44532	24,5967	44759	20.0020	46613	74,1451
48255	20,6665	48605	25,4572	48769	20.0486	50633	10,4968
52390	20,0718	52614	15,0161	52779	19.9505	54646	23,6016
56408	19,4129	56636	19,3368	56802	20.0162	58653	20,0382
60412	19,9216	60654	21,0341	60812	20.1519	61066	19,9425
64417	20,0242	61571	13,2988	64069	19.8566	---	---
65721	33,4246	---	---	---	---	---	---

**Tabla IX - Zona 2-Valores obtenidos de Retardo**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Retardo [ms]						
4014	19,9725	4018	19,8893	4224	21,1196	4018	19,8905
8028	19,9668	8046	22,1340	8251	18,9049	8024	19,9296
12044	19,9807	12056	19,9479	12494	23,1887	12043	19,9956
16049	20,0275	16057	20,0054	16496	24,1092	16071	20,0412
20056	22,1378	20096	20,2985	20503	15,7133	20074	20,0161
24067	19,9536	24099	19,7194	24547	20,5287	24083	19,9431
28068	20,0029	28109	20,0484	28578	19,4736	28089	20,0312
32077	20,0461	32116	19,9381	32586	20,0390	32109	19,9996
36088	20,2583	36136	19,9983	36590	20,2235	36121	20,0598
40096	19,8427	40150	19,9705	40757	21,0452	40122	19,9040

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Retardo [ms]						
44119	20,0145	44154	20,0206	45074	21,1616	44129	20,0371
48134	19,9758	48155	20,0060	49092	18,6877	48151	20,0100
52134	20,2030	52174	19,9912	53102	19,9509	52170	19,9950
56135	22,2224	56177	20,0194	57146	27,1397	56182	20,0586
60157	20,0128	60187	20,0458	61155	17,7385	60201	19,9955
61618	20,0181	60614	19,4168	61647	20,5092	60473	19,4257

**Tabla X - Zona 3-Valores obtenidos de Retardo**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Retardo [ms]						
4010	19,9498	4021	19,0577	4095	22,4990	4014	19,9690
8017	9,9353	8021	20,0006	8133	17,9479	8020	20,0299
12024	20,0377	12030	20,0417	12206	20,6763	12034	20,0727
16051	20,0341	16172	21,0251	16209	22,7443	16040	20,0287
20057	19,9273	20188	18,9441	20222	23,7451	20221	20,9033
24067	20,0497	24204	20,0818	24222	15,8110	24233	19,1053
28074	20,0345	28213	37,1173	28231	33,6884	28256	20,5248
32088	19,8734	32213	14,8158	32275	14,2871	32269	19,9664
36103	19,9763	36214	20,1075	36316	20,2060	36272	20,0157
40126	20,4219	40223	19,9420	40721	27,5298	40288	20,1826
44139	19,6700	44237	20,2731	44860	17,4665	44309	19,9031
48152	19,9669	48244	19,9349	48872	18,9233	48310	20,2104
52168	19,9793	52267	20,0142	53042	24,3874	52315	20,3271
56177	20,0445	56269	20,1143	57064	17,5638	56334	19,7004
60202	20,0266	60279	19,9483	61174	21,0753	60363	20,0467
---	---	60364	21,3375	61343	7,3352	64377	20,1689
---	---	---	---	---	---	65777	19,4432

**Tabla XI - Zona 4-Valores obtenidos de Retardo**

- Jitter

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Jitter [ms]						
4002	6,8929	4017	3,9989	4004	16,7640	4003	7,3829
8026	5,5599	8049	2,8754	8014	12,1057	8010	6,1750
12026	4,7246	12053	8,0274	12034	13,5234	12019	4,9976
16036	4,5776	16058	2,9116	16034	7,6981	16033	6,0025
20059	4,8410	20072	7,0418	20034	12,1814	20037	5,2343
24088	3,5628	24080	4,6302	24053	11,0155	24055	8,4502
28096	3,0251	28105	7,0331	28063	11,6241	28065	6,7977
32098	2,9499	32111	7,6523	32159	10,1507	32086	7,0848
36117	3,1962	36127	3,0833	36210	13,6631	36104	8,1176
40132	3,0085	40142	6,7706	40224	8,8104	40118	7,1190
44140	3,2796	44143	3,3848	44403	10,9884	44118	5,5840
48159	2,9934	48149	6,3734	48403	12,6179	48143	4,3864
52167	3,1075	52160	3,0358	52529	12,4537	52149	4,1936
56167	3,6129	56161	1,7653	56541	17,7737	56153	3,9880
60177	3,0016	60185	7,0894	60549	14,4088	60159	4,6194
60807	2,7134	63509	4,1089	62129	15,6530	64169	5,4242
---	---	---	---	---	---	68171	3,8455
---	---	---	---	---	---	72180	4,8380
---	---	---	---	---	---	76188	4,6211
---	---	---	---	---	---	76517	4,5931

**Tabla XII - Zona 1-Valores obtenidos de Jitter**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Jitter [ms]						
4007	8,3129	4071	20,2119	4662	21,5111	4012	10,8547
8014	12,8959	8257	22,4391	8665	28,1948	8013	16,7239
12087	9,0057	12286	23,8812	12679	17,9813	12019	11,3774
16142	12,3736	16303	12,5295	16690	12,5449	16055	11,2050
20155	15,3734	20305	5,6010	20698	14,8483	20063	10,2246
24160	12,2275	24313	11,3574	24709	17,2469	24262	14,8269
28183	9,7154	28323	12,9054	28711	14,4176	28290	12,8073
32189	15,8667	32370	11,3931	32717	18,1795	32303	12,8889
36207	19,1398	36442	18,7026	36738	18,5355	36306	11,0174
40210	10,5674	40523	26,5334	40759	16,2013	40311	9,9128
44225	7,8886	44532	22,5121	44759	11,6534	46613	22,8818
48255	8,3675	48605	37,8269	48769	10,8803	50633	23,8355
52390	11,9216	52614	21,7548	52779	12,6882	54646	14,8914
56408	12,6636	56636	22,6853	56802	7,6156	58653	7,3666
60412	13,9422	60654	22,9596	60812	15,4237	61066	6,3263
64417	15,7887	61571	17,7526	64069	12,9459	---	---
65721	13,8046	---	---	---	---	---	---

*Tabla XIII - Zona 2-Valores obtenidos de Jitter*

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Jitter [ms]						
4014	5,5936	4018	5,0664	4224	22,1186	4018	6,1214
8028	4,9556	8046	7,1309	8251	17,3099	8024	4,9277
12044	5,3510	12056	5,7614	12494	18,7266	12043	4,5114
16049	4,7501	16057	5,4482	16496	31,9571	16071	5,7417
20056	6,7443	20096	10,2464	20503	19,6731	20074	4,5459
24067	7,6861	24099	13,3450	24547	15,0840	24083	3,9070
28068	8,3323	28109	5,4177	28578	14,1386	28089	4,3270
32077	4,9009	32116	3,4719	32586	14,1407	32109	4,3540
36088	6,1159	36136	3,0836	36590	13,9810	36121	5,3123

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Jitter [ms]						
40096	6,3922	40150	5,1990	40757	12,8998	40122	5,5727
44119	7,2171	44154	3,8734	45074	19,1714	44129	3,8881
48134	6,0932	48155	3,0170	49092	26,8321	48151	4,7027
52134	5,9870	52174	3,3455	53102	14,3157	52170	5,0858
56135	6,0419	56177	2,4419	57146	30,1502	56182	5,3855
60157	4,0989	60187	3,9404	61155	19,2661	60201	5,1572
61618	5,9748	60614	3,9027	61647	12,0146	60473	6,3614

**Tabla XIV - Zona 3-Valores obtenidos de Jitter**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Jitter [ms]						
4010	14,2560	4021	10,6358	4095	21,9197	4014	19,1922
8017	13,0115	8021	9,0522	8133	25,3504	8020	9,8903
12024	9,5762	12030	8,8216	12206	28,3188	12034	15,5526
16051	9,4133	16172	11,5389	16209	29,0754	16040	12,8166
20057	8,9313	20188	14,2425	20222	33,7373	20221	12,0217
24067	8,9933	24204	5,2393	24222	24,9736	24233	12,7519
28074	14,0550	28213	21,0065	28231	33,4175	28256	11,7337
32088	7,5207	32213	17,7261	32275	23,7100	32269	12,6809
36103	5,6864	36214	13,1707	36316	22,6097	36272	11,4679
40126	7,9102	40223	10,9546	40721	30,2275	40288	15,7715
44139	13,9670	44237	14,8816	44860	27,9873	44309	16,7806
48152	6,9260	48244	19,0234	48872	25,2096	48310	17,7887
52168	6,4785	52267	9,2569	53042	28,0689	52315	15,9576
56177	6,8308	56269	9,6615	57064	21,4724	56334	13,1757
60202	6,1811	60279	12,9712	61174	26,2116	60363	17,7921
---	---	60364	4,5925	61343	30,1113	64377	14,1014
---	---	---	---	---	---	65777	12,8678

**Tabla XV - Zona 4-Valores obtenidos de Jitter**

- Ancho de Banda

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
4002	70,1266	4017	70,9307	4004	69,4222	4003	70.9703
8026	80,8950	8049	80,7562	8014	80,9505	8010	80.8720
12026	80,8160	12053	73,4667	12034	73,5285	12019	80.7120
16036	80,8597	16058	80,6942	16034	80,8279	16033	80.8995
20059	80,8000	20072	80,5839	20034	80,8880	20037	80.8597
24088	80,7762	24080	80,8800	24053	80,8597	24055	74.3687
28096	80,7642	28105	80,7921	28063	80,5848	28065	79.7520
32098	80,7760	32111	80,7403	32159	80,3360	32086	80.8438
36117	80,0884	36127	80,8320	36210	76,8893	36104	80.7483
40132	80,7881	40142	80,7085	40224	80,8995	40118	80.9075
44140	80,6800	44143	80,8400	44403	80,1927	44118	80.8080
48159	80,7721	48149	80,6846	48403	79,1774	48143	80.7801
52167	80,7881	52160	80,8640	52529	73,4325	52149	80.9234
56167	80,7520	56161	80,7680	56541	78,4086	56153	80.7799
60177	80,7440	60185	73,3511	60549	76,0461	60159	80.7881
60807	80,8500	63509	80,9006	62129	78,1684	64169	80.8836
---	---	---	---	---	---	68171	80.8000
---	---	---	---	---	---	72180	80.7440
---	---	---	---	---	---	76188	80.8438
---	---	---	---	---	---	76517	81.1000

**Tabla XVI - Zona 1-Valores obtenidos de Ancho de Banda**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
4007	65,8918	4071	70,2151	4662	53,8797	4012	67,4215
8014	80,0385	8257	79,6488	8665	161,9606	8013	79,3085
12087	74,3691	12286	78,1557	12679	81,4880	12019	82,5360
16142	73,3083	16303	84,1912	16690	80,9120	16055	80,6720
20155	72,8622	20305	80,2894	20698	80,3248	20063	80,6812
24160	73,8829	24313	80,3280	24709	81,2000	24262	80,8589
28183	80,8199	28323	80,4663	28711	80,5040	28290	80,0145
32189	77,7117	32370	80,6660	32717	80,5579	32303	73,0756
36207	78,4080	36442	78,1106	36738	80,9379	36306	80,0487
40210	80,3900	40523	79,5689	40759	74,4831	40311	80,7721
44225	81,8693	44532	88,9521	44759	80,4320	46613	64,1318
48255	80,2215	48605	95,6100	48769	80,5680	50633	164,0313
52390	81,2738	52614	136,4794	52779	81,1701	54646	79,6612
56408	80,8580	56636	82,0692	56802	80,7881	58653	80,3920
60412	80,3264	60654	71,5393	60812	78,6653	61066	80,8595
64417	81,1040	61571	102,0754	64069	80,0878	---	---
65721	75,0359	---	---	---	---	---	---

**Tabla XVII - Zona 2-Valores obtenidos de Ancho de Banda**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
4014	70,7821	4018	70,9069	4224	70,8640	4018	71,0416
8028	80,7960	8046	74,0308	8251	80,3080	8024	80,8995
12044	80,9313	12056	80,8358	12494	81,3027	12043	80,8995
16049	80,8000	16057	80,6880	16496	66,8145	16071	80,5891
20056	74,0066	20096	80,2894	20503	105,9639	20074	80,8640

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
24067	80,8119	24099	81,3241	24547	80,6660	24083	80,7403
28068	80,7600	28109	80,8960	28578	80,7729	28089	80,8560
32077	80,7840	32116	81,1144	32586	80,5360	32109	80,7164
36088	80,4283	36136	80,8677	36590	80,3394	36121	80,7680
40096	80,7921	40150	80,3900	40757	80,1131	40122	80,7483
44119	80,8199	44154	81,2880	45074	80,1725	44129	80,7840
48134	80,7801	48155	80,7280	49092	108,2493	48151	80,7244
52134	79,9596	52174	80,8677	53102	103,4746	52170	80,5652
56135	73,7600	56177	80,8560	57146	65,6537	56182	80,8960
60157	80,6527	60187	80,7600	61155	97,4655	60201	80,8677
61618	81,0301	60614	80,8000	61647	83,7333	60473	80,8000

**Tabla XVIII - Zona 3-Valores obtenidos de Ancho de Banda**

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
4010	66,5473	4021	74,1915	4095	66,8044	4014	71,3632
8017	84,8398	8021	80,6320	8133	83,0933	8020	81,2960
12024	80,9840	12030	80,9840	12206	89,6812	12034	80,7200
16051	80,9154	16172	80,7797	16209	92,8727	16040	81,0320
20057	81,0030	20188	81,0113	20222	69,0083	20221	79,3280
24067	80,6640	24204	80,9520	24222	109,1352	24233	83,4286
28074	80,6160	28213	58,1185	28231	55,5025	28256	78,4408
32088	80,7050	32213	103,8874	32275	114,0071	32269	80,8836
36103	80,9950	36214	80,3136	36316	80,7040	36272	80,5040
40126	80,2518	40223	80,8995	40721	69,9100	40288	80,5789
44139	80,4078	44237	79,8626	44860	84,4219	44309	80,3089
48152	81,3055	48244	80,4935	48872	80,6868	48310	80,5657
52168	80,7960	52267	81,8388	53042	81,3567	52315	79,8213
56177	80,6960	56269	81,1417	57064	88,8943	56334	81,3333
60202	80,9154	60279	80,5652	61174	72,6974	60363	80,2308

O.L.S.R.		B.A.T.M.A.N		W.I.N.G		Roofnet	
Tiempo [ms]	Ancho de Banda [Kbps]						
---	---	60364	80,4000	61343	119,0261	64377	81,0613
---	---	---	---	---	---	65777	80,4000

**Tabla XIX - Zona 4-Valores obtenidos de Ancho de Banda**

**Análisis de pérdida de paquetes por zona para cada protocolo de enrutamiento** (los valores se detallan en porcentaje):

ZONA	Detalle	PROTOCOLO			
		O.L.S.R.	B.A.T.M.A.N.	W.I.N.G.	ROOFNET
ZONA 1	Paquetes totales	3011	3180	3109	3806
	Paquetes perdidos	2	18	36	10
	Porcentaje de paquetes perdidos	0.07%	0.57%	1.16%	0.26%
ZONA 2	Paquetes totales	3039	3094	3155	3056
	Paquetes perdidos	1	27	17	1
	Porcentaje de paquetes perdidos	0.03%	0.87%	0.54%	0.03%
ZONA 3	Paquetes totales	3132	3013	3036	3025
	Paquetes perdidos	6	14	9	2
	Porcentaje de paquetes perdidos	0.19%	0.46%	0.30%	0.07%
ZONA 4	Paquetes totales	3039	3002	3031	3291
	Paquetes perdidos	0	7	16	4
	Porcentaje de paquetes perdidos	0.00%	0.23%	0.53%	0.12%
<b>Promedio (%)</b>		0.07%	0.53%	0.63%	0.12%

**Tabla XX – Pérdida de paquetes por zona para cada protocolo**

Como se puede apreciar, cada protocolo tiene valores de paquetes perdidos muy por debajo del 10%. No obstante, OLSR lleva la ventaja frente a los demás protocolos con un 0.07% de paquetes perdidos, seguido por Roofnet con un 0.12%. B.A.T.M.A.N. y W.I.N.G. muestran mayor porcentaje de pérdida de paquetes con un 0.53% y 0.63%, respectivamente, que no son valores que pueden afectar en gran medida a la comunicación, pero claramente se puede apreciar una ligera ventaja para OLSR en este aspecto.

**CONCLUSIONES Y  
RECOMENDACIONES**

## Conclusiones

1. Todos los protocolos de enrutamiento que fueron empleados en este proyecto (OLSR, B.A.T.M.A.N., W.I.N.G. y Roofnet), mostraron muy buenos valores de jitter, retardo, ancho de banda y pérdida de paquetes. Por lo tanto, cualquiera de ellos puede ser empleado para implementar una red inalámbrica mallada confiable.
2. De los protocolos proactivos, OLSR fue el protocolo con mejores valores en los parámetros de evaluación, mostrando sus debidas ventajas ante el otro protocolo de esta clase, B.A.T.M.A.N., el cual en términos generales y en cada zona, presentó buenos valores pero no logró superar a OLSR.
3. De los protocolos reactivos, Roofnet superó a WING, a pesar de que este fue creado bajo las bases del primero. WING fue el protocolo que tuvo los resultados mayores y más variantes de jitter, ancho de banda y retardo; y aunque sus valores de pérdida de paquetes no fueron excesivos, fue el protocolo que presentó mayor cantidad de paquetes perdidos en la red.

4. De entre los protocolos de mayor rendimiento en cada clase, en términos generales y considerando cada uno de los cuatro parámetros empleados para determinar el protocolo más eficiente, OLSR supera a Roofnet en cada una de las zonas establecidas, constituyendo el protocolo a considerar en primera instancia en la implementación de redes de este tipo.

## **Recomendaciones**

1. Investigar el firmware de OpenWrt que es apropiado para cada tipo de enrutador, puesto que esto evitará posteriores daños al equipo.
2. Verificar la comunicación entre los enrutadores de la red con el Gateway para evitar tener problemas con la conectividad a Internet y poder obtener un envío correcto de paquetes Voip.

3. Evitar realizar pruebas de captura de paquetes ante la presencia de muchas personas puesto que pueden ocasionar interferencia para la red, con lo cual no obtendríamos una comparación eficiente entre los protocolos.

4. Se recomienda como trabajo a futuro el uso de redes con un número mayor de nodos y el uso de pruebas adicionales de saturación, a fin de poner a un estrés mayor a los protocolos de enrutamiento y así mostrar una perspectiva diferente a lo iniciado en este proyecto.

# BIBLIOGRAFÍA

(1) Ian Fuat Akyildiz and Xudong Wang.

“Wireless mesh networks”

(2) Sudip Misra, Subhas Chandra Misra and Isaac, Woungang,

“Guide to wireless mesh networks”.

(3) Izaskun Pellejero

“Fundamentos y aplicaciones de seguridad en redes WLAN”

(4) Jungfang Wang, Bin Xie and Dharma P. Agrawal

“Journey from Mobile Ad Hoc Networks to Wireless Mesh Networks”

(5) Ekram Hossain and Kin Leung

“Wireless mesh networks- Architectures and Protocols”

(6) Características de enrutador WRT54GL,

<http://www.linksysbycisco.com/EU/en/products/WRT54GL>, fecha de consulta mayo 2011.

(7) Características de enrutador Meraki Outdoor

[http://meraki.com/products\\_services/access\\_points/outdoor/](http://meraki.com/products_services/access_points/outdoor/), fecha de consulta mayo 2011.

(8) Características de enrutador Dlink Dir 825, <http://www.dlink.com/DIR-825>,

fecha de consulta mayo 2011.

- (9) Particularidades de sniffer Wireshark, <http://www.wireshark.org/> fecha de consulta Junio 2011.
- (10) Programa X-lite <http://www.counterpath.com/x-lite.html>, fecha de consulta Junio 2011.
- (11) Firmware OpenWrt <https://openwrt.org/> fecha de consulta Junio 2011.
- (12) Paquetes disponibles para cada tipo de enrutador <http://wiki.openwrt.org/oldwiki/hardware/linksys> , fecha de consulta Julio 2011.
- (13) Tipos de firmware para el enrutador Dlink Dir 825. <http://wiki.openwrt.org/toh/d-link/dir-825> , fecha de consulta Julio 2011.
- (14) Cómo instalar Wing <http://www.wing-project.org/> , fecha de consulta Mayo 2011.
- (15) Modo monitor para redes ad-hoc [http://en.wikipedia.org/wiki/Monitor\\_mode](http://en.wikipedia.org/wiki/Monitor_mode) , fecha de consulta Julio 2011.
- (16) Cómo instalar OLSR <http://wiki.openwrt.org/inbox/mesh.olsr> , fecha de consulta Abril 2011.

# **ANEXOS**

# ANEXO A: Código de Matlab para generación de gráficos

```
*****
%ZONA 1:
%delta0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'D9377:D12387');
%jitter0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'E9377:E12387');
%BW0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'G9377:G12387');

%deltaB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'P3048:P6049');
%jitterB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'Q3048:Q6049');
%BWB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'S3048:S6049');

%deltaW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AN3084:AN6114');
%jitterW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AO3084:AQ6114');
%BWW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AQ3084:AQ6114');

%deltaR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AB3301:AB6580');
%jitterR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AC3301:AC6580');
%BWR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA1.xls', 'AE3301:AE6580');
*****

%ZONA 2:
%delta0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'D8891:D11929');
%jitter0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'E8891:E11929');
%BW0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'G8891:G11929');

%deltaB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'P3189:P6323');
%jitterB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'Q3189:Q6323');
%BWB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'S3189:S6323');

%deltaW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AN3118:AN6139');
%jitterW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AO3118:AQ6139');
%BWW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AQ3118:AQ6139');

%deltaR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AB3837:AB7642');
%jitterR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AC3837:AC7642');
%BWR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA2.xls', 'AE3837:AE7642');
*****

%ZONA 3:
%delta0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'D8578:D11709');
%jitter0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'E8578:E11709');
%BW0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'G8578:G11709');

%deltaB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'P3103:P6148');
%jitterB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'Q3103:Q6148');
%BWB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'S3103:S6148');

%deltaW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AN3215:AN6369');
%jitterW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AO3215:AQ6369');
%BWW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AQ3215:AQ6369');

%deltaR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AB3065:AB6007');
```

```

%jitterR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AC3065:AC6007');
%BWR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA3.xls', 'AE3065:AE6007');
%*****

%*****
%ZONA 4:
delta0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'D8336:D11374');
jitter0=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'E8336:E11374');
BWO=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'G8336:G11374');

deltaB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'P3044:P6056');
jitterB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'Q3044:Q6056');
BWB=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'S3044:S6056');

deltaw=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AN3099:AN6134');
jitterW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AO3099:AQ6134');
BWW=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AQ3099:AQ6134');

deltaR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AB3053:AB6077');
jitterR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AC3053:AC6077');
BWR=xlsread('C:\Users\Joedward\Documents\MATLAB\ZONA4.xls', 'AE3053:AE6077');
%*****

tiempo0=0;
jitter_acum0=0;
BW_acum0=0;
i=0;
j=1;
contador0=0;
flago = 0;

tiempoB=0;
jitter_acumB=0;
BW_acumB=0;
contadorB=0;
flagB = 0;

tiempow=0;
jitter_acumW=0;
BW_acumW=0;
contadorW=0;
flagw = 0;

tiempoR=0;
jitter_acumR=0;
BW_acumR=0;
contadorR=0;
flagR = 0;

while(i<size(delta0,1)-1)
    while(tiempo0<4000 && flago == 0)
        i=i+1;
        contador0=contador0+1;
        tiempo0=tiempo0+delta0(i);
        jitter_acum0=jitter_acum0+jitter0(i);
        BW_acum0=BW_acum0+BWO(i);
        if (i>size(delta0,1)-1)
            flago = 1;
        end
    end
    deltaPO(j)=tiempo0/contador0;
    jitterPO(j)=jitter_acum0/contador0;
    BWPO(j)=BW_acum0/contador0;
    if(j==1)
        tiempo_real0(j)=tiempo0;
    else
        tiempo_real0(j)=tiempo0+tiempo_real0(j-1);
    end
end

```

```

        j=j+1;
        tiempo0=0;
        contador0=0;
        jitter_acum0=0;
        BW_acum0=0;
    end

    i=0;
    j=1;
    while(i<size(deltaB,1)-1)
        while(tiempoB<4000 && flagB == 0)
            i=i+1;
            contadorB=contadorB+1;
            tiempoB=tiempoB+deltaB(i);
            jitter_acumB=jitter_acumB+jitterB(i);
            BW_acumB=BW_acumB+BWB(i);
            if (i>size(deltaB,1)-1)
                flagB = 1;
            end
        end
        deltaPB(j)=tiempoB/contadorB;
        jitterPB(j)=jitter_acumB/contadorB;
        BWPB(j)=BW_acumB/contadorB;
        if(j==1)
            tiempo_realB(j)=tiempoB;
        else
            tiempo_realB(j)=tiempoB+tiempo_realB(j-1);
        end
        j=j+1;
        tiempoB=0;
        contadorB=0;
        jitter_acumB=0;
        BW_acumB=0;
    end

    i=0;
    j=1;
    while(i<size(deltaw,1)-1)
        while(tiempow<4000 && flagw == 0)
            i=i+1;
            contadorw=contadorw+1;
            tiempow=tiempow+deltaw(i);
            jitter_acumw=jitter_acumw+jitterw(i);
            BW_acumw=BW_acumw+BWW(i);
            if (i>size(deltaw,1)-1)
                flagw = 1;
            end
        end
        deltaPW(j)=tiempow/contadorw;
        jitterPW(j)=jitter_acumw/contadorw;
        BWPW(j)=BW_acumw/contadorw;
        if(j==1)
            tiempo_realw(j)=tiempow;
        else
            tiempo_realw(j)=tiempow+tiempo_realw(j-1);
        end
        j=j+1;
        tiempow=0;
        contadorw=0;
        jitter_acumw=0;
        BW_acumw=0;
    end

    i=0;
    j=1;
    while(i<size(deltaR,1)-1)
        while(tiempoR<4000 && flagR == 0)

```

```

        i=i+1;
        contadorR=contadorR+1;
        tiempoR=tiempoR+deltaR(i);
        jitter_acumR=jitter_acumR+jitterR(i);
        BW_acumR=BW_acumR+BWR(i);
        if (i>size(deltaR,1)-1)
            flagR = 1;
        end
    end
    deltaPR(j)=tiempoR/contadorR;
    jitterPR(j)=jitter_acumR/contadorR;
    BWPR(j)=BW_acumR/contadorR;
    if(j==1)
        tiempo_realR(j)=tiempoR;
    else
        tiempo_realR(j)=tiempoR+tiempo_realR(j-1);
    end
    j=j+1;
    tiempoR=0;
    contadorR=0;
    jitter_acumR=0;
    BW_acumR=0;
end

retardo=plot(tiempo_realO,deltaPO,tiempo_realB,deltaPB,tiempo_realW,deltaPW,tiempo_realR,
deltaPR);
set(retardo,'Linewidth',2,'LineStyle','--';':';'-';':'})
set(retardo,'Color',{'r';'g';'b';'k'})
grid on
xlabel('tiempo [ms]'), ylabel('retardo [ms]')
legend(retardo,'OLSR','BATMAN','WING','ROOFNET')
title('RETARDO VS. TIEMPO')

figure(2);
ancho_banda=plot(tiempo_realO,BWPO,tiempo_realB,BWPB,tiempo_realW,BWPW,tiempo_realR,BWPR)
;
set(ancho_banda,'Linewidth',2,'LineStyle','--';':';'-';':'})
set(ancho_banda,'Color',{'r';'g';'b';'k'})
grid on
xlabel('tiempo [ms]'), ylabel('BW [Kbps]')
legend(ancho_banda,'OLSR','BATMAN','WING','ROOFNET')
title('ANCHO DE BANDA VS. TIEMPO')

figure(3);
jitter=plot(tiempo_realO,jitterPO,tiempo_realB,jitterPB,tiempo_realW,jitterPW,tiempo_realR,jitterPR);
set(jitter,'Linewidth',2,'LineStyle','--';':';'-';':'})
set(jitter,'Color',{'r';'g';'b';'k'})
grid on
xlabel('tiempo [ms]'), ylabel('jitter [ms]')
legend(jitter,'OLSR','BATMAN','WING','ROOFNET')
title('JITTER VS. TIEMPO')

```