

**DISEÑO E IMPLEMENTACIÓN DE UN ISP CON ACCESO INALÁMBRICO  
PARA SOPORTAR SERVICIOS DE INTERNET Y TELEFONÍA IP EN EL  
LABORATORIO DE TELECOMUNICACIONES DE LA UNIVERSIDAD  
AUTÓNOMA DE OCCIDENTE**

**LUIS HERNANDO VILLA AVILA  
JHORMAN ANDRES VILLANUEVA VIVAS**

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE  
FACULTAD DE INGENIERÍA  
DEPARTAMENTO DE AUTOMÁTICA Y ELECTRÓNICA  
PROGRAMA DE ELECTRÓNICA Y TELECOMUNICACIONES  
SANTIAGO DE CALI  
2013**

**DISEÑO E IMPLEMENTACIÓN DE UN ISP CON ACCESO INALÁMBRICO  
PARA SOPORTAR SERVICIOS DE INTERNET Y TELEFONIA IP EN EL  
LABORATORIO DE TELECOMUNICACIONES DE LA UNIVERSIDAD  
AUTONOMA DE OCCIDENTE**

**LUIS HERNANDO VILLA AVILA  
JHORMAN ANDRES VILLANUEVA VIVAS**

**Proyecto de grado para optar por el título de  
Ingeniero Electrónico y Telecomunicaciones**

**Director  
HELMUT ALEXANDER RUBIO WILSON  
Ingeniero Electrónico y de Telecomunicaciones  
Master en Sistemas Inalámbricos**

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE  
FACULTAD DE INGENIERÍA  
DEPARTAMENTO DE AUTOMÁTICA Y ELECTRÓNICA  
PROGRAMA DE ELECTRONICA Y TELECOMUNICACIONES  
SANTIAGO DE CALI  
2013**

**Nota de aceptación:**

**Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Electrónico y Telecomunicaciones**

**ZEIDA MARIA SOLARTE**

**Jurado**

**HECTOR JOSE GOMEZ**

**Jurado**

**Santiago de Cali, 30 de Mayo del 2013**

## CONTENIDO

	pág.
<b>GLOSARIO</b>	<b>12</b>
<b>RESUMEN</b>	<b>14</b>
<b>INTRODUCCIÓN</b>	<b>15</b>
<b>1. ANTECEDENTES</b>	<b>17</b>
<b>2. PROBLEMA DE INVESTIGACIÓN</b>	<b>19</b>
<b>2.1 PLANTEAMIENTO DEL PROBLEMA</b>	<b>19</b>
<b>3. JUSTIFICACIÓN</b>	<b>20</b>
<b>4. OBJETIVO</b>	<b>21</b>
<b>4.1 OBJETIVO GENERAL</b>	<b>21</b>
<b>4.2 OBJETIVOS ESPECÍFICOS</b>	<b>21</b>
<b>5. MARCO DE REFERENCIA</b>	<b>22</b>
<b>5.1 MARCO TEÓRICO</b>	<b>22</b>
<b>5.1.1 ISP</b>	<b>22</b>
<b>5.1.2 Arquitectura de un ISP</b>	<b>26</b>
<b>5.1.2.1 Red de Acceso</b>	<b>28</b>
<b>5.1.2.2 Red de Núcleo</b>	<b>33</b>
<b>5.1.3 Gestión de la red</b>	
<b>5.1.3.1 FCAPS.</b>	<b>41</b>

5.1.3.2	Protocolos de gestión de red.	42
5.1.4	Servicios ofrecidos por el ISP	
5.1.4.1	Internet	43
5.1.4.2	Telefonía IP	43
6.	DISEÑO DEL ISP CON ACCESO INALÁMBRICO	51
6.1	DISEÑO DE LA RED DE NÚCLEO	54
6.1.1	Servicios de Red	57
6.1.1.1	Servicio NAT	57
6.1.1.2	Servicio DNS	57
6.1.1.3	Servicio DHCP	57
6.1.2	Servicios de Gestión	58
6.1.2.1	Directorio de Usuarios	58
6.1.2.2	Autenticación	59
6.1.2.3	Control de Ancho de Banda	60
6.1.2.4	Monitoreo y control de Red de Acceso	61
6.1.3	Diseño del servicio de telefonía IP	62
6.1.3.1	Servicios y funcionalidades	62
6.1.3.2	Selección de la distribución	63
6.1.3.3	Medición de Calidad de Servicio	66
6.2	DISEÑO DE LA RED DE ACCESO	69
7.	IMPLEMENTACIÓN DEL ISP CON ACCESO INALÁMBRICO	71

<b>7.1 CONFIGURACIÓN DE SERVICIOS DE RED</b>	<b>72</b>
7.1.1 Servicio NAT	72
7.1.2 Servicio DNS	72
7.1.3 Servicio DHCP	72
<b>7.2 CONFIGURACIÓN DE SERVICIOS DE GESTIÓN</b>	<b>73</b>
7.2.1 Configuración para Directorio de Usuarios	73
7.2.2 Configuración de Autenticación	75
7.2.3 Configuración para Control de Ancho de Banda	78
7.2.4 Configuración de monitoreo y control de la Red de Acceso	82
<b>7.3 CONFIGURACIÓN DEL SERVICIO DE TELEFONÍA IP</b>	<b>83</b>
7.3.1 Configuración de los servicios para VoIP	84
7.3.2 Configuración de teléfonos	87
7.3.3 Configuración del VoIPMonitor	90
<b>7.4 CONFIGURACIÓN DEL LA RED DE ACCESO</b>	<b>93</b>
7.4.1 Configuración de los módulos airGrid M5	95
7.4.2 Configuración de los módulos Rocket M5	99
7.4.3 Configuración de los módulos CPE NanoStation M5	101
<b>8. CONCLUSIONES</b>	<b>104</b>
<b>9. RECOMENDACIONES</b>	<b>107</b>
<b>BIBLIOGRAFÍA</b>	<b>108</b>
<b>ANEXOS</b>	<b>113</b>

## LISTA DE CUADROS

	pág.
<b>Cuadro 1. Distribución de canales protocolo 802.11a</b>	<b>33</b>
<b>Cuadro 2. Características técnicas del PC para la red de núcleo</b>	<b>54</b>
<b>Cuadro 3. Características y Propiedades de las distribuciones Zeroshell, BrazilFW y pFSense</b>	<b>55</b>
<b>Cuadro 4. Asignaciones de ancho de banda a los rangos de IP y a las direcciones MAC de los cuatro usuarios que adquieren los servicios</b>	<b>58</b>
<b>Cuadro 5. Información de los Usuarios que adquieren los servicios del ISP</b>	<b>59</b>
<b>Cuadro 6. Características y funcionalidades de Trixbox y Elastix</b>	<b>65</b>
<b>Cuadro 7. Valores máximos en los parámetros de QoS para el servicio de VoIP</b>	<b>68</b>
<b>Cuadro 8. Antenas a utilizar en la implementación de la red inalámbrica</b>	<b>69</b>
<b>Cuadro 9. Teléfonos de usuarios para acceder al servicio de VoIP</b>	<b>87</b>
<b>Cuadro 10. Parámetros de Configuración para la airGrid M5 modo Access Point</b>	<b>95</b>
<b>Cuadro 11. Parámetros de Configuración para la airGrid M5 modo Station</b>	<b>97</b>
<b>Cuadro 12. Parámetros de Configuración de los Rocket M5</b>	<b>99</b>
<b>Cuadro 13. Parámetros de Configuración de los 4 Nanostation</b>	<b>101</b>

## LISTA DE FIGURAS

	pág.
<b>Figura 1. ISP de Nivel 1</b>	<b>24</b>
<b>Figura 2. ISP de nivel 2</b>	<b>24</b>
<b>Figura 3. ISP de nivel 3</b>	<b>25</b>
<b>Figura 4. Arquitectura de un ISP</b>	<b>26</b>
<b>Figura 5. Estructura interna de un ISP</b>	<b>27</b>
<b>Figura 6. Enlace punto a punto</b>	<b>31</b>
<b>Figura 7. Enlace punto a multipunto</b>	<b>31</b>
<b>Figura 8. Arquitectura típica de una red WLAN</b>	<b>33</b>
<b>Figura 9. Topología de red para establecer conexión Radius</b>	<b>36</b>
<b>Figura 10. El directorio LDAP para ejemplo.org</b>	<b>39</b>
<b>Figura 11. Transporte de la información de gestión y administración de los elementos</b>	<b>40</b>
<b>Figura 12. Arquitectura de VoIP</b>	<b>44</b>
<b>Figura 13. Diagrama de Bloques del ISP</b>	<b>51</b>
<b>Figura 14. Diagrama de red implementado para ofrecer servicio de internet y VoIP</b>	<b>52</b>
<b>Figura 15. Interfaz web principal del Zeroshell</b>	<b>71</b>
<b>Figura 16. Configuración del servicio NAT en Zeroshell</b>	<b>72</b>
<b>Figura 17. Menú DHCP</b>	<b>73</b>
<b>Figura 18. Menú USERS</b>	<b>74</b>
<b>Figura 19. Formulario para la creación de usuarios</b>	<b>74</b>



<b>Figura 20. Creación de grupos de usuarios</b>	<b>75</b>
<b>Figura 21. Menú Accounting</b>	<b>76</b>
<b>Figura 22. Creación de la clase de contabilización</b>	<b>76</b>
<b>Figura 23. Creación del portal cautivo</b>	<b>77</b>
<b>Figura 24. Ventana de Autenticación</b>	<b>78</b>
<b>Figura 25. Ventana emergente Popup</b>	<b>78</b>
<b>Figura 26. Configuración para gestión de ancho de banda</b>	<b>79</b>
<b>Figura 27. Creación de las clases de QoS</b>	<b>79</b>
<b>Figura 28. Nombre de la clase para el plan de 4 Mbps</b>	<b>80</b>
<b>Figura 29. Características para el plan de 4 Mbps</b>	<b>80</b>
<b>Figura 30. Opción Classifier del Zeroshell donde se especifica el rango de IP al cual se le va a limitar el ancho de banda</b>	<b>81</b>
<b>Figura 31. Creación de nueva regla para un ancho de banda determinado</b>	<b>81</b>
<b>Figura 32. Asignación de clases creadas a la interfaz de red</b>	<b>82</b>
<b>Figura 33. Monitoreo y control de red airControl</b>	<b>83</b>
<b>Figura 34. Pantalla de inicio de la interfaz web de Elastix</b>	<b>84</b>
<b>Figura 35. Parqueo de llamadas en Elastix</b>	<b>85</b>
<b>Figura 36. Configuración del Buzón de Voz</b>	<b>86</b>
<b>Figura 37. Configuración de la llamada en espera</b>	<b>86</b>
<b>Figura 38. Cuentas de usuario para el softphone</b>	<b>88</b>
<b>Figura 39. Parámetros para crear una cuenta de usuario</b>	<b>88</b>
<b>Figura 40. Conexión del teléfono IP</b>	<b>89</b>
<b>Figura 41. Conexión para uso del teléfono análogo</b>	<b>90</b>

<b>Figura 42. Portal de inicio CDR</b>	<b>90</b>
<b>Figura 43. Monitoreo de llamadas en tiempo real</b>	<b>91</b>
<b>Figura 44. Resumen de llamada para el usuario destino</b>	<b>92</b>
<b>Figura 45. Medición de QoS para el usuario fuente</b>	<b>92</b>
<b>Figura 46. Creación de Alertas para mediciones de QoS</b>	<b>93</b>
<b>Figura 47. Interfaz web del airOS</b>	<b>94</b>

## LISTA DE ANEXOS

	pág.
<b>Anexo A: Sistema operativo AirOS</b>	<b>113</b>
<b>Anexo B: Configuración de Teléfonos</b>	<b>134</b>
<b>Anexo C: Información sobre VoIP Monitor</b>	<b>139</b>
<b>Anexo D: Características de airControl</b>	<b>140</b>
<b>Anexo E: características del servidor de VoIP Elastix</b>	<b>143</b>
<b>Anexo F: Prueba de tráfico para el enlace inalámbrico</b>	<b>146</b>
<b>Anexo G: Configuración del servidor DNS</b>	<b>153</b>
<b>Anexo H: Configuración de la distribución Zeroshell</b>	<b>157</b>
<b>Anexo I: Manual de Usuario</b>	<b>163</b>

## GLOSARIO

**ANCHO DE BANDA:** se define técnicamente como la cantidad de información o de datos que se puede enviar a través de una conexión de red en un periodo de tiempo dado. El ancho de banda se indica generalmente en bytes por segundo (bps), kilobytes por segundo (kbps), o megabytes por segundo (Mbps)

**ARQUITECTURA DE RED:** una arquitectura de red se puede definir como el conjunto de capas y protocolos que constituyen un sistema de comunicaciones.

**ASTERISK:** software de licencia GLP para la gestión PBX utilizando telefonía IP.

**CDRs:** call detail records, contienen información detallada sobre la procedencia de las llamadas

**CODECS:** viene del inglés coder-decoder, convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo.

**CPE:** customer premises equipment, equipo local del cliente, es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación.

**ECO:** se define como una reflexión retardada de la señal acústica original.

**E-MODEL:** modelo computacional útil para los planificadores de transmisión, que ayuda a garantizar que los usuarios estarán satisfechos con el rendimiento de transmisión de extremo a extremo.

**G.711 A-LAW/U-LAW:** estándar de la ITU-T para la codificación de audio. Para este estándar existen dos métodos principales, el u-Law, usado en Estados Unidos y Japon y el A-law (usado en Europa y el resto del mundo).

**IEEE 802.11a/n:** estándar que define el uso de los dos niveles inferiores de la arquitectura OSI, especificando sus normas de funcionamiento en una WLAN. El estándar IEEE 802.11a/n es el más reciente ya que también existe el IEEE 802.11 b/g.

**iLBC:** codec open-source desarrollado por Global IP Solutions.

**IMS:** ip multimedia subsystem, es una arquitectura global de acceso, servicios y conectividad que permiten diversas clases de servicios multimedia a usuarios terminales usando el protocolo IP.

**ITU-T:** sector de normalización de las telecomunicaciones de la UIT (UIT-T), con sede en Ginebra (Suiza), es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT).

**ITU-T G.107:** recomendación que da el algoritmo para el llamado E-model

**JITTER:** variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdidas de sincronización o por las diferentes rutas seguidas por los paquetes para llegar a su destino.

**LATENCIA:** denominado también retardo (delay). Se define como el tiempo que tarda un paquete en llegar desde la fuente al destino.

**MAC:** media access control, identificador de 48 bits (6 bloques hexadecimales) que corresponden de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física y es única para cada dispositivo.

**MIMO:** multiple input multiple output, es una tecnología que se refiere a enlaces de radio con múltiples antenas en el lado del transmisor y del receptor.

**MOS:** mean opinion score, es un método subjetivo de medida de la calidad de servicio que resulta en un promedio de opinión de los usuarios. Es la evaluación subjetiva más ampliamente usada, estandarizada en la recomendación ITU-T P.800

**PACKET LOSS:** pérdida de paquetes

**PORTAL CAUTIVO:** es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por internet de forma normal.

**PROTOCOLO AAA:** protocolo que realiza tres funciones: Autenticación, Autorización, Contabilización.

**QoS:** quality of service, efecto global de las prestaciones de un servicio que determinan el grado de satisfacción de un usuario al utilizar dicho servicio

**SNIFFER:** programa que captura tramas de la red.

**THROUGHPUT:** velocidad real de transporte. Se define como la tasa promedio de los paquetes entregados con éxito sobre un canal de comunicación.

**WLAN:** red de área local inalámbrica

## RESUMEN

Los proveedores de servicios de internet (ISP) son empresas que proporcionan información muy restringida en cuanto a su arquitectura interna de red, funcionamiento y procedimientos empleados para prestar los servicios que ofrecen. Además de esto en la Universidad Autónoma de Occidente no se encuentra información que permita conocer dichos procesos.

Por tal razón se propone éste proyecto denominado Diseño e implementación de un ISP con acceso inalámbrico para soportar servicios de internet y telefonía IP en el laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente, para el cual se elaborará una guía que permita a los estudiantes interesados por las telecomunicaciones conocer y comprender el funcionamiento real de los proveedores de servicios de internet.

El proyecto se presenta en 7 capítulos organizados así:

El primer capítulo trata sobre los antecedentes que se han realizado anteriormente en la UAO sobre ISP y telefonía IP.

El segundo capítulo muestra el planteamiento del problema.

El tercer capítulo presenta los objetivos tanto generales como específicos.

El cuarto capítulo muestra la justificación del por qué se realiza este proyecto.

El quinto capítulo trata sobre el marco teórico que muestra lo qué es un ISP, su arquitectura, en qué consiste la red de acceso, la red de núcleo, la gestión de la red, qué servicios ofrece el ISP y lo relacionado con los protocolos de la telefonía IP.

El sexto capítulo muestra paso por paso el diseño del ISP con acceso inalámbrico que soporta servicios de Internet y telefonía IP.

Y finalmente, el séptimo capítulo expone la implementación paso por paso del ISP con acceso inalámbrico que soporta servicios de Internet y telefonía IP.

**Palabras claves: ISP, Redes Inalámbricas, VoIP, Arquitectura de Red, Servicios de Red, Gestión de Red, Autenticación.**

## INTRODUCCIÓN

Los proveedores de servicios de internet (ISP) son empresas que brindan conexión a Internet a sus clientes a través de diferentes tecnologías de acceso como DSL, Cable módem, Wifi, entre otros. Estos ISP han tenido una amplia expansión y evolución alrededor del mundo, ofreciendo internet a todos los hogares, empresas e instituciones que requieren de este servicio para sus labores diarias y una comunicación permanente. Con la evolución de la digitalización y empaquetamiento de la voz, los ISP actuales además ofrecen el servicio de Telefonía IP, que permite la comunicación por voz a diferentes usuarios utilizando una arquitectura de red similar a la que se da en internet, Web hosting, DNS, entre otros. De igual forma y paralelo a la evolución de los servicios de la red, la implementación de redes de acceso inalámbricas se han hecho populares gracias a su versatilidad y bajo costo.

En Colombia se pueden conocer diferentes ISP que ofrece sus servicios de internet y telefonía IP como es el caso de Movistar, Claro, UNE, ETB; y a nivel local como es el caso de Ecali, ERT, entre otros. Cada proveedor tiene su determinada tarifa de conexión, sus planes de ancho de banda según la petición del usuario. Además deben velar por una buena calidad del servicio para que no se presenten inconvenientes tanto para la transmisión de datos en Internet como para la transmisión de voz por telefonía IP.

Recientemente la Universidad Autónoma de Occidente adquirió los equipos de telecomunicaciones necesarios para implementar la red de acceso de un ISP a pequeña escala, sin embargo no se encuentra aún con ningún procedimiento o montaje establecido que permita observar el funcionamiento y estructura de la red si se tratara de ofrecer servicios de internet y telefonía IP utilizando dicha tecnología en el mundo real.

Por la anterior razón, este proyecto pretende diseñar e implementar una red Wifi Airmax con dos áreas de cobertura unidas inalámbricamente por un enlace punto a punto, donde además se establece un servidor que permite autenticar, autorizar y tarificar usuarios, junto con un sistema de gestión de red, y control de ancho de banda dependiendo de la necesidad del usuario, con el fin de soportar el servicio de internet y telefonía IP en el laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente. Este proyecto permite tener una herramienta para que los estudiantes de la facultad de Ingeniería interesados en el área de las telecomunicaciones tengan un concepto general y claro del funcionamiento de un ISP y de la forma en que soporta los servicios de internet y telefonía IP a usuarios, teniendo un amplio panorama desde cómo se administra el servicio hasta cómo se

transmite la información por el medio físico, que en este caso es inalámbrico. Con base a lo anterior se genera un documento o guía que permite mostrar el procedimiento establecido para brindar dichos servicios.



## 1. ANTECEDENTES

Se han realizado diferentes diseños e implementaciones en el campo de las telecomunicaciones y las redes de computadores a nivel de tesis, pero no se han desarrollado implementaciones de redes inalámbricas para proveer servicio de internet y telefonía IP, y que a su vez ofrezca un proceso de aprendizaje sobre el funcionamiento de un proveedor de servicio de internet, como se pretende en este proyecto. Estos diseños que se han realizado tienen conceptos y aplicaciones relacionados a la telefonía IP, al diseño de redes LAN, a la red inalámbrica, estructura de red de datos, entre otros temas que van de la mano con la temática que se maneja en este documento.

Se realizó la implementación de un PBX utilizando Asterisk integrado a la plataforma ZTE de Emcali, el cual el software es implementado en Fenalco con el fin de brindar una oportunidad para el aprovechamiento de los múltiples servicios en telefonía IP como tecnología óptima para la comunicación de voz y datos, y obtener beneficios económicos del servicio. Se implementa en Asterisk música de fondo mientras el usuario se encuentra en espera, se instaura una contestadora automática que dirija llamadas automáticamente a diversas áreas de la empresa, se instaura un grabador de llamadas y se pretende utilizar Asterisk como pasarela para unas aplicaciones existentes sobre plataforma Windows con soporte SIP<sup>1</sup>.

Se realizó el desarrollo e implementación de un servicio de operadora automática bajo Asterisk para Emcali Telecomunicaciones, en el cual se amplían los servicios ofrecidos a los clientes de red inteligente de Emcali Telecomunicaciones, ya que se requería de un servicio de operadora automático que no necesitara de una infraestructura de software o hardware en comparación con otras soluciones de telefonía IP, y que por medio de algunas políticas y recomendaciones facilitara la implementación de futuros servicios. En este proyecto se definen los requerimientos y las herramientas a utilizar para posteriormente diseñar e implementar el servicio de operadora automática sobre la red multiservicios de Emcali Telecomunicaciones<sup>2</sup>.

---

<sup>1</sup> GARCIA CORTÉS, Juan Sebastián. Implementación de un PBX utilizando Asterisk integrado a la plataforma ZTE de Emcali. Trabajo de Grado Ingeniero Informático. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería. 2009.

<sup>2</sup> ESCOBAR PAZ, Lina Marcela. Desarrollo e implementación de un servicio de operadora automática bajo Asterisk para Emcali Telecomunicaciones. Trabajo de grado Ingeniero Informático. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería. 2008.

Se llevó a cabo la implementación de una red Wireless (WLAN) con seguridad basada en autenticación con Public Key Infrastructure (PKI), en donde la autenticación se ejecuta con VPN y Token PKI. Esta implementación se realizó en las instalaciones de Johnson y Johnson en Cali, Colombia, para permitir el acceso inalámbrico seguro de los empleados de dicha compañía de acuerdo a las políticas y lineamientos globales de la empresa para la implementación de redes inalámbricas. El montaje se realizó con equipos CISCO (Access Point) y Nortel Networks (switchcontivity), teniendo en cuenta la capacidad de cobertura de la red y la cantidad de equipos que se requieren. Se configura el Access Point en el equipo contivity para la autenticación VPN y en los VLANs. Con este proyecto se provee beneficios de movilidad, convivencia y acceso a la red donde el cableado estructurado no puede llegar y donde además se provee soporte a la infraestructura wireless, incluyendo capacitación y soporte al usuario final<sup>3</sup>.

Otro proyecto que se llevó a cabo fue el diseño de la red de datos del edificio Versalles de la Alcaldía de Cali, que nace de las necesidades de compartir los recursos y traspaso de documentos entre los usuarios del edificio Versalles y el CAM y solucionaría los problemas actuales de conectividad y comunicación proponiendo un diagnóstico y análisis de tráfico general de la red y diseño de funcionalidad, escalabilidad y adaptabilidad de la misma. Se toman en cuenta las normas y recomendaciones para la realización de redes clásicas, los elementos a utilizar en la red, los tipos de conectividad, el tipo de cableado, la infraestructura y distribución de la red, el direccionamiento, los tipos de comunicaciones, los accesos, tráfico y control de paquetes. Adicionalmente, se realiza la simulación del diseño en un software disponible que permita evaluar la posible solución a la problemática que abarca el proyecto<sup>4</sup>.

Los anteriores diseños e implementaciones que fueron realizados, referente a la temática de las telecomunicaciones, muestran que no se ha ejecutado un proyecto que tenga presente el funcionamiento de una ISP y que este servicio tanto de internet como telefonía IP sea transmitido por una red inalámbrica, además de dar un proceso de aprendizaje a los estudiantes para que conozcan todo el procedimiento de administración y transmisión en una ISP.

---

<sup>3</sup> LOBOA GONZALEZ, Harry Famith. Implementación de una red Wireless (WLAN) con seguridad basada en autenticación con Public Key Infrastructure (PKI). Trabajo de grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2006.

<sup>4</sup> ALVARADO GUZMAN, Jesús. Diseño de la red de datos del edificio Versalles de la Alcaldía de Cali. Trabajo de Grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2009

## **2. PROBLEMA DE INVESTIGACIÓN**

### **2.1. PLANTEAMIENTO DEL PROBLEMA**

Cabe resaltar que en la Universidad Autónoma de Occidente no hay montajes de ISP y no se encuentra ningún manual o guía que permita conocer de forma detallada el funcionamiento de un ISP, teniendo en cuenta que las compañías ISP ofrecen poca información respecto a su estructura interna y funcionamiento, por lo cual es muy difícil para los estudiantes de telecomunicaciones ver y comprender el funcionamiento real de un proveedor de servicios de internet.

Por tal razón se pretende diseñar e implementar una red inalámbrica, con la cual se pueda soportar el servicio de internet y telefonía IP a una zona. Para esto es necesario montar servidores que permitan autenticar, autorizar y tarificar usuarios, como también tener un sistema de gestión de fallos, control de ancho de banda, y dependiendo de la necesidad del usuario, ofrecer un servicio Dobleplay.

Todo lo anterior se pretende que funcione en tiempo real y su implementación utiliza un esquema similar que usan los ISP, con lo cual se dejará documentación referente y guías que permitan entender su proceso de implementación, operación y mantenimiento.

### 3. JUSTIFICACIÓN

Es importante manejar las tecnologías existentes en redes de comunicación que permitan entender el proceso de cómo un ISP presta los servicios de voz y datos, con el fin de ampliar el conocimiento de la forma en que se administra y se transporta el servicio de internet y de cómo llega a los usuarios finales, además de poder aplicar la tecnología de VoIP para realizar llamadas telefónicas.

Se desea mostrar el funcionamiento de un ISP de forma clara y objetiva, que el estudiante en telecomunicaciones pueda analizar y comprender toda su funcionalidad a partir de un modelo a pequeña escala y lo más importante, es que pueda interactuar con el sistema y ampliar el conocimiento de lo que se tiene en el mundo real.

El estudiante en telecomunicaciones y cualquier persona interesada en esta temática conocerá desde los servidores que se necesitan para autenticar, autorizar y tarificar el servicio de Internet a los usuarios de una red, su configuración, su interacción con el medio físico, hasta el medio de transmisión que se utiliza en la comunicación, el cual es inalámbrico donde se maneja la tecnología WIFI.

Por lo anterior, se resalta la importancia de tener una implementación real de una red inalámbrica que ofrezca servicio de internet y de telefonía IP en el laboratorio de telecomunicaciones y que esto pueda servir como herramienta de aprendizaje para los estudiantes interesados en este tema, ya que hace falta un procedimiento establecido o guía sobre cómo realizar la estructura de una red que permita ofrecer dichos servicios.

## **4. OBJETIVOS**

### **4.1 OBJETIVO GENERAL**

Diseñar e implementar una arquitectura de red que permita soportar servicios de voz y datos, empleando tecnologías de acceso inalámbrico de banda ancha presentes en el laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente.

### **4.2 OBJETIVOS ESPECÍFICOS**

Son planteados los siguientes objetivos específicos que llevarán al cumplimiento del objetivo general

- Diseñar e implementar una red WIFI Airmax con dos áreas de cobertura unidas inalámbricamente por un enlace punto a punto.
- Implementar un servidor en Linux que permite autenticar, autorizar y tarificar usuarios.
- Implementar un sistema de gestión fallos y control de la red.
- Realizar un sistema que permita controlar el ancho de banda de los usuarios dependiendo del pago de su tarifa.
- Implementar un servicio Dobleplay que integre internet y telefonía IP.
- Elaborar un documento guía para que el sistema pueda ser aprovechado como herramienta de enseñanza y aprendizaje.

## 5. MARCO DE REFERENCIA

### 5.1 MARCO TEÓRICO

Para el diseño de un proveedor de servicio de internet (ISP) con acceso inalámbrico se requiere del conocimiento de distintos conceptos y aplicaciones de tecnologías que son base fundamental para su posterior implementación. Es importante comenzar con el concepto, funcionamiento y estructura de un ISP para conocer el proceso de cómo se prestan los distintos servicios. Principalmente un ISP está conformado por una red de acceso y una de red de núcleo; en la red de acceso se encuentran diferentes tecnologías que permiten la conexión final con los usuarios, en este caso se enfatiza en la red inalámbrica donde se maneja la tecnología WIFI. En la red de núcleo se encuentran todos los equipos y servidores que realizan la autenticación de los clientes, el control de ancho de banda, el encaminamiento del tráfico, la señalización, el envío y recibimiento de mensajes por internet (correo electrónico) entre otros servicios que permitan un control y distribución óptimo del servicio de internet. El segundo servicio que ofrece el ISP es el de Telefonía IP que consiste en la transmisión de paquetes de voz utilizando redes de datos y realizando la comunicación por medio del protocolo IP (Internet Protocol) para ejecutar llamadas de voz.

**5.1.1 ISP.** Internet Service Provider, ISP, es una compañía que suministra el servicio de internet a sus usuarios, a través de diferentes tecnologías como DSL, Cable modem, Dial-up y Wifi. Un ISP también ofrece servicios como email, Web hosting, DNS, FTP, voz sobre IP (VoIP), mensajería multimedia entre otros.

Entre los objetivos de estas compañías se tiene:

- Mantener siempre la conectividad entre internet y sus clientes, para ello se debe disponer de un sistema de gestión de fallas.
- Mantener siempre los servicios básicos de un ISP.

Entre las consideraciones principales a tener en cuenta para diseñar un ISP a pequeña y mediana escala se encuentran:

- Cuál es el número de clientes conmutados y dedicados.
- Cuál es el ancho de banda asignado a los clientes.
- Cuáles servicios se prestarán en forma local desde la red interna, y cuáles desde Internet.
- Cuál es la estimación absoluta y porcentual de tráfico local y externo.

- Qué nivel de tolerancia a fallas se desea para el Sitio.
- Qué tiempo promedio, y mínimo entre fallos se espera.
- Cuál será el tiempo de recuperación de en fallos.
- Qué alternativas de redundancia se utilizarán<sup>5</sup>.

La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio. En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente. Los ISP son designados por una jerarquía basada en su nivel de conectividad a la backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior<sup>6</sup>.

**Nivel 1:** En la parte superior de la jerarquía de ISP están los ISP de nivel 1, como se muestra en la figura 1.

Éstos son grandes ISP a nivel nacional o internacional que se conectan directamente al backbone de Internet. Los clientes de ISP de nivel 1 son ISP de menor nivel o grandes compañías y organizaciones. Debido a que se encuentran en la cima de la conectividad a Internet, ofrecen conexiones y servicios altamente confiables. Entre las tecnologías utilizadas como apoyo de esta confiabilidad se encuentran múltiples conexiones al backbone de Internet. Las principales ventajas para los clientes de ISP de nivel 1 son la confiabilidad y la velocidad. Debido a que estos clientes están a sólo una conexión de distancia de Internet, hay menos oportunidades de que se produzcan fallas o cuellos de botella en el tráfico. La desventaja para los clientes de ISP de nivel 1 es el costo elevado<sup>7</sup>.

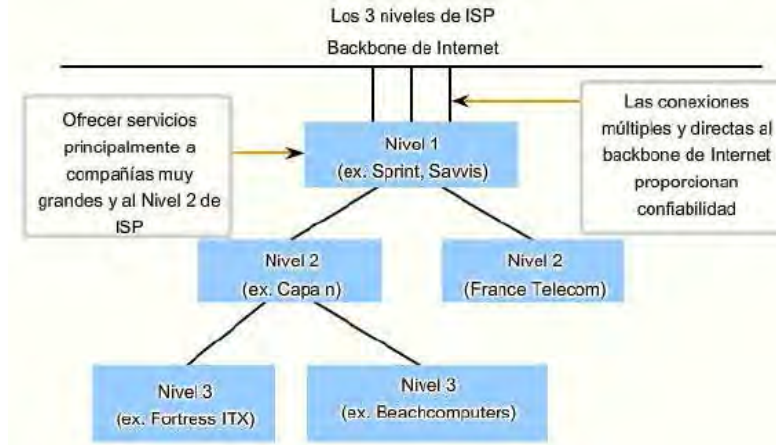
---

<sup>5</sup> Proveedor Servicio de Internet ISP [En línea]. Guayaquil: Escuela Superior Politécnica del Litoral, 2005 [consultado 07 de Mayo de 2013]. Disponible en Internet: [http://www.dspace.espol.edu.ec/bitstream/123456789/5614/17/ISP\\_Capitulo2.docx](http://www.dspace.espol.edu.ec/bitstream/123456789/5614/17/ISP_Capitulo2.docx)

<sup>6</sup> Capítulo 6 Direccionamiento de la red: IPv4 [En línea]. Cisco Networking Academy, 2007 [consultado 11 de Febrero de 2013]. Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>

<sup>7</sup> Capítulo 6 Direccionamiento de la red: IPv4, Op. cit., Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>

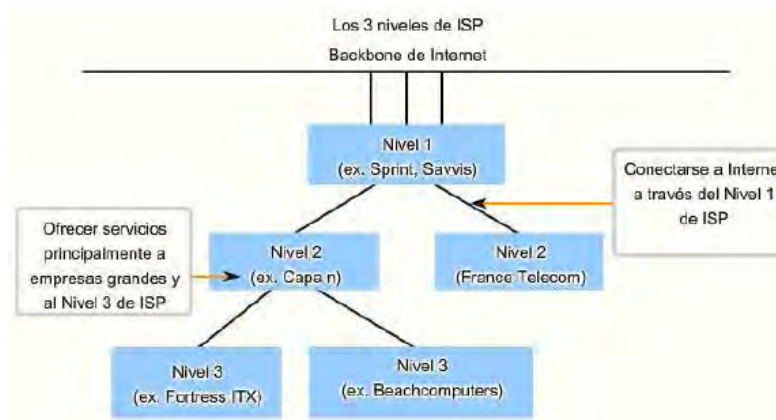
**Figura 1. ISP de Nivel 1**



**Fuente:** Capitulo 6 Direccionamiento de la red: IPv4 [En línea]. Cisco Networking Academy, 2007 [consultado 11 de Febrero de 2013]. Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>

**Nivel 2:** Los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1, como se muestra en la figura 2.

**Figura 2. ISP de nivel 2**



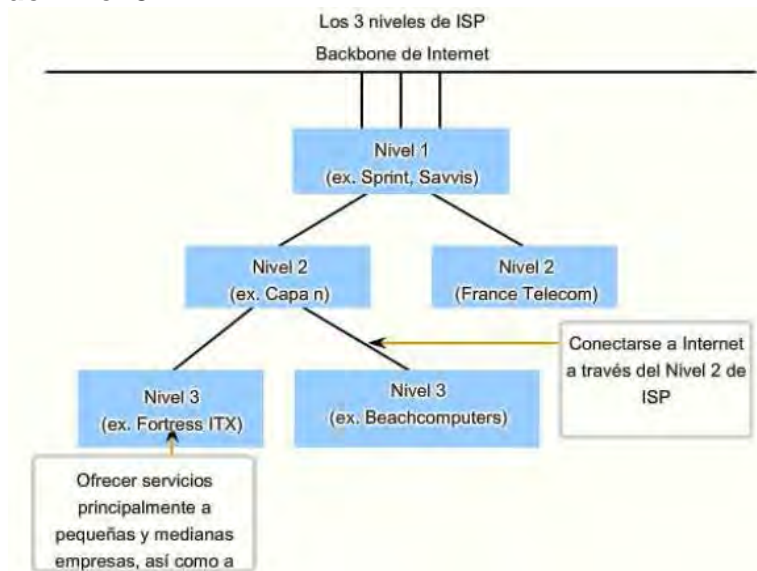
**Fuente:** Capitulo 6 Direccionamiento de la red: IPv4 [En línea]. Cisco Networking Academy, 2007 [consultado 11 de Febrero de 2013]. Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>



Los ISP de nivel 2 generalmente se centran en los clientes empresa. Estos ISP normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus propios servicios como DNS, servidores de correo electrónico y servidores web. Otros servicios ofrecidos por los ISP de nivel 2 pueden incluir desarrollo y mantenimiento de sitios web, e-commerce/e-business y VoIP. La principal desventaja de los ISP de nivel 2, comparados con los ISP de nivel 1, es el acceso más lento a Internet. Como los IPS de Nivel 2 están al menos a una conexión más lejos de la backbone de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1<sup>8</sup>.

**Nivel 3:** Los ISP de nivel 3 compran su servicio de Internet de los ISP de nivel 2, como se muestra en la figura 3.

**Figura 3. ISP de nivel 3**



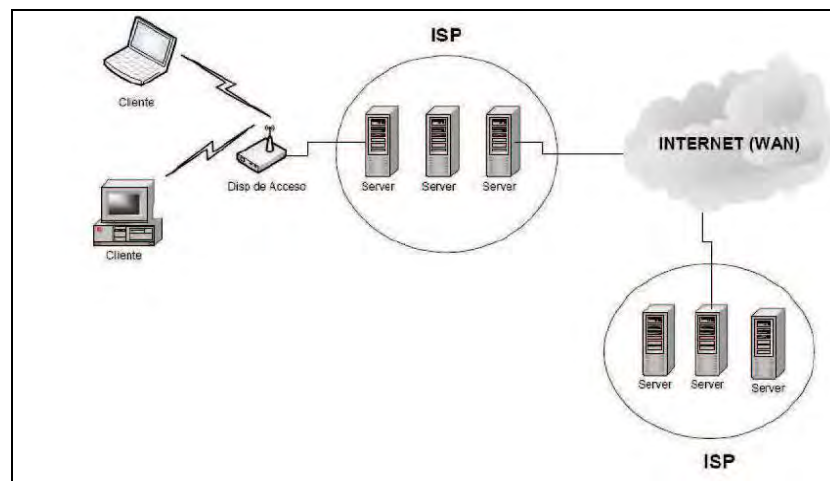
**Fuente:** Capítulo 6 Direccionamiento de la red: IPv4 [En línea]. Cisco Networking Academy, 2007 [consultado 11 de Febrero de 2013]. Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>

<sup>8</sup> Capítulo 6 Direccionamiento de la red: IPv4, Op. cit., Disponible en Internet: <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/APENDICE.Direccionamiento-de-la-red.pdf>

El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica. Típicamente, los clientes del nivel 3 no necesitan muchos de los servicios requeridos por los clientes del nivel 2. Su necesidad principal es conectividad y soporte. Estos clientes a menudo tienen conocimiento escaso o nulo sobre computación o redes. Los ISP de nivel 3 suelen incluir la conectividad a Internet como parte del contrato de servicios de red y computación para los clientes. A pesar de que pueden tener un menor ancho de banda y menos confiabilidad que los proveedores de nivel 1 y 2, suelen ser buenas opciones para pequeñas y medianas empresas.

**5.1.2 Arquitectura de un ISP.** Los proveedores de servicios de internet ofrecen los recursos necesarios tanto de hardware como de software, para que a través de ellos se permita el acceso a la red o a una conexión a internet.

**Figura 4. Arquitectura de un ISP**



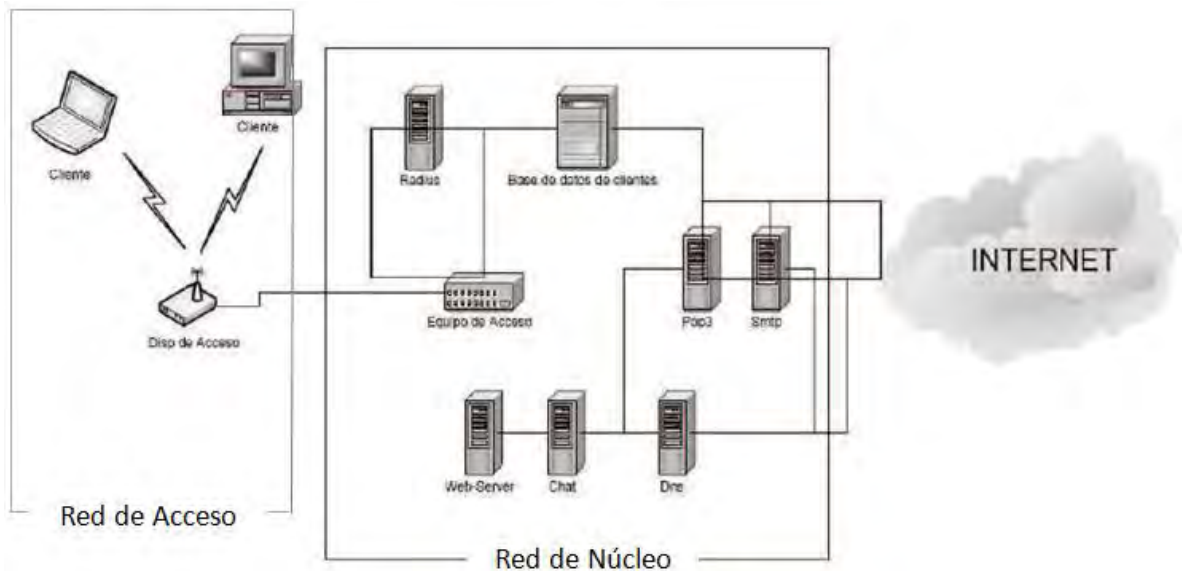
**Fuente:** VELASCO RIVERA, Milton René. Diseño de un WISP en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema wireless mesh con tecnología wi-fi. Trabajo de grado Ingeniero Electrónico y Telecomunicaciones. Quito: Escuela Politécnica Nacional. Facultad de Ingeniería Eléctrica y Electrónica, 2000. p. 32.

La calidad de servicio, incluyendo una rápida conectividad, es esencial en la prestación de servicios IP, de ahí que el diseño de la infraestructura de los proveedores de internet se caracterice actualmente por una elevada redundancia

en todos los elementos de alta escalabilidad y fiabilidad, y por la presencia de múltiples enlaces de alta capacidad<sup>9</sup>.

Un ISP inalámbrico se encuentra conformado de equipos servidores, equipos de administración, equipos de facturación, etc., los mismos que permiten realizar un control de cada uno de los recursos del ISP. Los sistemas ISP permiten también brindar el servicio de acceso a Internet, y además permite la comunicación entre clientes inalámbricamente, mediante un dispositivo de acceso<sup>10</sup>. La arquitectura de un ISP se puede organizar en dos secciones como se muestra en la figura 5:

**Figura 5. Estructura interna de un ISP**



**Fuente:** VELASCO RIVERA, Milton René. Diseño de un WISP en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema wireless mesh con tecnología wi-fi. Trabajo de grado Ingeniero Electrónico y Telecomunicaciones. Quito: Escuela Politécnica Nacional. Facultad de Ingeniería Eléctrica y Electrónica, 2000. p. 36.

---

<sup>9</sup> VELASCO RIVERA, Milton René. Diseño de un WISP en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema wireless mesh con tecnología wi-fi. Trabajo de grado Ingeniero Electrónico y Telecomunicaciones. Quito: Escuela Politécnica Nacional. Facultad de Ingeniería Eléctrica y Electrónica, 2000. p. 50.

<sup>10</sup> *Ibíd.*, p. 36.

- **Red de núcleo:** El núcleo es donde se localizan los equipos de alta capacidad de transmisión. En este bloque se encuentran los elementos centrales de red, los cuales son capaces de administrar y gestionar. Aquí se encuentran los servidores AAA, la plataforma de servicio, la red IMS y sistemas de cobros, servicio de correo electrónico, etc. La cantidad de tráfico que circula por esta red depende de la densidad de routers de concentración ya que las exigencias de las redes actuales son cada vez mayores. Igualmente cuando la velocidad de acceso se incrementa, su rendimiento mejora, siendo la densidad de routers la que logra evitar que se produzcan picos en partes de la red<sup>11</sup>.

- **Red de acceso:** La red de acceso es la que conecta al usuario directamente con la red, donde los únicos dispositivos de red más allá de la capa de acceso pueden ser teléfonos IP, puntos de acceso inalámbrico u otros en las instalaciones del cliente<sup>12</sup>.

**5.1.2.1 Red de Acceso.** La red de acceso conecta los terminales de usuario, de forma individual con el núcleo de la red. Existen dos grandes tipos de redes de acceso:

- Acceso por cable físico, dentro del cual se encuentran las siguientes tecnologías:

- Bucle digital de abonado. (xDSL)
- Redes híbridas de fibra óptica y cable coaxial. (HFC)
- Fibra óptica
- Comunicaciones por línea eléctrica (PLC).
- Ethernet

- Acceso inalámbrico:

- Bucle inalámbrico (WLL)
- Redes de acceso por satélite
- Redes locales inalámbricas (WLAN)

- **Redes Inalámbricas.** Las redes inalámbricas (wireless network) son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas. Normalmente, el emisor tiene una sola antena, pero puede tener varias, ya que

---

<sup>11</sup> VELASCO RIVERA, Op. Cit, p. 39.

<sup>12</sup> Ibíd., p. 40.

existen sistemas que emplean dos, tres e incluso hasta cuatro antenas. Unas antenas se usan para emisión, otras para la recepción y normalmente, la mayoría de veces, la misma antena permite actuar de ambos modos.

Las redes inalámbricas no solo se emplean para realizar conexiones de datos, con frecuencia se utilizan para emitir señal de televisión, en telefonía, para seguridad, para sensores, domótica, etc<sup>13</sup>. Las ventajas que ofrece este medio son muchas:

- Rápida instalación de la red: No necesita cablear, ni pedir permisos de obras, levantar las calles y calzadas de las ciudades, etc.
- Permiten movilidad: el medio de transmisión (de envío y recepción) no está sujeto a ningún cable, lo que permite una movilidad dentro del radio de recepción de la señal.
- Menos costes de mantenimiento: al no tener cableado, los costes de mantenimiento se reducen.
- Accesibilidad: casi todos los móviles, PDA y portátiles soportan o incluyen varias tecnologías inalámbricas.
- Productividad: las redes inalámbricas propician colaboración, el teletrabajo, etc.
- Es la única solución para zonas a las que no llega el cableado, como es el caso de zonas rurales diseminadas.

Pero también tiene desventajas insalvables e impredecibles:

- Interferencias externas: de otros emisores de microondas.
- Falta de seguridad: al emitirse libremente por el aire puede ser interceptado por cualquiera, lo que requiere aumentar la seguridad y la encriptación.
- Más costes iniciales: los dispositivos, antenas, etc. son más caros.
- La velocidad es más limitada.

---

<sup>13</sup> ANDREU GOMEZ, Joaquín. Servicios en red. Madrid: Editex, 2010. p. 212.

Actualmente, la libertad que ofrecen las redes inalámbricas hace que sean las que más proliferan. Además, los nuevos dispositivos móviles (teléfonos, PDA, mini portátiles, etc), que llevan incorporadas estas tecnologías, están vendiéndose exponencialmente<sup>14</sup>.

La red inalámbrica que se maneja para el acceso de los clientes al ISP es la WLAN, en donde se implementa la tecnología WIFI basada en el estándar IEEE 802.11.

Las redes inalámbricas utilizan las bandas de radiofrecuencia ISM (Industrial, Scientific and Medical), en las bandas 2.4 y 5 GHz. Estas bandas permiten el funcionamiento de sistemas sin necesidad de licencia y atendiendo a la normativa propia de potencia emitida de cada país<sup>15</sup>. También existen bandas licenciadas como las que usa la telefonía móvil y la tecnología Wimax.

A la telefonía móvil se le atribuyen las bandas de frecuencia 824-849 MHz y 869-894 MHz. A la tecnología Wimax se le atribuyen las bandas de frecuencia 3400-3600 MHz<sup>16</sup>.

Las redes inalámbricas permiten tres configuraciones distintas:

- **Enlaces punto a punto:** Generalmente se usan para conectarse a internet donde dicho acceso no está disponible de otra forma. Unos de los lados del enlace punto a punto estará conectado a internet, mientras que otro utiliza el enlace para acceder al mismo. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto seguros de más de 30 Km. Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a internet, se pueden configurar este tipo de enlaces para transmitir grandes cantidades de datos (incluyendo audio y video) entre dos puntos, aún en ausencia de conexión a internet<sup>17</sup>. Esta configuración se puede observar en la figura 6.

---

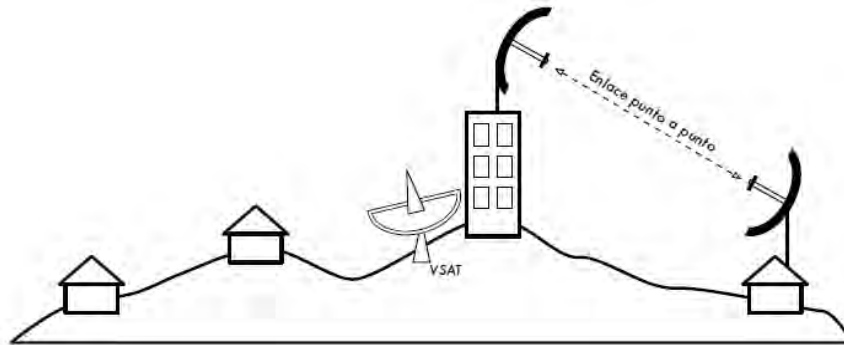
<sup>14</sup> ANDREU, Op. cit., p.212

<sup>15</sup> SALLENTO ROIG, Oriol y VALENZUELA GONZÁLEZ, Jose L. Principios de comunicaciones móviles. Barcelona: Universidad Politécnica de Cataluña, 2003. p. 38.

<sup>16</sup> Cuadro Nacional de Atribución de Bandas de Frecuencia [En línea]. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, 2010 [consultado 1 de Abril de 2006]. Disponible en Internet: <http://archivo.mintic.gov.co/mincom/documents/portal/documents/root/espectro%20radioelectrico/CuadroNacionalAtribucionBandasdeFrecuencias2010.pdf>

<sup>17</sup> FLICKENGER, Rob y AICHELE, Corinna. Redes inalámbricas en los países en desarrollo. 2 ed. Londres: Limehouse Book Sprint Team, 2007. p. 30-31.

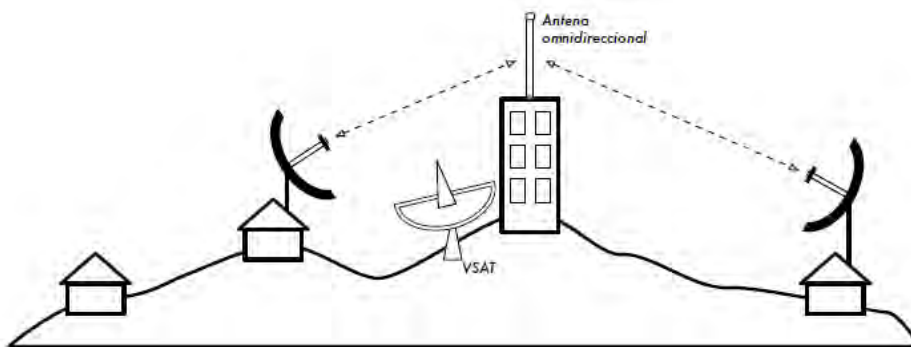
**Figura 6. Enlace punto a punto**



**Fuente:** FLICKENGER, Rob y AICHELE, Corinna. Redes inalámbricas en los países en desarrollo. 2 ed. Londres: Limehouse Book Sprint Team, 2007. p. 30.

- **Punto a multipunto:** En esta red varios nodos están conectados a un punto central. El ejemplo típico de esta disposición es el uso de un punto de acceso inalámbrico que provee conexión a varios computadores portátiles. Los computadores portátiles no se comunican directamente unos con otros, pero deben estar en el rango del punto de acceso para utilizar la red<sup>18</sup>.

**Figura 7. Enlace punto a multipunto**



**Fuente:** FLICKENGER, Rob y AICHELE, Corinna. Redes inalámbricas en los países en desarrollo. 2 ed. Londres: Limehouse Book Sprint Team, 2007. p. 31.

- **Multipunto a multipunto:** También es denominado red *ad hoc* o en malla (mesh). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los

---

<sup>18</sup> FLICKENGER y AICHELE, Op. cit., p. 31.

nodos se comunican directamente entre sí. El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. Las buenas implementaciones de redes *mesh* son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red *mesh* es tan sencillo como agregar más nodos. Si uno de los nodos tiene acceso a internet, esa conexión puede ser compartida por todos los clientes<sup>19</sup>.

- **Arquitectura de redes WLAN.** Una red inalámbrica de área local WLAN 802.11a consiste en una estructura que posee un conjunto básico de servicios o Basic Service Set (BSS) compuesta de estaciones o nodos inalámbricos que son conectadas a una capa de distribución de red o DS. Cada BSS está conformado por nodos móviles o estaciones que acceden al medio a través del acceso múltiple por detención de portadora con evasión de colisiones (CSMA/CA), el cual determina que nodo tiene derecho a transmitir o recibir información en el medio inalámbrico de radio propagación.

Las estaciones en un BSS obtienen acceso a la capa DS y por lo tanto a otros nodos inalámbricos fuera de su área de cobertura a través del AP (Access Point). La capa DS soporta la movilidad de los nodos mediante direccionamiento e integración de forma transparente a la computación interna de la información en las estaciones<sup>20</sup>. Como se observa en la figura 8, los AP (Access Point) que están conectados a un sistema de distribución (DSS) deben situarse estratégicamente para proporcionar la mayor cobertura a sus clientes. Siguiendo este esquema, los puntos de acceso funcionan proporcionando servicios de conectividad, actuando como servidor, y las maquinas que se conectan al punto de acceso funcionan como clientes.

El IEEE ratificó en julio de 1999 el estándar en 802.11a, que con una modulación 64-QAM y la codificación OFDM (Orthogonal Frequency Division Multiplexing) alcanza velocidades de hasta los 54 Mbps, pero utiliza frecuencias superiores a los 5 GHz, lo que produce incompatibilidades con el 802.11b y 802.11g; presenta un alcance limitado de 50 m, lo que implica tener que instalar más puntos de acceso<sup>21</sup>. Esta banda tan alta estaba asignada para fuerzas públicas y servicios de urgencias (Bomberos, Cruz Roja, etc) para posteriormente liberarse, por lo que

---

<sup>19</sup> FLICKENGER y AICHELE, Op. cit., p. 32.

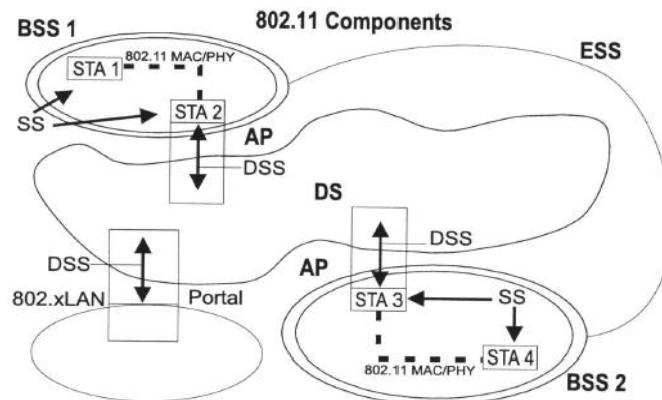
<sup>20</sup> PRIETO, Gustavo y GARCÍA, Antonio. Diseño de una Red Inalámbrica IEEE 802.11 FH/CDMA con Protocolo IP para Monitoreo y Control. En: 2001 Montevideo VII Workshop Iberchip, Memorias, IEEE, 2001, p 3

<sup>21</sup> HUIDOBRO, José M. y BLANCO SOLSONA, Antonio. Redes inalámbricas en los países en desarrollo. 2 ed. Madrid: Thomson Paraninfo, 2006. p. 98.



este estándar es relativamente el “más nuevo” para el uso público. La distribución de los canales para el protocolo 802.11a se presentan en el cuadro 1.

**Figura 8. Arquitectura típica de una red WLAN**



**Fuente:** PRIETO, Gustavo y GARCÍA, Antonio. Diseño de una Red Inalámbrica IEEE 802.11 FH/CDMA con Protocolo IP para Monitoreo y Control. En: 2001 Montevideo VII Workshop Iberchip, Memorias, IEEE, 2001, p 3.

**Cuadro 1. Distribución de canales protocolo 802.11a**

Canal	Frecuencia (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
149	5745
153	5765
157	5785
161	5805

**5.1.2.2 Red de Núcleo.** Esta red ha ido evolucionando en sus dos estructuras básicas desde la transmisión analógica y conmutación de circuitos, hasta la digitalización de la transmisión y conmutación avanzada, con técnicas de paquetes, observándose una marcada tendencia a la integración con redes

móviles y hacia la tecnología de transporte All-IP basada en el protocolo IP. En la red de núcleo es necesario aprovechar con eficiencia los portadores de gran capacidad disponibles, por lo que se transmiten simultáneamente gran número de señales de banda de base multiplexadas<sup>22</sup>. La red de núcleo está constituido por:

- Un conjunto de nodos de conmutación, interconectados según determinadas topologías para el encaminamiento del tráfico y la señalización. Los nodos disponen de capacidad software que permite la habilitación de funciones de inteligencia de red, que plasman de los llamados servicios de red inteligente, tales como los de buzón, contestador automático o encaminamiento de llamadas.
- La red de transmisión, red de transporte o red dorsal (backbone network) constituida por medio de transmisión sobre portadores físicos de gran capacidad (fibra, radio) que permiten la transferencia de grandes volúmenes de información entre dos nodos, según determinadas jerarquías.
- Un conjunto de servidores: servidor DNS, servidor DHCP, servidor de autenticación, servidor de base de datos. A continuación se describen las características de cada uno de estos.

- **Servidor DNS.** El servidor de nombres de dominio (DNS) es el servicio encargado de brindar la resolución de nombres para todos los equipos del ISP. Este sistema realiza traducciones de IP a un nombre determinado, sin que el usuario se dé cuenta, a través del uso de un Esquema Jerárquico de Nombres. El servidor de nombres de dominio se basa en un servidor DNS (Domain Name Server), que es el que permite traducir nombres a direcciones IP. Los recursos que considera DNS no son solo las direcciones IP y los nombres, sino que también considera: información de host, nombres canónicos, alias de host, nombres de servidores de correo de un dominio, etc<sup>23</sup>.

El sistema DNS se basa en un modelo cliente-servidor distribuido, en el que los DNS clientes interrogan acerca de cierta información a los servidores DNS. En ocasiones un servidor DNS se involucra en el proceso de resolución interrogando él mismo a otros servidores DNS, por lo que puede actuar también como cliente; en este caso se dice que actúa de manera recursiva haciendo como de *proxy* DNS, es decir, redirigiendo la consulta a otro servidor DNS. En la RFC 1035 se

---

<sup>22</sup> FIGUEIRAS, Aníbal. Una panorámica de las telecomunicaciones. Madrid: Prentice Hall, 2002. p. 99.

<sup>23</sup> TANENBAUM, Andrew. Redes de computadoras. 4 ed. México: Pearson Educación, 2003. p. 580.

especifica que DNS puede funcionar sobre UDP y sobre TCP. EN ambos casos emplea el puerto 53 por defecto<sup>24</sup>.

- **Servidor DHCP.** Un servidor de Protocolo de Configuración Dinámica de Host (DHCP) asigna dinámicamente direcciones IP a los hosts en una red. Este servicio no garantiza necesariamente su propia caja y este servicio es normalmente de un servidor de archivos o un controlador de dominio. El protocolo DHCP es de red TCP/IP que permite a los nodos de una red obtener sus parámetros de configuración automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que, generalmente, un servidor posee unos rangos de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento qué interfaz ha estado en posesión de esa IP, por asociación a su dirección MAC, cuánto tiempo la ha tenido y a quién se la ha asignado después. Algunos routers tienen listas de IP en vez de rangos, y algunos servidores asocian la IP a nombres de equipos o DNS<sup>25</sup>.

El funcionamiento del protocolo DHCP es de la siguiente forma: El servidor DHCP escucha al puerto 67/UDP. Cuando un cliente le pide una IP por puerto 68/UDP (lanzando con la dirección broadcast un paquete que contiene su dirección MAC), este le contesta con una IP libre y su MAC, entonces el servidor espera a que el cliente le conteste. Si se tiene varios servidores DHCP, el cliente solo responderá al primer servidor que le haya asignado la IP<sup>26</sup>.

- **Servidor de autenticación.** Este equipo recibe las peticiones del equipo de acceso en relación al usuario que está validando, es decir verifica que el nombre de usuario y contraseña que le está dando el equipo de acceso sea correcto y qué tipo de cliente es: si es ADSL, inalámbrico, solo mail, etc. Está conectado con la base de datos de clientes. El protocolo que se maneja en este servidor es el Protocolos AAA, el cual cumple tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting).

---

<sup>24</sup> GIMÉNEZ GUZMÁN, José M. y LOPEZ MERAYO, María. Aplicaciones de Internet. Alcalá: Universidad de Alcalá, 2012. p. 194.

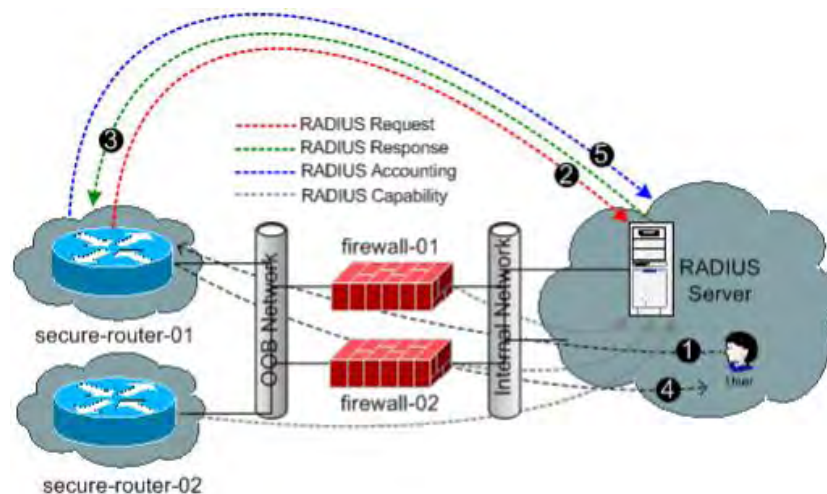
<sup>25</sup> ANDREU, Op. cit., p.12.

<sup>26</sup> ANDREU, Op. cit., p.13.

La autenticación es el proceso por el cual se prueba la identidad de un cliente ante un servidor. La autorización se refiere a la concesión de privilegios específicos a un usuario basándose en su identidad (autenticada) y los privilegios que solicita. La contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Un tipo de protocolo AAA es el protocolo Radius. Radius es un protocolo ampliamente usado en el ambiente de las redes para dispositivos tales como routers, servidores y switches entre otros. Es utilizado para proveer autenticación centralizada, autorización y manejo de cuentas para acceso dial-up, redes privadas (VPN) y, recientemente, para redes de acceso inalámbrico. Radius facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente.

Un cliente Radius envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje Radius al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores Radius. Los mensajes Radius son enviados como mensajes UDP<sup>27</sup>. La figura 9 presenta un esquema simple de la topología de red asumida al establecer una conexión Radius autenticada con un router.

**Figura 9. Topología de red para establecer conexión Radius**



**Fuente:** RADIUS (Remote Access Dial-up Service). Puebla: Instituto Tecnológico de Estudios Superiores de Monterrey, 2007. p. 6.

<sup>27</sup> RADIUS (Remote Access Dial-up Service). Puebla: Instituto Tecnológico de Estudios Superiores de Monterrey, 2007. p. 2.

El proceso que se visualiza en la figura es:

- 1: El router otorga al usuario acceso con los privilegios apropiados.
- 2: EL router puede enviar al servidor Radius el dato de contabilidad cuando el usuario finalice la sesión.
- 3: El usuario inicializa una conexión al router.
- 4: El router emite un „access-request’ Radius al servidor.
- 5: El servidor chequea los usuarios para la autenticación de la base de datos y emite un „access-reject’ con los privilegios apropiados.

- **Base de datos de clientes.** Contiene todo tipo de información con respecto al cliente: datos administrativos, dirección de correo electrónico, nombre de usuarios, numero de abonado, que tipo de abonado tiene, si está habilitado para conectarse o no. Existe diversos modelos de bases de datos que permiten almacenar información para leer o escribir. En este caso, se toma un servicio que permite realizar esta función el cual es el Sistema de Directorios, que permite guardar información de los usuarios incluyendo la rápida lectura de los datos.

Un servicio de directorio es un tipo de base de datos, pero no es una base de datos relacional. Una base de datos relacional está diseñada para procesar miles de cambios por minuto ya sea para ingresar, modificar o eliminar datos, como por ejemplo los sistemas de base de datos usados en e-commerce; los sistemas de directorios, como los directorios LDAP, están fuertemente diseñados y optimizados para el rendimiento en la lectura de la información, como por ejemplo sistemas de autenticación para páginas web o para un determinado servicio, directorios de información, sistemas de correos electrónicos, etc.

- Servicio de Directorio. Este servicio permite el almacenamiento de todo tipo de información el cual consta de un listado de la información sobre alguna clase de objetos como las personas. Los directorios pueden utilizarse para hallar información sobre un objeto concreto o, en sentido contrario, hallar objetos que cumplen un determinado requisito. Entre los datos que se almacenan están: nombre, ID del usuario, la dirección, el correo electrónico, el número de teléfono, etc.

La información de directorio puede ponerse a disposición de los usuarios mediante interfaces Web, como hacen muchas organizaciones; no obstante, también los

programas necesitan tener acceso a la información de los directorios. Estos pueden utilizarse para almacenar otros tipos de información, de manera parecida a como hacen los directorios de sistemas de archivos. El protocolo de acceso a directorios más utilizado es el Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol, LDAP)<sup>28</sup>.

LDAP se trata de un conjunto de protocolos abiertos utilizados para acceder y modificar información almacenada y centralizada en una red. Se le puede considerar como una base de datos de objetos de distintas clases. Según la RFC 2251. Al igual que las bases de datos tradicionales, una base de datos LDAP se puede consultar para extraer la información que almacena. A diferencia de las bases de datos tradicionales, una base de datos LDAP es especialmente apta para operaciones de lectura, búsqueda y navegación en vez de serlo para operaciones de escritura<sup>29</sup>.

A la estructura jerárquica de LDAP se le conoce como árbol de información del directorio (directory information tree, DIT). La parte superior de la jerarquía se reconoce como elemento raíz, la ruta completa hacia cualquier nodo en la estructura del árbol se le conoce como Nombre Diferenciado (Distinguished Name, DN) del nodo u objeto. Al igual que DNS, la estructura de un directorio LDAP refleja límites geográficos, como un estado o ciudad, y límites organizacionales, como funciones, departamentos o unidades de organización (Organizational Units, OU).

En la figura 10 se visualiza el directorio LDAP para una compañía como tal, el cual tiene por nombre Ejemplo S.A y presenta diferentes subdivisiones o unidades organizacionales dentro de sí, como el departamento de ingeniería, el departamentos de ventas y el departamento de I+D.

Se puede observar que el DN para el objeto que se toma como muestra en el directorio es “dn:uid=yyang , ou=ventas, dc=ejemplo, dc=org”. LDAP puede servir como una completa Solución para la Administración de Identidad dentro de una organización; puede proporcionar servicios de autenticación y autorización para usuarios. El directorio LDAP funciona con el modelo cliente-servidor, en donde el cliente tiene las opciones de consultar al servidor de directorio, escudriñar la

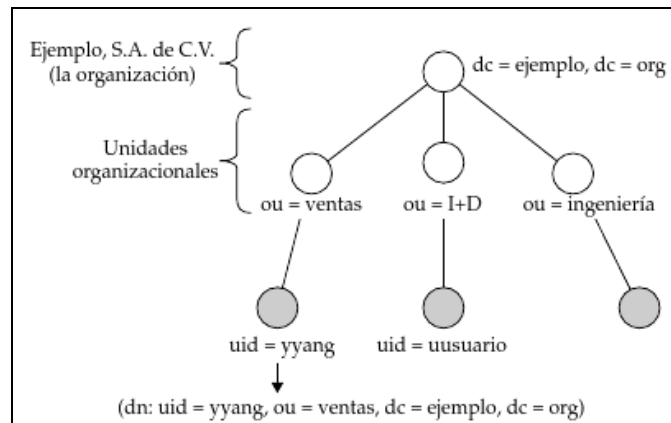
---

<sup>28</sup> SILBERSCHATZ, Abrahan y KORTH, Henry. Fundamentos de base de datos. Madrid: McGraw-Hill, 2006. p. 719.

<sup>29</sup> SHAH, Steve y SOYINKA, Wale. Manual de administración de Linux. México: McGraw-Hill Professional, 2010. p. 538.

información almacenada en el servidor, o intentar la modificación/actualización de la información del servidor LDAP<sup>30</sup>.

**Figura 10. El directorio LDAP para ejemplo.org**



**Fuente:** SHAH, Steve y SOYINKA, Wale. Manual de administración de Linux. Mexico: McGraw-Hill Professional, 2010. p. 539.

La implementación de fuente abierta de LDAP para desarrollar el servidor de directorios tiene por nombre **OpenLDAP**. Es un conjunto de programas integrado por los siguientes componentes: slapd, slurpd y libraries, los cuales implementan el protocolo LDAP, y varias herramientas más para uso tanto del lado del cliente como del lado del servidor<sup>31</sup>.

**5.1.3 Gestión de la red.** La gestión de red posibilita la monitorización y el mantenimiento de las redes con vistas a mantener su funcionamiento, a detectar y reparar fallos, a detectar posibles problemas antes de que se conviertan en fallos, a asegurar el cumplimiento de los requisitos contractuales y a mantener los cambios de configuración necesarios como la inclusión de nuevos usuarios, nuevas conexiones a otras redes o nuevas tarifas<sup>32</sup>.

La gestión de redes puede ser vista como una estructura que contenga múltiples capas:

---

<sup>30</sup> SHAH y SOYINKA, Op. cit., p. 539

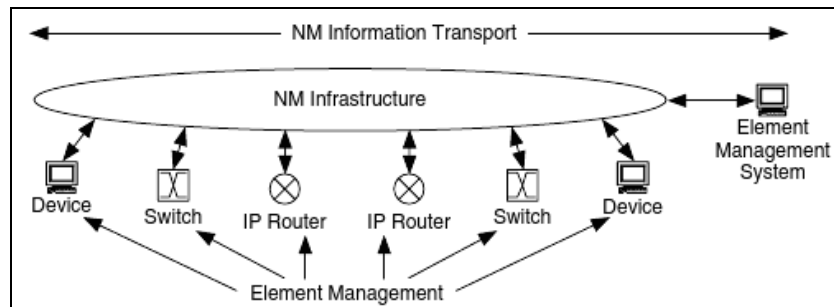
<sup>31</sup> SHAH y SOYINKA, Op. cit., p. 541

<sup>32</sup> AREITIO, Javier. Seguridad de la información: Redes, informática y sistemas de información. Madrid: Paraninfo, 2008. p. 278.

- **Gestión de Negocio:** La gestión de los aspectos de negocios de una red, por ejemplo, la gestión de presupuesto/recursos, planeación y acuerdos.
- **Gestión de Servicio:** La gestión de distribución de servicios a los usuarios, por ejemplo, para proveedores de servicio este incluiría la administración del acceso al ancho de banda, la capacidad de datos y la distribución de aplicaciones.
- **Gestión de elementos de Red:** La gestión de una colección de dispositivos de red similar, por ejemplo, routers de acceso o sistemas de administración del suscriptor. De igual forma, la gestión de dispositivos individuales de la red, por ejemplo, un router sencillo, un switch o un hub<sup>33</sup>.

La gestión de red puede ser dividido en 2 funciones básicas: el transporte de la información de gestión a través del sistema, y la administración de los elementos de información de la red de gestión, como se muestra en la figura 11.

**Figura 11. Transporte de la información de gestión y administración de los elementos**



**Fuente:** AREITIO, Javier. Seguridad de la información: Redes, informática y sistemas de información. Madrid: Paraninfo, 2008. p. 302.

Estas funciones consisten de una variedad de tareas, Monitoreo, Configuración, Solución de Problemas y Planeación, que son realizados por usuarios, administradores y personal de la red. Uno de los primeros retos en desarrollar una arquitectura de gestión de red es definir lo que realmente significa gestión de red para la organización que estará realizando las tareas y recibiendo los servicios finales, es decir, los usuarios o clientes del sistema<sup>34</sup>.

<sup>33</sup> McCABE, James. Network Analysis, Architecture, and Design. 3 ed. Burlington, USA: Morgan Kaufmann, 2007. p. 300.

<sup>34</sup> McCABE, Op. cit., p. 302.



**5.1.3.1 FCAPS.** En la gestión de red se incluyen cinco tareas: gestión de Fallos, gestión de Configuración, gestión de Contabilidad, gestión de Desempeño y gestión de Seguridad.

- **Gestión de Fallos.** Su objetivo son detectar errores, aislar los fallos y restaurar el servicio, utilizando acciones como la reconfiguración remota, la reparación o cambio del hardware o la petición de la restauración del servicio al proveedor. Es necesaria la prevención de tormentas de eventos, ya que un único fallo puede causar que muchas medidas activen alarmas. El software de gestión de red replica múltiples eventos, dando lugar a demasiada información, que se encuentra duplicada.

- **Gestión de Configuración.** Genera automáticamente un grafo de red actualizado y detecta las incorrecciones entre las configuraciones deseadas y reales. Así mismo permite descubrir la topología, la conectividad entre computadores, la configuración de las tablas de encaminamiento, de los parámetros de protocolo y puertos y posibilita un servicio de seguimiento continuo de configuración mediante la recogida de los datos históricos que permitan volver a la configuración anterior de trabajo. Además permite la distribución automática de cambios.

- **Gestión de Desempeño.** El objetivo es la prevención de los problemas de rendimiento relacionados con la carga de tráfico de la red o la inadecuada configuración. Algunas de las medidas empleadas son la utilización de un enlace de transmisión, la carga de CPU en routers, la tasa de pérdida de paquetes, los retardos de los paquetes y los fallos de enlaces de transmisión.

- **Gestión de Contabilidad.** Se ocupa de medir los parámetros de utilización de la red para poder controlar a los individuos o grupos de usuarios, y de esta forma, aplicar las tarifas y facturar el consumo de recursos de red.

- **Gestión de Seguridad.** Su misión es controlar el acceso a los recursos de red, de acuerdo a las guías locales para que la red no pueda ser sabotada de forma accidental o intencionada y evitar el acceso a la información sensible por ninguna entidad que no disponga de la autorización apropiada<sup>35</sup>.

---

<sup>35</sup> AREITIO, Op. cit., p. 278.

**5.1.3.2 Protocolos de gestión de red.** En los mecanismos de gestión de red, se incluye los protocolos de gestión de red. Hay actualmente dos protocolos de gestión de red: El protocolo de gestión de red simple (SNMP) y el protocolo de información de gestión común (CMIP). CMIP incluye CMIP sobre TCP/IP (CMOT). Estos protocolos de gestión de red proveen los mecanismos para recuperación, cambio y transporte de datos de administración a través de la red.

SNMP ha tenido un uso extendido y forma la base para muchos sistemas de gestión de red públicos y comerciales, ya que provee facilidad para obtener y configurar parámetros de dispositivos de red. Esto es hecho a partir de los comandos SNMP *get* (para obtener el valor de un parámetro), *get-next* (para obtener el valor del siguiente parámetro en la lista), y *set* (para cambiar el valor de un parámetro).

Los parámetros que son accesibles vía SNMP son agrupados dentro de bases de información de gestión o MIBs. SNMP es usado en mecanismos de monitoreo, instrumentación y configuración. SNMP provee acceso a las variables de la base de información de gestión (MIB), incluyendo estos en MIB-II y otros estándares MIB. SNMP es el método más común para acceder a los datos de gestión de red<sup>36</sup>.

**5.1.4 Servicios ofrecidos por el ISP.** El ISP provee varios servicios a los usuarios de acuerdo a su requerimiento y al paquete que desean utilizar. En sí, la mayoría de los ISP ofrecen los servicios dependiendo de 3 clientes objetivos: hogares, negocios y grandes empresas. Para los hogares y negocios se ofrecen dos servicios básicamente: el de internet y el de telefonía IP; el servicio de internet varía dependiendo de las capacidades que se requieran, la telefonía IP varía dependiendo de las líneas que se requieran: locales o de larga distancia.

En las grandes empresas se ofrecen servicios más amplios y de mayor cobertura, además de mayores capacidades de envío y respuesta de información, donde se maneja una carga pesada de datos y se requiere altas velocidades de transmisión; aquí se puede encontrar el servicio de red privada virtual que permite la interconexión entre sucursales de una determinada empresa, el servicio de Data Center, conferencias vía WEB, etc.

---

<sup>36</sup> McCABE, Op. cit., p. 303-304.

**5.1.4.1 Internet.** Internet es una red mundial de computadoras que permite a sus usuarios, mediante una computadora o una terminal (celulares, tabletas electrónicas, etc) conectarse hacia servidores localizados en instituciones educativas, proveedores comerciales y otras organizaciones para la obtención de información. Internet ofrece, además, otros servicios importantes como correo electrónico, boletines de noticias, transferencia de archivos mediante FTP, conferencias, conversaciones interactivas, y acceso remoto a muchas bases de datos, así como en la búsqueda y recuperación de información como WWW, entre otros servicios.

Internet está conformado, esencialmente, por un gran conjunto de redes de conmutación de datos que se interconectan mediante computadoras de propósito especial para resultar en una gran y única red mundial. Para adoptar muchos tipos de redes, Internet proporciona un mecanismo para interconectar redes arbitrarias, así como el software para transferir datos a través de las conexiones<sup>37</sup>. Internet se organiza como mínimo en cuatro niveles, que son:

- **Red Troncal:** Es la espina dorsal de Internet. Está formado por la interconexión de grandes redes de los principales operadores comerciales, redes académicas y de investigación.
- **Redes de proveedores de tránsito y Acceso internacional:** son redes de ámbito geográfico mucho más reducido.
- **Redes de proveedores de acceso local (ISPs):** Son redes que están orientados a dar servicio al usuario final. Generalmente las empresas y particulares contratan accesos a estos ISPs.
- **Redes corporativas y usuarios finales:** Redes propias de las organizaciones (empresas e instituciones). Son el nivel inferior de la jerarquía de Internet. Su conexión se realiza a través de un proveedor de Acceso.

**5.1.4.2 Telefonía IP.** La telefonía IP llamada Voz sobre IP se puede definir como la transmisión de paquetes de voz utilizando redes de datos, la comunicación se realiza por medio del protocolo IP (Internet Protocol), permitiendo establecer llamadas de voz y fax sobre conexiones IP.

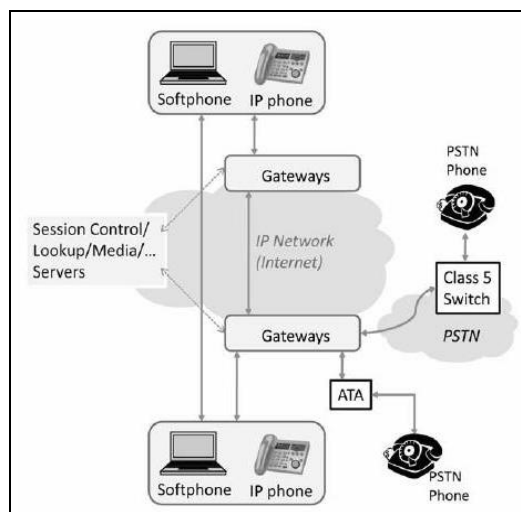
---

<sup>37</sup> AZNAR LOPEZ, Andrés. La red internet: El modelo TCP/IP. Madrid: Grupo Abantos Formación y Consultoría, 2005. p. 7.

El servicio de telefonía IP se monta sobre un programa de software libre denominado Asterisk, que es una aplicación de una central telefónica PBX. Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI (red digital de servicios integrados) tanto básicos como primarios. Asterisk tiene licencia GPL (General Public License) y es un software nativo de Linux y es sobre esta plataforma donde su operación es óptima.

Desde un punto de vista arquitectural, el requerimiento mínimo para habilitar una llamada VoIP es tener dos partes escuchando, teniendo cada uno un dispositivo para realizar la llamada equipado con un códec VoIP y conectado sobre una red IP. Sin embargo, como VoIP se convierte en un servicio mainstream con un usuario demandando servicios que igualan y reemplazan los servicios de nivel PSTN, se han introducido nuevos componentes funcionales dentro de la arquitectura de VoIP. Consecuentemente, la actual arquitectura de VoIP se está involucrando rápidamente para añadir nuevos servicios sobre VoIP y en direccionar varios temas específicos para el despliegue de VoIP sobre redes portadoras, LAN de empresa, etc<sup>38</sup>. La arquitectura de VoIP se muestra en la figura 12.

**Figura 12. Arquitectura de VoIP**



**Fuente:** GANGULY, Samrat y BHATNAGAR, Sudeept. VoIP: Wireless, P2P and New Enterprise Voice over IP. Hoboken, USA: Wiley, 2008. p. 19.

<sup>38</sup> GANGULY, Samrat y BHATNAGAR, Sudeept. VoIP: Wireless, P2P and New Enterprise Voice over IP. Hoboken, USA: Wiley, 2008. p. 18.

Los requerimientos arquitecturales básicos son derivados de los escenarios de despliegues que permite un modelo de comunicación flexible. Hay ciertos tipos de modelos de comunicación que la arquitectura debe soportar:

- Internet a Internet: Este tipo de llamadas incluyen aquellos que se originan entre dos teléfonos conectados al terminal de internet y la ruta entera se encuentra dentro de la red IP.
- Internet a PSTN: Estas llamadas son realizadas cuando el usuario que realiza la llamada tiene un teléfono conectado a Internet mientras el usuario destino está conectado al PSTN. Aquí la llamada pasa a través del segmento PSTN e Internet.
- PSTN a Internet: En este caso, el usuario que realiza la llamada está conectado a la PSTN mientras el usuario destino de la llamada tienen un teléfono conectado a Internet. Aquí, también, la llamada pasa a través del segmento PSTN e Internet.
- PSTN a PSTN vía Internet: Hay un caso donde la llamada se origina y termina en dispositivos conectados a la PSTN pero el enrutamiento de la llamada es realizado sobre Internet. Este tipo de comunicaciones son usadas típicamente para llamadas internacionales.
- Internet a Internet vía PSTN: La llamada se origina y termina en dispositivos conectados a Internet pero una parte del enrutamiento de la llamada está sobre el PSTN. Este puede ser el caso cuando el enlace del circuito conmutado a través del PSTN reduce el retardo de comunicación mientras la trayectoria de Internet fin a fin puede tener un retardo esperado más alto.

Para soportar estos modelos, la arquitectura debe reunir los siguientes requerimientos funcionales:

- Descubrimiento de Dirección: Cuando se inicializa una llamada, hay una necesidad para descifrar la ubicación del destino. El destino puede ser un teléfono IP en el cual la dirección puede ser una dirección IP o un Identificador de Recurso Uniforme (URI) de Internet. La dirección puede además ser un único userID como es usado en muchas aplicaciones de VoIP P2P. Para soportar los teléfonos PSTN, el destino puede ser un número telefónico PSTN.
- Interoperabilidad de Dispositivo: Un dispositivo para llamadas de VoIP de diferentes proveedores debe ser interoperable para poder comunicarse usando el mismo protocolo. Un teléfono VoIP de un proveedor A debe ser capaz de llamar a un teléfono VoIP de un proveedor B.
- Interoperabilidad con teléfonos PSTN: Para permitir llamadas hacia y desde teléfonos PSTN, la arquitectura debe proveer funcionalidades que ofrezca la traslación a nivel de protocolo y transcodificación a nivel de datos de VoIP.

- **Control de nivel de sesión:** En diferentes escenarios de desarrollo, varias funcionalidades de control de nivel de sesión empiezan a ser importantes. Tales funcionalidades incluyen autorización de nivel sesión, autenticación, etc.
- **Funcionalidades de nivel media:** Se refieren a servicios ofrecidos a la voz actual sobre datos que son transportados a través de protocolos de transporte media tales como RTP (Real Time Protocol). Esto permite mezclar llamadas para conferencias múltiples, transcodificación, etc.
- **Interoperabilidad entre Componentes:** Todos los componentes funcionales de una arquitectura de VoIP deben ser interoperable para usar protocolos estándar (tales como SIP/H.323)<sup>39</sup>.

- **Componentes Funcionales.**

- **Dispositivos de llamada VoIP.** Estos son los dispositivos que un usuario final requiere para iniciar o recibir una llamada. Estos incluyen:

- ✓ **Teléfono IP:** Un teléfono IP es un dispositivo el cual puede conectarse directamente a Internet. Presenta un software que permite la comunicación con otros dispositivos de VoIP; este software puede proveer la funcionalidad para establecer una llamada y el protocolo necesario para transportar los paquetes de voz. Un teléfono IP puede conectarse a una red usando conexión Ethernet o puede ser un teléfono de VoIP Wi-Fi que se conecta a Internet usando las redes inalámbricas IEEE 802.11.

- ✓ **Softphone:** Un softphone es un teléfono implementado en software. Se manejan en un computador o un PDA (Personal Digital Assistant) y un usuario puede usarlo para marcar cualquier número ya sea de teléfonos tradicionales o de extensiones. VoIP no distingue entre un softphone y un hardphone. En efecto, esto permite al usuario hacer llamadas PC a PC o de PC a PSTN.

- ✓ **Teléfono Análogo:** Un teléfono análogo es tradicionalmente usado para conectarse a la PSTN.

- ✓ **Adaptador de Teléfono Análogo (ATA):** Si un usuario desea utilizar un teléfono análogo para conectarlo a Internet, se puede usar un ATA. Un ATA autónomo contiene la lógica para comunicarse con el proveedor de servicio sobre Internet y trasladar la comunicación hacia y desde el teléfono análogo.

---

<sup>39</sup> GANGULY, Op. cit., p. 20.

➤ **Gateway.** Quizás el más importante componente para establecer la viabilidad de un sistema VoIP es un Gateway. La tarea de un Gateway es sentarse en el borde de dos diferentes tipos de red y ayudar a estos en la comunicación. En el caso de VoIP, estas dos redes pueden ser Internet y la PSTN. Típicamente, un Gateway consiste en dos principales componentes: un Gateway Controller y un Media Gateway.

El Gateway Controller es responsable de las siguientes funciones: traducir la información en un formato que cada red pueda entender, permitir la interoperación de la señalización. Por ejemplo, cuando se está soportando PSTN, el Gateway Controller puede traducir la información de señalización SIP para una llamada de VoIP en la equivalente información de señalización SS7 sobre PSTN. Esta traducción permite que una solicitud de llamada en la red IP sea remitida a la PSTN y viceversa. Habilitar la interoperación de la señalización es importante en el mundo dividido de VoIP donde ambos protocolos SIP y H.323 coexisten para la señalización a nivel de sesión.

Un Media Gateway es un componente asociado con el Gateway Controller y realiza las tareas similares pero a nivel de media. Un media Gateway ejecuta la transcodificación media, por ejemplo, antes de reenviarse el dato de VoIP de las redes IP a la PSTN, el media Gateway ofrece la transcodificación de los paquetes basados en VoIP en la red IP a los frames correspondientes en la red TDM de la PSTN.

➤ **Media Server.** En ciertos desarrollos de arquitecturas, las funcionalidades del media gateway pueden ser aumentados por otro componente llamado media server. El media server tiene el rol de procesar el stream RTP de VoIP para proveer decodificación de tono Multi Frecuencia de Tono Dual (Dual-Tone Multi-Frequency, DTMF), mezclando múltiples media streams dentro de una conferencia, procesamiento de scripts VoiceXML, reconocimiento de voz, texto para conversación de voz, grabación de voz, etc.

➤ **Session Control Server.** El servidor de control de sesión (Session Control Server) tiene el papel general de ofrecer funcionalidades a nivel de sesión tales como autenticación, autorización y admisión de llamadas IP. El mismo papel puede soportar enrutamiento de llamada y reenvío a otra red o proveedor de servicio y puede mantener estados sobre las llamadas en marcha. Hay otros roles auxiliares en proveer funcionalidades tales como la identificación de llamada, llamada en espera o la interacción con servidores de aplicación. El servidor de

control de sesión es además un componente opcional en una arquitectura y puede ser integrado como parte del gateway controller<sup>40</sup>.

- **Protocolos de VoIP.** Los protocolos definen los mensajes de comunicación, su significado y la lógica correspondiente. Los protocolos son requeridos para varios propósitos en VoIP:

- ✓ Descubrir una dirección. Estos protocolos proveen un soporte para descubrir la ubicación del destinatario cuando se inicializa una llamada.

- ✓ Señalización de llamada. Estos protocolos realizan la tarea de establecer y terminar una llamada entre 2 usuarios que se comunican.

- ✓ Control de Gateway. Estos protocolos proveen la señalización necesaria para controlar la funcionalidad de un Gateway.

- ✓ Transporte de Media. La voz actual es transmitido sobre protocolos de transporte de media.

En el contexto de VoIP, los protocolos son determinados para establecer llamadas de voz de extremo a extremo. Generalmente, existen 2 tipos de protocolos para VoIP:

- **Protocolos de señalización.** Estos protocolos son usados para realizar la función auxiliar relacionado a establecer y mantener una llamada. Estas tareas incluyen<sup>41</sup>:

- ✓ Ubicación del destinatario de la llamada: Esto implica encontrar la ubicación actual (en la red) del destino de la llamada cuando alguien intenta comunicarse con este.

- ✓ Determinación de Disponibilidad: El protocolo debe decidir si el grupo de llamada está disponible y si no, entonces saber dónde la llamada es redireccionada.

- ✓ Negociación de parámetros de sesión: El usuario que realiza la llamada y el que lo recibe deben estar de acuerdo sobre los parámetros usados en la transferencia

---

<sup>40</sup> GANGULY, Op. cit., p. 21-22.

<sup>41</sup> GANGULY, Op. cit., p. 60



de media con el fin de comunicar. Estos parámetros incluyen el tipo de media, la codificación a ser usada, etc.

- ✓ **Modificación de la sesión:** Mientras una llamada está en curso, las partes pueden decidir cambiar el contenido de las transferencias de media.
- ✓ **Finalización de la sesión:** Cuando las partes deciden terminar la llamada, ellos necesitan señalar apropiadamente de que la llamada está completada.

Entre los protocolos de señalización se encuentran:

- ✓ **Protocolo de Iniciación de Sesión (SIP):** Es un protocolo de señalización usado para establecer sesiones sobre Internet. Una sesión podría ser tan simple como una llamada telefónica de dos caminos o podría ser tan estructurado como una conferencia multimedia de multipartes, etc. SIP permite a los proveedores construir servicio de voz convergente y multimedia. SIP define simplemente como uno o más dispositivos participantes pueden inicializar, modificar y terminar sesiones.

- ✓ **Protocolo H.323:** Es un estándar propuesto por la ITU para sostener transporte de media. Fue diseñado específicamente para todas las formas de media (audio y video) y comunicaciones de datos sobre redes basadas en IP. Se utiliza en los desarrollos actuales de VoIP. Fundamentalmente, H.323 es un estándar que abarca todas las formas de comunicación multimedia sobre redes que no tienen soporte para garantizar QoS.

➤ **Protocolos de Transporte.** Estos protocolos son usados para el transporte actual en las llamadas. Realiza la digitalización de la voz en forma de paquetes. Los paquetes de voz son llevados entre las partes de una llamada usando estos protocolos. Por lo tanto, la codificación/decodificación, el empaquetado y el transporte de los paquetes de VoIP son realizados por estos protocolos. El protocolo más usado para estos propósitos es el Protocolo de Transporte en Tiempo Real (RTP)<sup>42</sup>.

**Protocolo de Transporte en Tiempo Real (RTP):** Este protocolo permite transportar paquetes de datos con características de tiempo real. Puede utilizar ambos protocolos TCP y UDP como una capa de transporte pero en la mayoría de los casos usa UDP. Los paquetes de VoIP necesitan ser liberados en tiempo real desde paquetes retardados volviéndose sin sentido en un corto tiempo. Por lo

---

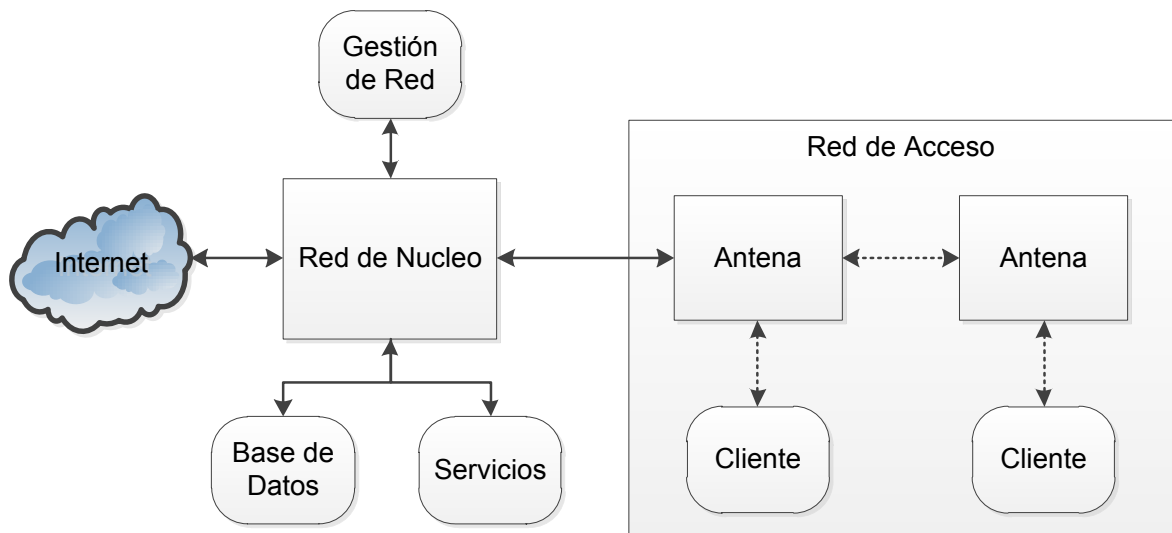
<sup>42</sup> GANGULY, Op. cit., p. 70

tanto, usando TCP, se retransmitirán los paquetes perdidos ofreciendo una pequeña ganancia. RTP sobre UDP sirve como un excelente vehículo para estos paquetes de datos. En general, RTP es usado en el transporte de voz y datos de video. RTP facilita el transporte de datos en tiempo real para permitir el sellado de tiempo de los paquetes. La media actual forma el payload de un paquete RTP.

## 6. DISEÑO DEL ISP CON ACCESO INALÁMBRICO

Se desea diseñar e implementar un ISP con acceso inalámbrico que permita soportar servicios de Internet y telefonía IP en el laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente, en el cual cuatro equipos clientes conectados a su respectiva antena reciben estos servicios. El nivel de ISP que se va a establecer es de nivel 3 y se compone por una red de núcleo y una red de acceso como se observa en la figura 13.

**Figura 13. Diagrama de Bloques del ISP**

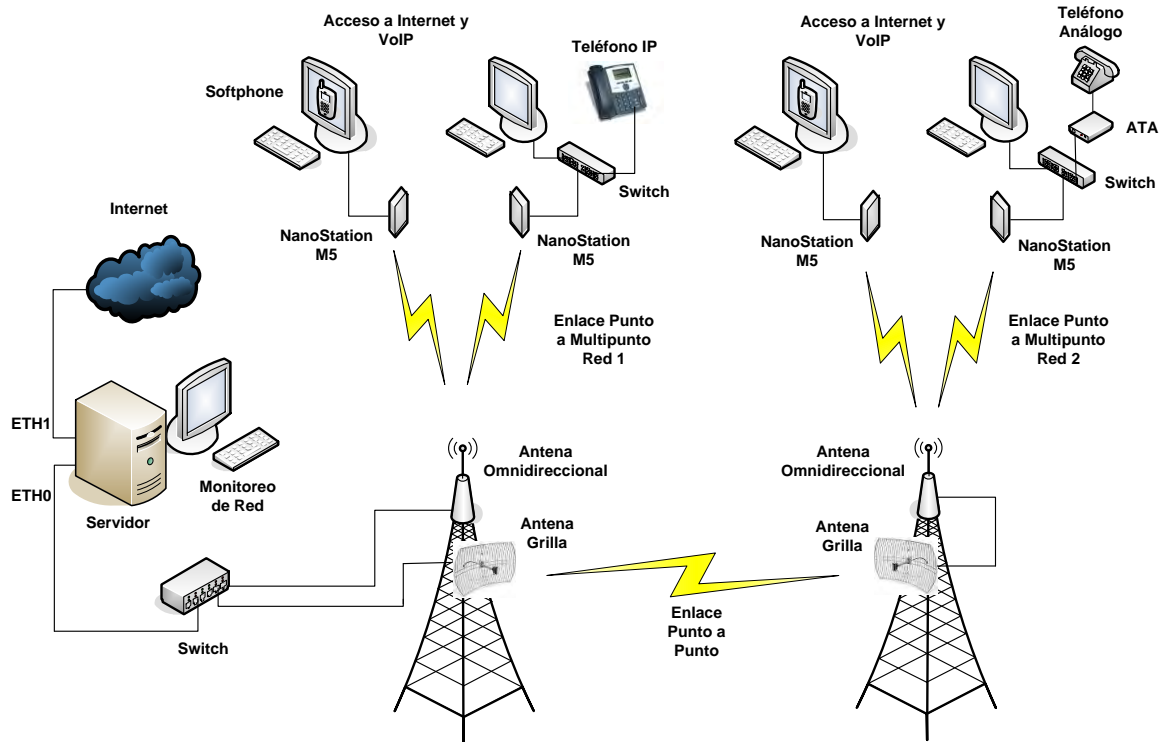


El servicio de Internet que toma el ISP se realiza por un canal no dedicado perteneciente al laboratorio de Telecomunicaciones de la UAO. El bloque de la red de núcleo se compone de servidores que implementarán los servicios de red y servicios de autenticación y autorización a los usuarios, además de llevar un registro de los recursos consumidos y su respectiva tarificación. Igualmente se incluye la gestión de la red para monitorear, configurar y controlar todo lo relacionado al enlace inalámbrico, a la seguridad de la red y al rendimiento de esta.

El bloque de la red de acceso se compone del enlace inalámbrico que permite la conexión del cliente al ISP, utilizando antenas que se basan en tecnología WIFI. Las conexiones que se realizan en la red inalámbrica se constituyen de un enlace punto a punto y de dos enlaces punto a multipunto. El enlace punto a punto se

implementa para dar los servicios de voz y datos a un sitio distante y el enlace punto a multipunto se efectúa para dar cobertura de red a una determinada zona. En la figura 14, se observa el diseño propuesto de la red para que el ISP ofrezca el servicio de Internet y telefonía IP.

**Figura 14. Diagrama de red implementado para ofrecer servicio de internet y VoIP**



La red de núcleo está compuesta por el servidor que ofrece los distintos servicios de red como el servicio DHCP, DNS, Radius, NAT. Se compone también del servidor AAA, del administrador de ancho de banda y del administrador de la base de datos que contiene información de los usuarios. Junto al servidor se encuentra el monitor que visualiza todo lo relacionado a la configuración y control de la red, en cuanto al QoS, seguridad, y permite el acceso de igual forma a la gestión de la red inalámbrica.

En la red de núcleo se estipula el ancho de banda que cada usuario tendrá, las autenticaciones de los usuarios y el monitoreo de la red en general. El servidor tiene dos interfaces de red: una interfaz denominada ETH1 tiene conectada la red pública que ofrece Internet y en la otra interfaz denominada ETH0 se encuentra la red privada o LAN que ofrece el servicio estipulado de Internet y telefonía IP a los usuarios finales; el servicio de Internet que toma el ISP se realiza por un canal no

dedicado, ya que el ETH1 se encuentra conectado a la red de la UAO y por ende se presentan varias restricciones de accesibilidad a algunas páginas, producto del servidor Proxy o restricciones de velocidad para realizar descargas en programas P2P.

El ETH0 se conecta a un switch, en donde se encuentra conectada la antena omnidireccional de la Red 1 que realiza la conexión punto a multipunto y la antena grilla que realiza la conexión punto a punto con la otra antena grilla que se ubica en un punto distante. De esta manera se realiza la conexión entre la red de núcleo y la red de acceso.

La red de acceso está compuesta por un enlace inalámbrico punto a punto entre dos antenas grilla y por dos enlaces inalámbricos punto a multipunto, teniendo en cada enlace una antena omnidireccional y dos CPE (Equipo Local del Cliente) que se encuentra conectado a un switch para dar conexión a un PC y a un teléfono IP.

En la comunicación VoIP se manejan: 2 softphone que se instalan en dos PC respectivamente, un teléfono IP que permite una conexión Ethernet directa hacia el switch y un teléfono análogo que se encuentra conectado a un ATA para que realice la conversión de conexión RJ-11 a una conexión Ethernet y poder así transmitir VoIP.

El primer área de cobertura de enlace punto a multipunto tiene por nombre RED 1, el cual se encuentra conectado a la red de núcleo, y la segunda área de cobertura de enlace punto a multipunto tiene por nombre RED 2, el cual se encuentra conectado de forma directa a la grilla para poder obtener los paquetes de voz y datos a partir del enlace punto a punto.

La arquitectura mostrada en la figura 14 se puede asimilar como el servicio que permite ofrecer internet y telefonía IP a usuarios ubicados en sitios muy distantes, ya que en este caso el ISP ofrece los servicios a la Red 1, la cual se encuentra ubicada en una ciudad, como por ejemplo Cali, y por medio del enlace punto a punto se ofrecen los mismos servicios a la Red 2 la cual podría estar ubicado en otro sitio como puede ser Jamundí, situado a 17.41 km de la ciudad de Cali.

Esta analogía presenta una idea más clara y exacta referente a la implementación del ISP con acceso inalámbrico en el laboratorio de telecomunicaciones, ya que se visualiza el uso de su implementación en un caso de la vida real.

## 6.1 DISEÑO DE LA RED DE NÚCLEO

Se planea montar todos los servicios de la red de núcleo en un computador de escritorio el cual presenta las características técnicas mostradas en el cuadro 2. Este equipo se encuentra ubicado en el laboratorio de telecomunicaciones.

**Cuadro 2. Características técnicas del PC para la red de núcleo**

Marca	Dell
Modelo	Studio XPS 435
Procesador	Intel Core i7, Chipset Intel X58
Memoria	SDRAM DDR3 1066MHz de tres canales hasta 24GB
Disco Duro	Hasta 1.5TB configurado con un disco duro SATA de 7200 RPM.
Comunicaciones	Dos tarjetas LAN Ethernet (Gigabit) 10/100

**Fuente:** PC de escritorio Dell Studio XPS 435 [En línea]. Dell Colombia, 2013 [consultado 16 de enero de 2013]. Disponible en Internet: <http://www1.la.dell.com/co/es/corp/Computadoras/desktop-studio-xps-435/pd.aspx?refid=desktop-studio-xps-435&s=corp>

El sistema operativo que se estipula en el PC para generar los servicios de la red es Linux, utilizando la distribución Centos 6. En esta distribución se instala además el programa Oracle VM Virtual Box para generar máquinas virtuales y poder instalar otros sistemas basados en GNU/Linux los cuales son necesarios para las funciones de control y configuración de la red que se describen más adelante.

Para administrar la red local, tener un control sobre los usuarios del ISP y sus cuentas de pago, realizar tareas de QoS y de gestión de ancho de banda, existen diferentes distribuciones basadas en Linux que su mayoría son open source, que además de realizar las actividades anteriores también permiten proveer los servicios de red que una red LAN requiera, como el servicio de DHCP, DNS, NAT, RADIUS, entre otros.

Las distribuciones más utilizadas para tales fines son Zeroshell, Brazilfw y Pfsense, Estos programas permiten manejar un PC como Router y/o Firewall dentro de una red LAN. En el cuadro 3 se presentan las características y

propiedades principales de las anteriores distribuciones, donde la información contenida se adquiere directamente de sus páginas oficiales.

Se observa que las tres distribuciones presentan características similares en cuanto a los principales servicios que una red LAN demanda, pero analizando detenidamente cada una de ellas, la que más se ajusta a los servicios que se pretenden prestar por parte del ISP es la distribución Zeroshell basada en Linux, ya que ofrece un servicio completo de portal cautivo basado en autenticación Radius, incluyendo además otras funciones como la Autorización y la Contabilidad, que son la base del protocolo AAA.

**Cuadro 3. Características y Propiedades de las distribuciones Zeroshell, BrazilFW y pFSense**

<i>Distribuciones para administración de la red local</i>	<b>Zeroshell</b>	<b>BrazilFW</b>	<b>pfSense</b>
<b>Características</b>	Es una distribución de Linux, open source, para servidores con el objetivo de suministrar los principales servicios que una red LAN requiera. Se puede configurar y administrar utilizando el navegador web.	Es una mini distribución de Linux diseñado para ser usado como firewall y router. Puede realizar tareas avanzadas de ruteo y QoS, proporciona una interfaz web para administración, cuenta con agregados o funcionalidades extra llamados addons de fácil instalación.	Es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router. Se caracteriza por ser de código abierto y por contar con una interfaz web sencilla para su configuración. El proyecto es sostenido comercialmente por BSD Perimeter LLC.
<b>Servicios que ofrecen</b>	<ul style="list-style-type: none"> <li>• Balanceo de Carga</li> <li>• Conexiones UMTS/HSDPA usando módems 3g</li> </ul>	<ul style="list-style-type: none"> <li>• Servidor y cliente DHCP, servidor DNS, servidor SSH, servidor Proxy Squid.</li> <li>• NAT</li> </ul>	<ul style="list-style-type: none"> <li>• Firewall</li> <li>• NAT</li> <li>• Balanceo de carga</li> <li>• Servidor VPN</li> <li>• Servidor PPPoE</li> </ul>

**Cuadro 3. (Continuación)**

<i>Distribuciones para administración de la red local</i>	<b>Zeroshell</b>	<b>BrazilFW</b>	<b>pfSense</b>
<b>Servicios que ofrecen</b>	<ul style="list-style-type: none"> <li>• Servidor Radius para suministrar autenticación segura.</li> <li>• Portal cautivo que soporte web login en redes inalámbricas y cableadas.</li> <li>• Gestión de QoS y control de tráfico sobre una red saturada.</li> <li>• Servidor proxy http que es capaz de bloquear páginas web que contengan virus.</li> <li>• 802.1Q Virtual LAN</li> <li>• NAT, DHCP, DNS.</li> <li>• LDAP, NIS y autorización RADIUS.</li> <li>-Autoridad de certificación X509 para emisión y gestión de certificados electrónicos.</li> </ul>	<ul style="list-style-type: none"> <li>• QoS (Quality of service)</li> <li>• Soporte de bridge firewall</li> <li>• Servidor VPN</li> <li>• Cliente FTP</li> <li>• Bandwidthd-monitor gráfico.</li> <li>• Cliente PPPoE y soporte para Dial-up</li> <li>• Soporte de firewall a nivel 7-</li> <li>• Brazilfw cuenta con un administrador de addons homologados y certificados por la comunidad de Brazilfw. Estos addons son funciones extras que se pueden instalar, actualizar y desinstalar por medio del administrador.</li> </ul>	<ul style="list-style-type: none"> <li>• Servidor DNS</li> <li>• Portal cautivo</li> <li>• Servidor DHCP</li> <li>• Dinamyc DNS</li> <li>• Información en tiempo real del throughput de cada interface</li> <li>• Servidor PPTP</li> <li>• Reportes y monitoreo</li> <li>• Enrutamiento estático</li> <li>• Pfsense cuenta con un gestor de paquetes para ampliar sus funcionalidades, al elegir el paquete deseado el sistema automáticamente lo descarga y lo instala.</li> </ul>

Zeroshell posee una herramienta de QoS que permite hacer control de tráfico sobre redes VOIP (esto es importante ya que se va a prestar el servicio de telefonía IP) y gestión de ancho de banda por IP, lo cual permite tener diferentes planes de ancho de banda para determinados usuarios, según lo requieran.



La distribución BrazilfW dispone de un portal cautivo pero no es oficial de esta comunidad, por lo tanto no se encuentra información confiable y de soporte para su instalación y configuración; la distribución pfSense dispone de un portal cautivo oficial pero no es tan completo como el del Zeroshell, que sí integra el protocolo AAA. Las distribuciones BrazilFW y pfSense disponen de la herramienta de QoS pero no hacen control de tráfico a redes VOIP y no administran el ancho de banda por IP.

Además de lo anterior hay dos características importantes que tiene el Zeroshell frente a las otras dos distribuciones. Una es la posibilidad de crear un perfil donde en una base de datos quedan guardadas todas las configuraciones que se realicen, lo cual permite tener un respaldo de la información en caso de daños o averías en el servidor. Y la otra, es la cantidad de información de soporte en diferentes idiomas que se encuentra en la comunidad de Zeroshell sobre todo en los idiomas de inglés y español, que son idiomas estándares a nivel mundial. La mayoría de información que se encuentra para el BrazilFW es en portugués, ya que la comunidad desarrolladora de esta distribución es de Brazil. Y la comunidad de pfSense ofrece información de soporte en inglés pero no tan amplia como lo ofrece la comunidad del Zeroshell.

**6.1.1 Servicios de Red.** Se realiza la configuración y operación de los servicios que se requieren para la red, los cuales son:

**6.1.1.1 Servicio NAT.** Se planea montar un servicio NAT que permite dar salida de internet a toda la red local mediante una dirección IP pública. Este servicio se va a implementar en el Zeroshell.

**6.1.1.2 Servicio DNS.** Se requiere del servicio DNS para que los clientes de la red local puedan navegar a través de nombres de dominios y no introduciendo direcciones IP. En este servicio se establece un nombre de dominio al cual se le asigna una dirección IP. De igual forma se determina el nombre de la máquina del servidor y se define un alias para este último.

Para el diseño de este ISP se define el nombre de dominio como *labteleco.com* y se le asigna la dirección IP 192.168.1.100. Se estipula el nombre de la máquina como *server.labteleco.com*.

**6.1.1.3 Servicio DHCP.** Se requiere del servicio DHCP para asignar direcciones IP a los hosts en la red. Se establece que cada computador reciba una dirección

IP dependiendo de su dirección MAC, ya que como se explica más adelante, la asignación de ancho de banda se hace dependiendo de la dirección IP.

Para el diseño de este ISP, la asignación de la dirección IP de acuerdo al ancho de banda y a la dirección MAC del usuario, se muestra en el cuadro 4. La asignación del ancho de banda depende de la solicitud del cliente.

Los parámetros como la dirección IP de la puerta de enlace y la dirección IP del servidor DNS se establecen también en el servidor DHCP. Para el diseño de este ISP se define que la puerta de enlace tenga la dirección IP 192.168.1.60 la cual va a corresponder a la dirección IP con la que se configura el Zeroshell (Ver Anexo H).

**Cuadro 4. Asignación de la dirección IP de acuerdo al ancho de banda y a la dirección MAC del usuario que adquiere los servicios**

Ancho de banda	Rango de dirección IP	Dirección MAC
1 Mbps	192.168.1.101-192.168.1.150	A4:BA:DB:FB:92:62 00:1D:92:4A:C2:45
2 Mbps	192.168.1.151-192.168.1.200	00:1D:92:4A:A0:9E
4 Mbps	192.168.1.201-192.168.1.250	A4:BA:DB:FB:7C:23

## 6.1.2 Servicios de Gestión.

**6.1.2.1 Directorio de Usuarios.** En este diseño e implementación se estipula dar el servicio de internet y telefonía IP a 4 usuarios los cuales están afiliados al ISP. Estos usuarios se van a encontrar registrados en la plataforma de de ZeroShell y en la plataforma de Elastix para determinar las especificaciones del servicio de internet y telefonía IP respectivamente. Los datos de los cuatro clientes que reciben el servicio por parte del ISP y que son introducidos a la base de datos del ZeroShell se muestran en el cuadro 5.

**Cuadro 5. Información de los Usuarios que adquieren los servicios del ISP**

	<b>Ciente 1</b>	<b>Ciente 2</b>	<b>Ciente 3</b>	<b>Ciente 4</b>
<b>Nombre</b>	Luis	Jhorman	Paulo	Jonathan
<b>Apellido</b>	Villa	Villanueva	Libreros	Delgado
<b>Dirección</b>	Calle 3B N° 96-64	Calle 4A N° 66-64	Av. 4N N° 35-46	Av. 4N N° 45-12
<b>Teléfono</b>	4401020	4402030	3305060	3307080
<b>E-Mail</b>	luis.villa@ hotmail.com	jhorvi@ hotmail.com	paulo.lib@ hotmail.com	jona.delgado@ hotmail.com
<b>Nombre de Usuario</b>	luis.villa	jhorman.villanueva	paulo.libreros	jona.delgado
<b>CC</b>	1130598323	1131123478	1130984213	1130341234
<b>Passwd</b>	98323	23478	84213	41234

Es importante que el ISP tenga información detallada de cada uno de los usuarios, como se observa en los anteriores cuadros. El Zeroshell permite la creación de usuarios con su respectiva información personal que será guardada en una base de datos LDAP, la cual se basa en el proyecto OpenLDAP. LDAP es un protocolo basado en estándares que particularmente es utilizado para almacenar información que se desee leer desde muchas localizaciones. El protocolo de Acceso Ligerito a Directorio, mejor conocido como LDAP (por sus siglas en inglés), está basado en el estándar X.500, pero más simple y más realmente adaptado para satisfacer las necesidades del usuario.

**6.1.2.2 Autenticación.** Se realiza en dos formas:

- **Autenticación a nivel físico.** Para la autenticación a nivel físico, se debe tener en cuenta la dirección MAC de cada antena NanoStation M que el usuario emplea para la conexión a la red. Esta dirección MAC se debe ingresar a lista de control de acceso MAC (MAC ACL) que se encuentra en la Seguridad Inalámbrica (Wireless Security) de la antena omnidireccional airMAX Omni que actúan en la red como Access Point.

Las direcciones MAC que hacen parte de esta lista permiten o niegan la conectividad de los clientes a la red inalámbrica, para acceder o denegar posteriormente el servicio de internet y telefonía IP. Independiente del método de seguridad inalámbrica que se utilice (WPA, WPA2, WEP, etc.), las direcciones

MAC tienen que introducirse a la MAC ACL para restringir el acceso a la red de antenas no permitidas o que no se encuentren vinculadas a la ISP y así evitar el consumo no autorizado de cualquier servicio.

- **Autenticación a nivel lógico.** Por seguridad se necesita autenticar los usuarios para probar la identidad de éstos, se autoriza los servicios prestados por el ISP a todo usuario que tenga un contrato con ésta, y es necesario llevar un control en cuanto a costos y facturación.

Lo anterior se puede implementar con el Zeroshell ya que dispone de un servidor RADIUS integrado, el cual se basa en el servidor FreeRadius, que cumple con las funciones del protocolo AAA. Además el portal cautivo del Zeroshell comunica información sobre las conexiones usando este protocolo. El Zeroshell usa también el protocolo de autenticación Kerberos 5, que suministra autenticación confiable sobre redes abiertas e inseguras.

A cada usuario registrado al ISP se le otorga un username (nombre de usuario) y password (contraseña) para que se autenticuen y se les autorice hacer uso de los servicios prestados por parte del ISP, siempre y cuando esté el usuario al día en los pagos y facturas. Si el usuario no ha pagado en las fechas estipuladas se le suspende los servicios y no tendrá acceso a ellos.

**6.1.2.3 Control de Ancho de Banda.** Se establece los planes de servicio de internet para determinar el ancho de banda que tendrá cada usuario y poder realizar el respectivo control.

- **Planes de Servicio de Internet.** Los planes que se establecen para ofrecer el servicio de internet se definen por la capacidad de ancho de banda que el usuario va a consumir. Como los usuarios finales que consumen internet banda ancha son de carácter doméstico se determina para el ISP tres planes:

Internet Banda Ancha ilimitado de 1 Mbps: En este plan se obtiene una velocidad de descarga de hasta 1024 Kbps y una velocidad de carga de hasta 512 Kbps.

Internet Banda Ancha ilimitado de 2 Mbps: En este plan se obtiene una velocidad de descarga de hasta 2048 Kbps y una velocidad de carga de hasta 512 Kbps.

Internet Banda Ancha ilimitado de 4 Mbps: En este plan se obtiene una velocidad de descarga de hasta 4096 Kbps y una velocidad de carga de hasta 1024 Kbps.

Si el usuario desea una mayor capacidad de internet banda ancha, se puede proporcionar dicho plan, siempre y cuando no exceda la capacidad permitida a usuarios de sectores residenciales.

La distribución Zeroshell dispone de una herramienta denominada QoS que permite asignar ancho de banda por IP o por rango de IP, con lo cual se establece que en determinado rango de IP van a pertenecer los usuarios que solicitaron ancho de banda de 1 Mbps, en otro rango de IP los usuarios que solicitaron ancho de banda de 2 Mbps y en otro rango de IP los usuarios que solicitaron ancho de banda de 4 Mbps.

**6.1.2.4 Monitoreo y control de Red de Acceso.** Para tener un control de la red y verificar las posibles causas que pueden originar un problema en la misma, es necesario tener un sistema de monitoreo de antenas que permita detectar fallos para su posterior reparación. Aprovechando que las antenas que realizan la conexión de red para este ISP son de la compañía Ubiquiti Networks, se utiliza un software de monitoreo que ofrece de manera gratuita esta multinacional, y es el denominado **airControl**. Este programa es un potente e intuitivo servidor de administración de red basado en la Web, que permite a los operadores administrar de manera centralizada redes de dispositivos Ubiquiti.

Según su manual de usuario ofrece las siguientes características:

- Descubrir dispositivos Ubiquiti (punto de acceso y estaciones) que se encuentren en la red
- Reportar el estado de los dispositivos que se conecten: los dispositivos que sean administrados reportarán periódicamente una rutina de estado al servidor AirControl, el cual monitoreará el estado de las actualizaciones.
- Cambios en su configuración: la configuración AirOS de cada antena se puede cambiar desde el AirControl.
- Programación de tareas: ejecuta automáticamente actualizaciones del firmware, acciones de reinicio, de búsqueda de rango de IP, backup de configuración del dispositivo, Ping y comandos Shell. Se debe especificar la fecha de inicio y finalización de cada tarea.
- Se puede realizar remotamente un backup de la configuración del dispositivo o realizar restauración de la configuración.
- Graficas/estadísticas del dispositivo: valores de intensidad de señal, de potencia, etc.

- Mapa de la red: muestra la ubicación de los AP y estaciones en un mapa de imagen satelital, con datos como el área de cobertura de cada AP y el estado de los dispositivos.
- Agrupamiento de dispositivos: la auto-agrupación por defecto del sistema organiza los dispositivos Ubiquiti encontrados por la identificación de red y la versión de firmware.
- Speed Test: pruebas de velocidad entre dispositivos AirOS<sup>43</sup>.

### 6.1.3 Diseño del servicio de telefonía IP.

**6.1.3.1 Servicios y funcionalidades.** Para realizar el diseño del servicio de telefonía IP se debe tener en cuenta: la distribución que se requiere para implementar la telefonía sobre VoIP debe tener distintas características que permitan ofrecer un servicio de voz de óptima calidad, sin que se presenten pérdidas de información y datos, que permita integrar varias aplicaciones para otorgar distintas funcionalidades los cuales serán útiles en el sitio donde se preste el servicio de telefonía IP, además de ofrecer el control y monitoreo de las llamadas, entre otras configuraciones básicas.

Los servicios y funcionalidades que se establecen para desarrollar telefonía IP en el ISP son:

- Transferencia de Llamadas: Este servicio permite que una persona pueda transferir una llamada que tenga en la línea hacia otro número telefónico de un usuario, así este último se encuentre ocupado.
- Parqueo de Llamadas: El parqueo de llamadas o como se conoce en ingles “Parking Lot”, se utiliza para estacionar llamadas y luego ser recogidas por alguien. Esto sucede, por ejemplo, cuando una recepcionista recibe una llamada dirigida a alguna persona en especial y esta última no se encuentra en su sitio de trabajo, entonces ella procede a parquear la llamada mientras localiza al destinatario. Cuando lo localiza, le informa que tiene una llamada en el parqueadero “71” y posteriormente la llamada le es conectada<sup>44</sup>.

---

<sup>43</sup> AirControl User’s Guide [En línea]. Ubiquiti Networks, 2011 [consultado 28 de febrero de 2013]. Disponible en Internet: <http://wiki.ubnt.com/AirControl>

<sup>44</sup> MUÑOZ, Alfio. Elastix a ritmo de merengue. Santo Domingo: Elastix, 2010. p. 145.

- **Buzón de Voz:** Este servicio permite dejar mensajes de voz a un usuario cuando este no conteste una llamada telefónica ya sea porque se encuentre ocupado o no se encuentre presente para contestar la llamada. Cuando el usuario que realiza la llamada deja el mensaje, este queda almacenado en el buzón de voz y el usuario destino podrá revisarlo en cualquier momento.
- **Llamada en espera:** Este servicio permite aceptar una llamada entrante en una línea cuando esta se encuentre ocupada con otra llamada. El usuario que recibe la otra llamada entrante, presiona un número o botón para contestarla y el otro usuario con quien estaba conversando anteriormente queda escuchando una música de espera hasta que se retorne a la llamada inicial.

Existen otras funcionalidades que se pueden implementar en el servicio de telefonía IP, pero se determina que estos son los más indicados y básicos que deben tener los usuarios que reciban el servicio de VoIP.

Para implementar el servicio de voz sobre IP, se requiere de un software o distribución que ofrezca no solo la comunicación por teléfonos sino que además permita el uso de servicios y funcionalidades que ayuden a optimizar la comunicación.

**6.1.3.2 Selección de la distribución.** Se procede a seleccionar la distribución con que se implementa el servicio de VoIP en el ISP, teniendo en cuenta los servicios y funcionalidades que se establecieron, además de las implementaciones futuras que se puedan realizar con otras funcionalidades. Existen distintas distribuciones del sistema operativo GNU/Linux para generar centrales telefónicas por software basada en la PBX de código abierto Asterisk, entre esas se encuentran Trixbox, FreePBX, AsteriskNOW y Elastix. La distribución que más se ha utilizado por su estructura y funcionalidad es el Trixbox, pero también se encuentra la distribución Elastix que presenta una interfaz gráfica agradable, fácil de manejar y con varias funcionalidades que permite la fácil creación de una central telefónica. Por esta razón, se selecciona inicialmente estas dos distribuciones para analizar sus funcionalidades y escoger la más óptima para el diseño y posterior implementación del servicio de telefonía IP.

#### ➤ **Trixbox**

Trixbox se caracteriza como una plataforma de telefonía abierta que combina distintas herramientas para telefonía de recurso abierto. Es una distribución del sistema operativo GNU/Linux basada en Centos, que tiene la característica de ser una central telefónica (PBX) por software basada en el funcionamiento de código abierto Asterisk, desarrollado por la empresa Fonality.

Esta empresa ha desarrollado dos distribuciones de Trixbox para el servicio de VoIP: Trixbox CE (Community Edition) y Trixbox Pro. Una de las principales diferencias entre estas dos distribuciones es que el Trixbox CE es una solución basada en las instalaciones del cliente, en cambio el Trixbox Pro usa la tecnología Hybrid-Hosted de Fonality el cual pone al sistema PBX en las instalaciones del cliente pero la interface web para administrar el sistema es localizado en el centro de datos Fonality, permitiendo el monitoreo centralizado de sistemas remotos, actualización del sistema y servidores remotos de manera automática, etc.

En Trixbox Pro se debe pagar una suma de dinero para utilizar sus servicios, en Trixbox CE su uso es gratuito.

- Herramientas de Instalación Automatizada
- Festival Speech Engine
- Auto-configuración de Tarjeta Digium

Trixbox CE provee una simple interface web que ayuda a administrar y mantener el sistema. La función trixbox CE dashboard es dividido entre funciones de Usuarios y funciones de Administrador. La sección de usuario es accesible a todos los usuarios y las funciones de administrador son protegidos por un simple password de administrador<sup>45</sup>.

### ➤ **Elastix**

Elastix es un software de código abierto para el establecimiento de comunicaciones unificadas. El objetivo de Elastix es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial. Fue diseñado y desarrollado por PaloSanto Solutions. Elastix inició como una interfaz de reportación para llamadas de Asterisk. Posteriormente evolucionó hasta convertirse en una distribución basada en Asterisk, utilizando como sistema operativo Linux CentOS.

Elastix no solamente provee telefonía, integra otros medios de comunicación para hacer más eficiente y productivo el entorno de trabajo. Elastix permite integrar otras locaciones para centralizar las comunicaciones de la empresa y llevarlas a niveles globales. Un usuario de una corporación ubicada en Sudamérica comparte las mismas funcionalidades que otro ubicado en Asia además de tener una

---

<sup>45</sup> GARRISON, Kerry. Trixbox CE 2.6. Otton Birmingham, GBR: Packt Publishing, 2009. p. 20.



comunicación directa<sup>46</sup>. Después de tener la información suficiente sobre las anteriores distribuciones, se presenta las distintas características y funcionalidades que maneja Trixbox y Elastix en el cuadro 6.

**Cuadro 6. Características y funcionalidades de Trixbox y Elastix**

<b>Funcionalidades</b>	<b>Trixbox CE</b>	<b>Elastix</b>
Identificador de llamadas	✓	✓
Grabación de llamadas	✓	✓
Troncalización	✓	✓
Correo de Voz	✓	✓
Correo de voz a Email	✓	✓
Soporte de Fax	✓	✓
IVR Configurable y Flexible	✓	✓
Soporte para protocolos SIP e IAX, entre otros	✓	✓
Centro de Conferencias con Salas Virtuales	✓	✓
Soporte para grupos de tonos	✓	✓
Soporte para follow-me	✓	✓
Soporte para paging e intercom	✓	✓
Administración centralizada vía Web	✓	✓
Panel de Operador basado en Web	✓	✓
Interface de configuración web	✓	✓
Tarificación con reporte de consumo por destino	✓	✓
Soporte para colas de llamadas	✓	✓
Configurador de parámetros de red.	✓	✓
Música en espera	✓	✓
Acceso Web a correo de voz	✓	✓
Soporte para teléfonos analógicos (PSTN)	✓	✓
Soporte para Videoconferencias		✓
Servidor DHCP para asignación dinámica de LPS		✓
Soporte LDAP		✓
Reporte de detalle de llamadas (CDR)	✓	✓
Soporte para Callback		✓
Soporte para backup/restore a través de Web	✓	✓
Servicio de avisos y contestadora en Español	✓	✓

<sup>46</sup> Información del Producto Elastix [En línea]. Elastix, 2012 [consultado 15 de enero de 2013]. Disponible en Internet: <http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html>

Se puede observar en el cuadro 6, que la mayoría de las funcionalidades las posee ambas distribuciones. La diferencia es que Elastix es más robusto para ejecutar videoconferencias, presenta Callback y soporta LDAP. De acuerdo a las funcionalidades que se requieren para el diseño de la telefonía IP, se observa que las 2 distribuciones cumplen con estas características, además que ofrecen otras funcionalidades para implementaciones futuras en telefonía IP.

Con base a pruebas realizadas en proyectos de grado, se tiene que el Elastix es más confiable que el Trixbox ya que según los autores del proyecto “Diseño de una plataforma CRM integrada con Asterisk para la dirección comercial de Emcali Telecomunicaciones”, los eventos enviados por la interfaz AMI (Asterisk Manager Interface) eran completos y consistentes en todos sus envíos a comparación de Trixbox en donde los eventos eran inestables y en ocasiones incompletos<sup>47</sup>.

Un beneficio que presenta Elastix es la variada información que se puede encontrar para la configuración de esta distribución, como su página oficial en internet donde se realizan las descargas no solo de la misma distribución sino también de documentación y guías que permiten entender su funcionamiento y configuración; esta documentación es su mayoría viene en idioma español para los usuarios de habla hispana. Además, Elastix tiene distintos sitios de foro donde se puede compartir información, resolver dudas e inconvenientes y que en su mayoría vienen en idioma español.

Las anteriores características y argumentos conllevan a elegir a Elastix como la distribución con el cual se realiza la implementación del servicio de telefonía IP para el ISP.

**6.1.3.3 Medición de Calidad de Servicio.** Después de tener la distribución y las funcionalidades que se van a utilizar para desarrollar el servicio de telefonía IP, se establece el uso de una herramienta que permita medir la calidad de servicio en el servicio de VoIP.

Los diversos usos en la red tienen diferentes requisitos que exigen unos servicios de red más apropiados. Un tráfico creciente de la red requiere un ancho de banda creciente. QoS es el mecanismo de priorización de los paquetes de voz sobre los

---

<sup>47</sup> SAA, Alejandro y VELASCO, Diego. Diseño de una plataforma CRM integrada con Asterisk para la dirección comercial de Emcali Telecomunicaciones”. Trabajo de Grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2012.

datos cuando se cursa VoIP en una red de datos compartida. Al igual que existen factores que repercuten en los retardos en la red, existen también factores que intervienen en la calidad de la voz, tales como codificadores, ancho de banda, pérdida de paquetes, latencia, jitter y eco<sup>48</sup>.

Existen varios software y aplicativos que permiten medir la calidad del servicio de VoIP, entre esas se encuentra VoIPMonitor y VQManager. Estos programas permiten detectar los paquetes de voz para registrar las llamadas, visualizar los datos de conexión que establece el protocolo, visualizar información estadística sobre las llamadas en la red, mostrar los diferentes parámetros que intervienen en la calidad de servicio, etc.

Lamentablemente, el software VQManager fue sacado de circulación y de la venta. Por lo consiguiente, se decide usar el software VoIPMonitor para realizar las mediciones de QoS y tener información de llamadas. Una de las ventajas que presenta el programa VoIPMonitor es el registro que tiene de las llamadas ya sean en vivo o cuando han finalizado. Esto me permite tener un balance de todas las llamadas realizadas en determinadas fechas.

### ➤ **Parámetros de QoS**

Los parámetros de calidad de servicio que se van a medir son:

- MOS
- Jitter o IPDV
- Delay o IPTD
- Packet Loss o IPLR

Los parámetros Jitter, Delay y Packet Loss son establecidos con base a la Recomendación Y.1540 dada por la ITU-T que define los "Parámetros de calidad de funcionamiento a la disponibilidad y la transferencia de paquetes del protocolo Internet" que pueden ser usados para especificar y evaluar el rendimiento de velocidad, precisión, fiabilidad y disponibilidad en la transferencia de paquetes IP de los servicios de comunicación de datos IP internacionales que se aplican a

---

<sup>48</sup> HUIDOBRO MOYA, José Manuel y CONESA PASTOR, Rafael. Sistemas de Telefonía. 5 ed. Madrid: Paraninfo, 2006. p. 294.

servicios IP de extremo a extremo o punto a punto. El parámetro MOS se establece con base a la Recomendación P.800 dada por la ITU-T que define los “Métodos de determinación subjetiva de la calidad de transmisión telefónica”, en donde se plasma unas escalas de opinión referente a la calidad de voz dados por la ITU-T.

➤ **Sistema de Alarma**

Utilizando el programa VoIPMonitor, se implementa un sistema de alarma que permita indicar en qué momento ocurre un error o pérdida cuando se efectúe una llamada, con base a los parámetros de calidad de servicio y sus valores máximos establecidos para que se presente un óptimo servicio de VoIP. Los valores máximos de los parámetros de calidad de servicio se determinan con base a la Recomendación Y.1541 de la ITU-T que especifica los “Objetivos de calidad de funcionamiento de la red para servicios basados en el protocolo de internet”. Esta recomendación define las clases de QoS de la red con objetivos para los parámetros de calidad de funcionamiento de la red IP, en donde cada clase tiene una serie de servicios que son ofrecidos por los proveedores de red; estas clases son destinadas a ser las bases para acuerdos entre proveedores y entre los usuarios finales y sus proveedores.

Para el servicio de telefonía IP que se establece en el ISP, los límites máximos de los parámetros jitter, delay y packet loss corresponden a los servicios de Clase 1, que presentan características de tiempo real e interacción. El valor máximo del parámetro MOS se define dependiendo del códec que se esté manejando, que en este caso es el G.711. Con base a la anterior información, se presenta en el cuadro 7 los valores máximos que se debe tener en VoIP para garantizar la calidad de servicio.






**Cuadro 7. Valores máximos de los parámetros de QoS para VoIP**

<b>Parámetros de QoS</b>	<b>Valores Máximos</b>
Delay	400 ms
Jitter	50 ms
Packet Loss	0.1 %
MOS	4.1

## 6.2 DISEÑO DE LA RED DE ACCESO

La red inalámbrica se desarrolla utilizando dos antenas grilla que realizan la conexión punto a punto, dos antenas omnidireccionales MIMO de polaridad dual 2x2 que conectados a dos Radio MIMO 2x2 realizan la conexión punto a multipunto y cuatro CPE que realizan la conexión del enlace inalámbrico con cada cliente. A continuación se presenta en el cuadro 8 las antenas a utilizar con sus respectivas características.

**Cuadro 8. Antenas a utilizar en la implementación de la red inalámbrica**

Antena	Marca	Modelo	Frecuencia	Ganancia	Potencia	Imagen
Antena Grilla, airGrid M5	Ubiquiti Network	AGM5-HP-1114	5470 - 5825 Mhz	23 dBi	25 dBm	
Antena omni direccional airMAX Omni	Ubiquiti Network	AMO-5G10	5.45 - 5.86 GHz	10 dBi		
Radio MIMO 2x2: Rocket M	Ubiquiti Network	M5	5470 - 5825 MHz		27 dBm	
CPE, NanoStation M5	Ubiquiti Network	M5	5470 a 5825 MHz	14.6 - 16.1 dBi	27 dBm	
CPE, NanoStation loco M5	Ubiquiti Network	M5	5470 - 5825 MHz	13 dBi	23 dBm	

Cada dispositivo de Ubiquiti trae consigo su adaptador POE, donde se acopla la antena y la conexión LAN hacia un switch o computador. Dentro de la red inalámbrica se van a manejar tres switches, en donde se utiliza uno de estos para realizar la conexión entre la antena grilla, la antena omnidireccional y la red de núcleo; esto con el fin de brindar los servicios de voz y datos al área de cobertura de la Red 1 y a su vez, por medio del enlace punto a punto, ofrecer dichos servicios al área de cobertura de la Red 2. Los otros dos switches se utilizan para realizar la conexión entre el PC, el teléfono IP y la antena NanoStation M5, ya que el NanoStation otorga los paquetes de voz al teléfono y los paquetes de datos al PC.

Cada antena que se ubica en la red inalámbrica presenta un sistema operativo el cual permite la configuración de los parámetros de red, de los parámetros inalámbricos y de otras características referentes al uso y conexión de las antenas. El sistema operativo tiene por nombre airOS y es propio de Ubiquiti Networks. En airOS no solo se determinan los parámetros que debe llevar la antena para la comunicación inalámbrica, sino que también permite el uso de otras herramientas para el monitoreo de throughput, monitoreo de valores referentes a conceptos inalámbrico, para realizar pruebas de conexión o capacidad.

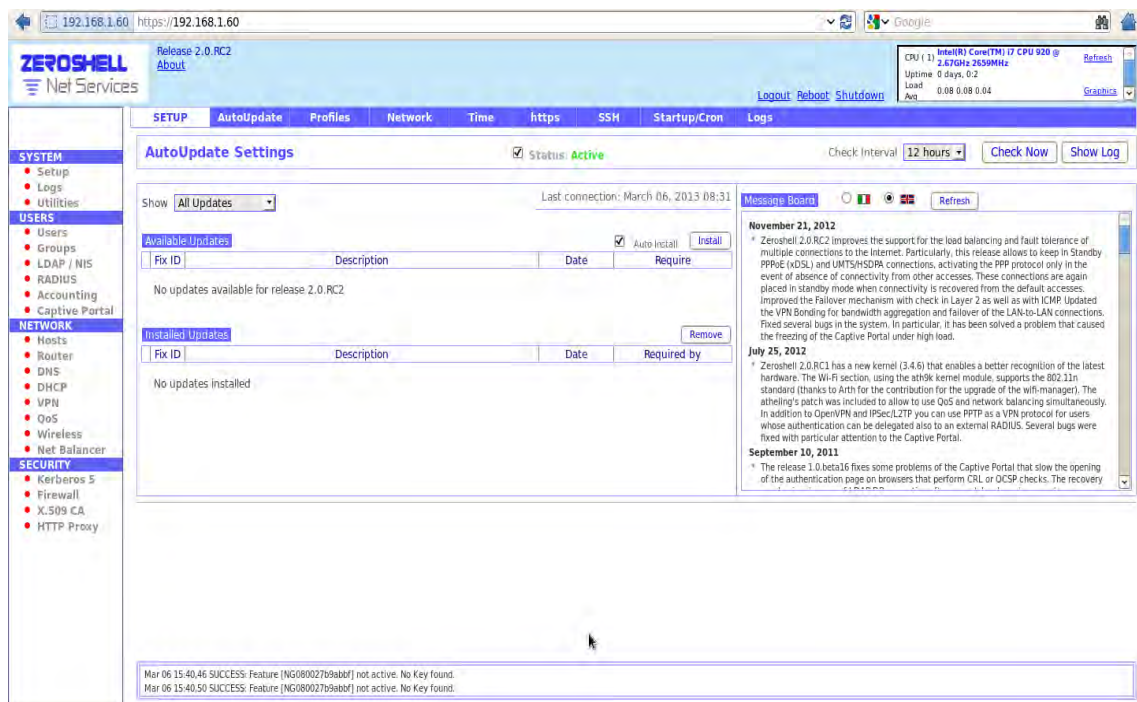
Para la configuración de la red inalámbrica se necesitan definir 3 frecuencias: una para el enlace punto a punto y las otras dos para los dos enlaces punto a multipunto respectivamente. Es necesario analizar el contexto donde se va a realizar esta implementación, en este caso el laboratorio de telecomunicaciones de la UAO, para saber que frecuencias hay presentes en el medio y evitar posibles interferencias. Utilizando un analizador de espectro se puede conocer las frecuencias en el medio.

## 7. IMPLEMENTACIÓN DEL ISP CON ACCESO INALÁMBRICO

La distribución que se implementa para realizar una administración centralizada de la red es el Zeroshell como se definió en el diseño de la red de núcleo. En primer lugar se instala la distribución como sistema operativo basado en Linux, que para esta implementación se realizó en Virtual Box. Posteriormente, se ejecuta la configuración del Zeroshell en la consola para definir la dirección IP que tendrá la distribución para que quede en red con la red LAN; el procedimiento de configuración de esta distribución se presenta en el Anexo H.

Al finalizar la configuración se ingresa a la interfaz web del Zeroshell mediante un navegador de internet, introduciendo como URL la dirección IP ya establecida. La interfaz se presenta en la figura 15.

Figura 15. Interfaz web principal del Zeroshell



The screenshot displays the Zeroshell web interface. At the top, the browser address bar shows the URL `https://192.168.1.60`. The page header includes the Zeroshell logo, the version `Release 2.0.RC2`, and system status information such as CPU usage, uptime, and load. A navigation menu is located below the header, with `AutoUpdate` selected. The main content area is titled `AutoUpdate Settings` and shows the `Status` as `Active`. It features a table for `Available Updates` and `Installed Updates`, both of which are currently empty. A `Message Board` on the right side displays several update logs, including one for `November 21, 2012` and another for `July 25, 2012`. A footer at the bottom of the page shows system logs for `Mar 06 15:40:46` and `Mar 06 15:40:50`.

Ya estando en la interfaz web, se procede a realizar las configuraciones de los servicios que se definieron para la red de núcleo, además de la autenticación, control de ancho de banda y creación de usuarios.

## 7.1 CONFIGURACIÓN DE SERVICIOS DE RED

**7.1.1 Servicio NAT.** La configuración del servicio NAT se realiza en el Zeroshell. Dentro de la interfaz web principal, como se observa en la figura 15, en el menú del lado izquierdo se accede a la configuración del Router para permitir darle salida de internet realizando NAT (Traducción de direcciones) entre la red interna y la red externa. Para implementar este servicio, se ingresa en la parte superior al menú NAT donde aparece una pantalla que indica las interfaces de red del sistema; se selecciona la interface ETH01, y se pasa a la ventana NAT Enable Interfaces como se muestra en la figura 16. Se guardan los cambios y se comprueba que desde la red local se pueda acceder a algún sitio de internet.

Hay que tener en cuenta que NAT utiliza IP Masquerade que es una técnica de traducción de muchos host a uno, es decir que permite a muchas direcciones IP privadas compartir simultáneamente una dirección IP pública.

**Figura 16. Configuración del servicio NAT en Zeroshell**



**7.1.2 Servicio DNS.** La configuración del servicio del DNS se realiza directamente en el sistema operativo Centos 6, realizando las modificaciones en unos archivos que se pueden observar en el Anexo G. En este mismo anexo se presenta el procedimiento de configuración.

**7.1.3 Servicio DHCP.** Para realizar la configuración del DHCP, se accede al menú DHCP ubicado en la parte izquierda de la interfaz principal del Zeroshell



(figura 15). Se abre una ventana como se observa en la figura 17. En la parte derecha donde se encuentra la etiqueta “Static IP Entries”, se presiona el botón Add para ingresar la dirección MAC del equipo del usuario y la dirección IP que obtendrá este último. En Description se puede especificar el nombre del plan de ancho de banda que se le asigna al usuario. Se guardan los cambios y se prueba que esté funcionando el servicio DHCP.

**Figura 17. Menú DHCP**

The screenshot shows a DHCP configuration window. At the top, it indicates 'Active on: ETH01 ETH00' and 'Subnet: 192.168.1.0/255.255.255.0'. There are buttons for 'New', 'Remove', and 'Show Log'. A 'Save' button is on the left, and an 'Enabled' checkbox is checked on the right.

The 'Dynamic IP Configuration' section includes:
 

- Default Lease Time:** Days: 00, Hours: 08, Minutes: 00
- Max Lease Time:** Days: 00, Hours: 12, Minutes: 00
- Three IP ranges (Range 1, Range 2, Range 3) with input fields for start and end addresses.

The 'Subnet Options' section (with an 'Advanced' button) includes:
 

- Default Gateway: 192.168.1.60
- DNS 1: 192.168.1.60
- DNS 2: (empty)
- DNS 3: (empty)
- Domain Name: (empty)

The 'Static IP Entries' section has 'Add', 'Edit', and 'Delete' buttons. It contains a table with the following data:

Fixed IP	MAC Address	Description
192.168.1.11	08:00:27:37:85:6F	1mbps

## 7.2 CONFIGURACIÓN DE SERVICIOS DE GESTIÓN

**7.2.1 Configuración para Directorio de Usuarios.** Para la creación de usuarios que van a ser los respectivos clientes del ISP, se accede al menú del lado izquierdo Users de la interfaz principal del Zeroshell y se ingresa a la pestaña Add para introducir los datos del usuario que se va a crear, como se muestra en la figura 18 .

Aparece un formulario, como se observa en la figura 19, que requiere información importante del usuario como su nombre, apellido, número de identificación, correo electrónico, teléfono de ubicación. Además de esto el formulario pide la creación de un username y password que sirven al usuario para autenticarse y poder hacer uso del servicio de internet; se escoge el grupo al cual va a pertenecer el usuario, es decir si va estar en los que solicitaron un ancho de banda de 1 Mbps o en los que solicitaron un ancho de banda de 2 Mbps, y se escoge el tipo de contabilización que se usa para la posterior facturación de los usuarios.

Figura 18. Menú USERS

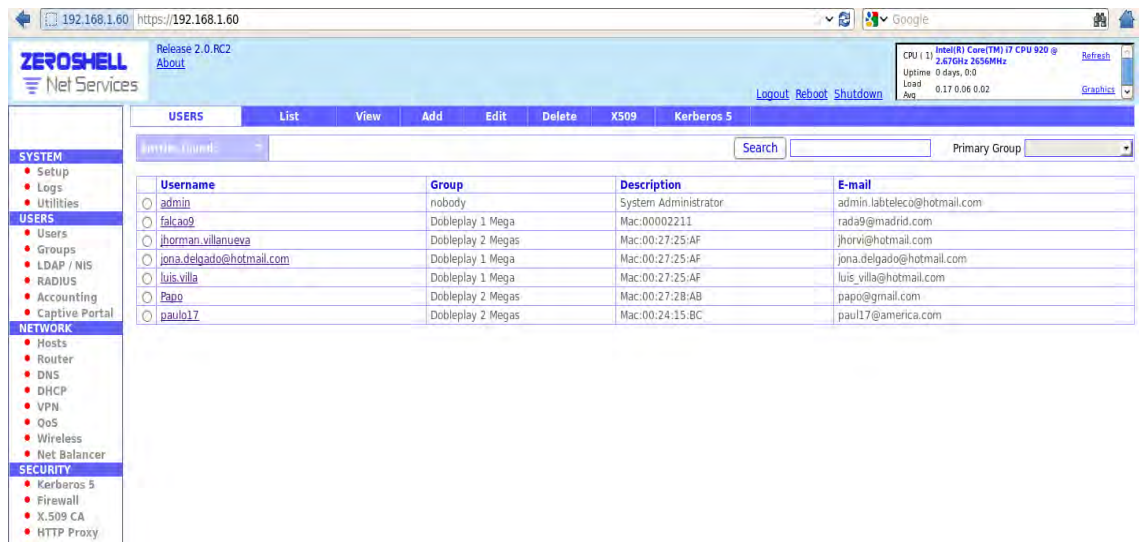
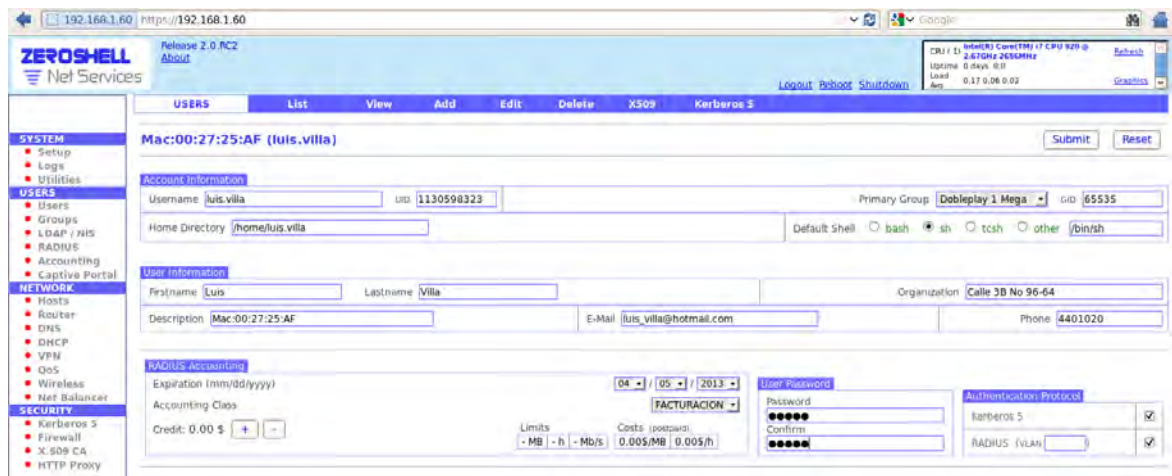


Figura 19. Formulario para la creación de usuarios



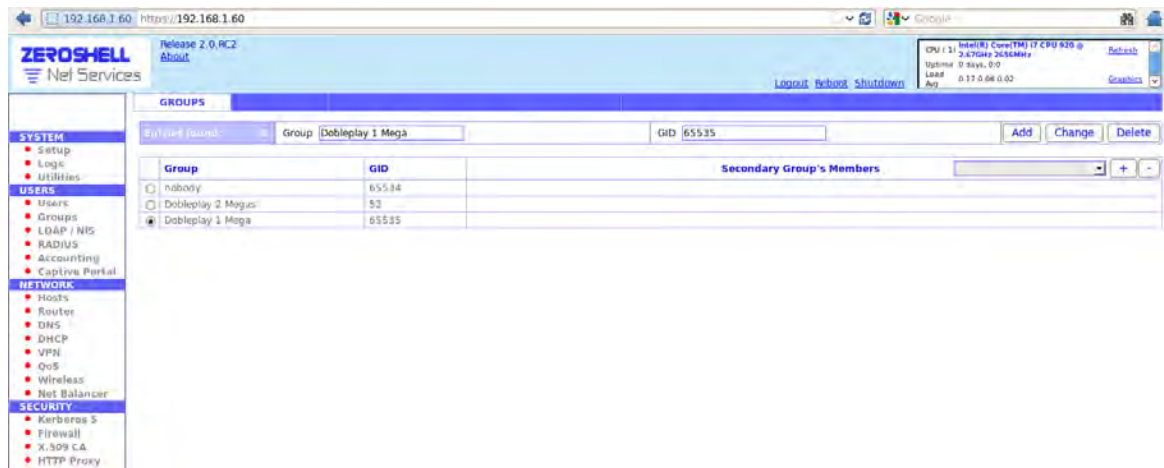
Se configura la fecha de corte de los servicios suministrados por el ISP, que en este caso son los primeros cinco días de cada mes y que deben actualizarse manualmente por el administrador del Zeroshell. Como protocolos de autenticación se escogen Kerberos 5 y Radius, protocolos que ya vienen seleccionados por defecto.

El formulario permite agregar información adicional en el campo Description, donde se puede ingresar la dirección MAC de la antena que le da la conexión

inalámbrica al usuario, esto con el hecho de tener información de gestión y control por si el usuario reporta fallas en la prestación de los servicios por parte del ISP. La creación del grupo y el tipo de contabilización para la facturación se explica a continuación, lo cual se hace también desde el Zeroshell.

- **Creación de grupo de Usuarios.** En el menú del lado izquierdo de la interfaz principal del Zeroshell (figura 15) se accede a Groups para obtener la interfaz de creación del grupo. En Group se ingresa el nombre que se le quiere dar al grupo y GID es el número de identificación del grupo; cuando se ingresan los respectivos datos se presiona Add y queda el grupo creado. En la figura 20 se observan dos grupos creados: Dobleplay 2 Megas y Dobleplay 1 Mega.

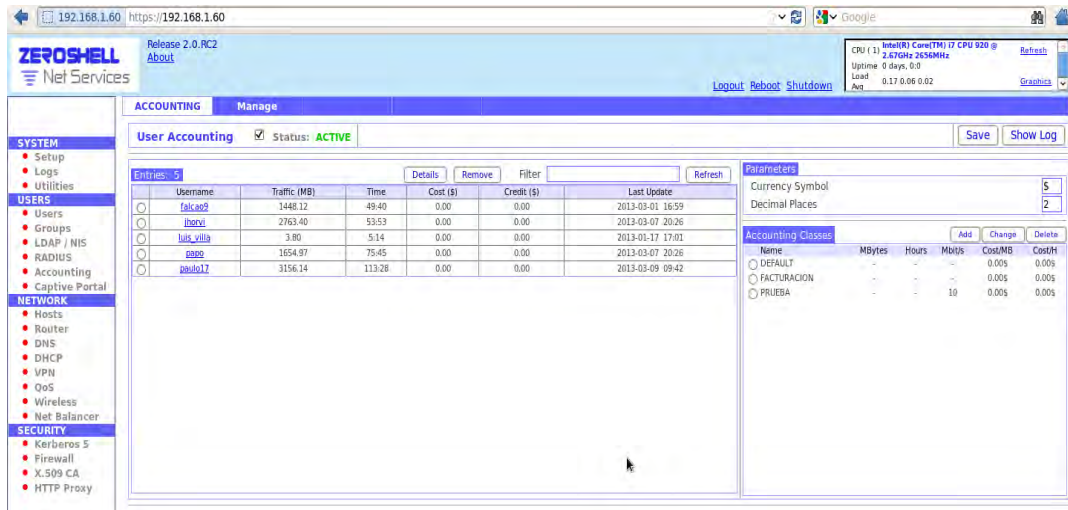
**Figura 20. Creación de grupos de usuarios**



## 7.2.2 Configuración de Autenticación.

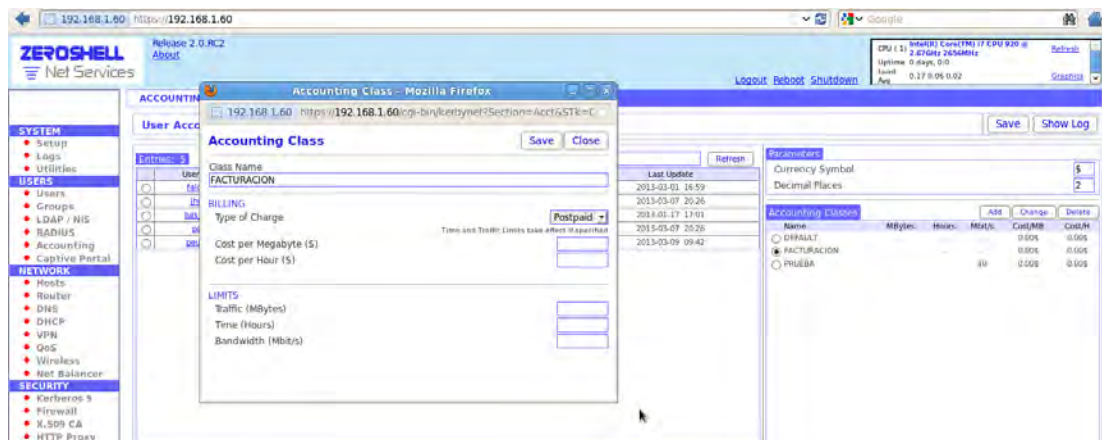
- **Creación de la clase de contabilización.** En el menú del lado izquierdo de la interfaz principal del Zeroshell (figura 15) se accede a Accounting que muestra el consumo de los recursos de red por parte de los usuarios, como se observa en la figura 21. Muestra información como el tráfico descargado, el total de tiempo que ha estado conectado, el costo y crédito si la cuenta que maneja el usuario es prepago y se le está cobrando por el tiempo que permanezca conectado o por la cantidad de tráfico descargado. Para esta ISP se maneja el tipo de cuenta Postpago, por ende estos valores (tráfico, tiempo, costo crédito) no importan mucho al administrador del Zeroshell.

Figura 21. Menú Accounting



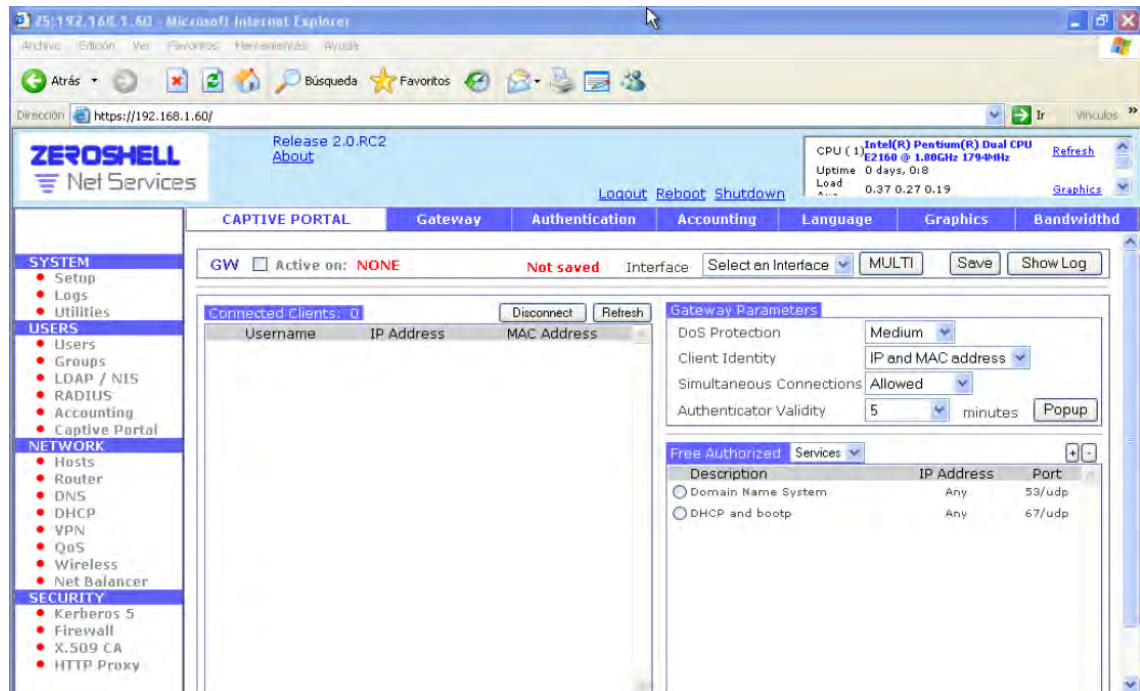
Para la creación de la clase de contabilización, se accede en parte derecha de la figura 21 a la sección de Accounting Classes y se presiona Add; sale una ventana como se observa en la figura 22 que solicita información como el nombre de la clase, para este caso se dio el nombre de FACTURACION, y el tipo de cuenta, que la que se utiliza para el ISP es Postpago (Postpaid). Los otros campos como Costo por Megabyte y Costo por Hora se dejan vacíos ya que éstos se utilizan para el tipo de cuenta Prepago. La otra opción que se puede configurar son los límites de Tráfico, tiempo y ancho de banda; si a un determinado usuario se le especifica un límite de tráfico, cuando llegue a ese límite automáticamente se le suspende el servicio de internet. Estos valores no son necesarios para esta ISP ya que el servicio de internet que se presta es ilimitado.

Figura 22. Creación de la clase de contabilización



- **Creación del portal cautivo.** Con las anteriores configuraciones ya se tiene lo necesario para la creación del portal cautivo, que se hace también desde el Zeroshell. Para ello, se accede en el menú del lado izquierdo de la interfaz principal (figura 15) a Captive Portal donde muestra una interfaz como se observa en la figura 23.

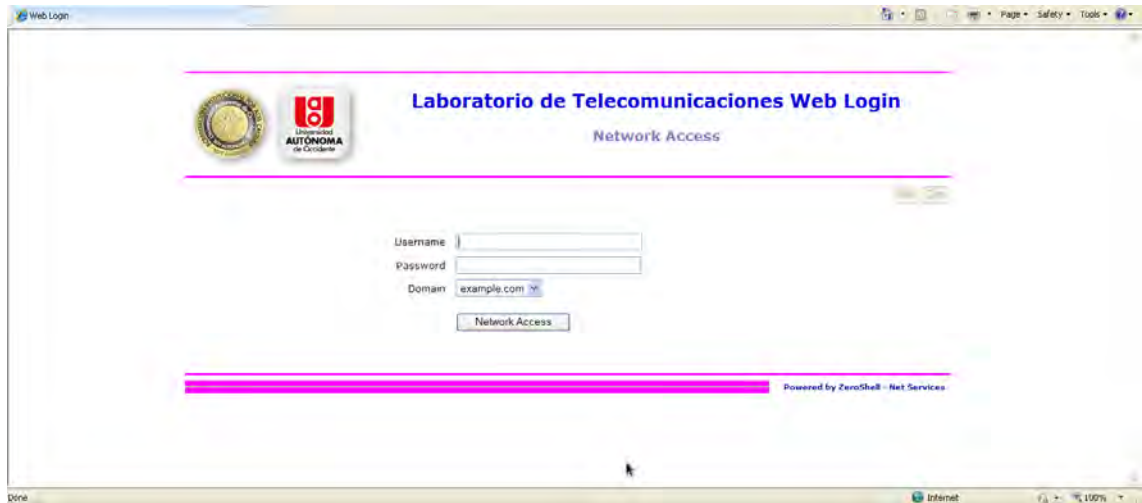
**Figura 23. Creación del portal cautivo**



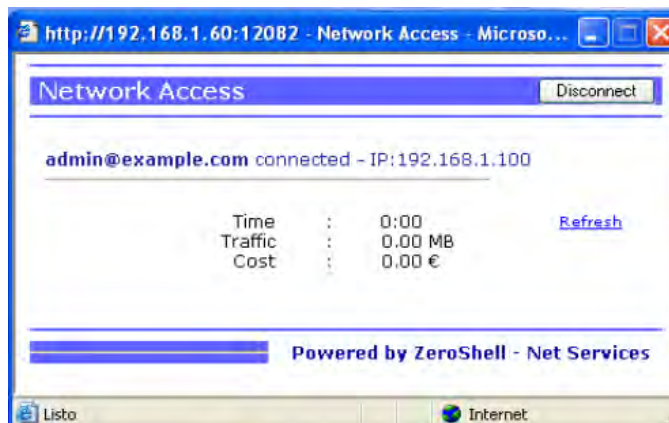
En Gateway (menú superior) se activa la casilla donde dice GW, se selecciona la interface ETH00, que es la interface que conecta la red local y donde se quiere aplicar el portal cautivo. Se presiona Save para guardar los cambios realizados y de esta forma ya se tiene el portal cautivo activado y funcionando. Al activar el portal cautivo automáticamente se activa el servidor Radius, que es quien hace la autenticación de los usuarios. Cada vez que un usuario entre a un navegador o browser, se visualizará una ventana de autenticación obligatoria, como se observa en la figura 24, donde el usuario debe ingresar sus Username y Password para acceder al servicio de Internet.

Si la autenticación es correcta, se podrá ver un popup (ventana emergente) como el de la figura 25, que muestra tiempo de conexión, cantidad de tráfico descargado y costo. Mientras esta ventana no se cierre el usuario podrá utilizar el servicio de Internet.

**Figura 24. Ventana de Autenticación**



**Figura 25. Ventana emergente Popup**

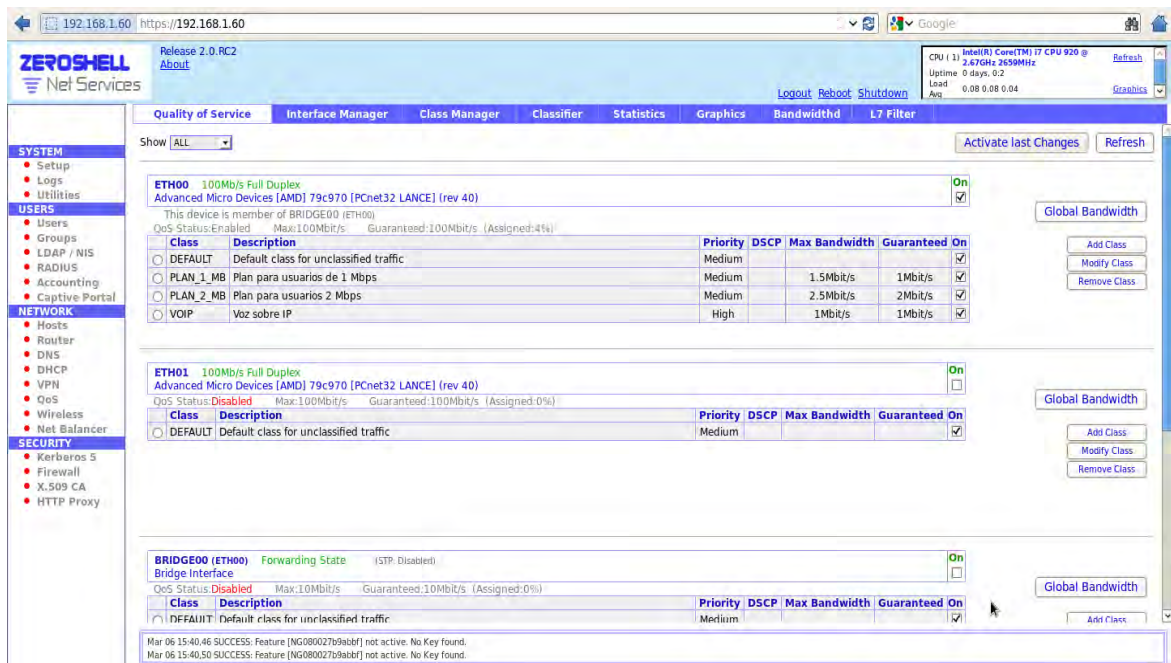


**7.2.3 Configuración para Control de Ancho de Banda.** Esta opción de QoS, que se encuentra en el menú del lazo izquierdo de la interfaz principal del Zeroshell (figura 15), permite realizar QoS (Quality of Service) y gestión de ancho de banda en el tráfico de red que lo atraviesa. Esta opción se visualiza en la figura 26.

Es aquí donde se configura los diferentes planes de anchos de banda que el ISP va proveer a los diferentes usuarios. Para esto es necesario crear un cierto número de tipos de tráfico, con un respectivo rango de IP, a los que se les asignan los parámetros de calidad de servicio, prioridad, ancho de banda mínimo

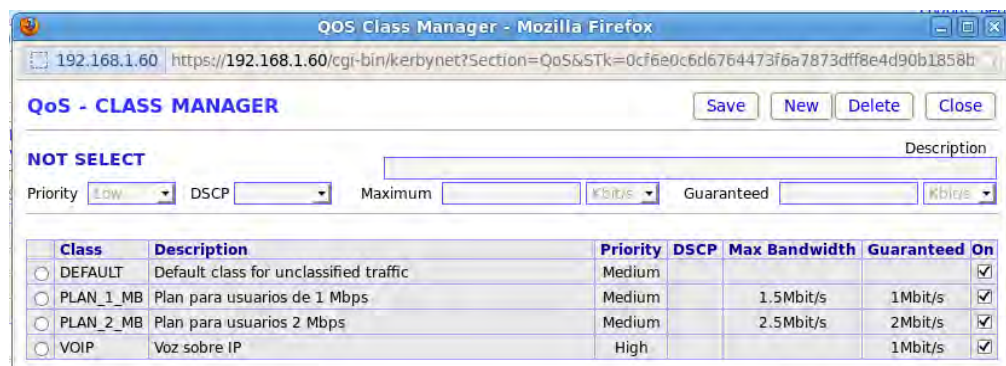
garantizado en caso de congestión de red y el máximo ancho de banda cuando la red no esté congestionada.

**Figura 26. Configuración para gestión de ancho de banda**



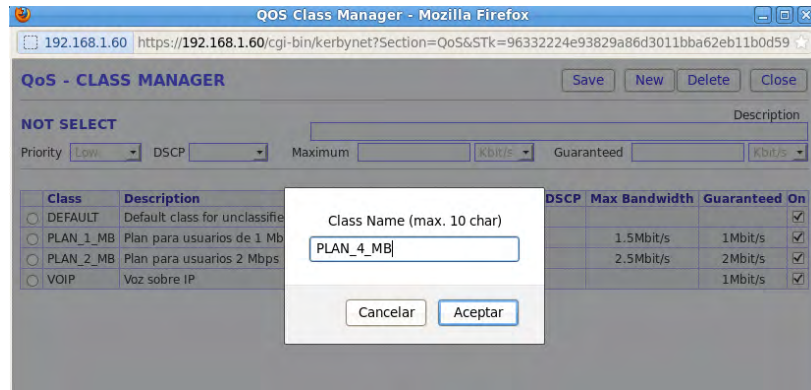
En Class Manager, que se encuentra en la parte superior del menú QoS, se crean las diferentes clases de QoS; al ingresar a Class Manager aparece una ventana como la que se observa en la figura 27.

**Figura 27. Creación de las clases de QoS**



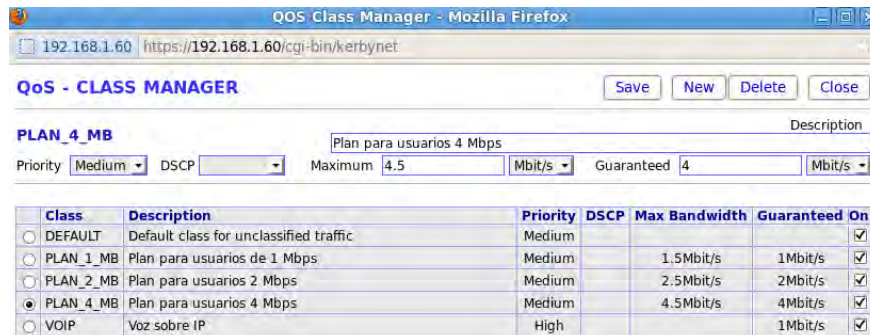
Para crear una nueva clase se presiona el botón New y aparece una ventana solicitando el nombre de la clase: para este caso se dio el nombre de PLAN\_4\_MB como se observa en la figura 28.

**Figura 28. Nombre de la clase para el plan de 4 Mbps**



Al presionar Aceptar se procede a llenar los datos adicionales como se observa en la figura 29. Maximum es el ancho de banda máximo que se puede alcanzar cuando no hay congestión y Guaranteed es el ancho de banda garantizado cuando la red se encuentra congestionada.

**Figura 29. Características para el plan de 4 Mbps**

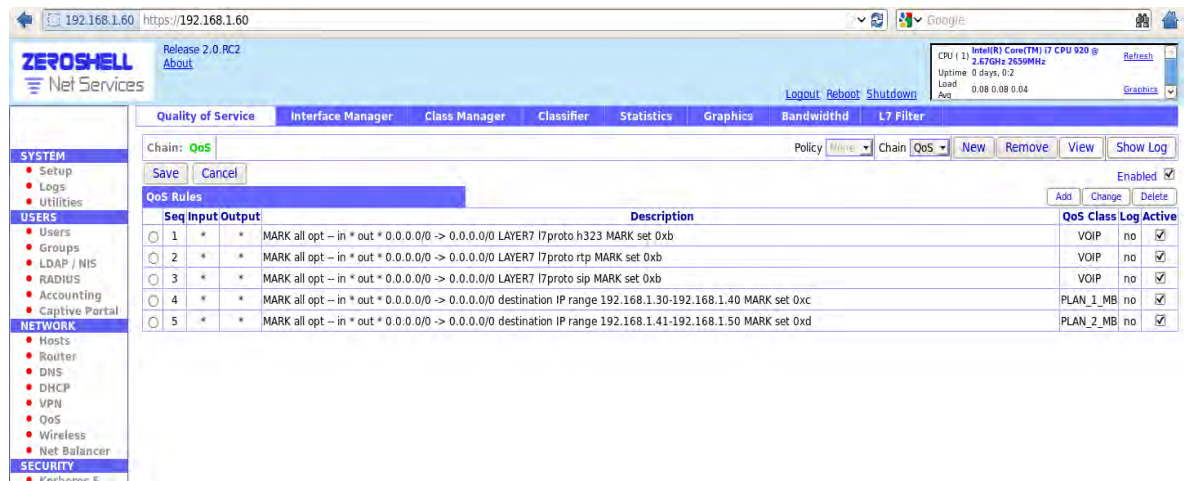


Hasta ahora se han creado las diferentes clases de QoS, pero todavía no se ha especificado a que rango de IPs se desea aplicar la gestión del ancho de banda. Lo anterior se hace en el Classifier como se muestra en la figura 30. Se presiona el botón Add para insertar la regla que permita limitar el ancho de banda para un rango determinado de IP.

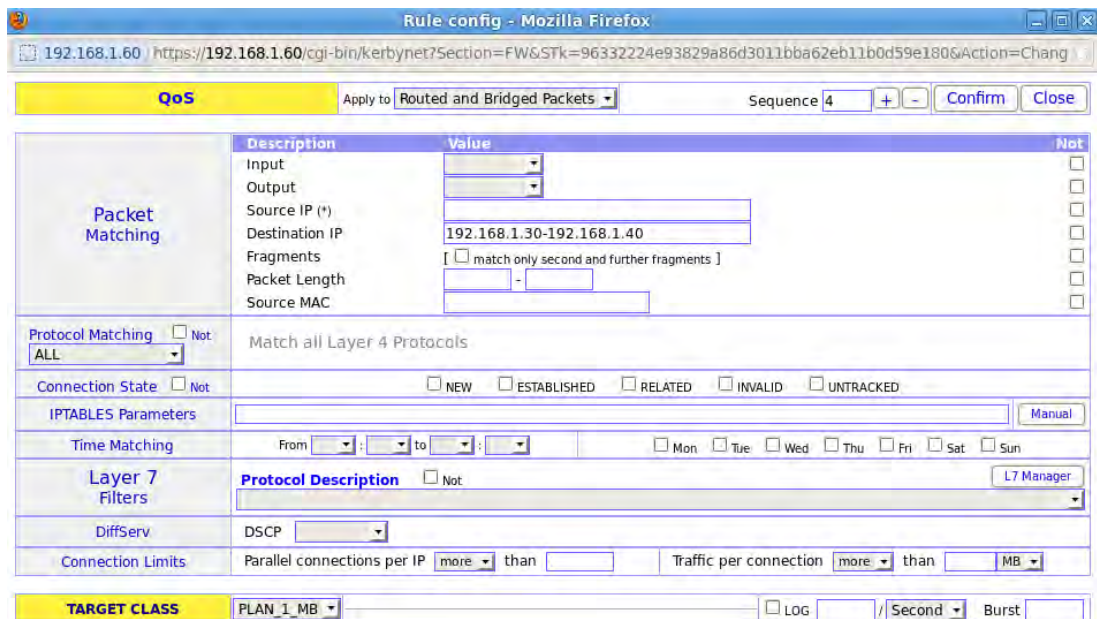


La ventana que se observa en la figura 31, en la sección de Destination IP, se coloca el rango de IP al cual se le quiere limitar el ancho de banda. En la parte inferior en TARGET CLASS se escoge la clase de QoS, que ya trae configurado el valor de ancho de banda, en este caso de 1 Mbps. Se presiona confirm y posteriormente Save y de esta forma se tiene la regla QoS configurada. Se debe verificar que la regla quede activa.

**Figura 30. Opción Classifier del Zeroshell donde se especifica el rango de IP al cual se le va a limitar el ancho de banda**



**Figura 31. Creación de nueva regla para un ancho de banda determinado**

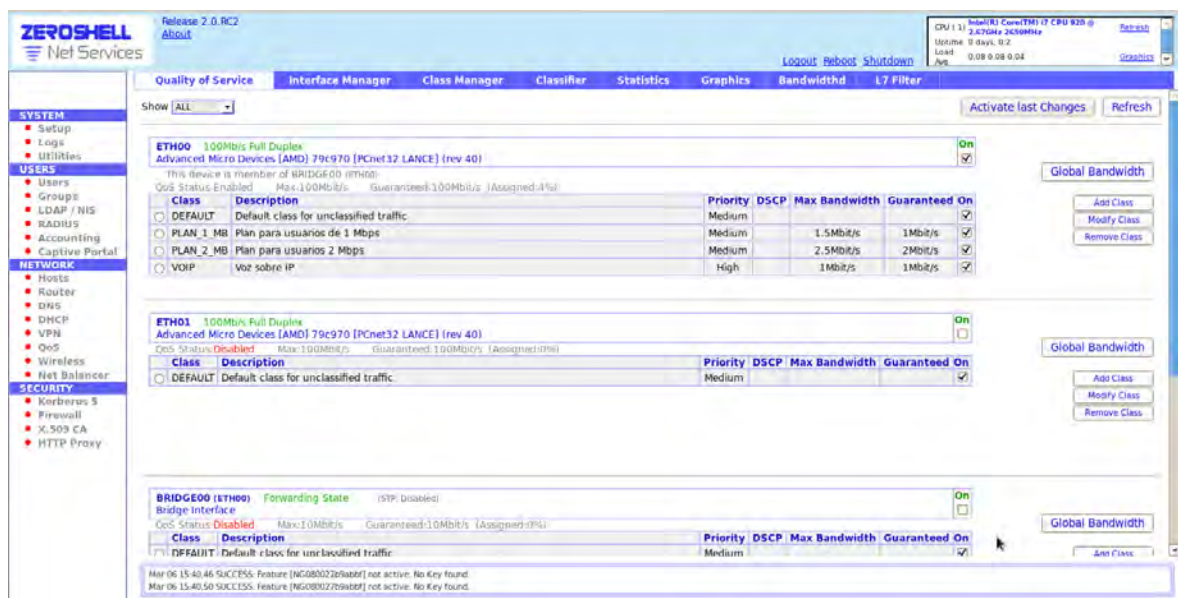


Se realiza la misma configuración anterior para los otros planes de ancho de banda con diferentes rangos de IP.

Ya por ultimo solo resta asignar las clases de QoS creadas a las interfaces de red, cuyo tráfico de salida se desea controlar. La interfaz que conecta a la red local en este ISP es la ETH00, por lo tanto es a la que se le agrega las clases de QoS, lo cual se hace desde el Interface Manager presionando el botón Add Class. Aparece una ventana con las diferentes clases que se desean agregar. Después de agregar las clases se guarda pulsando el botón Activate last changes y se verifica que las clases queden activas. De igual forma hay que activar el QoS para la interfaz ETH00 haciendo clic en el cuadro debajo de "On". Las anteriores características se observan en la figura 32.

Con la anterior configuración, QoS está trabajando para el tráfico de salida de la interfaz ETH00 y está realizando control de ancho de banda para la red local.

**Figura 32. Asignación de clases creadas a la interfaz de red**

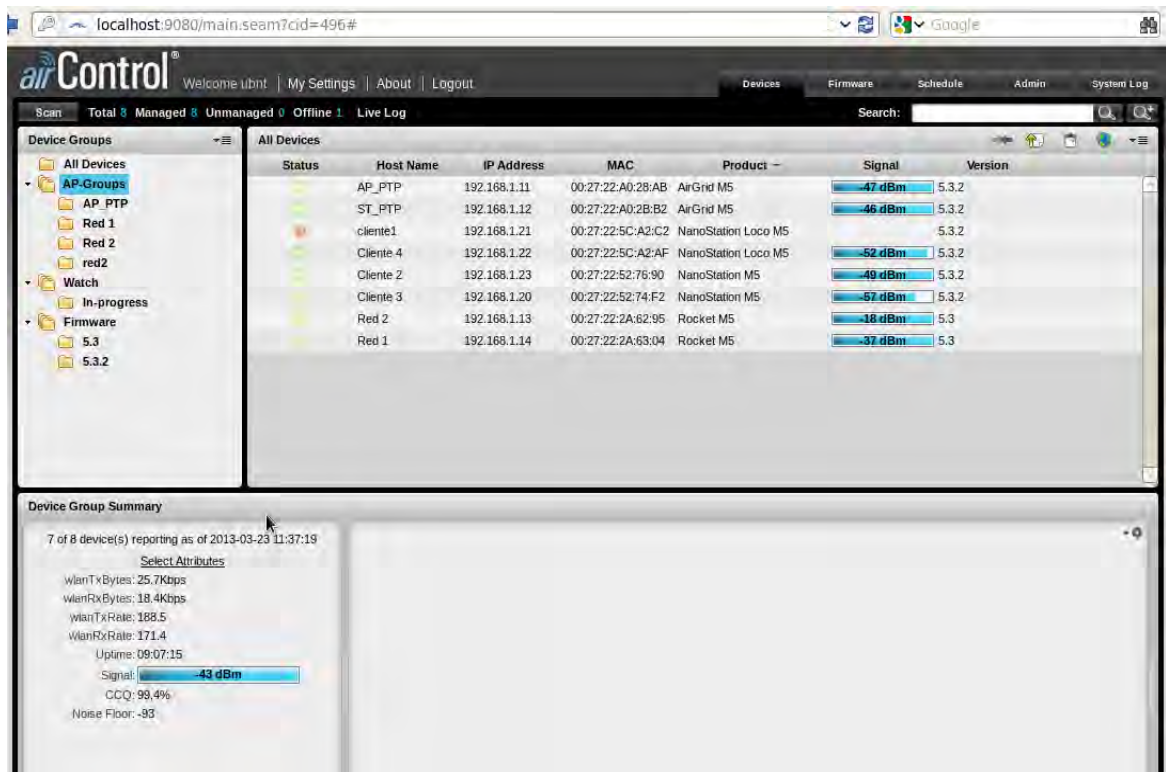


**7.2.4 Configuración de monitoreo y control de la Red de Acceso.** Desde cualquier browser o navegador de internet se ingresa como URL *localhost:9080* para acceder al software de gestion airControl, el cual pide un *Username* y *Password*, que por defecto son, *ubnt*, *ubnt* respectivamente. Si los anteriores

datos que se ingresan son correctos, se obtiene la interfaz que se observa en la figura 33.

Esta interfaz muestra los módulos Ubiquiti que están conectados a la red lo cual se comprueba verificando que el Status se encuentre en color verde, los que están desconectados, donde su Status aparece de color rojo, su Host Name, su respectiva dirección IP, la dirección MAC, el nivel de intensidad de señal, el nombre del producto, es decir si es Rocket M5, Airgrid M5 o Nanostation M5. Las características que componen al airControl se pueden observar en el Anexo D.

**Figura 33. Monitoreo y control de red airControl**



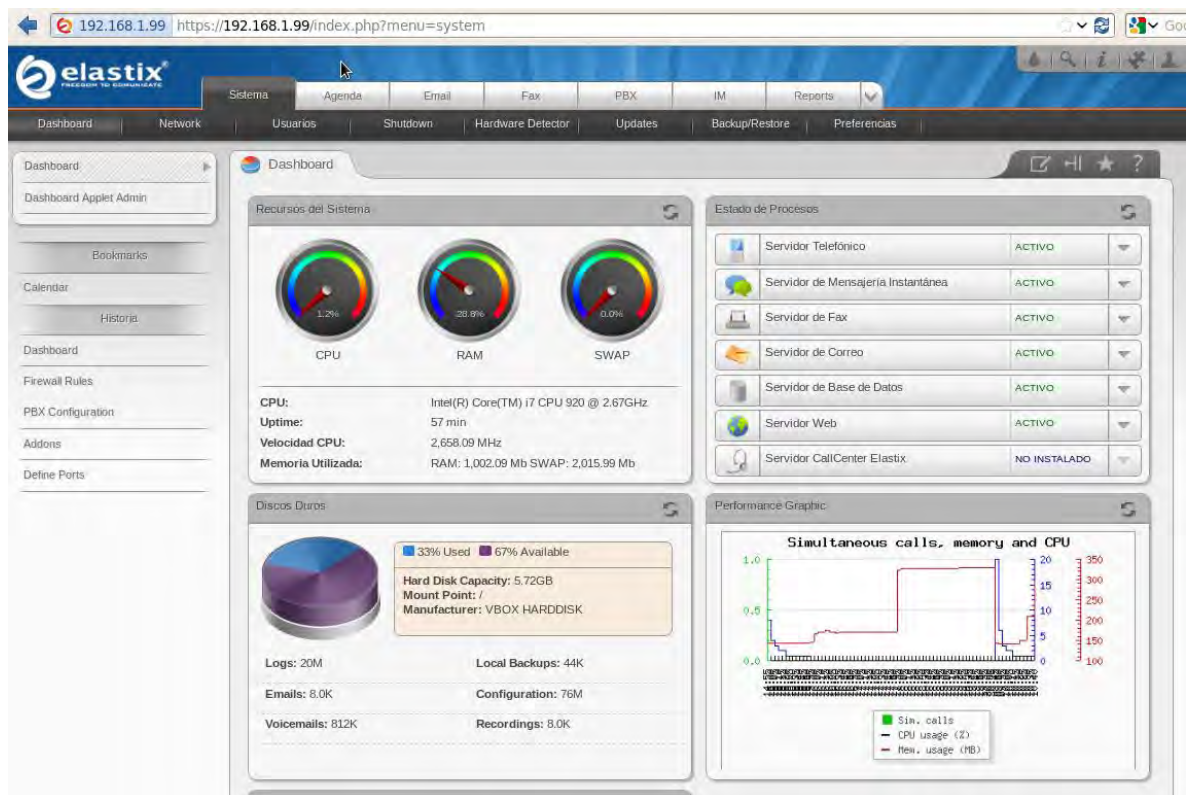
### 7.3 CONFIGURACIÓN DEL SERVICIO DE TELEFONÍA IP

Elastix fue la distribución seleccionada para implementar el servicio de telefonía IP, utilizando su interfaz web para generar las funcionalidades y aplicaciones. Para ingresar a esta interfaz, se introduce en el navegador o navegador de internet la dirección IP con la que se configuró el Elastix en la consola, el cual es 192.168.1.99. Se abre una ventana donde se introduce el usuario y la contraseña;

para ingresar como administrador, el usuario es “admin” y la contraseña es “Autonoma2012”.

Se presenta en la pantalla de inicio la opción Dashboard del menú Sistema, donde se visualiza los recursos del sistema, el estado de los procesos, información del disco duro y gráficas de rendimiento, como se muestra en la figura 34; en el estado de procesos se visualiza que servidores se encuentran activos o desactivos. El menú sistema presenta además opciones de Network, Usuarios, Shutdown, Hardware Detector, Updates, Backup/Restore y Preferencias. Las dos opciones más importantes en este menú son Network y Usuarios, los cuales se explican en el Anexo E. De igual forma, en el Anexo E se presenta la configuración para crear las extensiones de los usuarios con su respectivo nombre.

**Figura 34. Pantalla de inicio de la interfaz web de Elastix**

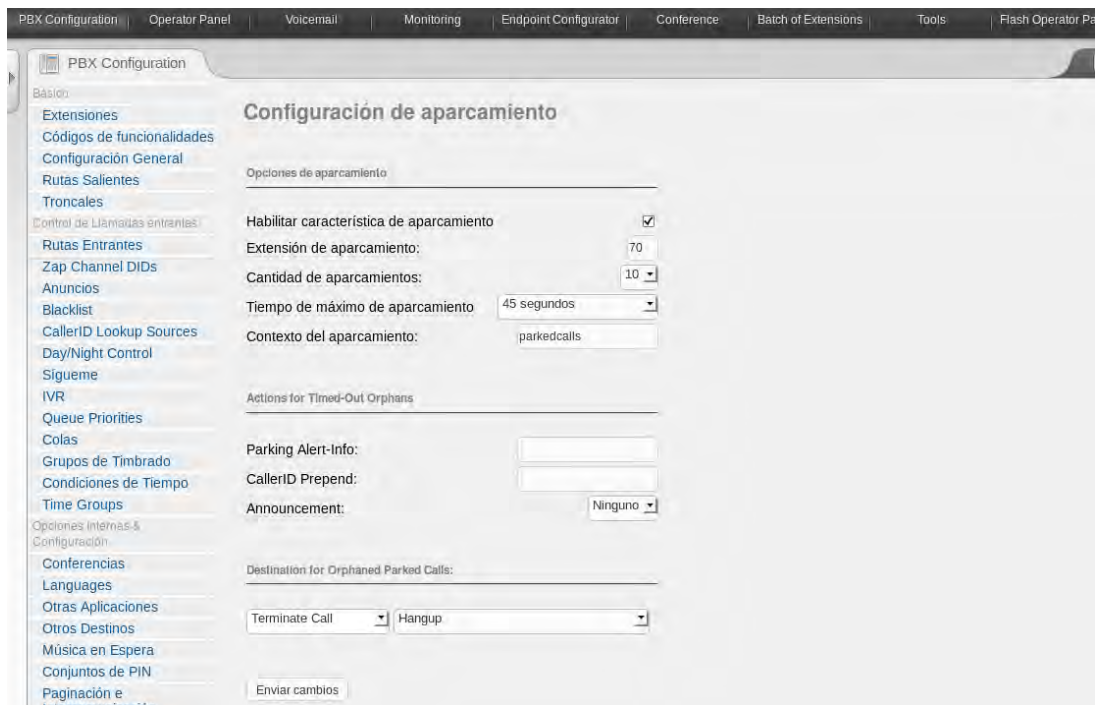


**7.3.1 Configuración de los servicios para VoIP.** Para la configuración de los servicios establecidos en el ítem 6.1.3.1, se utilizan las funcionalidades que se encuentran en la opción PBX Configuration del menú Sistema, ubicados en el lado izquierdo de la ventana.

- **Transferencia de Llamadas.** Por defecto, Elastix ya viene configurado con la funcionalidad de transferencia de llamadas, solo se debe digitar ## seguido del número de la extensión a donde se va a transferir la llamada.

- **Parqueo de Llamadas.** El parqueo de llamadas se realiza seleccionando la herramienta Estacionamiento, ubicado en la parte izquierda de la opción PBX Configuration. En la figura 35 se presenta los parámetros de este servicio. Los principales parámetros son: Habilitar las funcionalidades del parqueo de llamadas, la extensión del parqueo, el número de slots disponibles para el parqueo de llamadas, tiempo máximo en que permanece parqueada una llamada y el destino de una llamada cuando esta no puede ser parqueada; se introducen y se seleccionan los mismos valores y características que se presentan en la figura 35. Por último se presiona el botón *Enviar cambios* para guardar la configuración realizada.

**Figura 35. Parqueo de Llamadas en Elastix**



- **Buzón de Voz.** La configuración del buzón de voz se realiza ya sea en el momento en que se crea las extensiones o ingresando a cada extensión ya creada. En la figura 36 se observa los distintos parámetros para el uso del buzón de voz. Se utilizan dos parámetros principalmente los cuales son: Habilitar el

servicio y la contraseña para ingresar al buzón. Se establece la contraseña para cada uno de los 4 usuarios como los 4 últimos dígitos de la extensión correspondiente, por ejemplo la contraseña de Luis Villa es 1020 ya que su extensión es 4401020.

**Figura 36. Configuración del Buzón de Voz**

The screenshot shows the 'Voicemail & Directory' configuration interface. The 'Status' is set to 'Enabled'. The 'Voicemail Password' is '1020'. The 'Email Address' and 'Pager Email Address' fields are empty. The 'Email Attachment', 'Play CID', 'Play Envelope', and 'Delete Voicemail' options are all set to 'no'. The 'IMAP Username' and 'IMAP Password' fields are empty. The 'VM Options' field is empty. The 'VM Context' is set to 'default'.

- **Llamada en espera.** La configuración de la llamada en espera se realiza también en dos formas: en el momento en que se crea las extensiones o ingresando a cada extensión ya creada como se observa en la figura 37.

**Figura 37. Configuración de la llamada en espera**

The screenshot shows the configuration page for extension 4401020. The 'Display Name' is 'Luis Villa'. The 'Outbound CID' is empty. The 'Ring Time' is set to '10'. The 'Call Waiting' is set to 'Enable'. The 'Call Screening' is set to 'Disable'. The 'Pinless Dialing' is set to 'Disable'. The 'Emergency CID' is empty. A list of extensions is visible on the right side of the page, including 'Luis Villa <4401020>'.

Simplemente se habilita el Call Waiting y se presiona el botón *Enviar cambios*, obteniendo finalmente el servicio en funcionamiento.

**7.3.2 Configuración de teléfonos.** Los teléfonos que los usuarios utilizan para realizar las llamadas y acceder al servicio de VoIP se presentan en el cuadro 9. En cada teléfono se configura los parámetros y se establece las conexiones pertinentes, teniendo en cuenta que los servicios ofrecidos por Elastix deben estar ejecutándose, incluyendo las extensiones de cada usuario.

**Cuadro 9. Teléfonos de usuarios para acceder al servicio de VoIP**

<b>Teléfonos</b>	<b>Cantidad</b>	<b>Marca</b>	<b>Modelo</b>
Softphone	2	3CX	3CXPhone
Teléfono IP	1	Linksys Cisco	SPA921
Teléfono Análogo	1	Lucent	9101

- **Softphone.** El softphone se descarga de forma gratuita de la página oficial de 3CX® al sistema operativo de Microsoft Windows. Al finalizar la instalación del programa, se puede ejecutar el softphone.

Para ingresar el nombre y extensión de un usuario, se abre la ventana Accounts que permite visualizar las distintas cuentas creadas para el softphone como se muestra en la figura 38. En esta ventana se puede crear, editar y eliminar las cuentas de los usuarios; se selecciona la opción New para crear una nueva cuenta y aparece una ventana con los parámetros que se observan en la figura 39. Los principales parámetros que se configuran en esta ventana son el nombre de la cuenta de usuario, la identificación del usuario, el número de extensión, contraseña y la dirección IP del servidor PBX/SIP que corresponde a la IP del Elastix que es 192.168.1.99.

Al finalizar esta configuración, el softphone pasa de un estado Not connected al estado On Hook y queda listo para poder efectuar las llamadas. Como se estableció en el cuadro 9, se hace uso de dos softphone donde uno corresponde al usuario Jonathan Delgado con la extensión 3307080 y el otro corresponde al usuario Paulo Libreros con la extensión 3305060; en ambos casos se realiza el mismo procedimiento descrito anteriormente.

Figura 38. Cuentas de usuario para el softphone

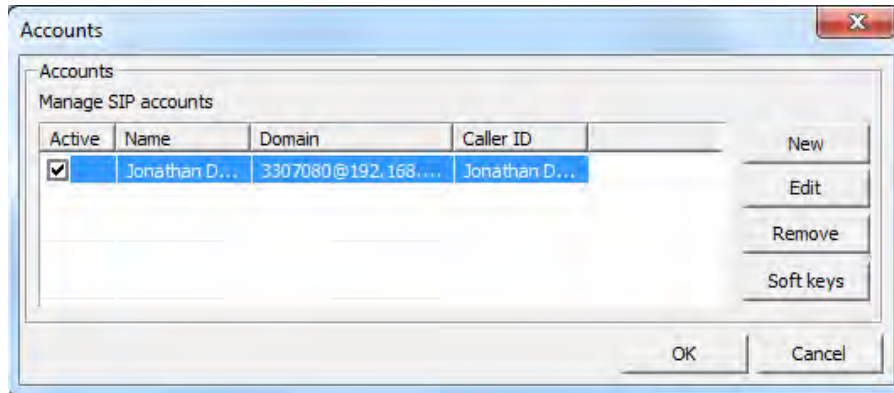
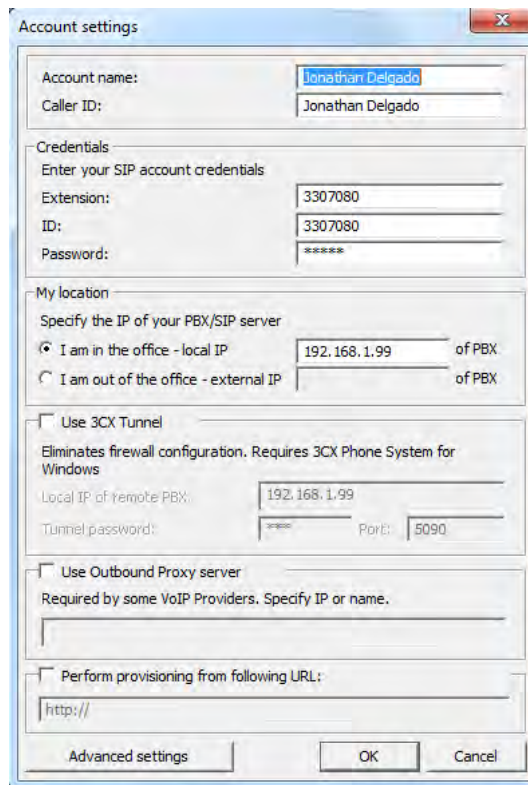


Figura 39. Parámetros para crear una cuenta de usuario

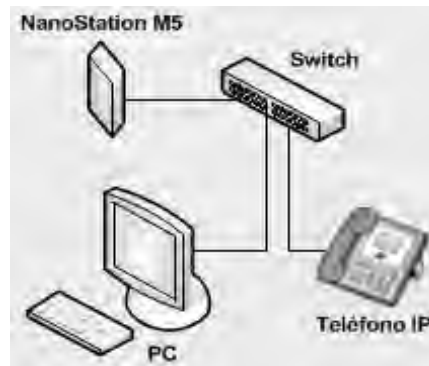


- **Teléfono IP.** El teléfono IP se configura tanto en el portal web donde se establecen los parámetros de configuración como en el panel que presenta el teléfono físicamente. La conexión que se realiza para el uso del teléfono se muestra en la figura 40. El teléfono IP y el PC se conectan en un switch junto al NanoStation M5 el cual realiza el enlace con la red inalámbrica.



En el panel del teléfono se establece la dirección IP que este tendrá y su respectiva máscara, ingresando al menú Network que se encuentra presente en los ajustes del teléfono (Setting). Para configurar los otros parámetros, se ingresa en el browser la dirección IP del teléfono para entrar portal web de Linksys. El procedimiento de configuración se presenta en el Anexo B.

**Figura 40. Conexión del teléfono IP**



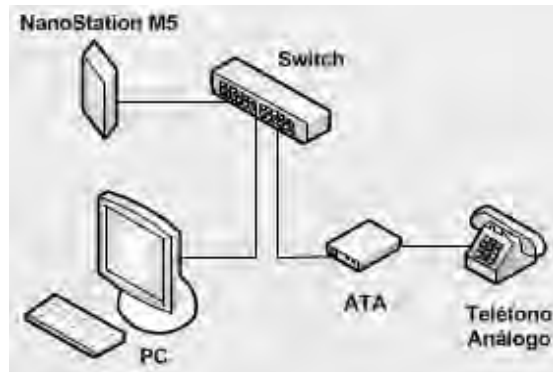
Al finalizar la configuración, el teléfono IP queda listo para efectuar llamadas.

- **Teléfono Análogo.** El teléfono análogo realiza una comunicación en redes PSTN y no sobre IP. Por lo tanto, para que este teléfono realice llamada sobre protocolo IP, se debe utilizar un ATA en donde se efectúe todas las configuraciones para acceder al servicio de VoIP. La conexión para el uso del teléfono análogo se presenta en la figura 41.

El teléfono se enlaza al ATA y este último se conecta a un switch junto al PC y el NanoStation M5 encargado de efectuar el enlace inalámbrico. El ATA que se implementa es de marca Linksys Cisco, modelo PAPT2, el cual contiene dos puertos RJ-45 para teléfonos análogos y un puerto RJ-45 para una conexión Ethernet.

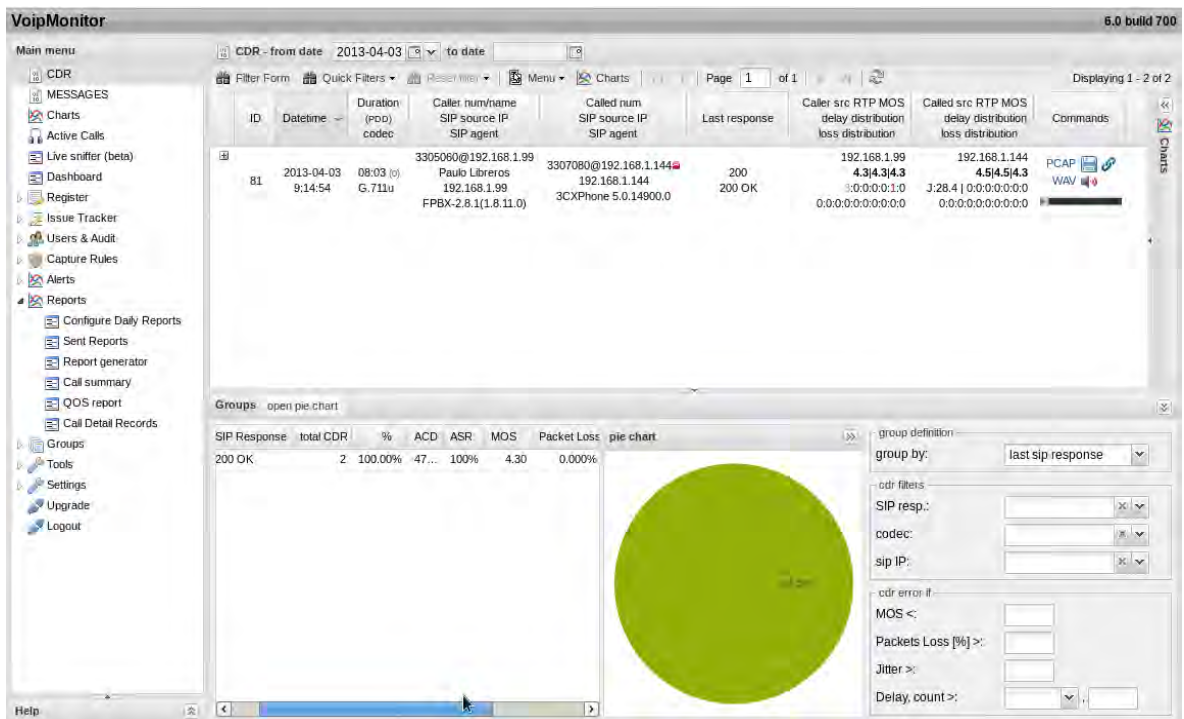
La configuración para utilizar el teléfono se realiza en el ATA, donde se manejan dos opciones: Uno es la configuración de los parámetros utilizando el teléfono al entrar a un menú de voz e ingresar una serie de códigos; la segunda configuración se realiza directamente en la interfaz web al ingresar la IP del ATA en el browser. La configuración del ATA por medio de la interfaz web se presenta en el Anexo B. Al finalizar la configuración, el teléfono análogo queda listo para efectuar llamadas.

Figura 41. Conexión para uso del teléfono análogo



**7.3.3 Configuración del VoIPMonitor.** Para ingresar a la interfaz web del VoIP monitor se introduce en el browser la dirección <http://localhost/voipmonitor>, en donde se observa una ventana de autenticación para ingresar al portal web. Se ingresa con el nombre de usuario “admin” y la contraseña “admin”. En la figura 42 se observa el portal de inicio CDR donde se visualiza distintas informaciones referentes a las llamadas realizadas

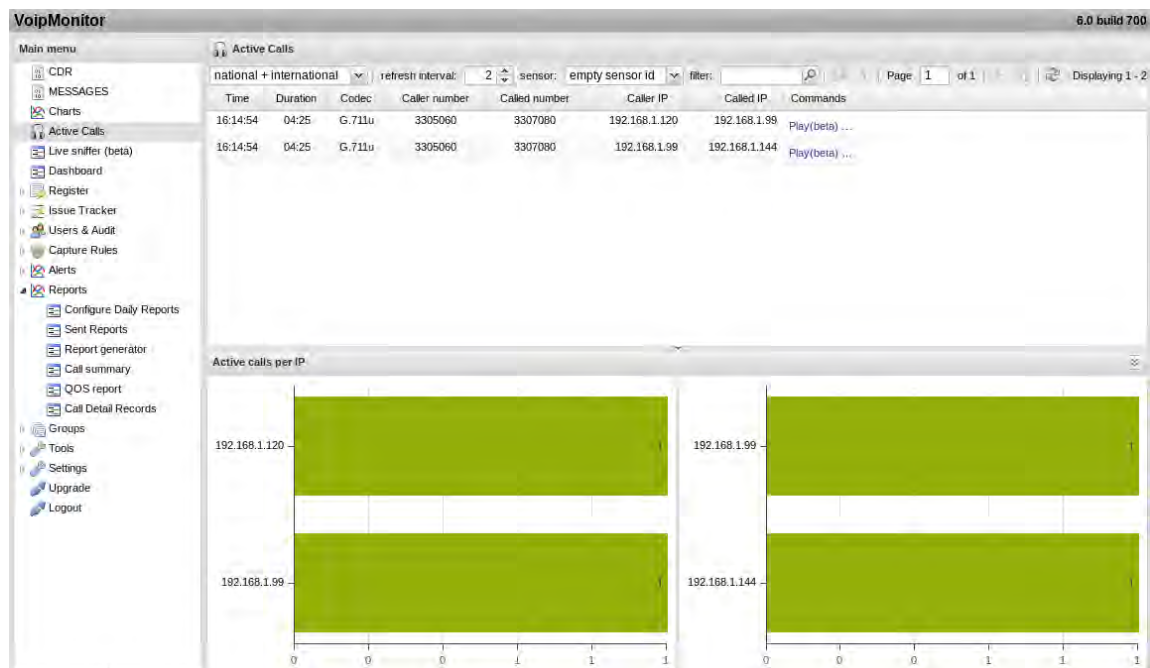
Figura 42. Portal de inicio CDR



El CDR muestra las características de las llamadas tanto del origen como del destino, información referente al protocolo RTP y algunas medidas de QoS que puedan interesar al personal que administra la red. En la parte izquierda de la figura 42 se ubica las distintas opciones para visualizar y configurar las llamadas registradas en el servicio de VoIP. Se puede obtener registro en tiempo real de las llamadas, gráficas estadísticas, reportes de QoS, resumen de la llamada, alertas, etc.

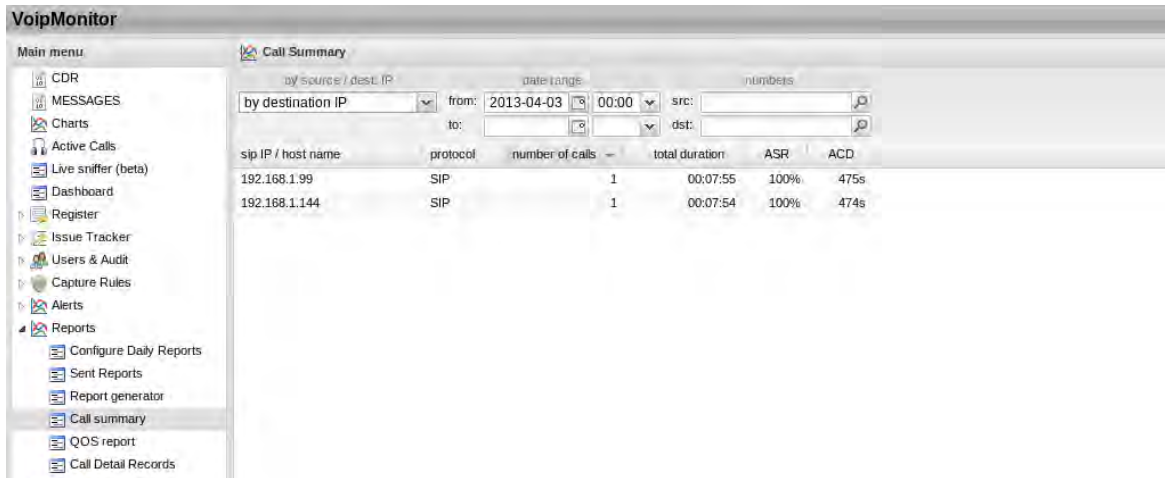
La opción Active Call permite monitorear las llamadas en tiempo real, ya que las otras opciones arrojan información cuando se ha finalizado la llamada. En la figura 43 se observa que se está realizando una llamada desde el usuario Paulo Liberos con extensión 3305060 hacia el usuario Jonathan Delgado con extensión 3307080; se visualiza además las direcciones IP de ambos usuarios.

**Figura 43. Monitoreo de llamadas en tiempo real**



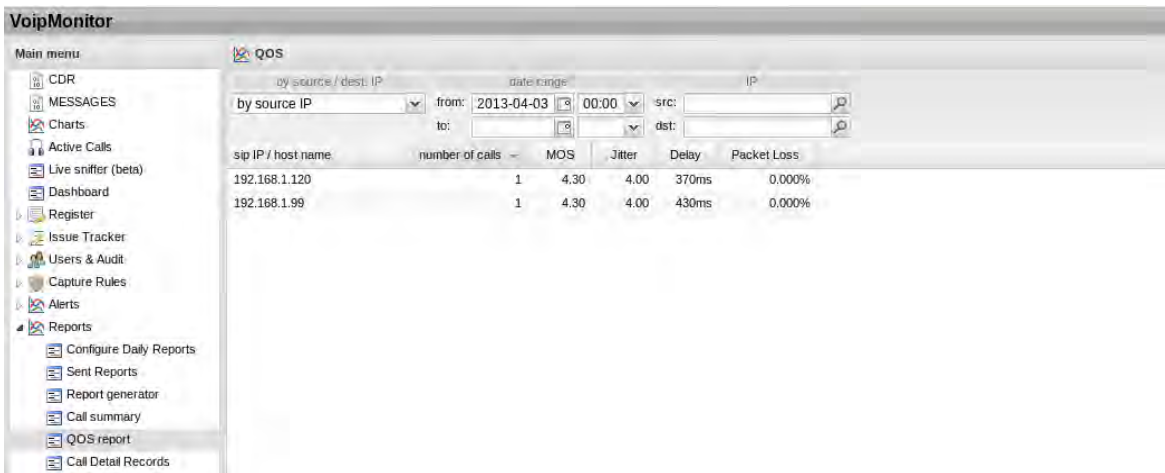
Al finalizar la llamada, se puede observar el resumen de esta en la opción Call Summary, que se encuentra dentro de Reports. En esta opción se visualiza las distintas características que presentó la llamada, ya sea en el usuario fuente representado con el IP 192.168.1.120 o en el usuario destino representado con la IP 192.168.1.144; se debe seleccionar el usuario destino o el usuario fuente para ver las propiedades de cada uno. Esta ventana se muestra en la figura 44.

**Figura 44. Resumen de llamada para el usuario destino**



Las mediciones de QoS de la llamada realizada se observan en la opción QoS Report, donde se encuentran las mediciones correspondientes al Jitter, Latencia o Delay, MOS y pérdida de paquetes. En la figura 45 se muestra las medidas para el usuario fuente con IP 192.168.1.120. De igual forma se puede seleccionar al usuario destino con IP 192.168.1.144 para observar sus medidas de QoS.

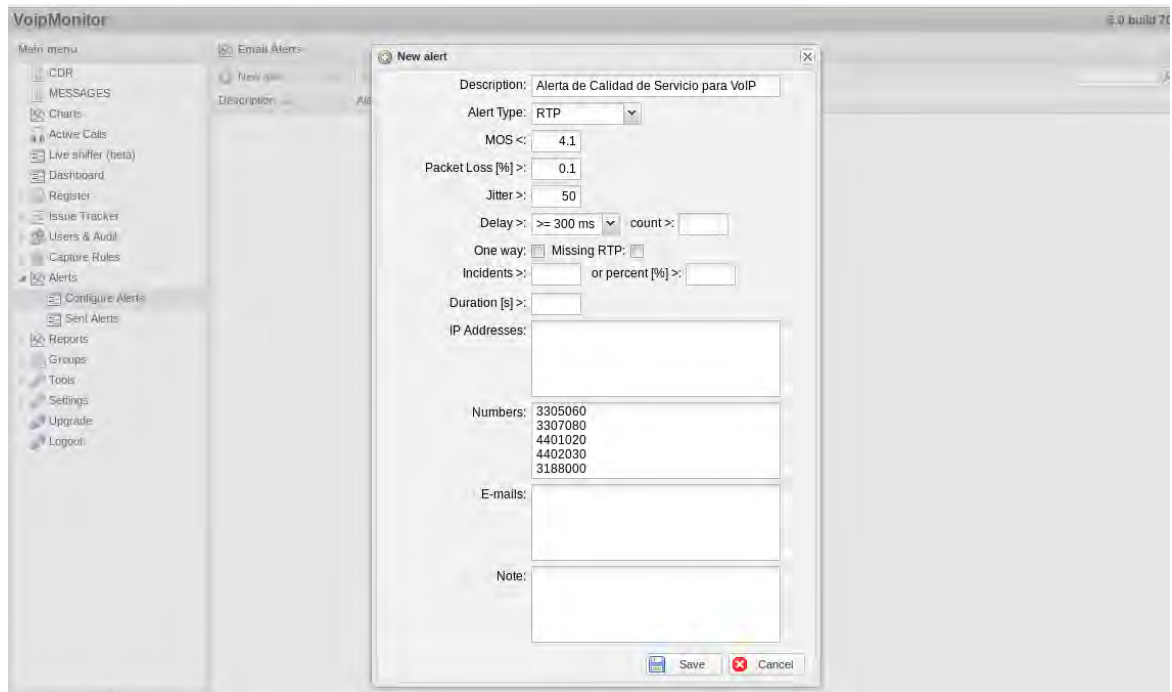
**Figura 45. Medición de QoS para el usuario fuente**



Para ingresar las alarmas correspondientes a las mediciones de QoS, en caso que se sobrepase un valor máximo y se presente errores de comunicación, se utiliza la opción Configure Alerts que se encuentra dentro de Alerts.

Se crea una nueva alerta y se introducen los valores máximos correspondientes al Jitter, pérdida de paquetes, latencia y MOS como se observa en la figura 46; además se introducen los números telefónicos en donde se activan las alarmas.

**Figura 46. Creación de Alertas para mediciones de QoS**



## 7.4 CONFIGURACIÓN DE LA RED DE ACCESO

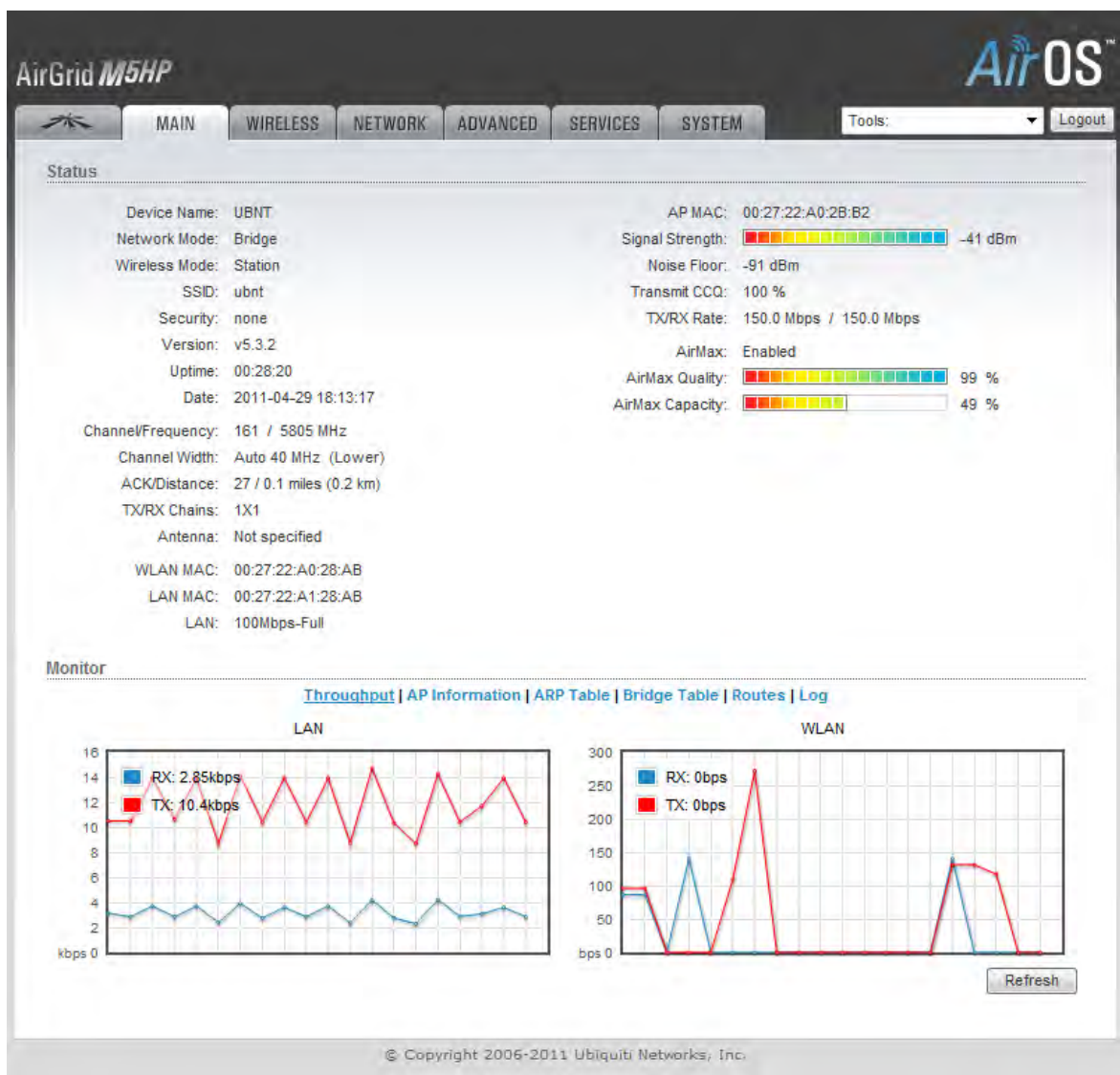
Para realizar la configuración de los parámetros de las antenas es necesario conectarla a un computador por medio de un cable Ethernet; este equipo debe estar configurado con una IP estática de tal forma que pueda quedar en red con la antena, es decir con una IP que se encuentre en la red 192.168.1.x.

Como se mencionó anteriormente cada antena tiene un sistema operativo interno llamado AirOS, al cual se ingresa desde cualquier navegador (browser) por medio de una dirección IP, que por defecto es 192.168.1.20. Al inicio es necesario especificar un usuario y contraseña de administrador, que por defecto son: usuario: ubnt; contraseña: ubnt. Si los anteriores datos son correctos aparece la interfaz principal de configuración de la antena y las pestañas Wireless, Network, Advanced, Services y System como se muestra en la figura 47. La configuración

de cada uno de los parámetros que componen las anteriores pestañas se presentan en el Anexo A.

Con base en la información anterior ahora se procede a configurar cada una de las antenas con los parámetros que se encuentran en los cuadros 10, 11, 12 y 13. Hay que tener en cuenta que parámetros como frecuencia, ancho de canal, entre otros, dependen del criterio del diseñador y del contexto donde se realice la implementación del enlace.

**Figura 47. Interfaz web del airOS**



**7.4.1 Configuración de los módulos airGrid M5.** Los parámetros de las antenas grilla airGrid M5 para generar el enlace punto a punto se presentan en el Cuadro 10 y Cuadro 11. Para que la conexión punto a punto se establezca, se necesita configurar una antena grilla como Access Point y la otra antena como Station, esto permite que las dos antenas se enganchen y queden enlazadas para efectuar la comunicación.

**Cuadro 10. Parámetros de Configuración para el airGrid M5 modo Access Point**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Access Point WDS
		SSID:	AP_PTP
		Country Code:	Colombia
		IEEE 802.11 Mode:	A/N mixed
		Channel Width:	40 MHz
		Channel Shifting:	Disabled
		Frequency, MHz:	5180
		Extension Channel:	Upper Channel
		Frequency Scan List:	Enabled: 5180 MHz
		Antenna:	11x14 – 23 dBi
		Output Power:	-6 dBm
	Max TX Rate, Mbps:	Automatic	
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
WPA Preshared Key:		12345	
MAC ACL:		Enable	
	Policy:	Allow 00:27:22:A0:2B:B2	
<b>NETWORK</b>	<i>Network Role</i>	Network Mode:	Bridge
		Disable Network	None
	<i>Network Settings</i>	Bridge IP Address:	Static
		IP Address:	192.168.1.11
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
Auto IP Aliasing	Enabled		
<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.1 miles (0.2 km)
		ACK Timeout:	28, Auto Adjust Enabled

**Cuadro 10. (Continuación)**

<b>ADVANCED</b>		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65	
<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
Enable Password Authentication :		Enabled	
<b>SYSTEM</b>	<i>Device</i>	Device Name:	AP_PTP
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

El cuadro 10 muestra los principales parámetros que hay que configurar para el funcionamiento del airGrid M5 en modo Access Point:

En la pestaña Wireless, de la interfaz principal del airOS (ver Figura 45), la opción Wireless Mode se configura como Access Point WDS. La opción SSID corresponde al nombre del área de cobertura del AP. La frecuencia que se maneja en esta antena debe ser distinta a las que se encuentran en los otros enlaces, para no afectar la comunicación. En la opción de Antenna, se define qué tipo de airGrid se está manejando, el cual es el de 23 dBi. El Max Tx Rate se determina como automático, ya que en esta opción se presenta un mejor rendimiento del Transmit CCQ para la antena; esta opción se aplica para la configuración de todas las antenas que componen el enlace inalámbrico. En la característica de Wireless Security, la opción MAC ACL se habilita para autorizar la conexión solo con el airGrid M5 en modo Station, introduciendo la dirección MAC de esta antena. Se configura la seguridad (Security) como WPA2, ya que es el algoritmo de seguridad inalámbrica más fuerte que existe, y se especifica una contraseña que tiene que ingresar el Station (cliente) para poderse conectar al AP.



En la pestaña Network, la opción Network Mode se establece como Bridge (Modo Puente) ya que esto permite que las dos antenas grilla se conecten de manera transparente sin necesidad de enrutamiento. En la opción IP address se establece la dirección IP que tendrá la antena. El resto de los parámetros de Network son similares para las dos antenas grilla.

En las pestañas Advanced y Service, todas las opciones y valores establecidos son similares para todas las antenas de la red inalámbrica. En la pestaña System, se ingresa el nombre de la antena y también se define el nombre de usuario del administrador. El resto de los parámetros y opciones no se modifican a menos que se requiera de alguno de éstos para realizar algún cambio que se desee implementar en la antena.

**Cuadro 11. Parámetros de Configuración para la airGrid M5 modo Station**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Station WDS
		SSID:	AP_PTP
		Lock to AP MAC:	00:27:22:2A:63:04
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	Auto 20/40 MHz
		Channel Shifting	Disabled
		Frequency Scan List, MHz	Enabled: 5180
		Antenna:	11x14 – 23 dBm
		Output Power	6 dBm
	Max TX Rate, Mbps	Automatic	
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
WPA Preshared Key:		12345	
<b>NETWORK</b>	Network Role	Network Mode:	Bridge
		Disable Network	None
	Network Settings	Bridge IP Address:	Static
		IP Address:	192.168.1.12
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
Auto IP Aliasing	Enabled		
<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.1 miles (0.2 km)

**Cuadro 11. (Continuación)**

<b>ADVANCED</b>		ACK Timeout:	28, Auto Adjust Enabled
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65
<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
	Enable Password Authentication :	Enabled	
<b>SYSTEM</b>	<i>Device</i>	Device Name:	ST_PTP
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

El cuadro 11 muestra los principales parámetros que hay que configurar para el funcionamiento del airGrid M5 en modo Station:

En la pestaña Wireless, en la parte Basic Wireless Settings, el SSID corresponde a la identificación del área de cobertura a la cual se va a enlazar la antena grilla para formar el enlace punto a punto; de igual forma, se define la dirección MAC (Lock to AP MAC) de la antena airGrid M5 en modo AP a la cual va a estar conectada. En la opción Frequency Scan List se introduce la frecuencia que se definió en la antena airGrid M5 en modo AP, ya que un enlace inalámbrico se genera con la misma frecuencia. El resto de los parámetros de Wireless son similares para las dos antenas grilla.

En la pestaña Network, la opción Network Mode se establece como Bridge (Modo Puente) por las razones que se explican anteriormente.

En la opción IP address se establece la dirección IP que tendrá la antena. En el parámetro System se ingresa el nombre del módulo y también se define el nombre de usuario de administrador; el resto de los parámetros y opciones no se modifican a menos que se requiera de alguno de estos para realizar algún cambio que se desee implementar en el módulo.

**7.4.2 Configuración de los módulos Rocket M5.** Los parámetros del Rocket M5 para las áreas de cobertura de la Red 1 y Red 2, se presentan en el cuadro 12. El Rocket M5 se encuentra conectado a la antena omnidireccional para generar las dos áreas de cobertura y establecer los puntos de acceso para los NanoStation M5

**Cuadro 12. Parámetros de Configuración de los Rocket M5**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Access Point WDS
		SSID:	Red 1 o Red 2
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	40 MHz
		Channel Shifting	Disabled
		Frequency, MHz	Para Red 1: 5220 Para Red 2: 5280
		Extension Channel	Lower Channel
		Frequency Scan List, MHz	Enabled Para Red 1: 5240 Para Red 2: 5260
		Output Power	-4 dBm
		Max TX Rate, Mbps	Automatic
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
		WPA Preshared Key:	12345
MAC ACL		Enable	
Policy:		Allow 00:27:22:5C:A2:C2 00:27:22:52:76:90 00:27:22:52:74:F2 00:27:22:5C:A2:AF	
<b>NETWORK</b>	<i>Network Role</i>	Network Mode:	Bridge
		Disable Network	None
	<i>Network Settings</i>	Bridge IP Address:	Static
		IP Address:	Red 1: 192.168.1.14 Red 2: 192.168.1.13

**Cuadro 12. (Continuación)**

<b>NETWORK</b>	<i>Network Settings</i>	Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled
<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.4 miles (0.6 km)
		ACK Timeout:	Auto Adjust
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65
<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
		Enable Password Authentication :	Enabled
<b>SYSTEM</b>	<i>Device</i>	Device Name:	AP_PTM
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

En la pestaña Wireless, la opción Wireless Mode se configura como Access Point WDS para generar el área de cobertura. La opción SSID corresponde al nombre que se le asigna al área de cobertura ya sea como Red 1 o como Red 2; en el diseño del enlace inalámbrico, se tiene que la Red 1 es el área de cobertura que se encuentra junto a la red de núcleo y la Red 2 es el área de cobertura que se encuentra ubicado en un sitio distante. La frecuencia que se maneja en el área de cobertura va ser distinta para los dos Rocket M5, esto con el fin de evitar interferencias entre los enlaces. En la característica de Wireless Security, la opción MAC ACL se habilita para establecer la autorización de conexión de los

NanoStation M5 a su determinado Access Point, esto se realiza tanto en la Red 1 como en la Red 2. Este procedimiento se lleva a cabo para aplicar autenticación a nivel físico en las conexiones, lo cual se explica en la sección de Autenticación. El resto de los parámetros Wireless son similares para ambos Rocket M5.

En la pestaña Network, la opción Network Mode se establece como Bridge (Modo Puente) ya que esto permite que cada Access Point de la Red 1 y Red 2 se conecte de modo transparente con cada uno de los NanoStation. Cada Rocket M5 tiene definido su dirección IP, correspondiente a la dirección de red definido para la red inalámbrica. El resto de los parámetros Network son similares para los dos módulos.

En la pestaña System, se ingresa el nombre del módulo y se define el nombre de usuario de administrador; ambas opciones se realizan para el access point de la Red 1 y de la Red 2. El resto de los parámetros y opciones no se modifican siempre y cuando se necesiten de alguno de estos para generar algún cambio que se desee implementar en el enlace punto a multipunto.

**7.4.3 Configuración de los módulos CPE NanoStation M5.** Los parámetros de configuración de los dos NanoStation M5 y de los dos NanoStation loco M5 se presentan en el cuadro 13.

**Cuadro 13. Parámetros de Configuración de los 4 Nanostation**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Station WDS
		SSID:	Red 1 o Red 2
		Lock to AP MAC:	00:27:22:2A:63:04
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	Auto 20/40 MHz
		Channel Shifting	Disabled
		Frequency Scan List, MHz	Enabled
		Output Power	8 dBm
		Max TX Rate, Mbps	Automatic
	<i>Wireless Security</i>	Security:	WPA2-AES
WPA Authentication:		PSK	
WPA Preshared Key:		12345	
<b>NETWORK</b>	Network Role	Network Mode:	Bridge
		Disable Network	None

**Cuadro 13. (Continuación)**

<b>NETWORK</b>	Network Settings	Bridge IP Address:	Static
		IP Address:	Para NanoStation M5: 192.168.1.20 192.168.1.23  Para NanoSt. loco M5: 192.168.1.21 192.168.1.22
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled
		<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>
Fragmentation Threshold:	Off		
Distance:	0.4 miles (0.6 km)		
ACK Timeout:	Auto Adjust		
Aggregation:	Enable: 32 Frames 50000 Bytes		
Multicast Data:	Allow All		
Enable Extra Reporting:	Enable		
Sensitive Threshold:	Off		
<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:		Enable
	Link Speed, Mbps:		100
<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65	
<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
	Enable Password Authentication :	Enabled	
<b>SYSTEM</b>	<i>Device</i>	Device Name:	User Station
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

En la sección Basic Wireless Settings de la pestaña Wireless, el SSID corresponde al área de cobertura a la cual se quiere conectar el NanoStation, ya sea a la Red 1 o a la Red 2; para este caso, hay dos módulos conectados a la Red 1 y otros dos módulos conectados a la Red 2; de igual forma, se define la dirección MAC del AP (Lock to AP MAC) al cual el NanoStation va a estar conectado, ya sea a la Red 1 o Red 2. La opción Frequency Scan List se habilita y se introduce la frecuencia del AP con el cual se conecta el modulo: para este caso, si se enlaza con la Red 1 la frecuencia es 5220 MHz y si se enlaza con la Red 2 la frecuencia es 5280 MHz. El resto de los parámetros Wireless son similares para los cuatro módulos.

En la pestaña Network, cada NanoStation tiene definido su dirección IP, correspondiente a la dirección de red definido para la red inalámbrica. La dirección IP de la puerta de enlace es la misma para los 4 módulos. El resto de los parámetros Network son similares para los cuatro módulos.

En la pestaña System se ingresa el nombre del módulo y se define el nombre de usuario de administrador; ambas opciones se establecen igual para los 4 módulos NanoStation. El resto de los parámetros y opciones no se modifican siempre y cuando se necesiten de alguno de estos para generar algún cambio que se desee implementar en el módulo.

## 8. CONCLUSIONES

- Existen software y distribuciones basados en Linux que permiten la integración de distintos servicios para el control y manejo de una red LAN, convirtiendo a un PC o maquina en un centro de mando en donde además se constituye la red de núcleo del ISP. Estas distribuciones toman las funcionalidades de un router y de un firewall, ofreciendo servicios de conectividad y de seguridad a los usuarios finales.
- El control y monitoreo de una ISP permite tener un óptimo funcionamiento y rendimiento al momento de soportar los servicios de Internet y telefonía IP a los usuarios. Por esta razón, tanto la red de acceso como la de núcleo requieren de un proceso de gestión de red para poder soportar servicios de buena calidad.
- La correcta configuración y asignación de los parámetros en la red WLAN es fundamental para su óptimo rendimiento y funcionamiento, teniendo en cuenta las características técnicas y funcionales de cada una de las antenas, además de las características del entorno en donde implemente el enlace inalámbrico, ya sea línea de vista, distancia, potencia, canales, entre otros.
- A través de antenas Ubiquiti pertenecientes al laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente es posible implementar una arquitectura de red inalámbrica la cual es administrada por la distribución basada en Linux, Zeroshell, y que junto al servidor de VoIP Elastix, soportan de forma satisfactoria los servicios de Internet y telefonía IP.
- La implementación de los servicios de red DHCP y NAT, el ingreso de información de los distintos usuarios, el control de ancho de banda y el servicio de autenticación en Zeroshell permiten obtener un sistema centralizado lo cual facilita el trabajo al administrador de la red.
- Mediante la configuración del Protocolo AAA del servidor RADIUS que se encuentra implementado en la distribución Zeroshell se logra autenticar, autorizar y tarificar a los usuarios, permitiendo tener control y monitoreo sobre las conexiones de los clientes al ISP.



- Al utilizar la opción de QoS de la distribución Zeroshell se logra limitar o garantizar el ancho de banda de los usuarios dependiendo del plan que requieran. Este control se realiza por dirección IP. El control de ancho de banda en grandes ISP se realiza a nivel de aplicación utilizando el nombre de usuario.
- La elaboración de una guía, a partir de la implementación de la red inalámbrica con antenas de la empresa Ubiquiti, la configuración del servidor de administración de la red Zeroshell, del servidor de telefonía IP Elastix y del software de gestión de red Aircontrol, permite a los estudiantes interesados por el área de las telecomunicaciones tener un concepto aproximado de cómo funcionan los pequeños ISP.
- La configuración de un servidor DNS permite a la red local, a través de un servicio de NAT, acceder a Internet a través de nombres de dominio y no por dirección IP, ya que en un principio este fue un problema que se presentó pues solo se podía acceder a internet a través de una dirección IP. Además de lo anterior el servicio DNS también permite que la red local tenga un nombre de dominio.
- La interferencia y el ruido son fenómenos que se presentan muy seguido en las implementaciones de redes inalámbricas, por eso es necesario configurar los Access Point con frecuencias que no interfiera a otras que estén en el mismo contexto. Con las antenas Ubiquiti y su sistema operativo airOS, mediante la herramienta Site survey, se puede explorar las frecuencias del sitio para configurar los Access Point con una que no interfiera.
- Es importante resaltar la variedad de aplicaciones GNU de código abierto como opción para que la universidad pueda realizar muchas implementaciones en el área de las telecomunicaciones sin necesidad de invertir en software licenciado
- Se debe garantizar el ancho de banda que consuma una llamada para tener una buena calidad de servicio en una transmisión VoIP. Este criterio se puede basar a partir del ancho de banda suministrado por el códec y que se comprueba realizando una llamada y midiendo el valor del throughput utilizando el airOS.

- La máxima capacidad de transmisión de datos entre la antena y el PC del cliente se ve limitado por el protocolo Ethernet el cual permite la comunicación de la antena y el PC; el valor limitado del throughput es de 100 Mbps. Por otra parte, el throughput real entre un NanoStation M5 y un Rocket M5 es de 150 Mbps según las pruebas realizadas en el laboratorio y que se corroboran con la información suministrada por su datasheet. El throughput real entre las antenas airGrid del enlace punto a punto es de 100 Mbps según las pruebas realizadas en el laboratorio y que igualmente se corroboran con la información suministrada por su datasheet.
- Dentro de la red inalámbrica es necesario realizar pruebas de tráfico que permitan saturar el canal para conocer la máxima capacidad de este último y determinar la cantidad de clientes que se puedan enlazar simultáneamente a un Access Point.

## 9. RECOMENDACIONES

- Si se realiza esta implementación en una localidad geográfica, se debe realizar los estudios y análisis correspondientes al espectro de frecuencia, ruido y otros factores que influyen en el espacio, ya que la implementación de este proyecto se realizó en un medio cerrado donde solo se presentó 2 frecuencias en la banda de 5 GHz correspondientes al Wifi de la universidad y no se presentó un nivel de ruido que afectara la comunicación. El diseñador debe conocer esta información para configurar los parámetros correspondientes a las antenas y así poder implementar el enlace inalámbrico sin que se presente inconvenientes.
- Es necesario que los estudiantes que quieran entender la arquitectura de red de un ISP y los procedimientos que se llevan a cabo para prestar los servicios, tengan un conocimiento sobre TCP/IP y tecnología inalámbrica.
- Es importante que los estudiantes estén familiarizados con el sistema operativo Linux y sus diversas distribuciones para que puedan entender sus comandos y puedan implementar servidores de red en este ambiente.
- El control de ancho de banda para este ISP se hizo por IP, pero se podría recomendar el diseño de una aplicación que permita gestionar ancho de banda por nombre de usuario.
- El servidor Elastix ofrece múltiples funciones además de las que se implementaron para este ISP. Es importante que los estudiantes conozcan estas funciones y puedan sacarle el mayor provecho a este importante servidor de telefonía IP.
- Para la instalación del Voipmonitor es necesario que descarguen la guía de la comunidad oficial ([www.voipmonitor.org](http://www.voipmonitor.org)) ya que es un poco tediosa su configuración. Se debe descargar de igual forma una licencia que expira a los 30 días, la cual pueden renovar inscribiéndose nuevamente a la comunidad o adquiriéndola por una suma de dinero.
- Es necesario que se entiendan conceptos de calidad de servicio como Jitter, latencia, pérdida de paquetes y MOS para que puedan comprender los software de medición de QoS.

## BIBLIOGRAFÍA

AirControl User's Guide [En línea]. Ubiquiti Networks, 2011 [consultado 2 de octubre de 2012]. Disponible en Internet: <http://wiki.ubnt.com/AirControl>

ALVARADO GUZMAN, Jesús. Diseño de la red de datos del edificio Versalles de la Alcaldía de Cali. Trabajo de Grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2009.

ANDREU GOMEZ, Joaquín. Servicios en red. Madrid: Editex, 2010. 300 p.

AREITIO, Javier. Seguridad de la información: Redes, informática y sistemas de información. Madrid: Paraninfo, 2008. 569 p.

AZNAR LOPEZ, Andrés. La red Internet: El modelo TCP/IP. Madrid: Grupo Abantos Formación y Consultoría, 2005. 62 p.

Cuadro Nacional de Atribución de Bandas de Frecuencia [En línea]. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, 2010 [consultado 1 de Abril de 2006]. Disponible en Internet: <http://archivo.mintic.gov.co/mincom/documents/portal/documents/root/espectro%20radioelectrico/CuadroNacionalAtribucionBandasdeFrecuencias2010.pdf>

ESCOBAR PAZ, Lina Marcela. Desarrollo e implementación de un servicio de operadora automática bajo Asterisk para Emcali Telecomunicaciones. Trabajo de grado Ingeniero Informático. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería. 2008.

Features BrazilFW [En línea]. BrazilFW-Firewall and Router, 2011 [consultado 4 de febrero de 2012]. Disponible en Internet: <http://www.brazilfw.com.br/forum/>

Features pfSense [En línea]. pfSense, 2013 [consultado 3 de febrero de 2013]. Disponible en Internet: [http://www.pfsense.org/index.php?option=com\\_content&task=view&id=40&Itemid=43](http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43)

Features Zeroshell [En línea]. Zeroshell, 2013 [consultado 4 de febrero de 2013]. Disponible en Internet: <http://www.zeroshell.org/>

FIGUEIRAS, Aníbal. Una panorámica de las telecomunicaciones. Madrid: Prentice Hall, 2002. 408 p.

FLICKENGER, Rob y AICHELE, Corinna. Redes de Área Local. 2 ed. Londres: Limehouse Book Sprint Team, 2007. 334 p.

GANGULY, Samrat y BHATNAGAR, Sudeept. VoIP: Wireless, P2P and New Enterprise Voice over IP. Hoboken, USA: Wiley, 2008. 278 p.

GARCIA CORTÉS, Juan Sebastián. Implementación de un PBX utilizando Asterisk integrado a la plataforma ZTE de Emcali. Trabajo de Grado Ingeniero Informático. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería. 2009.

GARRISON, Kerry. Trixbox CE 2.6. Otton Birmingham, GBR: Packt Publishing, 2009. 334 p.

GIMÉNEZ GUZMÁN, José M. y LOPEZ MERAYO, María. Aplicaciones de Internet. Alcalá: Universidad de Alcalá, 2012. p. 190.

HERRERA PÉREZ, Enrique. Tecnologías y redes de transmisión de datos. Primera edición. México DF, México: Editorial Limusa, 2003.  
<http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html>

HUIDOBRO MOYA, José Manuel y CONESA PASTOR, Rafael. Sistemas de Telefonía. 5 ed. Madrid: Paraninfo, 2006. 490 p.

HUIDOBRO, José M. y BLANCO SOLSONA, Antonio. Redes inalámbricas en los países en desarrollo. 2 ed. Madrid: Thomson Paraninfo, 2006. 331 p.

Información del Producto Elastix [En línea]. Elastix, 2012 [consultado 15 de enero de 2013]. Disponible en Internet:

INTERNATIONAL TELECOMMUNICATION UNION. Métodos de determinación subjetiva de la calidad de transmisión telefónica. Recomendación P.800. ITU –T, 1996. 39 p.

INTERNATIONAL TELECOMMUNICATION UNION. Objetivos de calidad de funcionamiento de la red para servicios basados en el protocolo de internet. Recomendación Y.1541. ITU –T, 2011. 66 p.

INTERNATIONAL TELECOMMUNICATION UNION. Parámetros de calidad de funcionamiento a la disponibilidad y la transferencia de paquetes del protocolo Internet. Recomendación Y.1540. ITU –T, 2011.

INTERNATIONAL TELECOMMUNICATION UNION. Parámetros de calidad de funcionamiento a la disponibilidad y la transferencia de paquetes del protocolo de Internet. Recomendación Y.1540. ITU –T, 2011. 50 p.

LOBOA GONZALEZ, Harry Famith. Implementación de una red Wireless (WLAN) con seguridad basada en autenticación con Public Key Infrastructure (PKI). Trabajo de grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2006.

McCABE, James. Network Analysis, Architecture, and Design. 3 ed. Burlington, USA: Morgan Kaufmann, 2007. p. 300.

MUÑOZ, Alfio. Elastix a ritmo de merengue. Santo Domingo: Elastix, 2010. 310 p.

PAREDES MORALED A, Rodrigo. Diseño e implementación de experiencias docentes para un sitio proveedor de servicios de internet. Trabajo de grado Ingeniero Civil Electricista. Santiago de Chile: Universidad de Chile. Facultad de Ciencias Físicas y Matemáticas, 2000.

PC de escritorio Dell Studio XPS 435 [En línea]. Dell Colombia, 2013 [consultado 16 de enero de 2013]. Disponible en Internet: <http://www1.la.dell.com/co/es/corp/Computadoras/desktop-studio-xps-435/pd.aspx?refid=desktop-studio-xps-435&s=corp>

POZO IDE, Cristian Andrés. WIMAX: Banda ancha móvil y comparación con HSDPA. Santiago de Chile, Marzo del 2007. Trabajo de grado (Ingeniero Civil Electrónico con especialización en Telecomunicaciones). Universidad Mayor. Facultad de Ingeniería.

PRIETO, Gustavo y GARCÍA, Antonio. Diseño de una Red Inalámbrica IEEE 802.11 FH/CDMA con Protocolo IP para Monitoreo y Control. En: 2001 Montevideo VII Workshop Iberchip, Memorias, IEEE, 2001, 10 p.

Proveedor Servicio de Internet ISP [En línea]. Guayaquil: Escuela Superior Politécnica del Litoral, 2005 [consultado 07 de Mayo de 2013]. Disponible en Internet:[http://www.dspace.espol.edu.ec/bitstream/123456789/5614/17/ISP\\_Capitulo2.docx](http://www.dspace.espol.edu.ec/bitstream/123456789/5614/17/ISP_Capitulo2.docx)

RADIUS (Remote Access Dial-up Service). Puebla: Instituto Tecnológico de Estudios Superiores de Monterrey, 2007. 22 p.

SAA, Alejandro y VELASCO, Diego. Diseño de una plataforma CRM integrada con Asterisk para la dirección comercial de Emcali Telecomunicaciones". Trabajo de Grado Ingeniero Electrónico. Santiago de Cali: Universidad Autónoma de Occidente. Facultad de Ingeniería, 2012.

SALLENT ROIG, Oriol y VALENZUELA GONZÁLEZ, Jose L. Principios de comunicaciones móviles. Barcelona: Universidad Politécnica de Cataluña, 2003. 222 p.

SHAH, Steve y SOYINKA, Wale. Manual de administración de Linux. Mexico: McGraw-Hill Professional, 2010. 655 p.

SILBERSCHATZ, Abraham y KORTH, Henry. Fundamentos de base de datos. Madrid: McGraw-Hill, 2006. 978 p.

TANENBAUM, Andrew. Redes de computadoras. 4 ed. México: Pearson Educación, 2003. 912 p.

VELASCO RIVERA, Milton René. Diseño de un WISP en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema wireless mesh con tecnología wi-fi. Trabajo de grado

Ingeniero Electrónico y Telecomunicaciones. Quito: Escuela Politécnica Nacional.  
Facultad de Ingeniería Eléctrica y Electrónica, 2000. 271 p.



## ANEXOS

### ANEXO A: Sistema operativo AirOS

#### PESTAÑA MAIN

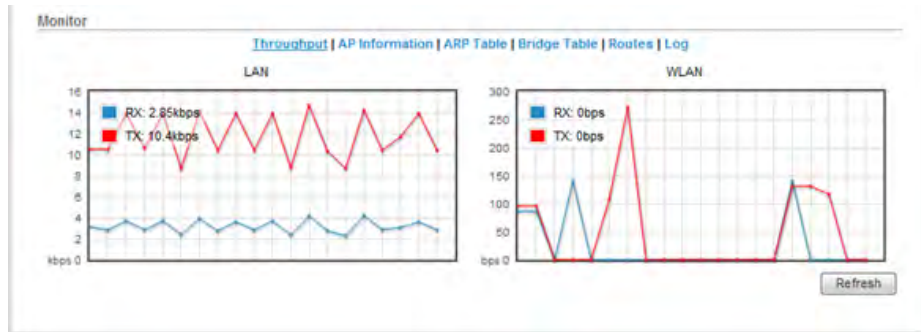
La pestaña principal (main) muestra información sobre el estado y características del enlace inalámbrico, sobre valores de configuración básica, configuración de red y sobre estadísticas de tráfico.

#### Interfaz sistema operativo AirOS



En la parte inferior se encuentra una sección denominada Monitor, que se compone de varias herramientas de monitoreo, entre las cuales se tiene:

## Throughput



Throughput muestra el tráfico de datos en las redes LAN y WLAN en dos formas: gráfica y numérica. La escala del gráfico (Bps, Kbps, Mbps) cambia dinámicamente dependiendo del valor medio de throughput. Las estadísticas son actualizadas automáticamente.

## AP Information

Monitor

[Throughput](#) | [AP Information](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

Access Point	00:27:22:A0:2B:62	
Device Name: UBNT	Negotiated Rate	Last Signal, dBm
Connection Time: 00:03:21	MCS0	N/A
Signal Strength: -45 dBm	MCS1	N/A
Noise Floor: -91 dBm	MCS2	N/A
ACK/Distance: 28 / 0.1 miles (0.2 km)	MCS3	N/A
CCQ: 100%	MCS4	N/A
Last IP: <a href="#">192.168.1.12</a>	MCS5	N/A
TX/RX Rate: 90.0 Mbps / 150.0 Mbps	MCS6	N/A
TX/RX Packets: 172 / 192	MCS7	-48
TX/RX Packet Rate, pps: 0 / 0		
Bytes Transmitted: 19656 (19.20 kBytes)		
Bytes Received: 36571 (35.71 kBytes)		

AP information aparece disponible cuando el modo inalámbrico (Wireless Mode) es Station. Esta herramienta muestra las estadísticas de conexión de los AP (Access Point) asociados con el dispositivo.

- Access Point: muestra la dirección MAC del AP.

- Connection Time (Tiempo de conexión): muestra la cantidad de tiempo que el dispositivo ha estado conectado al AP. El tiempo es expresado en días, horas, minutos y segundos.
- Signal Strength (Intensidad de la señal): El valor representa, en dBm, el último nivel de señal inalámbrica recibida.
- Noise Floor: muestra el valor actual (en dBm) del ruido ambiental (de interferencia) que el receptor recibe en la frecuencia de operación.
- CCQ (Client Connection Quality): El valor representa la calidad de la conexión al AP. Presenta un valor porcentual, para el cual 100% corresponde a un perfecto enlace.
- Last IP: muestra la última dirección IP del dispositivo.
- TX/RX Rate: muestra la tasa de datos, en Mbps, de los últimos paquetes transmitidos y recibidos.
- TX/RX Packets: muestra el número total de paquetes transmitidos y recibidos desde el Station durante el tiempo de conexión.
- TX/RX Packet Rate, pps: muestra el valor medio de la tasa de paquetes recibidos y transmitidos.
- Bytes Transmitted: muestra la cantidad total de datos (en Bytes) transmitidos durante la conexión.
- Bytes Received: muestra la cantidad total de datos (en Bytes) recibidos durante la conexión.
- Negotiated Rate/Last Signal, dBm: Los valores representan el nivel de señal inalámbrica recibida junto con la tasa datos de paquetes recibidos recientemente. N/A se muestra como la última señal si no fueron recibidos paquetes en esa tasa de datos específica.

Cuando el modo inalámbrico es AP, ya no aparece disponible la pestaña AP Information, sino la pestaña Station.

## Station

Monitor

[Throughput](#) | [Stations](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

Station MAC	Device Name	Signal / Noise, dBm	ACK	TX/RX, Mbps	CCQ, %	Connection Time	Last IP	Action
00:27:22:A0:28:AB	ST_PTP	-45 / -88	28	150 / 90	100	00:01:50	192.168.1.11	kick

- Station MAC: muestra la dirección MAC del Station.
- Signal/Noise, dBm: El valor Signal representa el último nivel de señal inalámbrica recibida, y el valor Noise represente el nivel de ruido.
- TX/RX, Mbps: El valor TX representa la tasa de datos, en Mbps, de los últimos paquetes transmitidos, y el valor RX representa la tasa de datos, en Mbps, de los últimos paquetes recibidos.

- CCQ, %: este índice evalúa la calidad de conexión del cliente inalámbrico (CCQ). El nivel es un valor porcentual para el cual 100% corresponde a un enlace perfecto.
- Connection Time: muestra el tiempo de conexión de cada Station enlazada al dispositivo. El tiempo es expresado en días, horas, minutos, y segundos.
- Last IP: muestra la última dirección IP del Station.

### ARP Table

Monitor

Throughput | AP Information | **ARP Table** | Bridge Table | Routes | Log

IP Address	MAC Address	Interface
192.168.1.10	A4:BA:DB:FB:8E:37	BRIDGE

Refresh

Muestra todas las entradas de la tabla del protocolo de resolución de direcciones (ARP) que están actualmente guardadas en el dispositivo. ARP se usa para asociar cada dirección IP a una única dirección MAC de cada dispositivo en la red.

- IP Address: muestra la dirección IP asignada al dispositivo de red.
- MAC Address: muestra la dirección MAC del dispositivo.
- Interface: muestra la interfaz que conecta a los dispositivos.

### Bridge Table

Monitor

Throughput | AP Information | ARP Table | **Bridge Table** | Routes | Log

MAC Address	Interface	Ageing Timer
00:27:22:2A:62:95	LAN	1.91
00:27:22:2A:63:04	WLAN	10.80
00:27:22:A0:2B:B2	WLAN	2.17
A4:BA:DB:FB:8E:37	LAN	0.07

Refresh

Disponible cuando el modo de red es Bridge. La tabla muestra las entradas en el sistema Bridge.

- Mac Address: el dispositivo de red identificado por su dirección MAC.
- Interface: muestra con qué interface se asocia el dispositivo de red: LAN o WLAN.
- Ageing Timer: muestra el tiempo de envejecimiento para cada dirección de entrada. Después de un específico timeout, si el dispositivo no ha recibido un paquete de la lista de direcciones, borrará esa dirección de la Bridge Table.

## Routes

Monitor

[Throughput](#) | [AP Information](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

Destination	Gateway	Netmask	Interface
192.168.1.0	0.0.0.0	255.255.255.0	BRIDGE
169.254.0.0	0.0.0.0	255.255.0.0	BRIDGE
0.0.0.0	192.168.1.1	0.0.0.0	BRIDGE

Refresh

Lista todas las entradas en la tabla de enrutamiento del sistema.

- Destination: muestra la dirección IP del dispositivo de destino.
- Gateway: muestra la dirección IP de la puerta de enlace apropiada.
- Netmask: muestra la máscara de red del dispositivo de destino.
- Interface: muestra la interfaz que el dispositivo de destino tiene activado.

## Log

Cuando está habilitado LOG, esta ventana muestra todos los eventos registrados del sistema.

## PESTAÑA WIRELESS

The screenshot displays the configuration page for the 'Wireless' tab in the AirGrid M5HP interface. The page is titled 'Basic Wireless Settings' and includes the following fields and controls:

- Wireless Mode:** Station WDS (dropdown)
- SSID:** AP\_PTP (text input) with a 'Select...' button
- Lock to AP MAC:** (checkbox, unchecked)
- Country Code:** Colombia (dropdown)
- IEEE 802.11 Mode:** A/N mixed (dropdown)
- Channel Width:** Auto 20/40 MHz (dropdown)
- Channel Shifting:** Disabled (dropdown)
- Frequency Scan List, MHz:**  Enabled, 5805 (text input) with an 'Edit...' button
- Auto Adjust to EIRP Limit:** (checkbox, unchecked)
- Antenna:** Not specified (dropdown)
- Output Power:** (slider) 8 dBm
- Max TX Rate, Mbps:** MCS 4 - 39 [90] (dropdown) with an 'Automatic' checkbox (unchecked)

Below the basic settings is the 'Wireless Security' section:

- Security:** WPA2-AES (dropdown)
- WPA Authentication:** PSK (dropdown)
- WPA Preshared Key:** (password field) with a 'Show' checkbox (unchecked)

A 'Change' button is located at the bottom right of the configuration area.

La pestaña Wireless contiene todo lo necesario para configurar parte del enlace inalámbrico. Esto incluye SSID, configuración de frecuencia y de canal, modo del dispositivo, tasa de datos, y seguridad inalámbrica.

- **Wireless Mode:** especifica el modo inalámbrico del dispositivo. El modo depende de los requisitos de la topología de red. AirOS soporta 4 modos: Station, Access Point, Station (WDS), Access Point (WDS).
- **Station (estación):** es un modo cliente, el cual se puede conectar con un AP (Access Point). Es comúnmente usado para enlazarse con un AP. En modo estación el dispositivo actúa como la estación del suscriptor (CPE) mientras se conecta con el Access Point primario definido por el SSID y re-direcciona todo el tráfico entrante y saliente de la red a los dispositivos conectados en la interfaz Ethernet.
- **Access Point:** este es un modo que conecta múltiples clientes. Es un modo de punto de acceso 802.11.
- **WDS (Modo puente transparente):** Representa sistemas de distribución inalámbrica. Es una función que permite la interconexión entre routers o puntos de acceso (Access Point). En la mayoría de casos se recomienda usar WDS porque habilita el tráfico transparente de capa 2. El protocolo WDS no es definido como un estándar, así que podría haber problemas de compatibilidad entre equipos de diferentes fabricantes.
- **Station (WDS):** este modo debería ser usado si el dispositivo está conectado a un AP en modo Access Point (WDS).
- **Access Point (WDS):** Access Point (WDS) permite a la capa 2 hacer un puente con dispositivos en modo Station (WDS).
- **SSID:** El identificador de servicio determinado (Service Set Identifier) es usado para identificar la red inalámbrica 802.11; debe ser especificado mientras se encuentre en el modo Access Point. SSID es el nombre de la red inalámbrica.
- **Select (disponible en modo Station solamente):** muestra la lista de APs disponibles al cual se puede conectar el Station.
- **Lock to AP MAC (disponible en modo Station solamente):** esto permite que la Station se mantenga conectada a un AP particular con una MAC específica. Es útil cuando hay múltiples APs usando el mismo SSID.
- **Country Code:** cada país tiene sus propias regulaciones de frecuencia y niveles de potencia. Para asegurar que la operación del dispositivo esté acorde a las regulaciones asegúrese de seleccionar correctamente el país en donde el dispositivo será utilizado. La lista de canales, los límites de potencia de salida, el IEEE 802.11 y los modos de anchura del espectro del canal serán fijados según las regulaciones del país seleccionado.
- **IEEE 802.11 Mode:** éste es el estándar de radio usado para la operación de su dispositivo basado en AirOS. 802.11b, 802.11g (2.4GHz) y 802.11a (5GHz) son modos antiguos, mientras que 802.11n (2.4GHz y/o 5GHz) es el estándar más reciente basado en la modulación OFDM. Las opciones que incluyen son:

- ✓ A/N mixed: se conecta a una red 802.11a o 802.11n. Este modo ofrece mejor compatibilidad. Es seleccionado por defecto en los dispositivos de la serie M5.
  - ✓ B/G/N mixed: se conecta a una red 802.11b o 802.11n. Este modo ofrece mejor compatibilidad. Es seleccionado por defecto en los dispositivos de la serie M2.
- Channel Width: muestra el ancho del espectro del canal de radio. Esta opción se puede usar para controlar el ancho de banda consumida por el enlace. El ancho del canal soportado por el canal inalámbrico es:
    - ✓ 5MHz - es el ancho de canal de 5 MHz.
    - ✓ 10MHz - es la anchura de canal de 10 MHz.
    - ✓ 20MHz - es la anchura estándar del canal (seleccionada por defecto).
    - ✓ 40MHz - es la anchura de canal de 40MHz.
    - ✓ Auto 20/40MHz - sólo disponible en modo Estación, ofrece mejor compatibilidad.
  - Channel Shifting: esta opción activa canales especiales que están fuera de la frecuencia de los canales estándares 802.11a/b/g/n. Esta es una característica propietaria desarrollada por Ubiquiti. Mientras las redes 802.11 tienen canales estándares (por ejemplo, canal 36 (5180 MHz), canal 40 (5200 MHz), y así sucesivamente, espaciados cada 5 MHz, channel shifting permite la operación de nuevos canales no-802.11 fuera de los canales estándar. Todos los canales se pueden desplazar por 5 MHz (en 802.11 a/n) o 2 MHz (en 802.11b/g/n) desde la frecuencia central del canal por defecto. Las ventajas de esto son el establecimiento de una red privada y una seguridad inherente. Usando la opción de desplazamiento de canal, las redes se vuelven inmediatamente invisibles a millones de dispositivos WiFi en el mundo.
  - Frequency, MHz (disponible en modo Access Point): el valor por defecto, Auto, permite al dispositivo seleccionar automáticamente la frecuencia. Se puede especificar una frecuencia de la lista desplegable.
  - Extension Channel (disponible solamente en modo Access Point con ancho de canal de 40 MHz): indica el uso de channel bonding, que permite a la red AirMax utilizar dos canales como si fuesen uno. Utilizar dos canales mejora el rendimiento de la conexión. Esta opción es seleccionada automáticamente por el sistema. Un canal de 40 MHz son dos canales de 20 MHz unidos. Extension Channel indica al radio añadir un canal ya sea por encima o por debajo del canal estándar existente. Por ejemplo, si se selecciona 5805 MHz (canal de 40 MHz) y por debajo del canal, el radio usará (5775 a 5795 MHz) + (5795 a 5815 MHz), pero si se selecciona 5805 MHz (40 MHz) y por encima del canal, el radio usará (5795 a 5815 MHz) + (5815 a 5835 MHz).

- Frequency List, MHz (disponible solamente en modo Access Point): múltiples frecuencias son disponibles para evitar interferencia entre AP cercanos. La lista de las frecuencias varía dependiendo del Código del País (Country Code) seleccionado, del modo IEEE 802.11 (IEEE 802.11 Mode), ancho del canal (Channel Width) y de las opciones del desplazamiento del canal (Channel Shifting).
- Frequency Scan List, MHz (disponible solamente en modo Station): Esto limitará la búsqueda solamente a los canales seleccionados. La ventaja de esto es que la búsqueda va ser más rápida así como un mejor filtrado de los AP no deseados en los resultados. La herramienta *Site Survey* buscará los puntos de acceso solamente en los canales seleccionados.
- Auto Adjust to EIRP Limit: esta opción debe permanecer habilitada para que obligue a la potencia de transmisión cumplir con las regulaciones del país seleccionado. Si se habilita, no se puede configurar EIRP por encima de la cantidad permitida por el dominio regulador. Para deshabilitar *Auto Adjust to EIRP Limit*, debes habilitar el *Installer EIRP Control* en la pestaña Advanced.
- Output Power: define la máxima potencia (en dBm) de salida del dispositivo. El nivel de potencia máximo de transmisión está limitado por las regulaciones de cada país.
- Max TX Rate, Mbps: define la tasa de datos (en Mbps) a la cual el dispositivo debe transmitir los paquetes inalámbricos. Se puede fijar una tasa de datos específica entre MCS 0 y MCS 7 (o MCS 15 para los dispositivos de 2x2). Se recomienda usar la opción *Automatic*, especialmente si se tiene problemas con la conexión o si se pierden una alta tasa datos. Si se selecciona un ancho de canal de 20 MHz, la tasa máxima de datos es MCS 7 (65 Mbps) o MCS 15 (130 Mbp). Si se selecciona un ancho de canal de 40 MHz, la tasa máxima de datos es MCS 7 (150 Mbps) o MCS 15 (300 Mbps).
- Automatic: si se habilita el algoritmo de tasas selecciona la mejor tasa de datos, dependiendo de las condiciones de calidad del enlace.

### **Wireless Security**

Esta sección permite determinar los parámetros que controlan cómo la estación del suscriptor se asocia a un dispositivo inalámbrico y el cifrado/descifrado de datos.

En modo Access Point, permite configurar los ajustes de seguridad inalámbrica que será usada por el dispositivo en la red inalámbrica. En modo Station, se ingresa las configuraciones de seguridad del AP al cual el dispositivo está asociado.

Seleccione el método de seguridad según la política de seguridad del Access Point. La estación del suscriptor deberá estar autorizada por el punto de acceso para acceder a la red y todos los datos de los usuarios transmitidos entre la



estación del suscriptor y el Access Point serán encriptados en caso de utilizarse los métodos de seguridad inalámbrica. AirOS soporta los siguientes métodos de seguridad:

- None: si se quiere una red abierta sin seguridad inalámbrica.
- WEP (Wired Equivalent Privacy): es el algoritmo de seguridad más viejo y menos seguro. Use métodos de seguridad WPA o WPA2 cuando sea posible.
- WPA (Wi-fi Protected Access): fue desarrollado como un método de encriptación más fuerte que el WEP.
- WPA-TKIP: modo de seguridad WPA con soporte TKIP (Temporal Key Integrity Protocol). TKIP usa el algoritmo de encriptación RC4. Hay una limitante en el desempeño al usar TKIP, por eso se recomienda usar mejor AES.
- WPA-AES: modo de seguridad WPA con soporte AES (Advanced Encryption Standard).
- WPA2: WPA2 fue desarrollado para fortalecer la seguridad de encriptación inalámbrica y ser más fuerte que WEP y WPA.
- WPA2-TKIP: modo de seguridad WPA2 con soporte TKIP.
- WPA2-AES: modo de seguridad WPA2 con soporte AES. Esta es la opción de seguridad disponible más fuerte. Si todos los dispositivos inalámbricos en la red soportan esta opción, se recomienda seleccionarla.
- WPA Authentication: define uno de los siguientes métodos de clave WPA si se utiliza el método de seguridad WPA o WPA2 (aplicable solamente para los modos Station y Station WDS).
  - ✓ PSK: Pre-shared Key, seleccionada por defecto. Con este método se especifica una contraseña. Esta clave pre compartida es una contraseña alfanumérica con mínimo 8 caracteres o 63 como máximo.
  - ✓ EAP: Extensible Authentication Protocol, método de autenticación IEEE 802.1x. Este método es comúnmente usado en redes empresariales.
- MAC ACL: La lista de control de acceso MAC proporciona la capacidad de negar o permitir a ciertos clientes conectarse con el Access Point (AP). Hay dos maneras de determinar la lista de control de acceso MAC:
  - ✓ Si la política del MAC ACL se fija en permitir (Allow), permite que ciertos clientes inalámbricos en la lista puedan conectarse al punto de acceso mientras que será negado para los clientes que no estén en dicha lista.
  - ✓ Si la política del MAC ACL se fija en rechazar (Deny), entonces sólo se negará el acceso a los clientes inalámbricos de la lista, y el resto de clientes mantendrá su acceso.

Las direcciones MAC de los clientes inalámbricos pueden ser agregadas y ser eliminadas usando los botones de Agregar (Add) y eliminar (Remove).

## PESTAÑA NETWORK

The screenshot shows the 'Network' configuration page in the AirOS interface. The 'Network Role' section has 'Network Mode' set to 'Bridge' and 'Disable Network' set to 'None'. The 'Network Settings' section has 'Bridge IP Address' set to 'Static' and 'IP Address' set to '192.168.1.11', 'Netmask' set to '255.255.255.0', 'Gateway IP' set to '192.168.1.1', 'Primary DNS IP' and 'Secondary DNS IP' fields, 'MTU' set to '1500', 'Spanning Tree Protocol' checkbox, 'Auto IP Aliasing' checked, and 'IP Aliases' with a 'Configure...' button. The 'VLAN Network Settings' section has 'Enable VLAN' checkbox. The 'Firewall Settings' section has 'Enable Firewall' checkbox and a 'Configure...' button. The 'Static Routes' section is visible at the bottom.

La pestaña red permite configurar funcionalidades de modo de red como bridge o routing, y configuraciones de IP.

- Network mode: especifica el modo de red del dispositivo. El modo depende de los requisitos de la topología de red. Modo bridge es adecuado si se tiene una red muy pequeña. Una red más grande tiene mucho más tráfico que requiere administración o gestión por un dispositivo, en este caso se usa el modo Router o SOHO router.

Modo bridge: el dispositivo remite todos los paquetes de administración y de datos de la red desde una interfaz de red a la otra sin ningún enrutamiento inteligente. Para los usos simples esto proporciona una solución de red eficiente y completamente transparente. Las interfaces WLAN (inalámbrica) y LAN (Ethernet) pertenecen al mismo segmento de red que tiene la misma dirección IP.

- Disable Network: deshabilita las interfaces WLAN, LAN, o WAN.

### **Network Settings**

- Bridge IP Address (Dirección IP del bridge): el dispositivo se puede fijar para utilizar una dirección IP estática o para obtener una dirección IP del servidor DHCP al que está conectado.

- ✓ DHCP: seleccione esta opción para asignar la dirección IP, la puerta de enlace y la dirección del DNS dinámicamente por el servidor local DHCP
  - ✓ Static (Estática): seleccione esta opción para asignar una dirección IP estática a la interfaz del bridge.
- IP Address (Dirección IP): especifica la dirección IP del dispositivo. Esta IP será usada para propósitos de administración del dispositivo.
  - Netmask (mascara): se especifica la máscara de red.
  - Gateway IP (IP puerta de enlace): típicamente esta es la dirección IP del router anfitrión, que suministra el punto de conexión a internet. El dispositivo AirOS dirigirá los paquetes de datos a la puerta de enlace si el anfitrión de destino no está dentro de la red local. La dirección IP de la puerta de enlace deberá encontrarse en el mismo segmento de red que el dispositivo AirOS.
  - Primary DNS IP (IP del DNS primario): especifica la dirección IP del servidor DNS primario.
  - Secondary DNS IP: especifica la dirección IP del servidor DNS secundario.
  - MTU: El Maximum Transmission Unit (MTU) es el tamaño máximo de paquetes (en bytes) que una red puede transmitir. El valor por defecto es 1500.
  - Spanning Tree Protocol (STP): múltiples bridge (puentes) interconectados forman redes más grandes usando el Spanning Tree Protocol IEEE 802.1d, el cual es utilizado para encontrar el camino más corto dentro de la red y eliminar loops de la topología.
  - Auto IP aliasing: si se habilita, automáticamente genera una dirección IP para la interfaz WLAN/LAN según corresponda. La dirección IP generada es una dirección IP clase B cuyo rango es 169.254.X.Y (máscara de red 255.255.0.0). La IP automática siempre comienza con 169.254.X.Y, donde X y Y son los últimos dígitos de la dirección MAC del dispositivo, por ejemplo si la dirección MAC es 00:15:6D:A3:04:FB, entonces la dirección IP será 169.254.4.251. La configuración del Auto IP Aliasing puede ser útil porque se puede acceder y administrar los dispositivos, así se pierda, desconfigure u olvide su dirección IP, ya que conociendo la dirección MAC se puede determinar la dirección IP del dispositivo.
  - IP Aliases: los alias de IP para la interfaz interna y externa de red pueden ser configurados. Los alias de IP pueden ser especificados usando la ventana de configuración de "IP Aliases", que se abrirá cuando se presione el botón Configure.
    - ✓ IP: dirección IP alternativa para la interfaz LAN o WLAN, que se puede utilizar para enrutamiento o para la administración del dispositivo.
    - ✓ Netmask (máscara): identificador del rango de direcciones para un IP alias en particular.
    - ✓ Comments (Comentarios): campo informal para dejar un comentario acerca de un IP alias en particular.

## VLAN network settings

Se pueden crear múltiples Virtual Local Area Networks (VLANs).

- VLAN ID: es un valor único asignado a cada VLAN en un solo dispositivo; cada VLAN ID representa una diferente VLAN. El rango VLAN ID es 2 a 4094.

## Firewall Settings

- Se pueden configurar reglas de firewall para las interfaces de red local y externa. La funcionalidad del firewall puede ser activada usando la opción Enable Firewall. Las reglas del firewall pueden ser configuradas, habilitadas o desactivadas presionando el botón Configure.
- Static Routes
- Se puede manualmente agregar reglas de enrutamiento estático a la tabla de enrutamiento del sistema; se puede configurar una regla que especifique una dirección IP de destino (o un rango de direcciones IP de destino) que pase a través de un específico Gateway (puerta de enlace).

## PESTAÑA ADVANCED

**Advanced Wireless Settings**

RTS Threshold: 2346  Off

Fragmentation Threshold: 2346  Off

Distance:  0.1 miles (0.2 km)

ACK Timeout: 28  Auto Adjust

Aggregation:  Enable  
32 Frames 50000 Bytes

Multicast Data:  Allow All

Enable Installer ERP Control:

Enable Extra Reporting:

Sensitivity Threshold, dBm: -86  Off

**Advanced Ethernet Settings**

Enable Autonegotiation:

Link Speed, Mbps: 100

Enable Full Duplex:

**Signal LED Thresholds**

LED1	LED2	LED3	LED4
94	80	73	65

Thresholds, dBm: -94 -80 -73 -65

**Traffic Shaping**

Enable Traffic Shaping:

La pestaña *Advanced* maneja los ajustes de enrutamiento avanzado y ajustes inalámbricos. La página de opciones avanzadas permite configurar ajustes avanzados que influyen en el rendimiento y comportamiento del dispositivo. Los ajustes inalámbricos avanzados son de uso exclusivo para los usuarios con conocimiento técnico avanzado que tienen la suficiente experticia sobre la tecnología inalámbrica LAN. Estos ajustes no deben ser cambiados a menos que se sepa qué efecto tendrán dichos cambios en el dispositivo.

### ***Advanced Wireless Settings***

- **RTS Threshold** (Si AirMax está habilitado, el RTS Threshold no es requerido): determina el tamaño de los paquetes de una transmisión y, mediante el uso de un Access Point (Punto de Acceso) ayuda a controlar el flujo de tráfico. El rango es entre 0-2346 bytes. El valor por defecto es 2346 que significa que RTS está deshabilitado, o como alternativa a esto se puede marcar la opción OFF.
- **Fragmentation Threshold**: especifica el tamaño máximo de un paquete antes que los datos se fragmenten en múltiples paquetes. El rango es entre 256 y 2346 bytes. Ajustes del Fragmentation Threshhold demasiados bajos pueden provocar un mal rendimiento de la red. Se recomienda no modificar o modificar muy levemente estos valores, ya que el valor por defecto 2346 es el óptimo en la mayoría de las redes inalámbricas.
- **Distance (distancia)**: define el valor de la distancia en millas (o kilómetros) mediante la barra (slider) o ingresando el valor manualmente. La fuerza de la señal y el throughput decaen con la distancia. Cambiar el valor de distancia modificara el ACK Timeout al valor adecuado para la distancia especificada.
- **ACK Timeout**: especifica el ACK Timeout. Cada vez que la Station (estación) recibe un frame de datos envía un frame ACK al AP (si no hubo errores de transmisión). Si la estación no recibe ningún frame ACK desde el AP dentro del ACK Timeout especificado, este volverá a reenviar el frame.
- **Auto Adjust**: se recomienda habilitar esta opción, que activará la característica de autoconfiguración del ACK Timeout. Para enlaces estables no es necesario activar esta opción.
- **Aggregation (agregación)**: parte del estándar 802.11n que permite enviar múltiples frames a través de la combinación de múltiples frames pequeños en uno de mayor tamaño. Esto crea un frame más grande, el cual combina pequeños frames con la misma fuente física, el mismo punto de destino final, y clase de tráfico (QoS) hacia un frame más grande con una cabecera de MAC común.
  - ✓ **Frame**: determina el número de frames combinados que conformarán el nuevo paquete.
  - ✓ **Bytes**: determina el tamaño (en bytes) del paquete más grande a ser enviado

- Multicast Data: permite pasar a los paquetes multicast (multidifusión). Esta opción está habilitada por defecto.
- Enable Installer ERP control: permite el control de la configuración *Auto Adjust to EIRP Limit* en la pestaña Wireless.
- Enable extra reporting: reporta información adicional, como el nombre del dispositivo, en los cuadros de administración 802.11. Esta información es comúnmente usada para identificación del sistema y reporte de estado en utilidades de descubrimiento (Discovery) y sistemas operativos de enrutamiento.
- Sensitivity Threshold, dBm: define el mínimo nivel de señal del cliente aceptado por el AP para que el cliente pueda conectarse. Si el nivel de señal del cliente cae más tarde, el cliente permanece conectado al AP.

### ***Advanced Ethernet Settings***

Por defecto la opción Auto está habilitada. El dispositivo automáticamente negocia los parámetros de transmisión, tales como velocidad y dúplex, con su contraparte. En ese proceso, los dispositivos de red primero comparten sus capacidades y luego escogen el modo de transmisión más rápido que ambos soportan.

- Link Speed, Mbps: especifica la velocidad de transmisión máxima del enlace.

### ***Signal Led Threshold***

Se pueden configurar los LEDS del dispositivo para que se enciendan cuando los niveles de señal recibidos alcanzan los valores definidos en los campos *Thresholds, dBm*. Esto permite que un técnico instale fácilmente un CPE AirOS sin ingresar a la configuración web del sistema (para alinear la antena).

### ***Traffic Shapping***

El traffic Shapping es usado para controlar el ancho de banda de subida y de bajada. El tráfico puede ser limitado en el dispositivo. Esto es QoS de capa 3.

- Incoming Traffic Limit: se especifica el valor máximo de ancho de banda (en Kbps) para el tráfico que pasa desde la interfaz inalámbrica a la interfaz Ethernet.
- Incoming Traffic Burst: especifica el volumen de datos (en Kbps) en el cual el Incoming Traffic Limit no será aplicado luego que la conexión sea establecida.
- Outgoing Traffic Limit: especifica el valor máximo de ancho de banda (en Kbps) para el tráfico que pasa desde la interfaz Ethernet a la interfaz inalámbrica.
- Outgoing Traffic Burst: especifica el volumen de datos (en Kbps) en el cual el Outgoing Traffic Limit no será aplicado luego que la conexión sea establecida.

- Entienda el Burst como el límite hasta el cual no habrá un control de ancho de banda, sobre dicha cantidad de datos se aplicará un límite.

## PESTAÑA SERVICES

En la pestaña Services se configura servicios de administración del sistema: Ping Watchdog, SNMP, servers (web, SSH, Telnet), NTP, DDNS, System Log y Device Discovery.

The screenshot shows the AirOS configuration interface with the 'SERVICES' tab selected. The interface is organized into several sections:

- Ping Watchdog:** Includes checkboxes for 'Enable Ping Watchdog', 'Ping Interval' (300 seconds), 'Startup Delay' (300 seconds), and 'Failure Count To Reboot' (3).
- SNMP Agent:** Includes checkboxes for 'Enable SNMP Agent', 'SNMP Community' (public), 'Contact', and 'Location'.
- Web Server:** Includes checkboxes for 'Use Secure Connection (HTTPS)', 'Secure Server Port' (443), 'Server Port' (80), and 'Session Timeout' (15 minutes).
- SSH Server:** Includes checkboxes for 'Enable SSH Server', 'Server Port' (22), 'Enable Password Authentication', and an 'Authorized Keys' button.
- Telnet Server:** Includes checkboxes for 'Enable Telnet Server' and 'Server Port' (23).
- NTP Client:** Includes checkboxes for 'Enable NTP Client' and 'NTP Server'.
- Dynamic DNS:** Includes checkboxes for 'Enable Dynamic DNS', 'Host Name', 'Username', and 'Password' (with a 'Show' button).
- System Log:** Includes checkboxes for 'Enable Log', 'Enable Remote Log', 'Remote Log IP Address', and 'Remote Log Port' (514).

### **Ping Watchdog**

- Enable Ping Watchdog: se configura para que el dispositivo AirOS realice continuamente un ping a una dirección IP definida por el usuario (por ejemplo la puerta de enlace de internet). Si el ping no recibe respuesta dentro de los parámetros definidos por el usuario, el dispositivo AirOS se reiniciará automáticamente. Esta opción crea una especie de mecanismo *anti-fallas*.
- IP Address To Ping: especifique la dirección IP del host al cual se le hará el ping.
- Ping interval: especifique el intervalo de tiempo (en segundos) entre cada petición de eco ICMP que se envía por ping Watchdog.
- Startup Delay: especifique el tiempo inicial de retraso (en segundos) hasta que la primera petición de eco ICMP sea enviada por la herramienta de ping

Watchdog. El valor de retraso inicial debe ser de al menos 60 segundos, ya que la inicialización de la interfaz de red y de la red inalámbrica toma un tiempo considerable si el dispositivo es reiniciado.

- Failure Count to Reboot: especifique el número de respuestas al eco ICMP. Si el número especificado de paquetes de respuesta al eco ICMP no se recibe continuamente, la herramienta de ping watchdog reiniciará el dispositivo. El valor por defecto es 3.

### **SNMP Agent**

- Enable SNMP Agent: Simple Network Monitor Protocol (SNMP) es un protocolo de capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de red. Los administradores de red usan SNMP para monitorear los dispositivos conectados a la red.
- SNMP Community: especifique la cadena de comunidad SNMP (SNMP Community String). Es requerida para autenticar el acceso a los objetos MIB (Management Information Base) y funciona como una contraseña embebida. El dispositivo soporta un community string de solo lectura; estaciones de administración autorizadas tienen acceso de lectura a todos los objetos en el MIB excepto la community string, que no tiene acceso de escritura. La comunidad SNMP por defecto es *public*.
- Contact: especifique el contacto que debería ser notificado en caso de emergencia.
- Location: especifique la ubicación física del dispositivo.

### **Web Server**

- Use secure connection (HTTPS): si se quiere usar el modo HTTPS; por defecto se usa el modo HTTP.
- Secure Server Port: si el modo HTTPS es usado, especifique el puerto TCP/IP del servidor Web. Por defecto es 443.
- Server Port: si el modo HTTP es usado, especifique el puerto TCP/IP del servidor web. Por defecto es 80.
- Session Timeout: especifica el máximo tiempo de espera antes que la sesión expire. Una vez la sesión expira, debes iniciar sesión de nuevo usando el username y password. El valor por defecto es 15 minutos.

### **SSH Server**

- Server Port: especifica el puerto TCP/IP del servidor SSH.
- Password Authentication: si se habilita, te debes autenticar usando credenciales de administrador para garantizar acceso SSH al dispositivo; de lo contrario se requiere una clave autorizada.



- Authorized Keys: click Edit para importar un archivo de clave pública para el acceso SSH al dispositivo en lugar de usar una contraseña de administrador.

### ***Telnet server***

- Server Port: especifica el puerto TCP/IP del servidor Telnet.

### ***NTP Client***

Network Time Protocol (NTP) es un protocolo para sincronizar los relojes de los sistemas informáticos mediante paquetes de datos en redes de latencia variable. Puede ser utilizado para fijar la hora del sistema AirOS. Si la opción System Log está activada, se muestra la hora del sistema junto a cada entrada que registre un evento al sistema.

- NTP Server: especifica la dirección IP o el nombre de dominio del servidor NTP.

### ***Dynamic DNS***

Dynamic Domain Name System (DDNS) es un servicio de red que notifica al servidor DNS en tiempo real de cualquier cambio en las configuraciones IP del dispositivo. Incluso si la dirección IP del dispositivo cambia, todavía se puede acceder al dispositivo a través de su nombre de dominio.

- Host Name: ingrese el nombre del host del servidor DDNS.
- Username: ingrese el nombre de usuario de la cuenta DDNS.
- Password: ingrese la contraseña de la cuenta DDNS.

### ***System Log***

- Enable log: esta opción activa la rutina de registro de los mensajes del System Log. Por defecto esta deshabilitada.
- Enable remote Log: habilita la función de enviar los mensajes de registro del sistema a un servidor remoto, que es especificado en los campos *Remote Log IP Address* y *Remote Log Port*.
- Remote Log IP Address: la dirección IP del host que recibe los mensajes de registro. Configure apropiadamente el host remoto para recibir mensajes mediante el protocolo syslog.
- Remote Log Port: el puerto TCP/IP que recibe los mensajes del registro. 514 es el puerto por defecto comúnmente usado.

### ***Device Discovery***

Discovery habilita el descubrimiento del dispositivo, por lo tanto los dispositivos pueden ser descubiertos por otros dispositivos Ubiquiti a través de la herramienta Discovery.

## PESTAÑA SYSTEM

La pestaña System contiene opciones administrativas. Esta página habilita al administrador para reiniciar el dispositivo, restablecer a los valores de fábrica, actualizar un nuevo firmware, respaldar o actualizar la configuración, y configurar la cuenta de administrador.

The screenshot shows the 'SYSTEM' configuration page for an AirGrid M5HP device. The page is organized into several sections:

- Device:** Fields for 'Device Name' (ST\_PTP) and 'Interface Language' (English).
- Date Settings:** Fields for 'Timezone' (GMT Western Europe 1), 'Enable Startup Date' (checkbox), and 'Startup Date' (calendar icon).
- System Accounts:** Fields for 'Administrator Username' (ubnt) and 'Enable Read-Only Account' (checkbox).
- Miscellaneous:** 'Enable Reset Button' (checked checkbox).
- Location:** Fields for 'Latitude' and 'Longitude'.
- Configuration Management:** Buttons for 'Backup Configuration: Download...', 'Upload Configuration', 'Examiner...', and 'Upload'.
- Device Maintenance:** Displays 'Firmware Version: XM.v5.3.2' and 'Build Number: 8909'. Buttons for 'Update...', 'Reboot...', 'Reset to Defaults...', and 'Support Info'.

### **Device**

- Device name: especifica el nombre del host.
- Interface Language: permite seleccionar el idioma de la interfaz de administración Web. Inglés es el idioma por defecto.

### **Date Settings**

- Timezone: especifica la zona horaria según el Greenwich Mean Time (GMT).
- Enable Startup Date: cuando se habilita, eres capaz de cambiar la fecha de inicio del dispositivo.

Startup Date: especifica la fecha de inicio del dispositivo. Para ingresar la fecha se puede dar click en el icono **Calendar** o se puede ingresar manualmente con el

siguiente formato: 2 dígitos del mes/2 dígitos del día/4 dígitos del año. Por ejemplo para diciembre 20, 2011, ingrese: 12/20/2011.

### ***System Accounts***

Se puede cambiar la contraseña de administrador para proteger el dispositivo de cambios no autorizados.

- Administrator Username: especifica el nombre del administrador. Puedes dar click en el Key button para cambiar la contraseña de administrador. La longitud de la contraseña es 8 caracteres como máximo.
- Enable Read-Only Account Name: si se activa esta opción, solo se puede ver y tener acceso a la pestaña Main, con lo cual se protege el dispositivo contra configuraciones no autorizadas. Por defecto esta opción se encuentra desactivada.
  - ✓ Read-Only Account Name: especifica el nombre de usuario de solo lectura.
  - ✓ Key button: dar click en este botón para cambiar la contraseña de solo lectura.

### ***Miscellaneous***

- Enable Reset Button: si se habilita se permite el uso del botón físico reset del dispositivo. Para prevenir un reset accidental a las configuraciones por defecto, deshabilite esta opción.

### ***Location***

Latitude y Longitude definen las coordenadas del dispositivo; son usadas para actualizar automáticamente la ubicación de los dispositivos en el aircontrol.

### ***Configuration Management***

- Backup Configuration: presione el botón Download (descargar) para descargar el archivo de configuración actual del sistema.
- Upload Configuration: presione el botón Examinar para seleccionar el archivo de la nueva configuración o especificar la ubicación del archivo. Presionando el botón upload comenzará la transferencia de la nueva configuración al sistema. Los ajustes de la nueva configuración serán visibles en las páginas de configuración del enlace, de la red, avanzados, de los servicios y del sistema de la interfaz web de administración.

## **Device Maintenance**

Los controles en esta sección permiten realizar tareas de mantenimiento como: reiniciar, volver a los valores por defecto, generar un informe de soporte y actualizar el firmware de los dispositivos.

- Update: utilice esta opción para actualizar el dispositivo con un nuevo firmware.
- Reboot (reinicio): presione el botón de Reboot para iniciar la rutina de reinicio del dispositivo. El efecto de Reboot es igual a desconectar la energía y volver a conectarla. La configuración del sistema no se modifica luego de que el ciclo de reinicio termine.
- Reset to default: presione el botón *Reset to default* para iniciar la rutina de reiniciar el dispositivo como cuando salió de fábrica, es decir que se vuelve a la configuración del sistema por defecto.
- Support Info: presione el botón Support Info para abrir el archivo de información del sistema. Esto genera un archivo de información de soporte que los ingenieros de soporte de Ubiquiti pueden utilizar para darle asistencia al cliente. Este archivo solamente necesita ser generado en caso de que sea solicitado.

## **TOOLS**

En la esquina superior derecha de la interfaz AirOS hay una lista desplegable de herramientas que sirven para administrar y monitorear los enlaces.

- Align Antenna: esta herramienta permite al instalador apuntar y optimizar la antena en la dirección más adecuada para mejorar la calidad de la señal. Al seleccionar esta herramienta se abre una nueva ventana con un indicador de nivel de señal (Signal Level).
  - ✓ Signal level: muestra la intensidad de la señal del último paquete recibido.
  - ✓ Noise Level: muestra el nivel de ruido (en dBm) de la señal inalámbrica recibida.
  - ✓ Max Signal: muestra la máxima intensidad de señal (en dBm). Para ajustar el rango del medidor Max Signal, use el Slider o ingrese manualmente el nuevo valor. Si se reduce el rango, el cambio de color será más sensible a las fluctuaciones de la señal.
- Site survey: esta herramienta busca las redes inalámbricas dentro del rango en todos los canales soportados por el dispositivo. En modo Station se puede cambiar la lista de canales. La herramienta Site survey reporta la dirección MAC, SSID, el nombre del dispositivo, el tipo de encriptación (si la tiene), relación Signal/Noise en dBm, frecuencia en GHz, y el canal inalámbrico de

- cada AP en el medio circundante. La búsqueda sobre el sitio puede ser actualizada presionando el botón Scan.
- Ping: se puede enviar Ping a otros dispositivos de la red directamente desde el dispositivo basado en AirOS. La herramienta ping usa paquetes ICMP para comprobar la calidad del enlace y para estimar la latencia de los paquetes entre dos dispositivos de red.
    - ✓ Select Destination IP: se tienen dos opciones, la primera es seleccionar una IP del sistema remoto de la lista desplegable, que es generada automáticamente, y la segunda es seleccionar la opción *specify manually* e ingresar la dirección IP.
    - ✓ Packet Count: ingrese el número de paquetes a enviar para la prueba del Ping.
    - ✓ Packet Size: especifique el tamaño del paquete.
  - Traceroute: esta herramienta permite seguir los saltos del dispositivo AirOS hacia una dirección IP seleccionada. Puede ser utilizada para encontrar la ruta que toma un paquete ICMP a través de la red hacia el host de destino.
    - ✓ Destination IP: ingrese la dirección IP del host de destino.
    - ✓ Resolve IP Address: seleccione esta opción para resolver las direcciones IP de forma simbólica en lugar de numérica.
  - Speed Test: esta herramienta permite comprobar la velocidad de conexión entre dos dispositivos airOS. Se puede usar el Speed Test para estimar un througput preliminar entre dos dispositivos de red.
    - ✓ Select Destination IP: tienes dos opciones, la primera es seleccionar la IP del sistema remoto de la lista desplegable, que es generada automáticamente, y la segunda es seleccionar *specify manually* e ingresar la dirección IP.
    - ✓ User: ingrese el username de administrador.
    - ✓ Password: ingrese la contraseña de administrador.
    - ✓ Show Advanced Options: habilita opciones adicionales de la herramienta Speed Test.
      - duplex: estima el throughput de entrada (RX) y de salida (TX) al mismo tiempo.
      - receive: estima el throughput de entrada (RX).
      - transmit: estima el throughput de salida (TX).
  - AirView: Utilice el analizador de espectro para analizar el entorno de ruido del espectro radioeléctrico y así seleccionar inteligentemente una frecuencia óptima para instalar un enlace punto a punto Airmax.

## ANEXO B: Configuración de Teléfonos

- Teléfono IP

En la pantalla de inicio de la interfaz web para la configuración del teléfono IP se encuentra todos los parámetros que actualmente tiene el teléfono IP ya sea en información del sistema, en información del producto, en el status del teléfono, en el status de la extensión o en el status de la llamada en la línea 1; esta información presenta de forma general el rendimiento de las llamadas y el funcionamiento del teléfono. En el menú System se introduce, si se desea cambiar, la IP del teléfono de modo estático con su respectiva mascara. En el menú Phone se introduce el nombre del usuario y la cantidad de extensiones que se utiliza. El usuario asignado para este teléfono IP es Luis Villa que presenta la extensión 4401020.

The screenshot displays the SIPURA Telephone Configuration web interface. At the top, the SIPURA logo and 'technology, inc.' are on the left, and 'Sipura Telephone Configuration' is on the right. Below the logo is a navigation menu with tabs: Info, System, SIP, Regional, Phone, Ext 1, and User. On the far right of the menu are links for 'User Login', 'basic', 'advanced', 'Personal Directory', and 'Call History'. The main content area is divided into several sections:

- System Information:**
  - DHCP: Disabled
  - Host Name: SipuraSPA
  - Current Netmask: 255.255.255.0
  - Primary DNS:
  - Secondary DNS:
  - Current IP: 192.168.1.170
  - Domain: 192.168.1.99
  - Current Gateway: 0.0.0.0
- Product Information:**
  - Product Name: SPA-921
  - Software Version: 4.1.10(b)
  - MAC Address: 000E08D3C65A
  - Licenses: None
  - Serial Number: 4MJ00H505046
  - Hardware Version: 1.0.1(541f)
  - Client Certificate: Installed
- Phone Status:**
  - Current Time: 1/1/2003 12:04:42
  - Elapsed Time: 00:04:42
  - Broadcast Pkts Sent: 0
  - Broadcast Pkts Recv: 567
  - Broadcast Pkts Dropped: 0
  - RTP Packets Sent: 0
  - RTP Packets Recv: 0
  - SIP Messages Sent: 46
  - SIP Messages Recv: 0
  - External IP:
  - Broadcast Bytes Sent: 0
  - Broadcast Bytes Recv: 42281
  - Broadcast Bytes Dropped: 0
  - RTP Bytes Sent: 0
  - RTP Bytes Recv: 0
  - SIP Bytes Sent: 21373
  - SIP Bytes Recv: 0
- Ext 1 Status:**
  - Registration State: Not Registered
  - Next Registration In: 0 s
  - Mapped SIP Port:
  - Last Registration At: 0/0/0 00:00:00
  - Message Waiting: Yes
- Line 1 Call 1 Status:**
  - Call State: Idle
  - Encoder:
  - Type:
  - Callback:
  - Peer Phone:
  - Packets Sent:
  - Bytes Sent:
  - Decode Latency:
  - Round Trip Delay:
  - Packet Error:
  - Tone: None
  - Decoder:
  - Remote Hold:
  - Peer Name:
  - Duration:
  - Packets Recv:
  - Bytes Recv:
  - Jitter:
  - Packets Lost:
  - Mapped RTP Port:

## Menu System

Info	<b>System</b>	SIP	Regional	Phone	Ext 1	User	<a href="#">User Login</a>	<a href="#">basic</a>	<a href="#">advanced</a>
							<a href="#">Personal Directory</a>		<a href="#">Call History</a>
<b>System Configuration</b>									
Enable Web Server:	yes			User Password:					
<b>Internet Connection Type</b>									
DHCP:	no								
Static IP:	192.168.1.170			NetMask:	255.255.255.0				
Gateway:									
<b>Optional Network Configuration</b>									
HostName:				Domain:	192.168.1.99				
Primary DNS:				Secondary DNS:					
DNS Query Mode:	Parallel			Syslog Server:					
Debug Server:				Debug Level:	0				

## Menú Phone

Info	System	SIP	Regional	<b>Phone</b>	Ext 1	User	<a href="#">User Login</a>	<a href="#">basic</a>	<a href="#">advanced</a>
							<a href="#">Personal Directory</a>		<a href="#">Call History</a>
<b>General</b>									
Station Name:	Luis Villa			Voice Mail Number:	101				
Text Logo:									
<b>Line Key 1</b>									
Extension:	1			Short Name:	\$USER				
ACD Ext:	1								
<b>Ring Tone</b>									
Ring1:	n=Classic-1;w=3;c=1								
Ring2:	n=Classic-2;w=3;c=2								
Ring3:	n=Classic-3;w=3;c=3								
Ring4:	n=Classic-4;w=3;c=4								
Ring5:	n=Simple-1;w=2;c=1								
Ring6:	n=Simple-2;w=2;c=2								
Ring7:	n=Simple-3;w=2;c=3								
Ring8:	n=Simple-4;w=2;c=4								
Ring9:	n=Simple-5;w=2;c=5								
Ring10:	n=Office;w=4;c=1								
<b>Audio Input Gain (dB)</b>									
Handset Input Gain:	0			Headset Input Gain:	0				
Speakerphone Input Gain:	0								

En el menú Ext 1 se habilita la línea, se introduce la dirección IP del servidor Elastix en el parámetro Proxy, se introduce la información del usuario como el nombre, la extensión y una contraseña, y se selecciona el códec con el que va a trabajar el teléfono IP.

## Menu Ext 1

Info	System	SIP	Regional	Phone	Ext 1	User
<a href="#">User Login</a>   <a href="#">basic</a>   <a href="#">advanced</a> <a href="#">Personal Directory</a>   <a href="#">Call History</a>						
<b>General</b>						
Line Enable:						yes
<b>NAT Settings</b>						
NAT Mapping Enable:	no			NAT Keep Alive Enable:	no	
<b>SIP Settings</b>						
SIP Port:	5060		SIP Debug Option:	none		
<b>Call Feature Settings</b>						
Message Waiting:	yes		Default Ring:	10		
Mailbox ID:						
<b>Proxy and Registration</b>						
Proxy:	192.168.1.99		Register:	yes		
Make Call Without Reg:	yes		Register Expires:	3600		
Ans Call Without Reg:	yes					
<b>Subscriber Information</b>						
Display Name:	Luis Villa		User ID:	4401020		
Password:	*****		Use Auth ID:	yes		
Auth ID:	4401020					
<b>Audio Configuration</b>						
Preferred Codec:	G729a		Use Pref Codec Only:	no		
Silence Supp Enable:	no		DTMF Tx Method:	Auto		

- **Configuración del ATA**

Al configurar el ATA en la interfaz web se presenta una ventana de inicio que muestra toda la información del sistema, información del producto y status del sistema.

## Interfaz web del ATA

LINKSYS® A Division of Cisco Systems, Inc.		Phone Adapter with 2 Ports for Voice-Over-IP						PAP2	
Voice		Info	System	SIP	Regional	Line 1	Line 2	User 1	User 2
Basic View (switch to advanced view)									
User Login									
<b>System Information</b>		DHCP:	Disabled		Current IP:	192.168.1.171			
		Host Name:	LinksysPAP		Domain:				
		Current Netmask:	255.255.255.0		Current Gateway:	192.168.1.60			
		Primary DNS:							
		Secondary DNS:							
<b>Product Information</b>		Product Name:	PAP2T		Serial Number:	FL00K223576			
		Software Version:	3.1.15(LS)		Hardware Version:	0.3.5			
		MAC Address:	687F74575637		Client Certificate:	Installed			
		Customization:	Open						
<b>System Status</b>		Current Time:	1/1/2003 12:10:27		Elapsed Time:	00:10:27			
		Broadcast Pkts Sent:	0		Broadcast Bytes Sent:	0			
		Broadcast Pkts Recv:	1458		Broadcast Bytes Recv:	101146			
		Broadcast Pkts Dropped:	0		Broadcast Bytes Dropped:	0			
		RTP Packets Sent:	0		RTP Bytes Sent:	0			
		RTP Packets Recv:	0		RTP Bytes Recv:	0			
		SIP Messages Sent:	114		SIP Bytes Sent:	59508			
		SIP Messages Recv:	0		SIP Bytes Recv:	0			
		External IP:							



En el menu System se ingresa todos los datos relacionados a la red como la direccion IP, la mascara, la puerta de enlace y se desabilita DHCP.

## Menu System

The screenshot shows the 'Menu System' configuration page for a 'Phone Adapter with 2 Ports for Voice-Over-IP'. The page is divided into several sections:

- System Configuration:** Includes 'Enable Web Server' (set to 'yes') and 'User Password' (empty field).
- Internet Connection Type:** Includes 'DHCP' (set to 'no'), 'Static IP' (192.168.1.171), 'Gateway' (192.168.1.60), and 'NetMask' (255.255.255.0).
- Optional Network Configuration:** Includes 'HostName', 'Domain', 'Primary DNS', 'Secondary DNS', 'DNS Query Mode' (set to 'Parallel'), 'Syslog Server', and 'Debug Level' (set to '0').

At the bottom, there are 'Save Settings' and 'Cancel Settings' buttons. The Cisco Systems logo is visible in the bottom right corner.

## Menu Line 1

The screenshot shows the 'Menu Line 1' configuration page for a 'Phone Adapter with 2 Ports for Voice-Over-IP'. The page is divided into several sections:

- SIP Settings:** Includes 'Line Enable' (set to 'yes') and 'SIP Port' (5060).
- Proxy and Registration:** Includes 'Proxy' (192.168.1.99), 'Register' (set to 'yes'), 'Make Call Without Reg.' (set to 'yes'), 'Register Expires' (3600), and 'Ans Call Without Reg.' (set to 'yes').
- Subscriber Information:** Includes 'Display Name' (Jhorman Villanuev), 'User ID' (4403040), 'Password' (masked with asterisks), 'Auth ID' (4403040), and 'Use Auth ID' (set to 'yes').
- Supplementary Service Subscription:** Includes a list of services with 'yes' or 'no' options: Call Waiting Serv., Block ANC Serv., Cfwd All Serv., Cfwd No Ans Serv., Cfwd Last Serv., Accept Last Serv., CD Serv., Call Return Serv., Three Way Call Serv., Attn Transfer Serv., MWI Serv., Block CID Serv., Dist Ring Serv., Cfwd Busy Serv., Cfwd Sel Serv., Block Last Serv., DND Serv., CWCD Serv., Call Back Serv., Three Way Conf Serv., Unattn Transfer Serv., and VMWI Serv.
- Audio Configuration:** Includes 'Preferred Codec' (G711u), 'Use Pref Codec Only' (set to 'no'), 'DTMF Tx Method' (Auto), 'Silence Supp Enable' (set to 'no'), and 'FAX CED Detect Enable' (set to 'yes').

En el menu Line 1 se configura los parametros y características referente a las llamadas. Se habilita la línea para que las llamadas entren en funcionamiento, se introduce la IP del servidor Elastix en la opción Proxy y el nombre del usuario con su respectiva extensión; el usuario asignado para este teléfono analógico es Jhorman Villanueva que presenta la extensión 4403040.

## **ANEXO C: Información sobre VoIP Monitor**

VoIPMonitor es un sniffer de paquetes de red de código abierto con front-end comercial para protocolos de VoIP SIP RTP y RTCP los cuales corren en el sistema GNU/Linux. Este sniffer es diseñado para analizar la calidad de llamada VoIP basado en parámetros de red – variación de retardo y pérdida de paquetes según el E-model ITU-T G.107 el cual predice la calidad en la escala MOS. Las llamadas con toda la estadística relevante son guardadas en la base de datos MySQL u ODBC. Los codecs soportados son el G.711 a-law/u-law y los soportes plugins comerciales G.722, G729a, G723, iLBC. Presenta una interfaz WEB GUI donde se puede visualizar todas las estadísticas, parámetros y reportes que se obtienen a partir de las llamadas. Presenta las siguientes características:

- Filtros globales para encontrar CDRs específicos basados en IP, números telefónicos parámetros cualitativos (pérdida/retardo/MOS).
- Detalles de la llamada en vivo.
- Flujo de mensajes SIP detallados con vista estilo wireshark.
- Escucha de llamadas directamente de la interfaz WEB.
- Filtros de grabación que permiten grabar voz (RTP) solo para algunas llamadas basadas en IP o números telefónicos.
- Gráfica de distribución de retardo y pérdidas para cada llamada.
- Fácil desarrollo.

## ANEXO D: Características del airControl

### Grupo de AP de la Red 1

Status	Host Name	IP Address	MAC	Product	Signal	Version
	Cliente 4	192.168.1.22	00:27:22:5C:A2:AF	NanoStation Loco M5	-52 dBm	5.3.2
	Cliente 3	192.168.1.20	00:27:22:52:74:F2	NanoStation M5	-57 dBm	5.3.2
	Red 1	192.168.1.14	00:27:22:2A:63:04	Rocket M5	-36 dBm	5.3

Device Group Summary  
3 of 3 device(s) reporting as of 2013-03-23 11:43:24

Select Attributes

- wlanTxBytes: 688Bps
- wlanRxBytes: 985Bps
- wlanTxRate: 193.0
- wlanRxRate: 156.0
- Uptime: 10:31:35
- Signal: -49 dBm
- CCQ: 99.1%
- Noise Floor: -93

Los dispositivos se organizan de acuerdo al SSID del Access Point. El AP de SSID Red 1 tiene conectadas las antenas de nombre Cliente 4 y Cliente 3.

### Modulos Offline

Status	Host Name	IP Address	MAC	Product	Signal	Version
	cliente1	192.168.1.21	00:27:22:5C:A2:C2	NanoStation Loco M5		5.3.2

En la pestaña *Offline* se puede verificar los módulos Ubiquiti que se encuentren desconectados.

## Información detallada de las antenas

The screenshot shows the airControl web interface. The top navigation bar includes 'Welcome ubnt', 'My Settings', 'About', and 'Logout'. The main content area is divided into several sections:

- Device Groups:** A sidebar on the left lists various device groups, including 'All Devices', 'AP.Groups', 'Red 1', 'Red 2', 'Watch', 'In-progress', and 'Firmware'.
- All Devices (1 selected):** A table displaying a list of devices with columns for Status, Host Name, IP Address, MAC, Product, Signal, and Version. The selected device is 'Red 2' with IP 192.168.1.13 and a signal of -30 dBm.
- Red 2 (192.168.1.13):** A detailed view of the selected device, showing its physical appearance (a Rocket M5 antenna), MAC address (00:27:22:2A:62:95), and various performance metrics like CCQ (100%), AMC (81%), and AMQ (88%). It also displays attributes such as Host Name, IP Address, MAC, Product, ESSID, and Uptime.
- Recent Events:** A log of system events, including SSH connection failures and device communication restoration.

Se puede dar doble clic sobre cualquiera de los módulos y obtener información respecto a la antena seleccionada, como su Host name, su dirección IP, su dirección MAC, CCQ, el valor de intensidad de señal, el ESSID, entre otros.

## Ubicación de la red inalámbrica en Google Earth

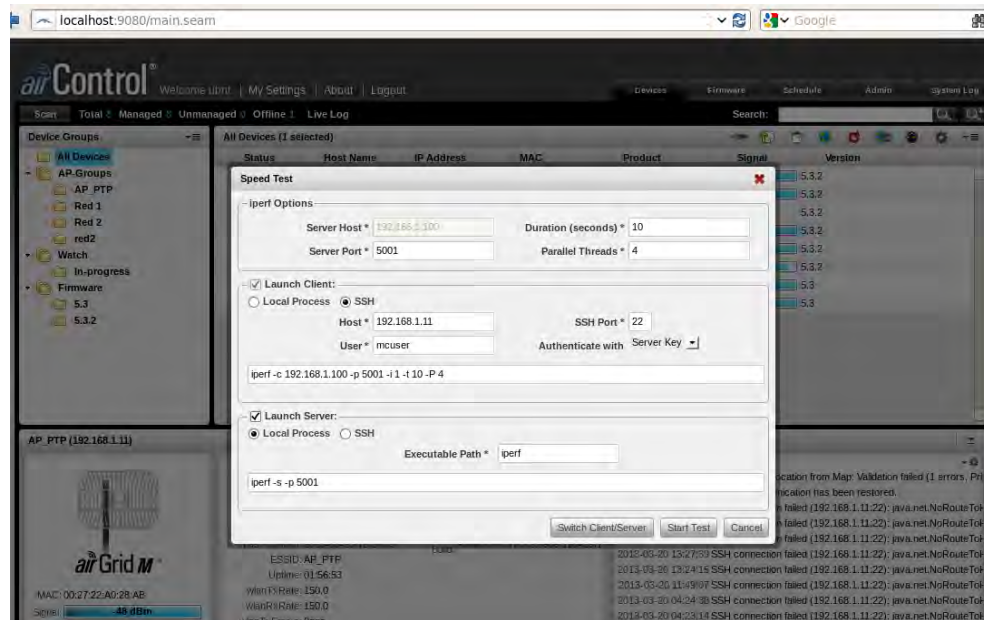
The screenshot shows the airControl web interface with the 'Device Map' view selected. The map displays the physical locations of the wireless network devices, overlaid on a Google Earth map of a city area. The devices are represented by colored circles, and their signal strength is indicated by the color of the circle. A 'Signal Legend' in the bottom right corner provides the following scale:

- Blue:  $\geq -60$
- Green:  $< -60$
- Yellow:  $< -70$
- Red:  $< -80$

The map shows several devices clustered in the center, with signal strengths ranging from -60 dBm to -80 dBm. The interface also includes a search bar and navigation controls for the map.

Otra opción importante que permite el airControl es la ubicación de los módulos en un mapa, donde cada AP puede mostrar su área de cobertura, puede mostrar información de cada uno de los dispositivos Ubiquiti como su Host name, su SSID, dirección MAC, dirección IP, etc. El mapa se puede mostrar también en forma satelital.

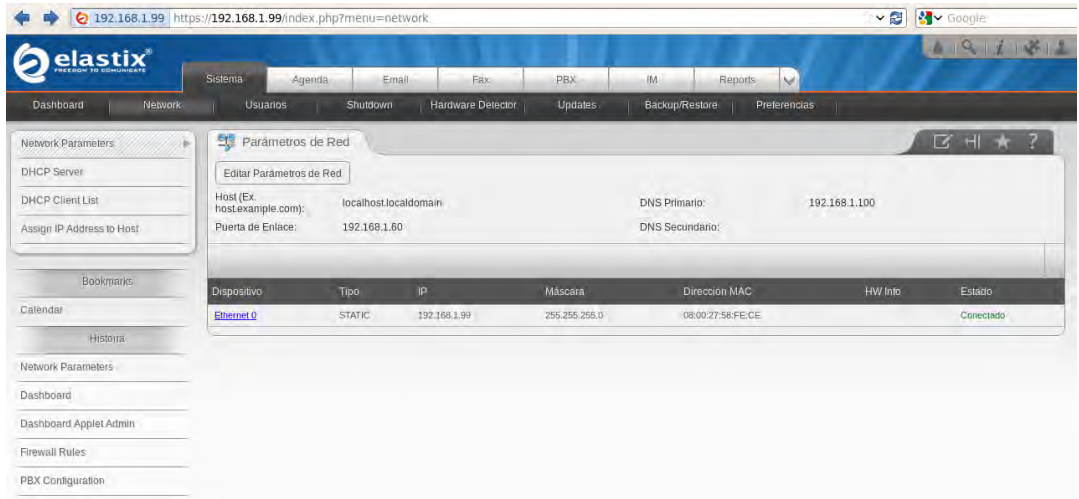
## Pruebas de Velocidad



El airControl permite realizar pruebas de velocidad con el Speed Test en cada una de las antenas.

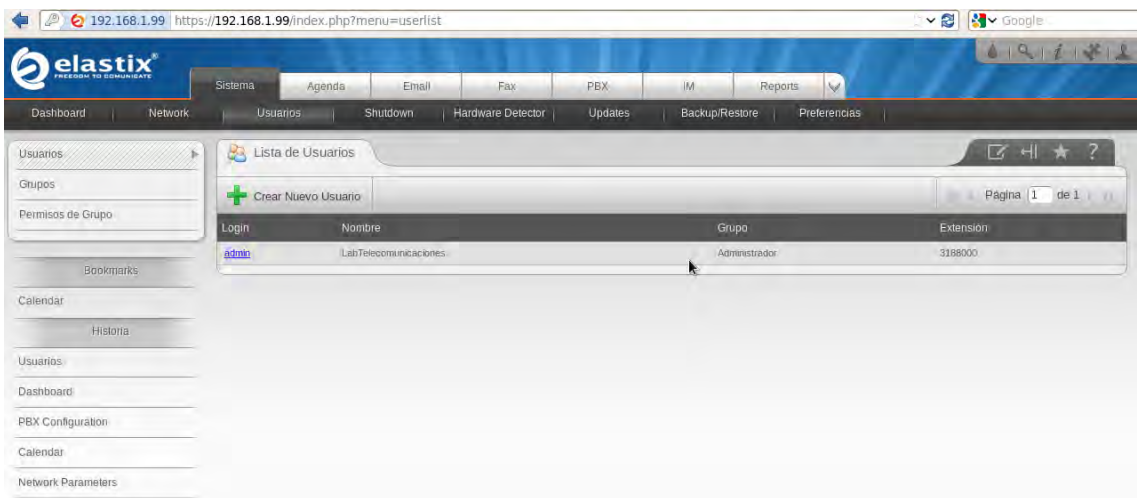
## Anexo E: Características del servidor de VoIP Elastix

### Configuración de la opción Network



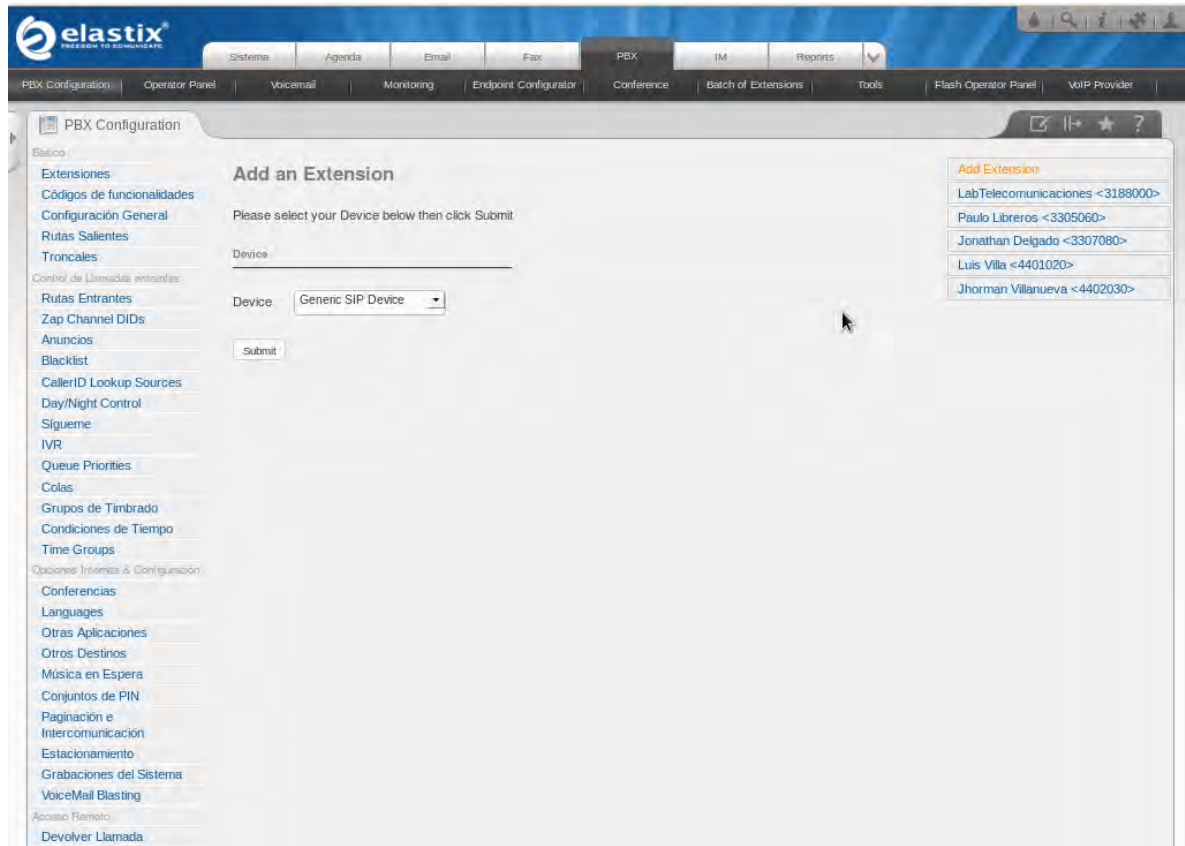
La opción Network permite configurar la IP del Elastix, la puerta de enlace, el DNS Primario, entre otras características. Estos parámetros son importantes para establecer la conexión del Elastix con la red LAN.

### Configuración de la opción Usuarios



La opción de Usuario permite establecer el perfil de administración asignándole un nombre, un grupo y una extensión.

## Creación de las extensiones de los usuarios



Para la creación de las extensiones de los usuarios, se ingresa al menú PBX y se selecciona la opción PBX Configuration. En esta opción se adiciona las extensiones eligiendo primero el protocolo de VoiP que maneja el dispositivo de comunicación, que en este caso es SIP Genérico, y se da click en Submit.

Se presenta una ventana en donde se ingresa los datos de la extensión: el número de la extensión, el nombre de la extensión y un número secreto en las opciones de dispositivo. Al finalizar la creación de la extensión se realiza el mismo procedimiento con los otros tres usuarios y el administrador, el cual tiene por nombre LabTeleco y la extensión 3188000. En PBX Configuration se pueden observar las extensiones creadas.



**elastix**  
FREEDOM TO COMMUNICATE

Sistema | Agenda | Email | Fax | **PBX** | IM | Reports

PBX Configuration | Operator Panel | Voicemail | Monitoring | Endpoint Configurator | Conference | Batch of Extensions | Tools | Flash Operator Panel | VoIP Provider

---

**PBX Configuration**

Básico

- Extensiones
- Códigos de funcionalidades
- Configuración General
- Rutas Salientes
- Troncales

Control de Llamadas Entrantes

- Rutas Entrantes
- Zap Channel DIDs
- Anuncios
- Blacklist
- CallerID Lookup Sources
- Day/Night Control
- Sigueme
- IVR
- Queue Priorities
- Colas
- Grupos de Timbrado
- Condiciones de Tiempo
- Time Groups

Opciones Internas & Configuración

- Conferencias
- Lenguajes
- Otras Aplicaciones
- Otros Destinos
- Música en Espera
- Time Groups

Opciones Internas & Configuración

- Conferencias
- Lenguajes
- Otras Aplicaciones
- Otros Destinos
- Música en Espera
- Conjuntos de PIN
- Paginación e Intercomunicación
- Estacionamiento
- Grabaciones del Sistema
- VoiceMail Blasting

Acceso Remoto

- Devolver Llamada
- DISA

Dirección

- freePBX Sin embeber

### Add SIP Extension

Add Extension

User Extension:

Display Name:

CID Num Alias:

SIP Alias:

---

Extension Options

Outbound CID:

Ring Time:

Call Waiting:

Call Screening:

Pinless Dialing:

Emergency CID:

---

Assigned DID/CID

Call Screening:

Pinless Dialing:

Emergency CID:

---

Assigned DID/CID

DID Description:

Add Inbound DID:

Add Inbound CID:

---

Device Options

This device uses sip technology.

secret:

dtmfmode:

---

Dictation Services

Dictation Service:

Dictation Format:

Email Address:

---

Language

Language Code:

**Add Extension**

LabTelecomunicaciones <3188000>

Paulo Libreros <3305060>

Jonathan Delgado <3307080>

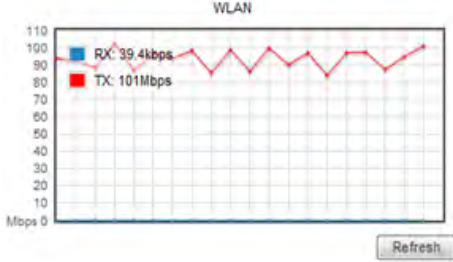
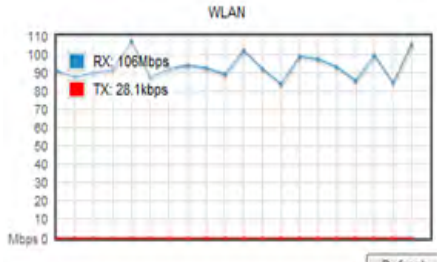
Jhorman Villanueva <4402030>

## ANEXO F: Pruebas de tráfico para el enlace inalámbrico

Se realizaron pruebas de tráfico para tener conocimiento de la capacidad máxima que puede soportar el enlace punto a punto y el enlace punto a multipunto. Se utiliza un software denominado TFGen que genera tráfico desde el computador donde se instala hacia cualquier host mediante su IP de destino, que en este caso son las antenas de Ubiquiti.

### Prueba de tráfico para el enlace Punto a Punto

Se transfieren paquetes a 150 Mbps en el enlace punto a punto utilizando el TFGen. Se muestra el valor de throughput del enlace formado por dos antenas grilla, donde una antena configurada con la dirección IP 192.168.1.12 actúa de transmisor y la otra antena configurada con la dirección IP 192.168.1.11 opera como receptor.

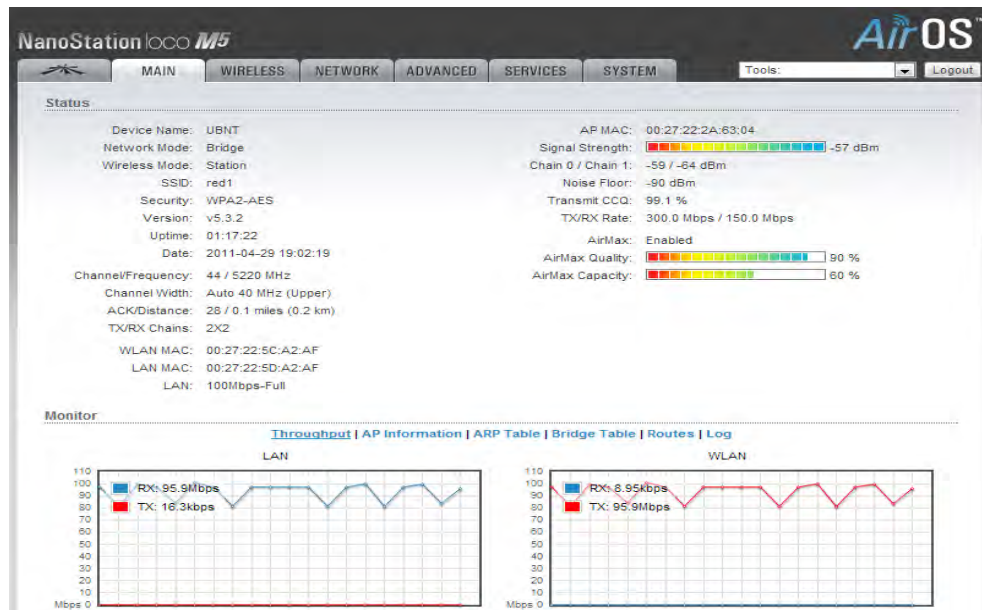
Dirección IP de la Antena Grilla	192.168.1.11	192.168.1.12
Gráfica Throughput	 <p>WLAN</p> <p>RX: 39.4kbps TX: 101Mbps</p> <p>Refresh</p>	 <p>WLAN</p> <p>RX: 106Mbps TX: 28.1kbps</p> <p>Refresh</p>

Según los anteriores datos se muestra que el máximo throughput del enlace punto a punto es de 100 Mbps. Por lo tanto, se comprueba la similitud del valor experimental con el valor teórico suministrado por el datasheet de la antena, que es de 100 Mbps.

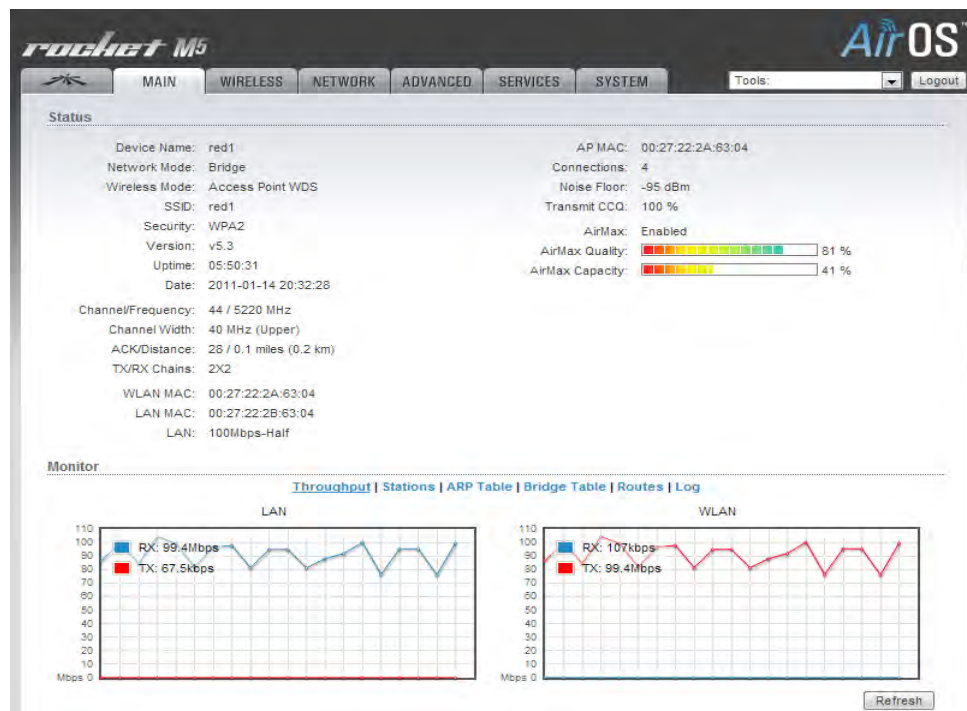
### Pruebas de Tráfico para el enlace Punto a Multipunto en la Red 1

Prueba 1: Para el área de cobertura 1 identificada con el SSID Red 1 se hicieron pruebas al enviar tráfico desde cada Station al AP. Se transmite tráfico de 300 Mbps por el canal con el programa TfGen desde el NanoStation Loco hasta el Access Point y el máximo throughput que alcanza es de 100 Mbps. Para cada

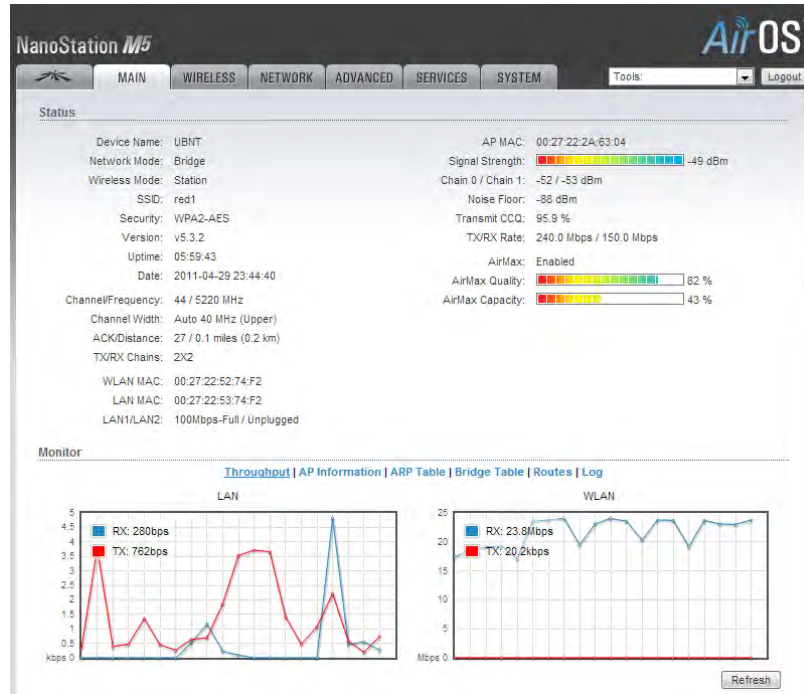
Station se comprobó que el máximo throughput o la máxima capacidad del canal es de 100 Mbps.



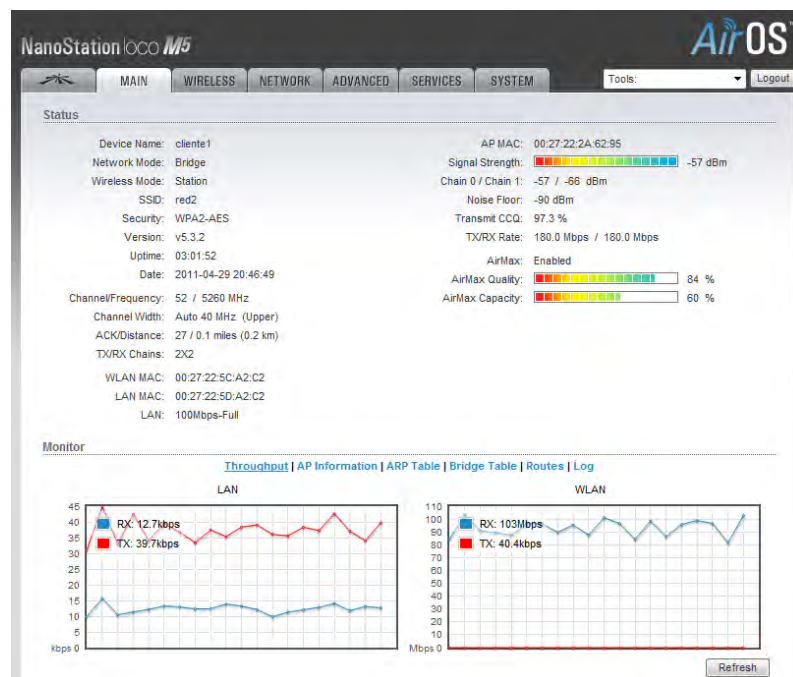
Prueba 2: Se transmite tráfico desde el AP hacia cada uno de los Station con paquetes de 50 Mbps; se observa que el total que trasmite el AP no supera los 100 Mbps.



Cada Station recibe un throughput entre 20 y 25 Mbps, es decir que la capacidad de su canal no supera los 25 Mbps cuando están recibiendo paquetes a la misma vez del AP. En la figura # se observa el throughput de uno de los NanoStation M5.



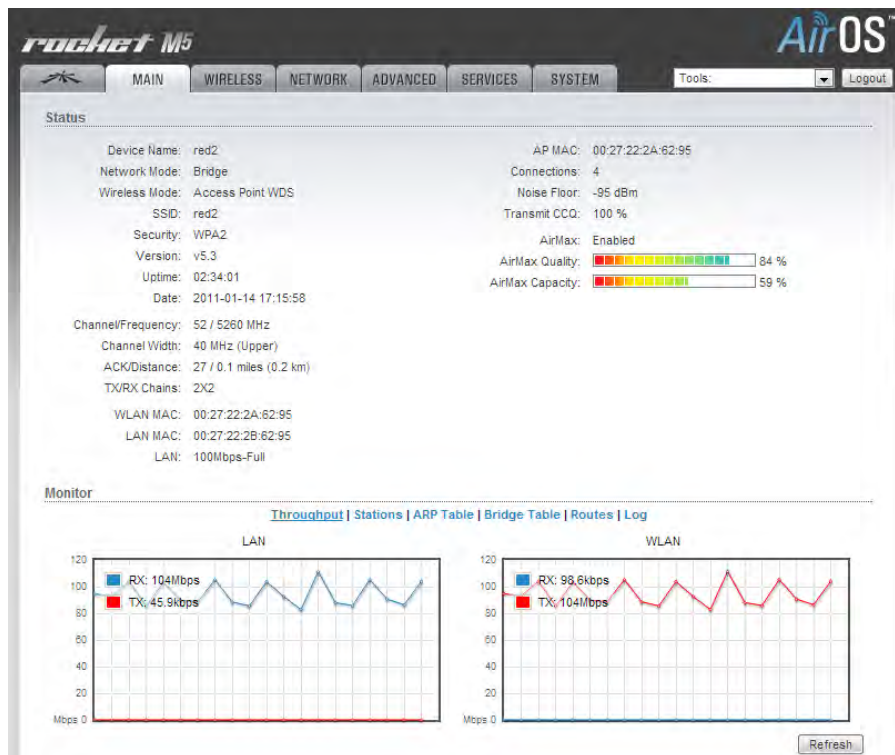
## Pruebas de Tráfico para el enlace Punto a Multipunto en la Red 2



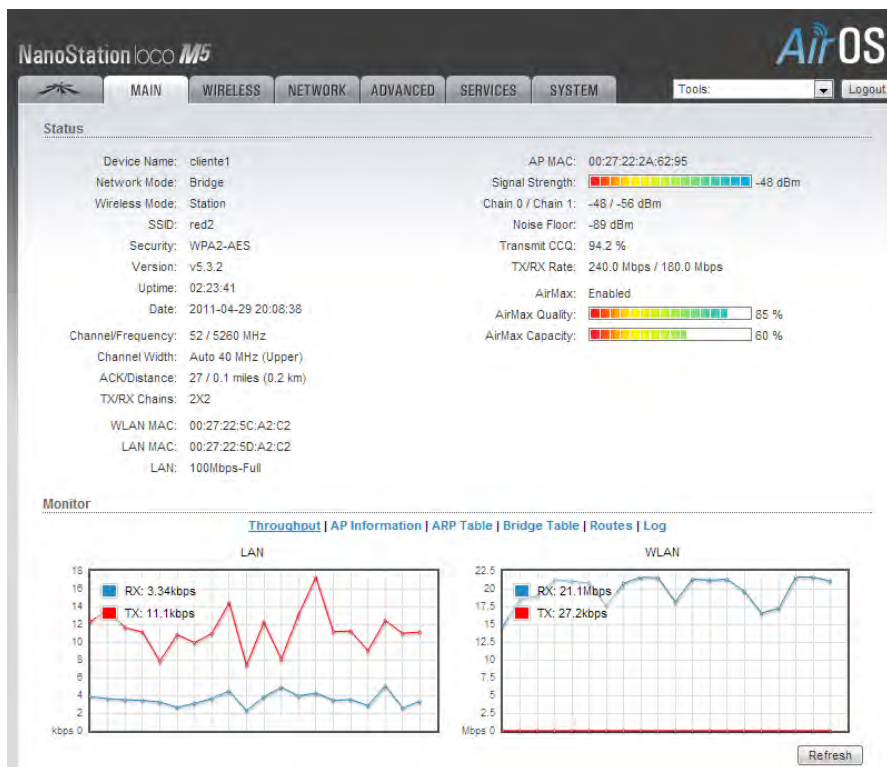
Para el área de cobertura 2 identificado con el SSID Red 2 se hicieron las mismas pruebas que para el área de cobertura 1. Se conectan los 4 Station al AP de la Red 2.

Prueba 1: Mediante el software TfGen se envía tráfico de 300 Mbps de un Station hacia el AP y se obtiene que la capacidad máxima del enlace es de 100 Mbps; esta misma capacidad se obtiene con los otros tres Station.

Prueba 2: Se envía tráfico de 50 Mbps desde el AP a cada uno de los Station a la misma vez. Se observa que el total de transmisión del AP es aproximadamente 100 Mbps.



Cada Station recibe paquetes entre 20 y 25 Mbps aproximadamente.



En las anteriores pruebas se puede analizar que el comportamiento, tanto de la Red 1 como de la Red 2, es bastante similar. Se comprueba que la mayor capacidad de transmisión para el enlace punto a punto y el enlace punto a multipunto es de 100 Mbps; la razón para el enlace punto a punto es que ésta es la capacidad máxima teórica que da como información el datasheet de las antenas grilla. Las antenas Rocket M5 y los NanoStation M5 permiten velocidades de hasta 150 Mbps según su respectivo datasheet, pero como la conexión de los NanoStation con el computador se hace mediante el protocolo Ethernet, la capacidad del enlace se limita a 100 Mbps. Es por esta razón que la capacidad del enlace punto a multipunto no sobrepasa los 100 Mbps.

Con los datos y pruebas realizadas, se concluye que se podrían tener 100 clientes conectados a cada Red si cada cliente consumiera 1 Mbps de ancho de banda. 50 clientes si cada uno consume 2 Mbps de ancho de banda y 25 clientes si cada uno consume 4 Mbps de ancho de banda.

### Pruebas realizadas con el Speed Test

Las pruebas que se realizan con la herramienta de monitoreo *Speed Test* que trae el sistema operativo AirOS de cada antena, permite evaluar el throughput Antena-Antena, por eso en los siguientes datos se muestra que la capacidad del enlace

Punto a Multipunto excede los 100 Mbps, pues ya no se tiene la restricción del protocolo Ethernet.

Air Max Quality: Calidad del enlace. Si el valor es bajo, podría ser que se tiene interferencia y se debe cambiar la frecuencia. Si el valor es mayor que 80 y no se nota ningún problema, no hay necesidad de hacer cambios.

AirMax Capacity: Relación de la tasa de transmisión actual sobre la tasa de transmisión máxima.

- Pruebas de Speed test en la Red 1

NanoStation M5: IP 192.168.1.22				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
59.52	54.26	113.78	84%	55%
57.76	54.31	112.07		
56.58	55.52	112.10		

NanoStation M5: IP 192.168.1.23				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
62.59	44.58	107.17	87%	56%
60.57	48.47	109.04		
61.34	45.90	107.24		

NanoStation M5: IP 192.168.1.20				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
60.88	51.48	112.36	86%	55%
59.80	53.12	112.92		
59.38	52.35	111.73		

NanoStation M5: IP 192.168.1.21				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
60.00	54.55	114.55	86%	56%
57.30	58.00	115.30		
59.42	55.01	114.43		

- Pruebas de Speed test en la Red 2

NanoStation M5: IP 192.168.1.22				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
74.20	71.14	145.34	84%	55%
82.64	60.42	143.06		
83.73	59.27	143.00		

NanoStation M5: IP 192.168.1.23				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
78.49	69.25	147.74	87%	56%
77.83	69.57	147.40		
81.09	65.65	146.74		

NanoStation M5: IP 192.168.1.20				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
82.15	64.76	146.91	86%	55%
81.26	63.49	144.75		
77.75	68.49	146.24		

NanoStation M5: IP 192.168.1.21				
RX (Mbps)	TX (Mbps)	Total (Mbps)	Air Max Quality	Airmax Capacity
87.61	56.43	144.04	86%	56%
80.47	64.58	145.05		
86.15	57.27	143.42		



## ANEXO G: Configuración del servidor DNS

Para la configuración del servidor DNS (Domain Named Service), se realiza los siguientes pasos:

1. Se define el nombre del dominio y de su servidor primario asociado, además de la dirección IP que va a tener el dominio. Estos parámetros se establecieron en el diseño de los servicios que componen a la red de núcleo del ISP:

Nombre del Dominio: labteleco.com

Nombre del servidor primario asociado: server.labteleco.com

Dirección IP asociado: 192.168.1.100

2. Se realiza la instalación de los paquetes requeridos para el servicio. Para ello, se ingresa al terminal del Centos 6 y se utiliza la instrucción *yum* para instalar los paquetes BIND. La instrucción *yum* permite descargar y actualizar paquetes del sistema a través de internet.

```
[root@labteleco /]# yum -y install bind bind-libs bind-utils
```

3. Se establece el inicio del servicio BIND en el sistema de arranque ejecutando la siguiente línea:

```
[root@labteleco /]# chkconfig --level 35 named on
```

La anterior línea indica que el servidor DNS estará disponible únicamente para los niveles de ejecución 3 y 5.

4. Se arranca el demonio del DNS para invocar el servidor de resolución de nombres para su inicio.

```
[root@labteleco /]# service named start
```

5. Se procede a editar el archivo de configuración principal *named.conf* y se adiciona la zona principal del dominio ya estipulado.

```
[root@labteleco /]# vi /etc/named.conf
```

Al ejecutar esta línea se presenta el siguiente código:

```

options {
#   listen-on port 53 { 127.0.0.1; };
#   listen-on-v6 port 53 { ::1; };
#   directory      "/var/named";
#   dump-file      "/var/named/data/cache_dump.db";
#   statistics-file "/var/named/data/named_stats.txt";
#   memstatistics-file "/var/named/data/named_mem_stats.txt";
#   allow-query    { localhost;192.168.1.0/24;};
#   recursion yes;

#   dnssec-enable yes;
#   dnssec-validation yes;
#   dnssec-lookaside auto;

/* Path to ISC DLV key */
#   bindkeys-file "/etc/named.iscdlv.key";

#   managed-keys-directory "/var/named/dynamic";
};

#logging {
#   channel default debug {
#       file "data/named.run";
#       severity dynamic;
#   };
#};

```

En la instrucción allow-query se escribe la dirección de red 192.168.1.0/24 de la cual hace parte el servidor DNS. Para crear la zona del dominio se ejecutan las siguientes líneas:

```

zone "." IN {
    type hint;
    file "named.ca";
};

#Dominio labteleco.com

zone "labteleco.com" IN {
    type master;
    file "labteleco.com.fwd";
    allow-update {none;};
};

#Dominio inverso labteleco.com

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "labteleco.com.rev";
    allow-update {none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

Para la zona del dominio se crean la zona directa que tiene el nombre del dominio labteleco.com y la zona inversa con la IP de la red 192.168.1. La zona directa realiza la consulta de la dirección IP a partir del nombre de dominio de dicha zona; La zona inversa realiza una consulta del nombre del dominio a partir de la dirección IP, utilizando el dominio "in-addr.arpa".

En cada una de las zonas se establece el tipo y el archivo donde se encuentra los parámetros de la respectiva zona; para la zona directa el tipo es master y el

archivo tiene por nombre labteleco.com.fwd, para la zona inversa el tipo es master y el archivo tiene por nombre labteleco.com.rev.  
Los archivos labteleco.com.fwd y labteleco.com.rev se encuentran en el directorio /var/named.

6. Se crean los archivos de la zona los cuales fueron mencionados en el archivo named.conf, es decir, la zona directa y la zona inversa. Para este caso, se comienza con la zona directa, creando el archivo con la siguiente línea:

```
[root@labteleco ~]# vi /var/named/labteleco.com.fwd
```

El archivo, como se mencionó anteriormente, estará ubicado en el directorio /var/named. Al abrir el archivo se introduce el siguiente código:

```
tTL 38400
@      IN      SOA    labteleco.com.  server.labteleco.com. (
                          1347662705
                          10800
                          3600
                          604800
                          38400 )

@      IN      NS     labteleco.com.
@      IN      A      192.168.1.100
server IN      A      192.168.1.100
www    IN      A      192.168.1.100
```

En el código se introduce los parámetros correspondientes a la zona directa, en donde se encuentra el registro de los recursos como el inicio de la autoridad SOA, el servidor de nombres NS y la dirección A. El registro tipo SOA indica el inicio de los datos de la zona y define los parámetros que afectan a todos los registros; para este caso se estipula el dominio labteleco.com y el nombre del servidor server.labteleco.com. El registro tipo A convierte un nombre de dominio en una dirección IP, que en este caso, se convierte www.labteleco.com a la dirección IP 192.168.1.100 y que de la misma forma sucede con server.labteleco.com. El registro tipo NS identifica el servidor de nombres para el dominio, que en este caso es labteleco.com.

En la zona inversa se crea el archivo con las siguientes líneas:

```
[root@labteleco ~]# vi /var/named/labteleco.com.rev
```

El archivo, como se mencionó anteriormente, estará ubicado en el directorio /var/named. Al abrir el archivo se introduce el siguiente código:

```
$ttl 38400
@      IN      SOA    labteleco.com.  server.labteleco.com (
                          1347662705
                          10800
                          3600
                          604800
                          38400 )

@      IN      NS     labteleco.com.
100    IN      PTR    labteleco.com.
100    IN      PTR    server.labteleco.com.]
```

En el código se introduce los parámetros correspondientes a la zona inversa, en donde se encuentra el registro de los recursos como el inicio de la autoridad SOA y el servidor de nombres NS como se explicó en el archivo de la zona directa. La diferencia es que ahora se introduce el registro tipo PTR en vez del registro tipo A. El registro tipo PTR es un puntero que convierte una dirección IP a un nombre de dominio, es decir, realiza lo contrario al registro tipo A; en este caso, se realiza la conversión de la dirección IP 192.168.1.100 al nombre labteleco.com y server.labteleco.com; el 100 que se encuentra al lado izquierdo hace referencia a la dirección IP.

7. Se resetea el servicio BIND con la siguiente línea: `services named restart`

8. Se asegura que el archivo `/etc/resolve.conf` contenga la IP del servidor DNS que ha sido levantado.

```
search labteleco.com
nameserver 192.168.1.100
```

## ANEXO H: Configuración de la distribución Zeroshell

Al momento de iniciar Zeroshell, este viene configurado con una IP por defecto que es la 192.168.0.75. La pantalla inicial que se observa de Zeroshell después de su instalación es la siguiente:

```
Z e r o S h e l l - Net Services 2.0.RC2           March 09, 2013 - 22:53
-----
Hostname : zeroshell.example.com
CPU (1)  : Intel(R) Pentium(R) Dual CPU E2160 @ 1.80GHz 1794MHz
Kernel   : 3.4.19-ZS
Memory   : 252404 kB                               http://192.168.0.75
Uptime   : 0 days, 1:49                             User      : admin
Load     : 0.00 0.01 0.05                           Password  : zeroshell
Profile  : Temporary EXAMPLE.COM configuration
-----
COMMAND MENU
<A> Activate Profile           <P> Change admin password
<D> Deactivate Profile       <T> Show Routing Table
<S> Shell Prompt             <F> Show Firewall Rules
<R> Reboot                   <N> Show Network Interface
<H> Shutdown                 <Z> Fail-Safe Mode
<B> Create a Bridge          <I> IP Manager
<W> WiFi Manager

                               Select: _
```

Se puede cambiar esa dirección IP por una dirección que quede en red con la LAN que se esté manejando; se presiona la letra I y se obtiene una serie de opciones con las cuales se pueden ajustar los parámetros de red.

```
-----
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)
Status: 100Mb/s Full Duplex
(1) 192.168.0.75 / 255.255.255.0 (up)
-----
ETH01 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)
Status: 100Mb/s Full Duplex
-----
Default Gateway: none
COMMANDS
<A> Add IP address           <D> Delete IP address
<M> Modify IP address       <G> Set Default Gateway
<S> Change Interface status <H> Dynamic IP configuration
<I> Show Info               <Q> Quit
>> _
```

Por ahora solo interesa cambiar la dirección IP del servidor Zeroshell, por lo tanto se presiona la letra M que permite tener la opción de modificar la dirección IP.

```

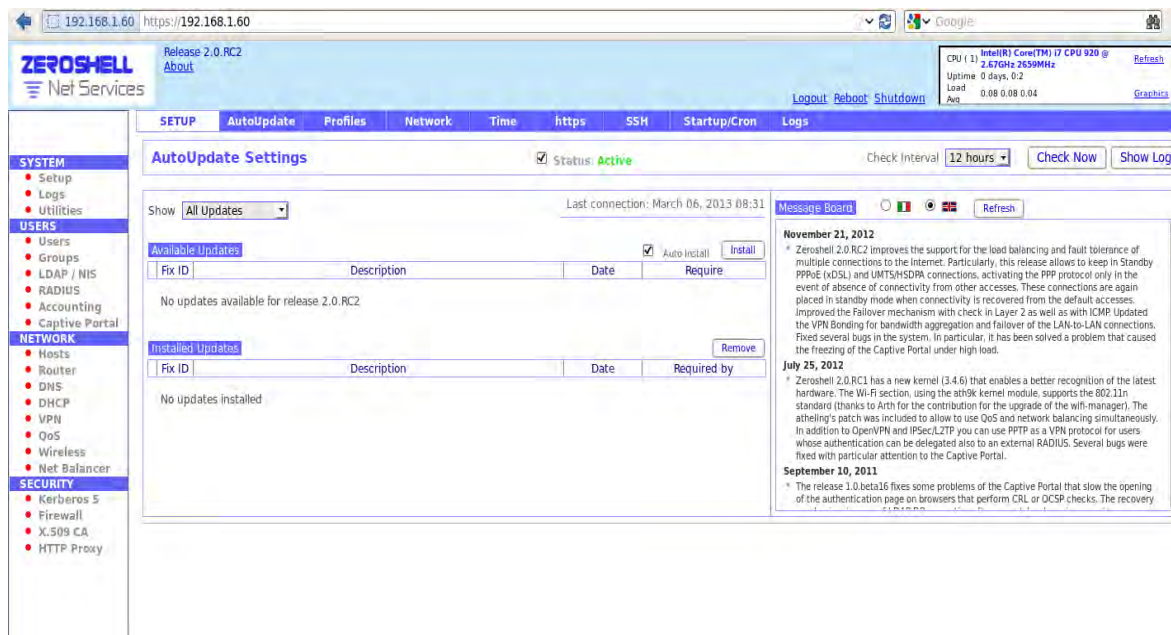
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)
Status: 100Mb/s Full Duplex
(1) 192.168.0.75 / 255.255.255.0 (up)
-----
ETH01 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)
Status: 100Mb/s Full Duplex
-----
Default Gateway: none

COMMANDS
<A> Add IP address           <D> Delete IP address
<M> Modify IP address       <G> Set Default Gateway
<S> Change Interface status <H> Dynamic IP configuration
<I> Show Info               <Q> Quit
>> m

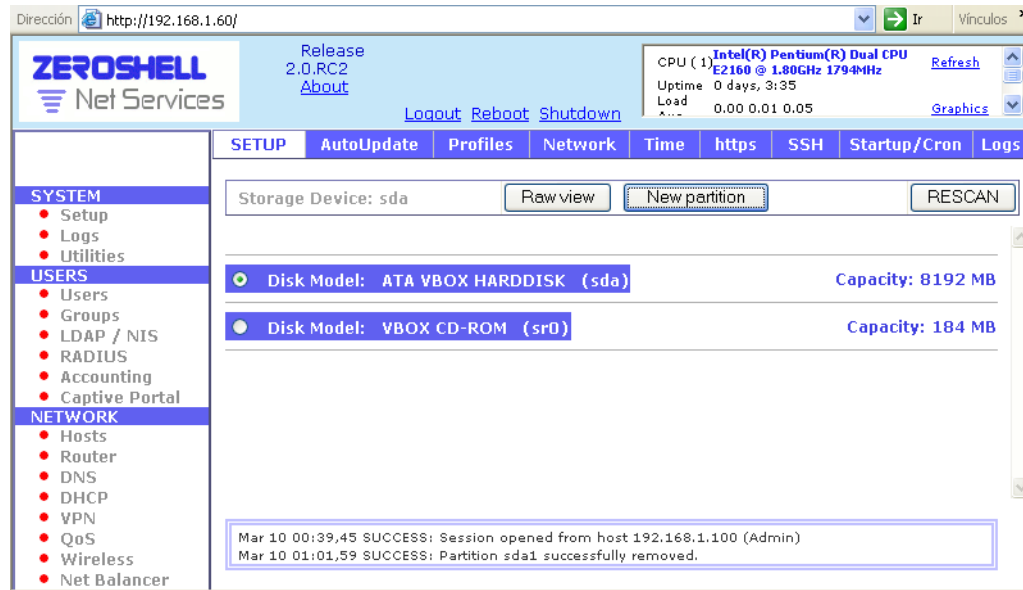
Interface [ETH00]:
-----
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)
Status: 100Mb/s Full Duplex
(1) 192.168.0.75 / 255.255.255.0 (up)
-----
IP to modify [1]:
IP [192.168.0.75]: 192.168.1.60
Netmask [255.255.255.0]:
IP status [up]: _

```

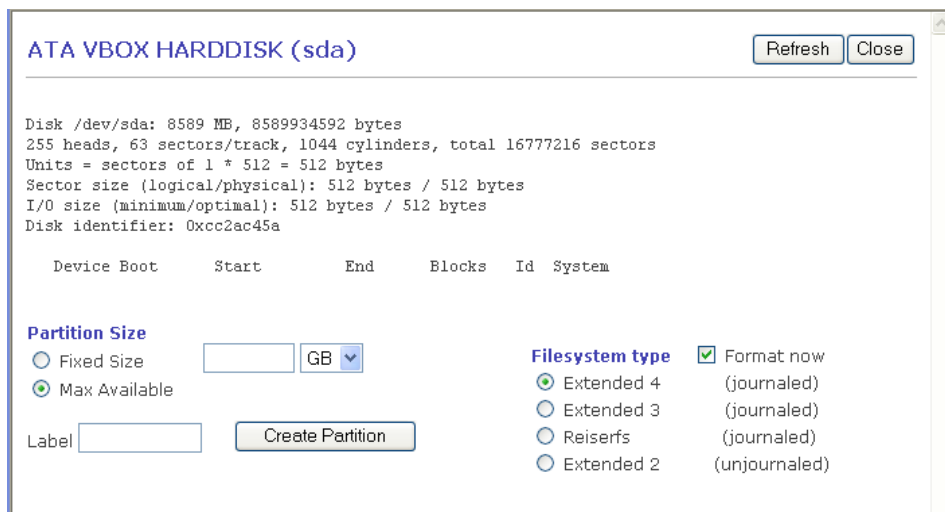
Se cambia la dirección IP 192.168.0.75 por la dirección 192.168.1.60, con la cual se puede acceder a la interfaz web de administración del Zeroshell desde cualquier navegador. El username y el password de acceso son admin y zeroshell respectivamente, valores que ya vienen por defecto pero si se quiere se pueden cambiar. La interfaz web como se observa en la siguiente figura permite realizar diferentes configuraciones de una manera más amigable y más fácil que la administración por línea de comandos.



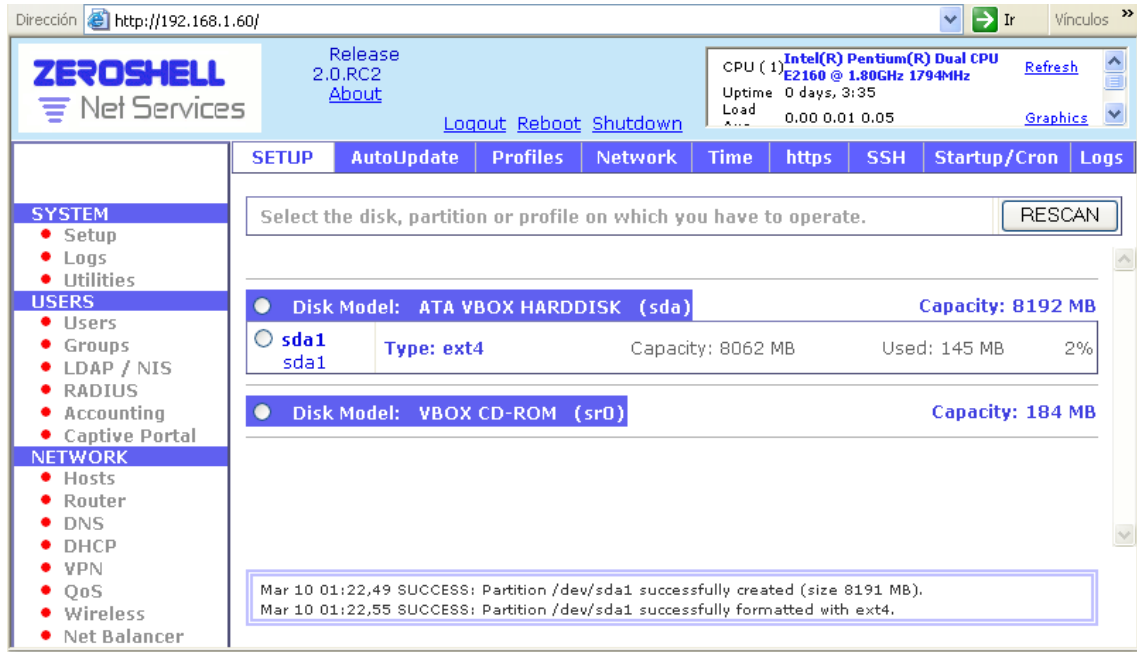
Para que todas las configuraciones que se realicen queden guardadas en una base de datos y no se borren cuando se apague o se reinicie el servidor Zeroshell, es necesario crear un perfil. Esto tiene grandes ventajas ya que se pueden guardar distintas configuraciones para realizar diferentes pruebas. Se debe crear una partición en el disco duro para almacenar el perfil y todas las configuraciones que se hagan, para esto se selecciona *Setup* ubicado en el menú izquierdo y en el menú superior se elige *Profiles*; se marca la etiqueta Disk model: ATA VBOX HARDDISK (sda) y se elige *New Partition*.



A continuación se accede a la ventana de creación de partición en el disco duro, donde va a quedar almacenada toda la configuración. El formato de la partición será *Extended 4* y el tamaño *Max Available* (Máximo disponible), que son opciones por defecto.



Una vez creada la partición aparecerá la página de *Profiles* con la nueva partición creada.



Para crear el perfil se selecciona la partición creada (sda1) y aparece un menú donde se debe seleccionar *Create Profile*, con lo cual aparece una ventana donde se debe suministrar unos datos necesarios. Aquí se puede cambiar la contraseña de administrador del servidor ZeroShell.

### ATA VBOX HARDDISK (sda)

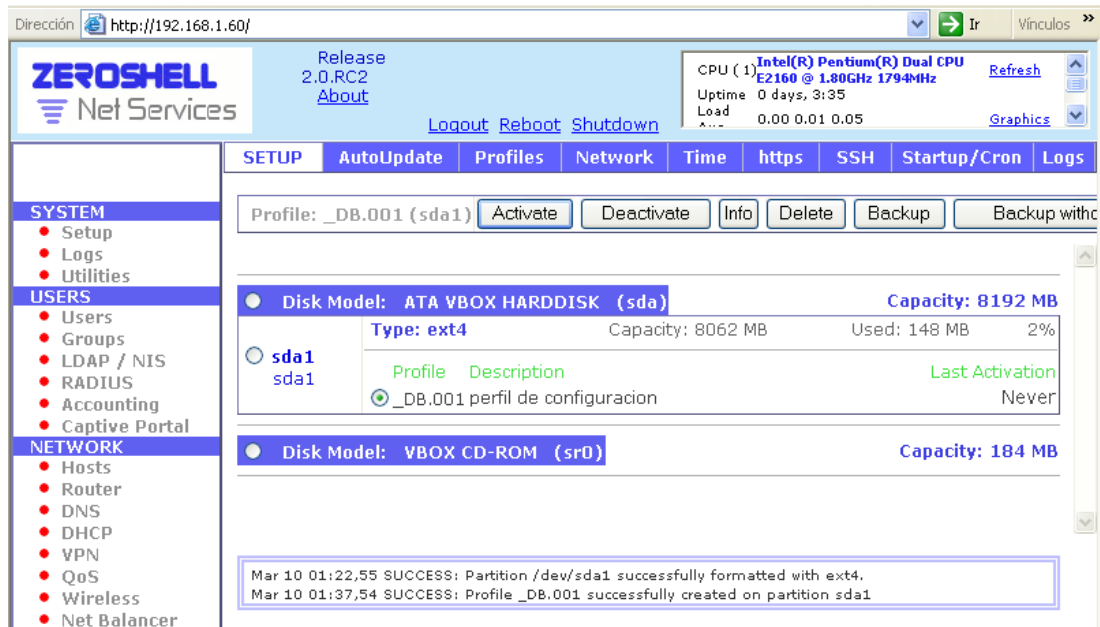
New Profile on partition sda1

Create Close

Description	<input type="text"/>
Hostname (FQDN)	<input type="text" value="zeroshell.example.com"/>
Kerberos 5 Realm	<input type="text" value="EXAMPLE.COM"/>
LDAP Base	<input type="text" value="dc=example,dc=com"/>
Admin password	<input type="password"/>
Confirm password	<input type="password"/>
<b>NETWORK CONFIG</b>	
Ethernet Interface	<input type="text" value="ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE"/>
IP Address / Netmask	<input type="text" value="192.168.1.60"/> / <input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>

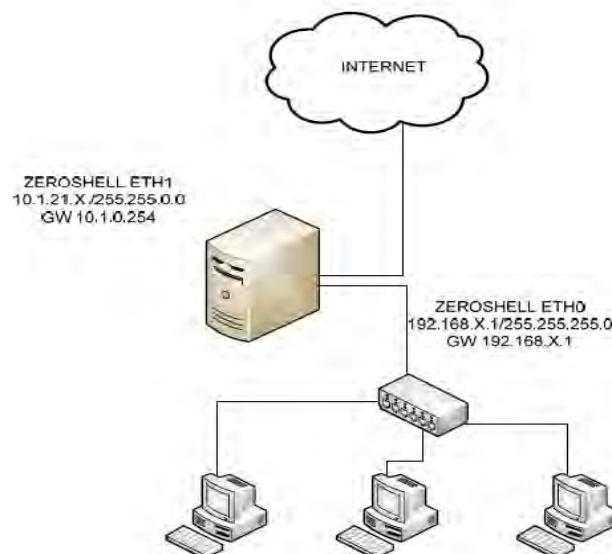


Se ingresa los datos necesarios y se pulsa *Create* en la parte superior derecha. Se selecciona el perfil *\_DB.001* y se presiona *Activate* para que el perfil quede activo y funcionando. Cuando se activa el perfil el sistema se reinicia con la configuración que se ha creado.

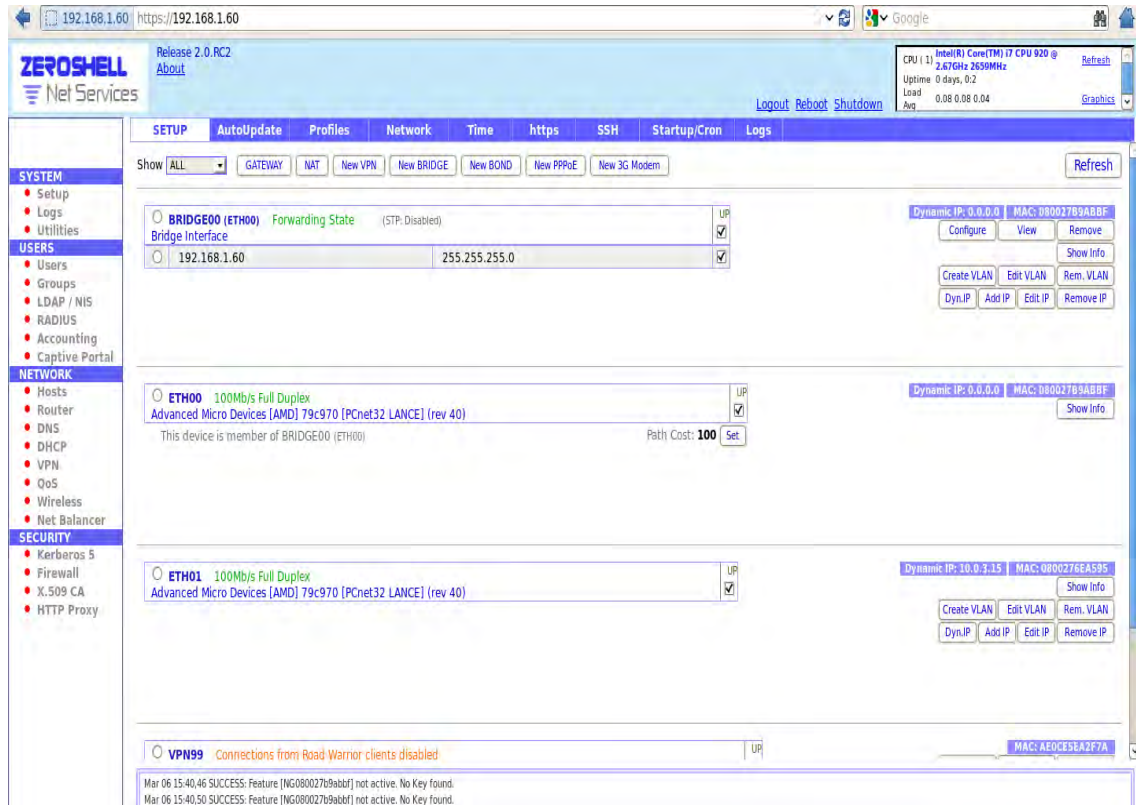


- **Configuración de la red**

Se va a realizar la configuración de red como se muestra en el siguiente esquema.



Se necesita activar dos interfaces de red, una que tenga salida a internet y otra con una dirección IP que conecte la red local. Para ello se ingresa a *Setup* y posteriormente en el menú superior se elige *Network*.



Como se observa en la anterior figura, ETH00 tiene configurada una dirección IP estática: 192.168.1.60, que es la que se comunica con la red local que se está manejando. Y ETH01 es la interfaz que da salida a internet, se configura con DHCP y toma la dirección IP dinámica 10.0.3.15.

## **ANEXO I: Manual de Usuario**

### **Manual de Usuario**

**Diseño e implementación de un ISP con acceso inalámbrico que soporte servicio de internet y telefonía IP**

**Universidad Autónoma de Occidente**

**Copyright 2013**

**14/05/13**

**Autor(es): Luis H. Villa A. Jhorman A. Villanueva V.**

## Contenido

- A. Objetivos
- B. Prerrequisitos Teóricos
- C. Instrumentos requeridos
- D. Fundamentación
- E. Procedimiento
  - 1. Arquitectura del ISP
  - 2. Configuración de las antenas
  - 3. Configuración del Enlace Punto a Punto
  - 4. Configuración del Enlace Punto a Multipunto
  - 5. Instalación del software de gestión airControl de Ubiquiti Networks
  - 6. Instalación del software VirtualBox
  - 7. Configuración de Servicios de Red
  - 8. Configuración de la distribución Zeroshell
  - 9. Configuración de la distribución Elastix
  - 10. Configuración de teléfonos
  - 11. Configuración del VoIPMonitor
  - 12. Nota

### **A. Objetivos:**

- Conocer el funcionamiento y los procedimientos de cómo los ISP prestan sus servicios.
- Comprender la Implementación de una red WIFI con dos áreas de cobertura unidas inalámbricamente por un enlace punto a punto.
- Entender la configuración del servicio AAA (Authentication, Authorization and Accounting) en el ISP implementado con la distribución Zeroshell.
- Conocer el funcionamiento del software AirControl de Ubiquiti Networks que realiza la gestión y monitoreo de la red inalámbrica.
- Implementar el control de ancho de banda para asignar diferentes planes de internet a usuarios utilizando la distribución Zeroshell.
- Implementar el servicio de DHCP y NAT para la red utilizando la distribución Zeroshell.
- Implementar una base de datos a partir de un servicio de directorio implementado con la distribución Zeroshell.
- Implementar el servicio de VOIP utilizando la distribución Elastix.
- Implementar distintas funcionalidades como buzón de voz, transferencia de llamadas que permitan un servicio integrado de VOIP utilizando la distribución de Zeroshell.
- Efectuar mediciones de QoS en el servicio de telefonía IP utilizando el software VOIPmonitor.

### **A. Prerrequisitos teóricos:**

- Tecnologías inalámbricas.
- Conceptos básicos de telecomunicaciones (frecuencia, ancho de banda, nivel de potencia de la señal, etc.).
- Características del espectro electromagnético.
- GNU Linux.
- Redes TCP/IP
- Gestión de Red
- Telefonía IP
- Arquitectura de redes
- Arquitectura de un ISP
- Calidad de Servicio (QoS) de VoIP
- NAT, DHCP, DNS
- Portal Cautivo

### **B. Instrumentos requeridos:**

- Dos Antenas Grilla Airgrid M5 de Ubiquiti Network

- Dos Antenas omnidireccional AirMax junto a su radio Rocket M5 de Ubiquiti Network
- Dos NanoStation M5 de Ubiquiti Network
- Dos NanoStation loco M5 de Ubiquiti Network
- 3 Switch de red
- Software Virtual Box
- Distribución basada en Linux Zeroshell
- Distribución de telefonía IP Elastix.
- Software de medición de calidad de servicio Voipmonitor
- Un Teléfono IP
- Un teléfono análogo
- Adaptador de teléfono análogo ATA
- Softphone modelo 3CXPhone
- Software de Gestión AirControl de Ubiquiti
- Un computador de escritorio con sistema operativo Linux Centos 6 con dos interfaces de red.
- Cuatro computadores

### **C. Fundamentación:**

#### **Servidor de autenticación**

Es el equipo que recibe las peticiones del equipo de acceso en relación al usuario que está validando, es decir verifica que el nombre de usuario y contraseña que le está dando el equipo de acceso sea correcto y qué tipo de cliente es: si es ADSL, inalámbrico, solo mail, etc. Está conectado con la base de datos de clientes. El protocolo que se maneja en este servidor es el Protocolo AAA, el cual cumple tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting).

#### **Servicio de Directorio**

Este servicio permite el almacenamiento de todo tipo de información el cual consta de un listado de la información sobre alguna clase de objetos como las personas. Los directorios pueden utilizarse para hallar información sobre un objeto concreto o, en sentido contrario, hallar objetos que cumplen un determinado requisito. Entre los datos que se almacenan están: nombre, ID del usuario, la dirección, el correo electrónico, el número de teléfono. Estos pueden utilizarse para almacenar otros tipos de información, de manera parecida a como hacen los directorios de sistemas de archivos. El protocolo de acceso a directorios más utilizado es el

Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol, LDAP)<sup>49</sup>.

## **Gestión de red**

La gestión de red posibilita la monitorización y el mantenimiento de las redes con vistas a mantener su funcionamiento, a detectar y reparar fallos, a detectar posibles problemas antes de que se conviertan en fallos, a asegurar el cumplimiento de los requisitos contractuales y a mantener los cambios de configuración necesarios como la inclusión de nuevos usuarios, nuevas conexiones a otras redes o nuevas tarifas<sup>50</sup>.

## **Telefonía IP**

La telefonía IP llamada Voz sobre IP se puede definir como la transmisión de paquetes de voz utilizando redes de datos, la comunicación se realiza por medio del protocolo IP (Internet Protocol), permitiendo establecer llamadas de voz y fax sobre conexiones IP.

## **Zeroshell**

Es una distribución de Linux, open source, para servidores con el objetivo de suministrar los principales servicios que una red LAN requiera. Se puede configurar y administrar utilizando el navegador web.

Entre los servicios que ofrecen se tiene:

- Balanceo de Carga
- Conexiones UMTS/HSDPA usando módems 3g
- Servidor Radius para suministrar autenticación segura.
- Portal cautivo que soporte web login en redes inalámbricas y cableadas.
- Gestión de QoS y control de tráfico sobre una red saturada.
- Servidor proxy http que es capaz de bloquear páginas web que contengan virus.
- 802.1Q Virtual LAN
- NAT, DHCP, DNS.
- LDAP, NIS y autorización RADIUS.
- Autoridad de certificación X509 para emisión y gestión de certificados electrónicos.

## **Elastix**

---

<sup>49</sup> SILBERSCHATZ, Abrahan y KORTH, Henry. Fundamentos de base de datos. Madrid: McGraw-Hill, 2006. p. 719.

<sup>50</sup> AREITIO, Javier. Seguridad de la información: Redes, informática y sistemas de información. Madrid: Paraninfo, 2008. p. 278.

Elastix es un software de código abierto para el establecimiento de comunicaciones unificadas. El objetivo de Elastix es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial. Fue diseñado y desarrollado por PaloSanto Solutions. Elastix inició como una interfaz de reportación para llamadas de Asterisk. Posteriormente evolucionó hasta convertirse en una distribución basada en Asterisk, utilizando como sistema operativo Linux CentOS. Elastix no solamente provee telefonía, integra otros medios de comunicación para hacer más eficiente y productivo el entorno de trabajo.

### **Medición de Calidad de Servicio**

QoS es el mecanismo de priorización de los paquetes de voz sobre los datos cuando se cursa VoIP en una red de datos compartida. Al igual que existen factores que repercuten en los retardos en la red, existen también factores que intervienen en la calidad de la voz, tales como codificadores, ancho de banda, pérdida de paquetes, latencia, jitter y eco<sup>51</sup>.

Jitter: variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdidas de sincronización o por las diferentes rutas seguidas por los paquetes para llegar a su destino.

Latencia: denominado también retardo (delay). Se define como el tiempo que tarda un paquete en llegar desde la fuente al destino.

MOS: mean opinion score, es un método subjetivo de medida de la calidad de servicio que resulta en un promedio de opinión de los usuarios. Es la evaluación subjetiva más ampliamente usada, estandarizada en la recomendación ITU-T P.800

PACKET LOSS: pérdida de paquetes debido a descartes de paquetes que no llegan a tiempo al receptor.

Los valores máximos de los parámetros de calidad de servicio se determinan con base a la Recomendación Y.1541 de la ITU-T que especifica los "Objetivos de calidad de funcionamiento de la red para servicios basados en el protocolo de internet". El valor máximo del parámetro MOS se define dependiendo del códec que se esté manejando, que en este caso es el G.711.

---

<sup>51</sup> HUIDOBRO MOYA, José Manuel y CONESA PASTOR, Rafael. Sistemas de Telefonía. 5 ed. Madrid: Paraninfo, 2006. p. 294.



Con base a la anterior información, se presenta en el cuadro 1 los valores máximos que se debe tener en VoIP para garantizar la calidad de servicio.

### **Cuadro 1. Valores máximos en los parámetros de QoS para el servicio de VoIP**

<b>Parámetros de QoS</b>	<b>Valores Máximos</b>
Delay	400 ms
Jitter	50 ms
Packet Loss	0.1 %
MOS	4.1

### **VoIPMonitor**

VoIPMonitor es un sniffer de paquetes de red de código abierto con front-end comercial para protocolos de VoIP SIP RTP y RTCP los cuales corren en el sistema GNU/Linux. Este sniffer es diseñado para analizar la calidad de llamada VoIP basado en parámetros de red – variación de retardo y perdida de paquetes según el E-model ITU-T G.107 el cual predice la calidad en la escala MOS.






Las llamadas con toda la estadística relevante son guardadas en la base de datos MySQL u ODBC. Los codecs soportados son el G.711 a-law/u-law y los soportes plugins comerciales G.722, G729a, G723, iLBC. Presenta una interfaz WEB GUI donde se puede visualizar todas las estadísticas, parámetros y reportes que se obtienen a partir de las llamadas. Presenta las siguientes características:

- Filtros globales para encontrar CDRs específicos basados en IP, números telefónicos parámetros cualitativos (perdida/retardo/MOS).
- Detalles de la llamada en vivo.
- Flujo de mensajes SIP detallados con vista estilo wireshark.
- Escucha de llamadas directamente de la interfaz WEB.
- Filtros de grabación que permiten grabar voz (RTP) solo para algunas llamadas basadas en IP o números telefónicos.
- Gráfica de distribución de retardo y pérdidas para cada llamada.
- Fácil desarrollo.

### **Antenas de Ubiquiti Networks**

La red inalámbrica se desarrolla utilizando dos antenas grilla que realizan la conexión punto a punto, dos antenas omnidireccionales MIMO de polaridad dual 2x2 que conectados a dos Radio MIMO 2x2 realizan la conexión punto a multipunto y cuatro CPE que realizan la conexión del enlace inalámbrico con cada cliente. A continuación se presenta las antenas a utilizar con sus respectivas características.

**Cuadro 2. Antenas a utilizar en la implementación de la red inalámbrica**

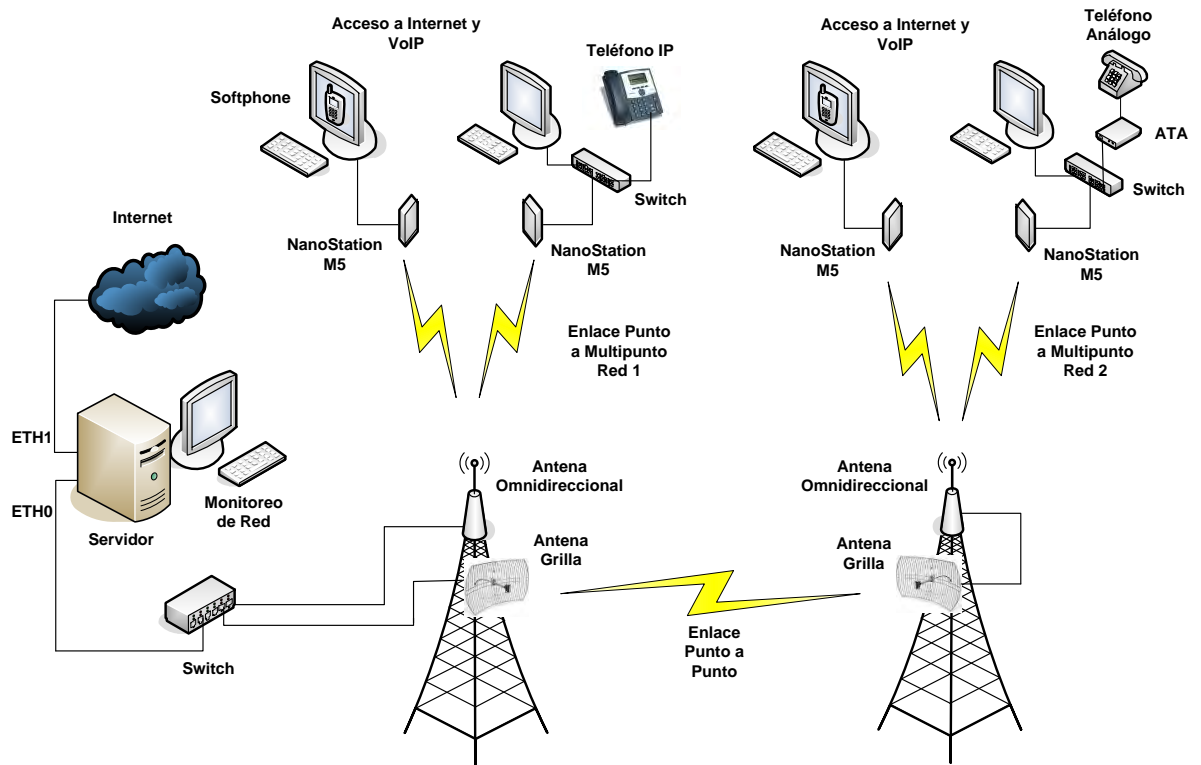
Antena	Marca	Modelo	Frecuencia	Ganancia	Potencia	Imagen
Antena Grilla, airGrid M5	Ubiquiti Network	AGM5-HP-1114	5470 - 5825 Mhz	23 dBi	25 dBm	
Antena omni direccional airMAX Omni	Ubiquiti Network	AMO-5G10	5.45 - 5.86 GHz	10 dBi		
Radio MIMO 2x2: Rocket M	Ubiquiti Network	M5	5470 - 5825 MHz		27 dBm	
CPE, NanoStation M5	Ubiquiti Network	M5	5470 a 5825 MHz	14.6 - 16.1 dBi	27 dBm	
CPE, NanoStation loco M5	Ubiquiti Network	M5	5470 - 5825 MHz	13 dBi	23 dBm	

## D. Procedimiento

### 1. Arquitectura del ISP

El esquema de red que se desea implementar es el que se muestra en la figura 1.

**Figura 1. Diagrama de red implementado para ofrecer servicio de internet y VoIP**



El equipo que contiene los servicios (DNS, DHCP, NAT) tiene conectado en la interfaz de red denominada ETH1 la red pública que ofrece Internet, y en la interfaz denominada ETH0 se encuentra la red privada o LAN que ofrece el servicio de internet y telefonía IP a los usuarios finales; la dirección IP que se tiene configurada en el ETH0 para este diseño es la 192.168.1.100.

En la comunicación VoIP se manejan 2 softphone, los cuales se instalan en dos PC respectivamente, un teléfono IP que permite una conexión Ethernet directa hacia el switch y un teléfono análogo que se encuentra conectado a un ATA para que realice la conversión de una conexión RJ-11 a una conexión Ethernet.

El primer área de cobertura de enlace punto a multipunto tiene por nombre RED 1, el cual se encuentra conectado a la red de núcleo, y la segunda área de cobertura de enlace punto a multipunto tiene por nombre RED 2, el cual se encuentra

conectado de forma directa a la grilla para poder obtener los paquetes de voz y datos a partir del enlace punto a punto.

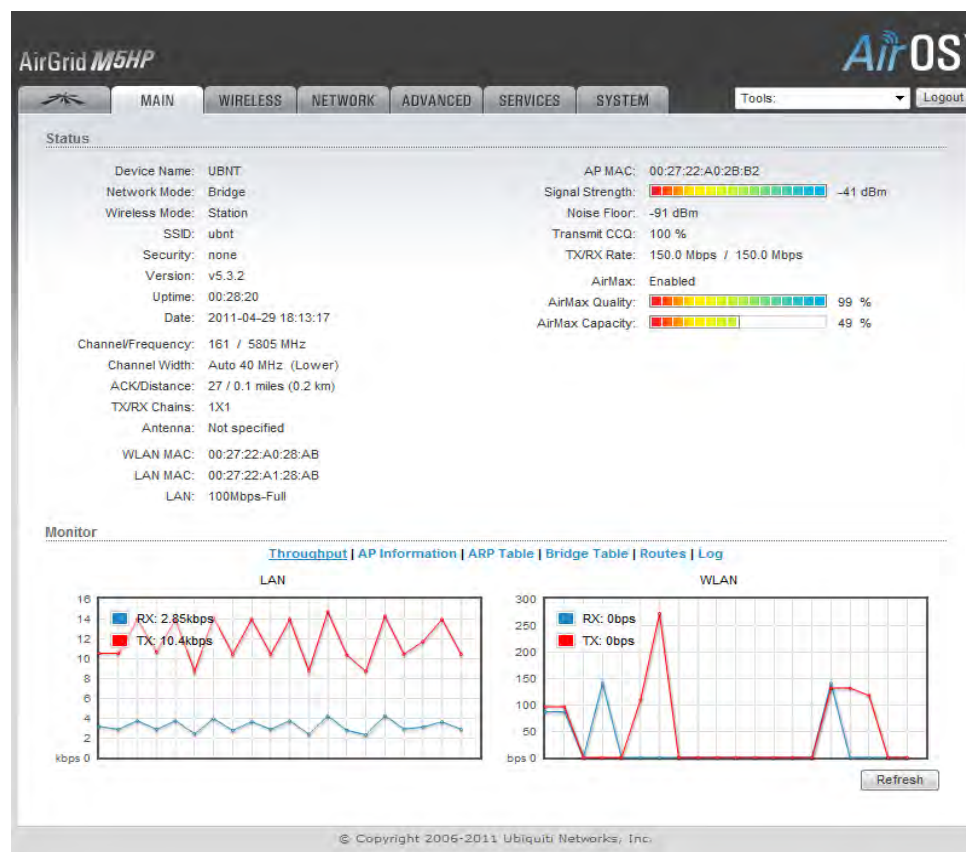
## 2. Configuración de las antenas.

**2.1.** Conectar puerto LAN del adaptador de la antena a un computador por medio de un cable Ethernet; luego se conecta la antena el puerto POE del adaptador por medio de un cable Ethernet. El PC debe estar configurado con una IP estática de tal forma que pueda quedar en red con la antena, es decir con una IP que se encuentre en la red 192.168.1.x.

**2.2.** Se ingresa al sistema operativo AirOS de la antena desde cualquier navegador (browser) por medio de una dirección IP, que por defecto es 192.168.1.20.

**2.3.** Al inicio es necesario especificar un usuario y contraseña de administrador, que por defecto son: usuario: ubnt; contraseña: ubnt. Si los anteriores datos son correctos aparece la interfaz de configuración de la antena como se observa en la figura 2.

**Figura 2. Interfaz de configuración de las antenas airOS**



### 3. Configuración del Enlace Punto a Punto

El enlace punto a punto se realiza con las dos antenas grilla Airgrid M5. Una de las Antenas se configura como Access Point y la otra como Station. Para realizar la configuración se accede al airOS de cada antena.

- **Parámetros de Configuración para la airGrid M5 modo Access Point**

3.1. Se ingresa a la pestaña Wireless y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 3.

**Cuadro 3. Parámetros de configuración de la Pestaña Wireless**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Access Point WDS
		SSID:	AP_PTP
		Country Code:	Colombia
		IEEE 802.11 Mode:	A/N mixed
		Channel Width:	40 MHz
		Channel Shifting:	Disabled
		Frequency, MHz:	5180
		Extension Channel:	Upper Channel
		Frequency Scan List, MHz:	Enabled: 5180
		Output Power:	-6 dBm (Mínimo)
		Max TX Rate, Mbps:	Automatic
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
		WPA Preshared Key:	12345
		MAC ACL:	Enable
		Policy:	Allow 00:27:22:A0:2B:B2

3.2. Se ingresa a la pestaña Network y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 4.

**Cuadro 4. Parámetros de configuración de la Pestaña Network**

<b>NETWORK</b>	<i>Network Role</i>	Network Mode:	Bridge
		Disable Network	None
	<i>Network Settings</i>	Bridge IP Address:	Static
		IP Address:	192.168.1.11
		Netmask:	255.255.255.0

		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled

3.3. Se ingresa a la pestaña Advanced y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 5.

**Cuadro 5. Parámetros de configuración de la Pestaña Advanced**

<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.1 miles (0.2 km)
		ACK Timeout:	28, Auto Adjust Enabled
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65

3.4. Se ingresa a la pestaña Services y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 6.

**Cuadro 6. Parámetros de configuración de la Pestaña Advanced**

<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
		Enable Password Authentication :	Enabled

3.5. Se ingresa a la pestaña Services y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 7.

**Cuadro 7. Parámetros de configuración de la Pestaña Advanced**

<b>SYSTEM</b>	<i>Device</i>	Device Name:	AP_PTP
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

- **Parámetros de Configuración para la airGrid M5 modo Station**

3.6. Se ingresa a la pestaña Wireless y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 7.

**Cuadro 7. Parámetros de configuración de la Pestaña Wireless**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Station WDS
		SSID:	AP_PTP
		Lock to AP MAC:	00:27:22:2A:63:04
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	Auto 20/40 MHz
		Channel Shifting	Disabled
		Frequency Scan List, MHz	Enabled: 5180
		Antenna:	11x14 – 23 dBm
		Output Power	6 dBm (Mínimo)
		Max TX Rate, Mbps	Automatic
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
		WPA Preshared Key:	12345

3.7. Se ingresa a la pestaña Network y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 8.

**Cuadro 8. Parámetros de configuración de la Pestaña Network**

<b>NETWORK</b>	Network Role	Network Mode:	Bridge
		Disable Network	None
	Network	Bridge IP Address:	Static

	Settings	IP Address:	192.168.1.12
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled

3.8. Se ingresa a la pestaña Advanced y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 9.

**Cuadro 9. Parámetros de configuración de la Pestaña Advanced**

<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.1 miles (0.2 km)
		ACK Timeout:	28, Auto Adjust Enabled
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65

3.9. Se ingresa a la pestaña Services y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 10.

**Cuadro 10. Parámetros de configuración de la Pestaña Services**

<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
		Enable Password Authentication :	Enabled



3.10. Se ingresa a la pestaña System y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 11.

**Cuadro 11. Parámetros de configuración de la Pestaña System**

<b>SYSTEM</b>	<i>Device</i>	Device Name:	ST_PTP
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

#### 4. Configuración del Enlace Punto a Multipunto

El enlace punto a multipunto se establece entre las antenas NanoStation M5 y el área de cobertura generada por el Rocket M5. A continuación se presenta los parámetros de configuración para el Rocket M5 y los NanoStation M5.

- **Parámetros de Configuración de los Rocket M5**

La configuración de los dos módulos Rocket M5 se realiza para las dos áreas de cobertura de la Red 1 y Red 2 respectivamente. Para realizar la configuración se accede al airOS de cada Rocket M5.

4.1. Se ingresa a la pestaña Wireless y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 12.

**Cuadro 12. Parámetros de configuración de la Pestaña Wireless**

<b>WIRELESS</b>	<i>Basic Wireless Setting</i>	Wireless Mode:	Access Point WDS
		SSID:	Red 1 o Red 2
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	40 MHz
		Channel Shifting	Disabled
		Frequency, MHz	Para Red 1: 5220 Para Red 2: 5280
		Extension Channel	Lower Channel
		Frequency Scan List, MHz	Enabled Para Red 1: 5220 Para Red 2: 5280
		Output Power	-4 dBm (Mínimo)
		Max TX Rate, Mbps	Automatic
	<i>Wireless</i>	Security:	WPA2-AES

	<i>Security</i>	WPA Authentication:	PSK
		WPA Preshared Key:	12345
		MAC ACL	Enable
		Policy:	Allow 00:27:22:5C:A2:C2 00:27:22:52:76:90 00:27:22:52:74:F2 00:27:22:5C:A2:AF

4.2. Se ingresa a la pestaña Network y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 13.

**Cuadro 13. Parámetros de configuración de la Pestaña Network**

<b>NETWORK</b>	<i>Network Role</i>	Network Mode:	Bridge
		Disable Network	None
	<i>Network Settings</i>	Bridge IP Address:	Static
		IP Address:	Red 1: 192.168.1.14 Red 2: 192.168.1.13
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled

4.3. Se ingresa a la pestaña Advanced y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 14.

**Cuadro 14. Parámetros de configuración de la Pestaña Advanced**

<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.4 miles (0.6 km)
		ACK Timeout:	Auto Adjust
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100

	<i>Setting</i>		
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65

4.4. Se ingresa a la pestaña Services y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 15.

**Cuadro 15. Parámetros de configuración de la Pestaña Services**

<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
		Enable Password Authentication :	Enabled

4.5. Se ingresa a la pestaña System y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 16.

**Cuadro 16. Parámetros de configuración de la Pestaña System**

<b>SYSTEM</b>	<i>Device</i>	Device Name:	AP_PTM
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

- **Parámetros de Configuración de los 4 módulos NanoStation**

La configuración de los 4 módulos NanoStation M5 se realiza para cada uno de los clientes. Para realizar la configuración se accede al airOS de cada NanoStation M5.

4.6. Se ingresa a la pestaña Wireless y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 17.

**Cuadro 17. Parámetros de configuración de la Pestaña Wireless**

<b>WIRELESS</b>	<i>Basic Wireless</i>	Wireless Mode:	Station WDS
		SSID:	Red 1 o Red 2

	<i>Setting</i>	Lock to AP MAC:	00:27:22:2A:63:04
		Country Code:	Colombia
		IEEE 802.11 Mode	A/N mixed
		Channel Width	Auto 20/40 MHz
		Channel Shifting	Disabled
		Frequency Scan List, MHz	Enabled
		Output Power	8 dBm (Mínimo)
		Max TX Rate, Mbps	Automatic
	<i>Wireless Security</i>	Security:	WPA2-AES
		WPA Authentication:	PSK
WPA Preshared Key:		12345	

4.7. Se ingresa a la pestaña Network y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 18.

**Cuadro 18. Parámetros de configuración de la Pestaña Network**

<b>NETWORK</b>	Network Role	Network Mode:	Bridge
		Disable Network	None
	Network Settings	Bridge IP Address:	Static
		IP Address:	Para NS M5: 192.168.1.20 192.168.1.23 Para NS loco M5: 192.168.1.21 192.168.1.22
		Netmask:	255.255.255.0
		Gateway IP:	192.168.1.1
		MTU:	1500
		Auto IP Aliasing	Enabled

4.8. Se ingresa a la pestaña Advanced y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 19.

**Cuadro 19. Parámetros de configuración de la Pestaña Advanced**

<b>ADVANCED</b>	<i>Advanced Wireless Settings</i>	RTS Threshold:	Off
		Fragmentation Threshold:	Off
		Distance:	0.4 miles (0.6 km)

		ACK Timeout:	Auto Adjust
		Aggregation:	Enable: 32 Frames 50000 Bytes
		Multicast Data:	Allow All
		Enable Extra Reporting:	Enable
		Sensitive Threshold:	Off
	<i>Advanced Ethernet Setting</i>	Enable Autonegotiation:	Enable
		Link Speed, Mbps:	100
	<i>Signal LED Thresholds</i>	Thresholds, dBm:	94 - 80 - 73 - 65

4.9. Se ingresa a la pestaña Services y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 20.

**Cuadro 20. Parámetros de configuración de la Pestaña Services**

<b>SERVICES</b>	<i>SNMP Agent</i>	Enable SNMP Agent:	Enabled
		SNMP Community:	public
		Contact:	Teleco
		Location:	UAO
	<i>SSH Server</i>	Enable SSH Server:	Enabled
		Server Port:	22
		Enable Password Authentication :	Enabled

4.10. Se ingresa a la pestaña System y se introduce los parámetros establecidos de las diferentes opciones que se muestran en la columna 3 del cuadro 21.

**Cuadro 21. Parámetros de configuración de la Pestaña System**

<b>SYSTEM</b>	<i>Device</i>	Device Name:	User Station
		Interface Language:	English
	<i>System Accounts</i>	Administrator Username:	ubnt

## 5. Instalación del software de gestión airControl de Ubiquiti Networks.

5.1. Se procede a descargar el software airControl de la página oficial de Ubiquiti Networks: <http://ubnt.com/aircontrol>.

**5.2.** Se instala en el PC que se asigna para gestión de la red teniendo en cuenta los requisitos mínimos: Java VM versión 6 o superior.

**5.3.** Si la instalación es correcta se ejecuta el navegador Web y se ingresa la dirección URL: <http://localhost:9080>. Una vez que se acceda a la aplicación debe aparecer una interfaz como se observa en la figura 7, donde se deben especificar las credenciales de administrador que por defecto son: Username: ubnt; Password: ubnt.

**Figura 7. Credenciales de administrador airControl.**



**5.4.** Si los datos de administrador son correctos aparece la interfaz principal del Aircontrol como se muestra en la figura 8. La interfaz del airControl muestra los dispositivos conectados (Status de color verde) y desconectados (Status de color rojo), muestra la dirección IP, la dirección MAC, el nivel de señal en dBm, de cada dispositivo. Si se presiona clic sobre cualquiera de los dispositivos, en la parte inferior de la interfaz muestra información detallada del dispositivo como se observa en la figura 9.

Figura 8. Interfaz principal del AirControl

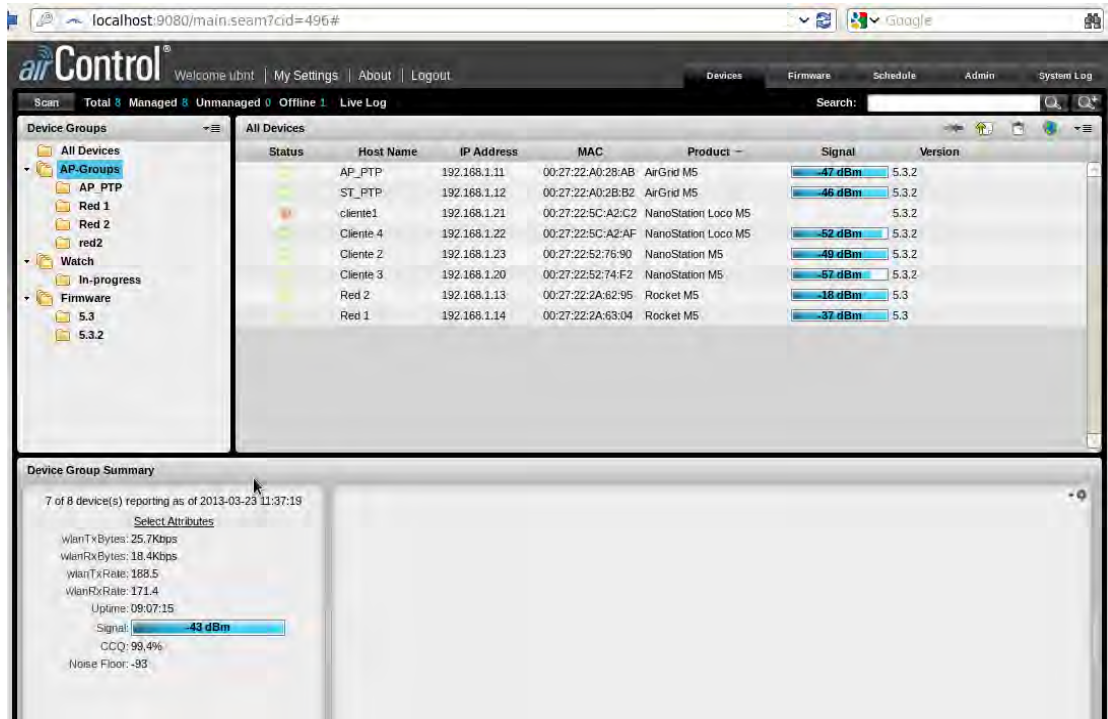
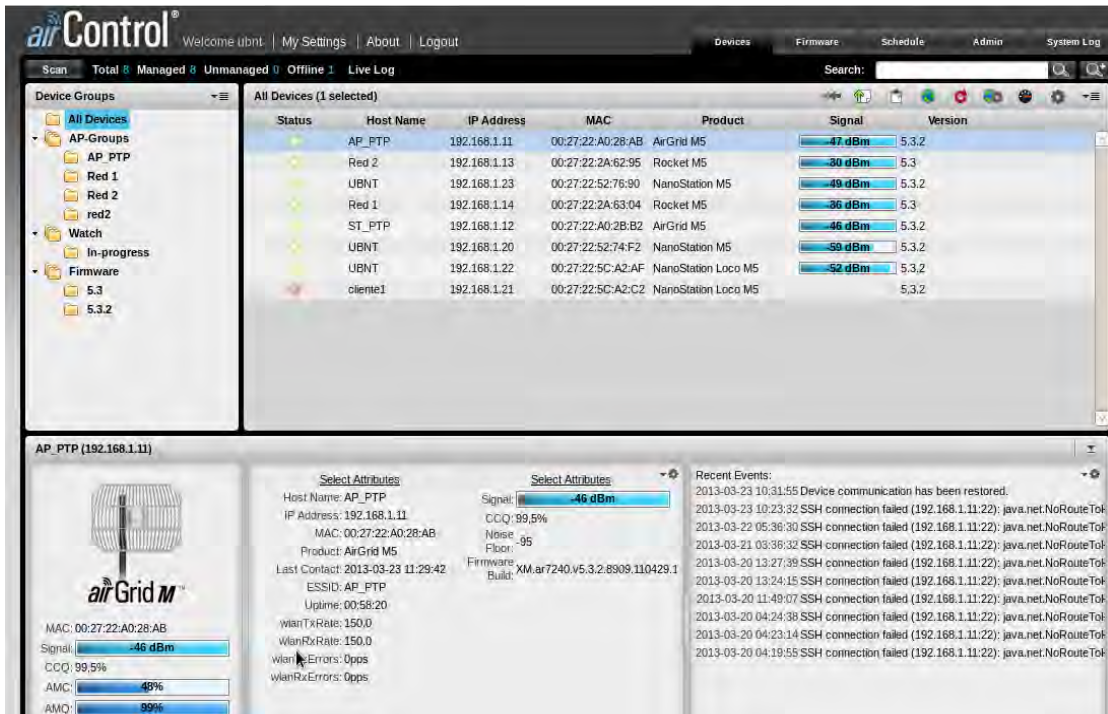
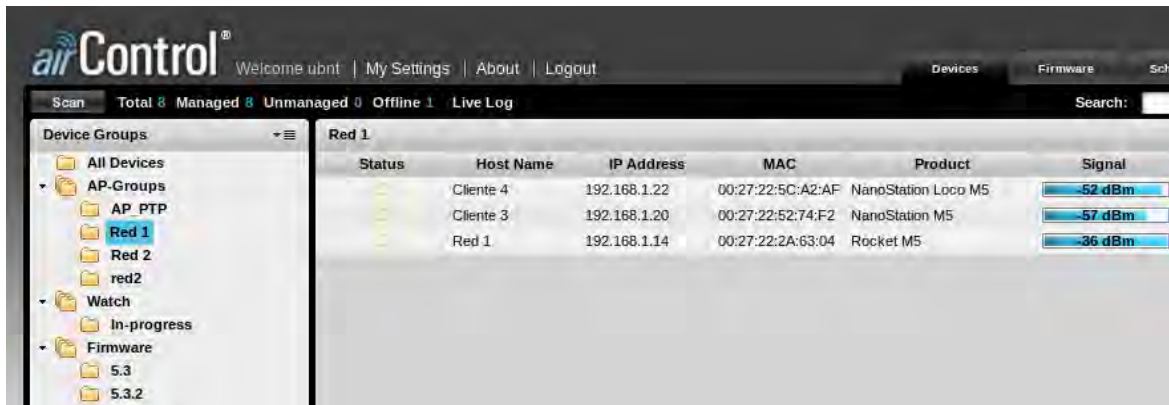


Figura 9. Información detallada de la antena



5.5. Se accede a la carpeta Red 1 de la ventana *Device Groups* ubicado en el lado izquierdo de la interfaz principal. Aquí se muestra los dispositivos que se encuentran conectados al AP. Por ejemplo en la figura 10 se muestran los dispositivos conectados al AP identificado con el SSID Red 1.

Figura 10. Información de los dispositivos conectados a la Red 1

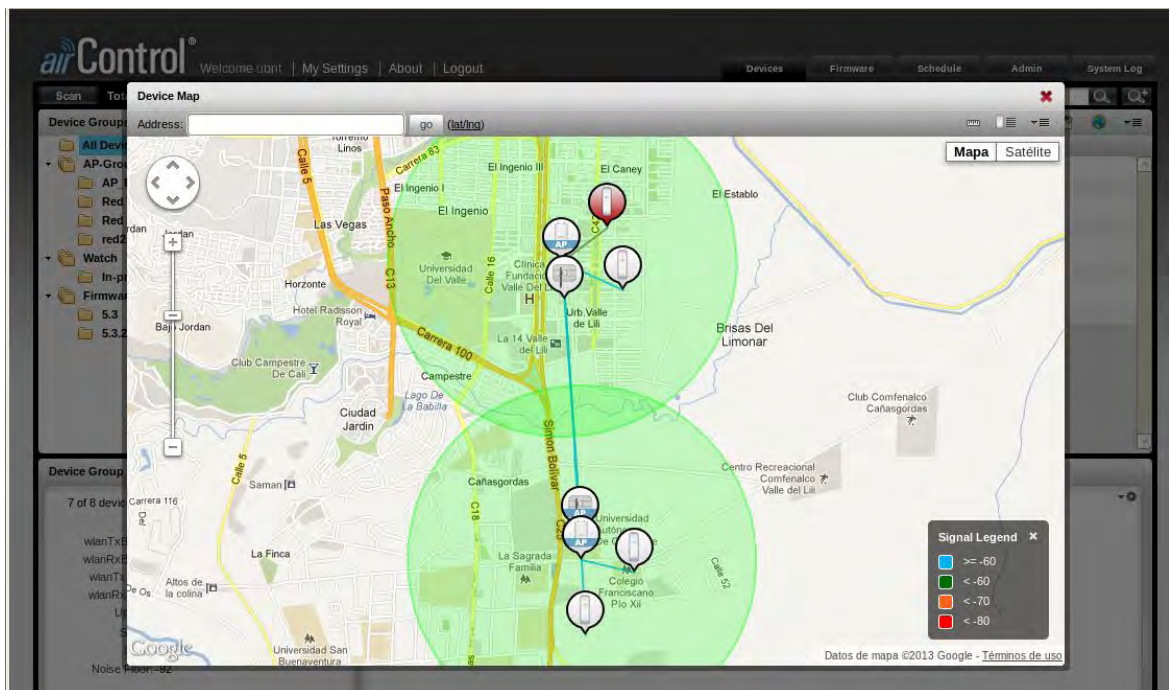


The screenshot shows the airControl web interface. On the left, a sidebar lists 'Device Groups' with 'Red 1' selected. The main area displays a table of connected devices for 'Red 1'.

Status	Host Name	IP Address	MAC	Product	Signal
Online	Cliente 4	192.168.1.22	00:27:22:5C:A2:AF	NanoStation Loco M5	52 dBm
Online	Cliente 3	192.168.1.20	00:27:22:52:74:F2	NanoStation M5	57 dBm
Online	Red 1	192.168.1.14	00:27:22:2A:63:04	Rocket M5	36 dBm

5.6. El airControl tiene una opción que permite ubicar los dispositivos en un mapa satelital, usando Google Chrome, donde cada AP muestra su área de cobertura, como se observa en la figura 11.

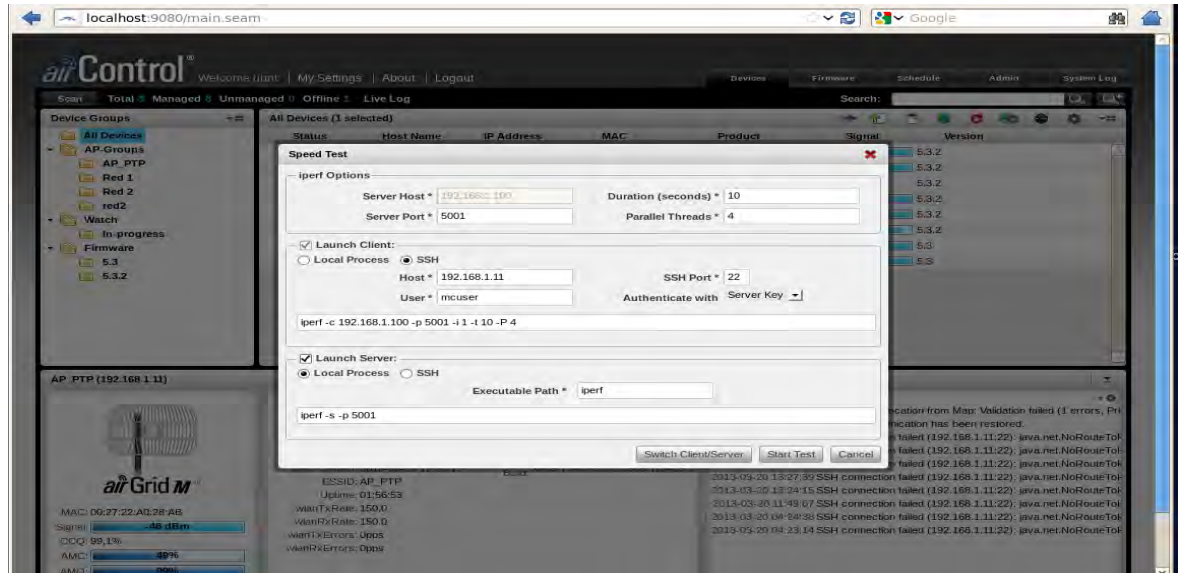
Figura 11. Mapa que muestra la ubicación geográfica de los dispositivos





5.7. El airControl también permite realizar operación de monitoreo como PING y pruebas de velocidad entre las antenas con la herramienta Speed Test, como se muestra en la figura 12.

Figura 12. Speed Test



6. **Instalación del Software VirtualBox:** Se instala el software VirtualBox en el computador con sistema operativo Centos 6, que posee dos interfaces de red. La distribución de Zeroshell y Elastix se instalan en VirtualBox como máquinas virtuales.

## 7. Configuración de Servicios de Red

Los servicios de red que se implementan en la red de núcleo del ISP son DNS, DHCP y NAT. El servicio DNS se configura directamente en el Centos 6; los servicios DHCP y NAT se configuran dentro del Zeroshell, realizando un procedimiento el cual se especifica más adelante en la configuración del Zeroshell.

Para la configuración del servidor DNS (Domain Named Service), se realiza los siguientes pasos:

7.1. Se define el nombre del dominio y de su servidor primario asociado, además de la dirección IP que va a tener el dominio. Estos parámetros se establecieron en el diseño de los servicios que componen a la red de núcleo del ISP:

Nombre del Dominio: labteleco.com

Nombre del servidor primario asociado: server.labteleco.com

Dirección IP asociado: 192.168.1.100

**7.2.** Se realiza la instalación de los paquetes requeridos para el servicio. Para ello, se ingresa al terminal del Centos 6 y se utiliza la instrucción *yum* para instalar los paquetes BIND. La instrucción *yum* permite descargar y actualizar paquetes del sistema a través de internet.

```
[root@labteleco ~]# yum -y install bind bind-libs bind-utils
```

**7.3.** Se establece el inicio del servicio BIND en el sistema de arranque ejecutando la siguiente línea:

```
[root@labteleco ~]# chkconfig --level 35 named on
```

La anterior línea indica que el servidor DNS estará disponible únicamente para los niveles de ejecución 3 y 5.

**7.4.** Se arranca el demonio del DNS para invocar el servidor de resolución de nombres para su inicio.

```
[root@labteleco ~]# service named start
```

**7.5.** Se procede a editar el archivo de configuración principal *named.conf* y se adiciona la zona principal del dominio ya estipulado.

```
[root@labteleco ~]# vi /etc/named.conf
```

Al ejecutar esta línea se presenta el siguiente código:

```
options {
#   listen-on port 53 { 127.0.0.1; };
#   listen-on-v6 port 53 { ::1; };
#   directory      "/var/named";
#   dump-file      "/var/named/data/cache_dump.db";
#   statistics-file "/var/named/data/named_stats.txt";
#   memstatistics-file "/var/named/data/named_mem_stats.txt";
#   allow-query   { localhost;192.168.1.0/24;};
#   recursion yes;

#   dnssec-enable yes;
#   dnssec-validation yes;
#   dnssec-lookaside auto;

/* Path to ISC DLV key */
#   bindkeys-file "/etc/named.iscdlv.key";

#   managed-keys-directory "/var/named/dynamic";
};

#logging {
#   channel default_debug {
#       file "data/named.run";
#       severity dynamic;
#   };
};
```

En la instrucción allow-query se escribe la dirección de red 192.168.1.0/24 de la cual hace parte el servidor DNS. Para crear la zona del dominio se ejecutan las siguientes líneas:

```
zone "." IN {
    type hint;
    file "named.ca";
};

#Dominio labteleco.com

zone "labteleco.com" IN {
    type master;
    file "labteleco.com.fwd";
    allow-update {none;};
};

#Dominio inverso labteleco.com

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "labteleco.com.rev";
    allow-update {none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Para la zona del dominio se crean la zona directa que tiene el nombre del dominio labteleco.com y la zona inversa con la IP de la red 192.168.1. La zona directa realiza la consulta de la dirección IP a partir del nombre de dominio de dicha zona; La zona inversa realiza una consulta del nombre del dominio a partir de la dirección IP, utilizando el dominio "in-addr.arpa". En cada una de las zonas se establece el tipo y el archivo donde se encuentra los parámetros de la respectiva zona; para la zona directa el tipo es master y el archivo tiene por nombre labteleco.com.fwd, para la zona inversa el tipo es master y el archivo tiene por nombre labteleco.com.rev. Los archivos labteleco.com.fwd y labteleco.com.rev se encuentran en el directorio /var/named.

**7.6.** Se crean los archivos de la zona los cuales fueron mencionados en el archivo named.conf, es decir, la zona directa y la zona inversa. Para este caso, se comienza con la zona directa, creando el archivo con la siguiente línea:

```
[root@labteleco ~]# vi /var/named/labteleco.com.fwd
```

El archivo, como se mencionó anteriormente, estará ubicado en el directorio /var/named. Al abrir el archivo se introduce el siguiente código:

```

$ttl 38400
@      IN      SOA    labteleco.com.  server.labteleco.com (
                          1347662705
                          10800
                          3600
                          604800
                          38400 )

@      IN      NS     labteleco.com.
@      IN      A      192.168.1.100
server IN      A      192.168.1.100
www    IN      A      192.168.1.100

```

En el código se introduce los parámetros correspondientes a la zona directa, en donde se encuentra el registro de los recursos como el inicio de la autoridad SOA, el servidor de nombres NS y la dirección A. El registro tipo SOA indica el inicio de los datos de la zona y define los parámetros que afectan a todos los registros; para este caso se estipula el dominio labteleco.com y el nombre del servidor server.labteleco.com. El registro tipo A convierte un nombre de dominio en una dirección IP, que en este caso, se convierte [www.labteleco.com](http://www.labteleco.com) a la dirección IP 192.168.1.100 y que de la misma forma sucede con server.labteleco.com. El registro tipo NS identifica el servidor de nombres para el dominio, que en este caso es labteleco.com.

**7.7.** En la zona inversa se crea el archivo con las siguientes líneas:

```
[root@labteleco ~]# vi /var/named/labteleco.com.rev
```

El archivo, como se mencionó anteriormente, estará ubicado en el directorio /var/named. Al abrir el archivo se introduce el siguiente código:

```

$ttl 38400
@      IN      SOA    labteleco.com.  server.labteleco.com (
                          1347662705
                          10800
                          3600
                          604800
                          38400 )

@      IN      NS     labteleco.com.
100    IN      PTR    labteleco.com.
100    IN      PTR    server.labteleco.com.

```

En el código se introduce los parámetros correspondientes a la zona inversa, en donde se encuentra el registro de los recursos como el inicio de la autoridad SOA y el servidor de nombres NS como se explicó en el archivo de la zona directa. La diferencia es que ahora se introduce el registro tipo PTR en vez del registro tipo A. El registro tipo PTR es un puntero que convierte una dirección IP a un nombre de dominio, es decir, realiza lo contrario al registro tipo A; en este caso, se realiza la conversión de la dirección IP 192.168.1.100 al nombre labteleco.com y

server.labteleco.com; el 100 que se encuentra al lado izquierdo hace referencia a la dirección IP.

**7.8.** Se resetea el servicio BIND con la siguiente línea: services named restart

**7.9.** Se asegura que el archivo /etc/resolve.conf contenga la IP del servidor DNS que ha sido levantado.

```
search labteleco.com
nameserver 192.168.1.100
```

## 8. Configuración de la distribución Zeroshell

Hasta aquí ya se tiene la red inalámbrica funcionando junto a su software de gestión de red, se procede ahora a mostrar los pasos de la configuración del Zeroshell, que es el software de administración de red.

**8.1.** Al momento de iniciar Zeroshell viene configurado con una IP por defecto que es la 192.168.0.75. La pantalla inicial que se observa de Zeroshell después de su instalación es la que se observa en la figura 12.

**Figura 12. Interfaz principal del Zeroshell**

```
Z e r o S h e l l - N e t S e r v i c e s  2.0.RC2           March 09, 2013 - 22:53
-----
Hostname : zeroshell.example.com
CPU (1)  : Intel(R) Pentium(R) Dual CPU E2160 @ 1.80GHz 1794MHz
Kernel   : 3.4.19-ZS
Memory   : 252404 kB                                     http://192.168.0.75
Uptime   : 0 days, 1:49                                 User      : admin
Load     : 0.00 0.01 0.05                               Password  : zeroshell
Profile  : Temporary EXAMPLE.COM configuration
-----
COMMAND MENU
<A> Activate Profile          <P> Change admin password
<D> Deactivate Profile       <T> Show Routing Table
<S> Shell Prompt             <F> Show Firewall Rules
<R> Reboot                   <N> Show Network Interface
<H> Shutdown                 <Z> Fail-Safe Mode
<B> Create a Bridge          <I> IP Manager
<W> WiFi Manager

                                     Select: _
```

**8.2.** Se presiona la letra I para cambiar la anterior dirección IP por una dirección que quede en red con la red local que se está manejando (en este caso la red local es 192.168.1.0). Se obtiene las opciones que se observan en la figura 13, con los cuales se pueden ajustar los parámetros de red.

**Figura 13. Modificación de parámetros de red**

```
-----  
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)  
Status: 100Mb/s Full Duplex  
(1) 192.168.0.75 / 255.255.255.0 (up)  
-----  
ETH01 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)  
Status: 100Mb/s Full Duplex  
-----  
Default Gateway: none  
COMMANDS  
<A> Add IP address           <D> Delete IP address  
<M> Modify IP address       <G> Set Default Gateway  
<S> Change Interface status <H> Dynamic IP configuration  
<I> Show Info               <Q> Quit  
>> _
```

**8.3.** Por ahora solo interesa cambiar la dirección IP del servidor Zeroshell, por lo tanto se presiona la letra M que permite tener la opción de modificar la dirección IP. En la figura 14 se observa que se cambia la dirección IP 192.168.0.75 por la dirección 192.168.1.60.

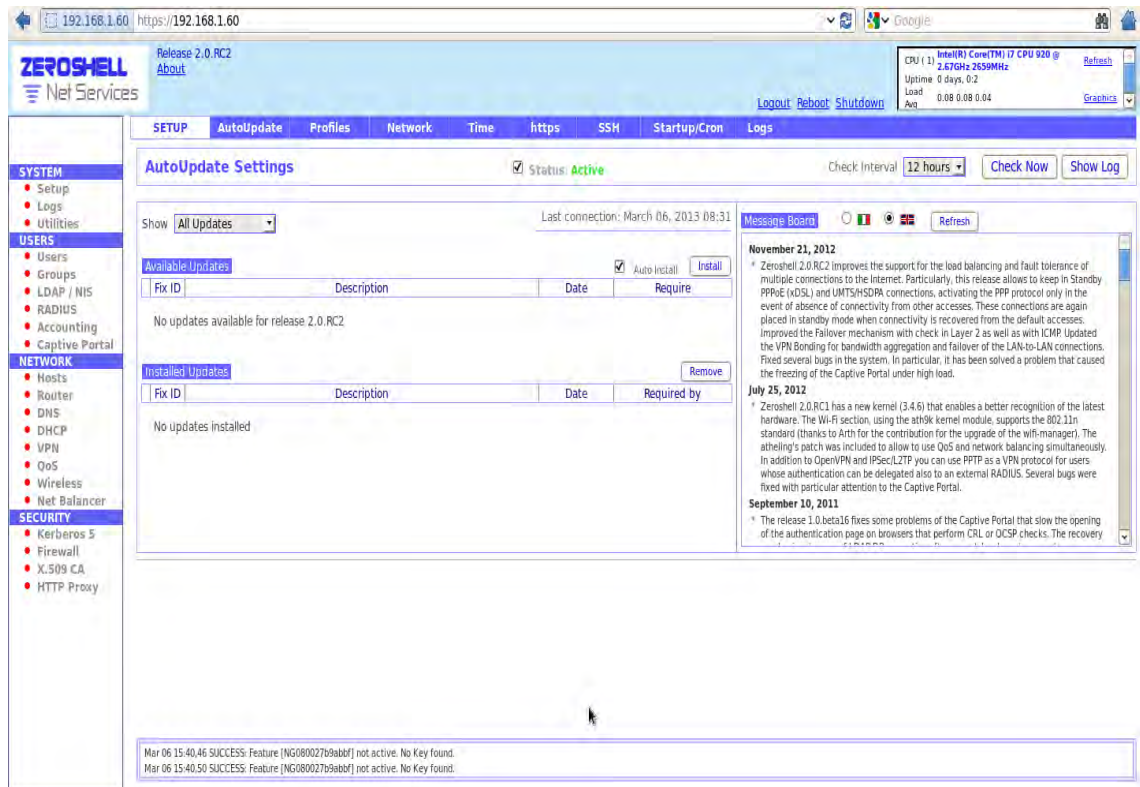
**Figura 14. Modificación de dirección IP**

```
-----  
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)  
Status: 100Mb/s Full Duplex  
(1) 192.168.0.75 / 255.255.255.0 (up)  
-----  
ETH01 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)  
Status: 100Mb/s Full Duplex  
-----  
Default Gateway: none  
COMMANDS  
<A> Add IP address           <D> Delete IP address  
<M> Modify IP address       <G> Set Default Gateway  
<S> Change Interface status <H> Dynamic IP configuration  
<I> Show Info               <Q> Quit  
>> m  
  
Interface [ETH00]:  
-----  
ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 40)  
Status: 100Mb/s Full Duplex  
(1) 192.168.0.75 / 255.255.255.0 (up)  
-----  
IP to modify [1]:  
IP [192.168.0.75]: 192.168.1.60  
Netmask [255.255.255.0]:  
IP status [up]:
```

**8.4.** Se accede a la interfaz web de administración del Zeroshell desde el navegador de internet que presenta el PC que administra la red, ingresando la dirección IP 192.168.1.60 como URL.

El username y el password de acceso son *admin* y *zeroshell* respectivamente, valores que ya vienen por defecto pero si se quiere se pueden cambiar. La interfaz web se observa en la figura 15. Esta interfaz permite realizar diferentes configuraciones de una manera más amigable y más fácil que la administración por línea de comandos.

**Figura 15. Interfaz principal del Zeroshell**



**8.5.** Se crea un perfil para que todas las configuraciones que se realicen queden guardadas en una base de datos y no se borren cuando se apague o se reinicie el servidor Zeroshell:

**8.5.1.** Se debe crear una partición en el disco duro para almacenar el perfil y todas las configuraciones que se hagan; se selecciona del menú izquierdo de la interfaz principal del Zeroshell, Setup y del menú superior se elige Profiles; se marca la etiqueta Disk model: ATA VBOX HARDDISK (sda) y se elige New Partition. Este procedimiento se observa en la figura 16.

**8.5.2.** Se accede a la ventana de creación de partición en el disco duro, donde va a quedar almacenada toda la configuración. El formato de la partición será Extended 4 y el tamaño Max Available (Máximo disponible), que son opciones por defecto, como se visualiza en la figura 17.

Figura 16. Creación de la partición y el perfil

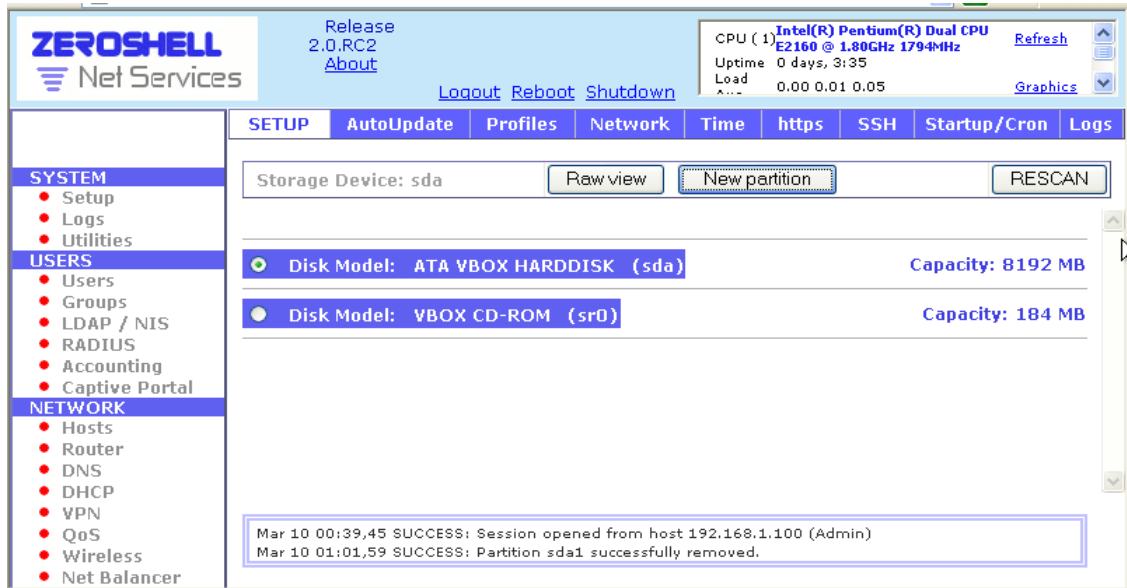
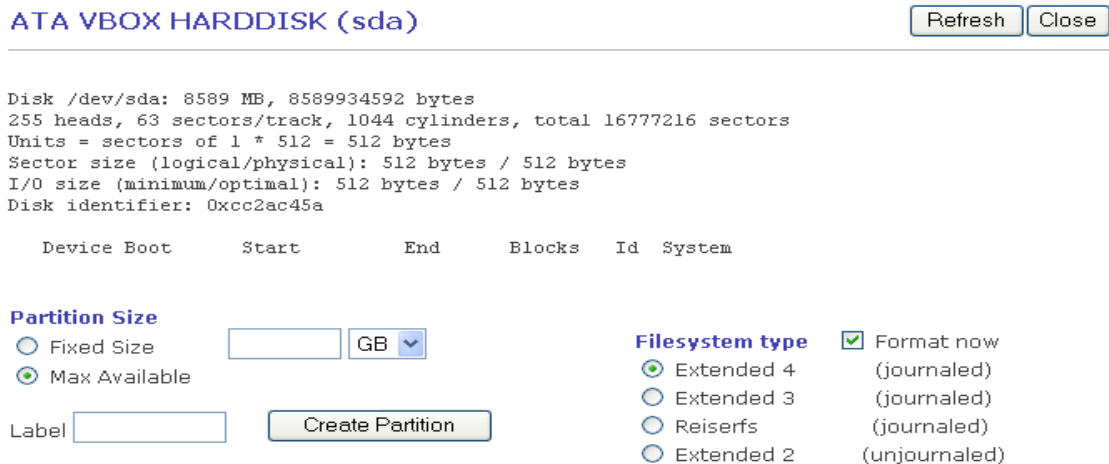


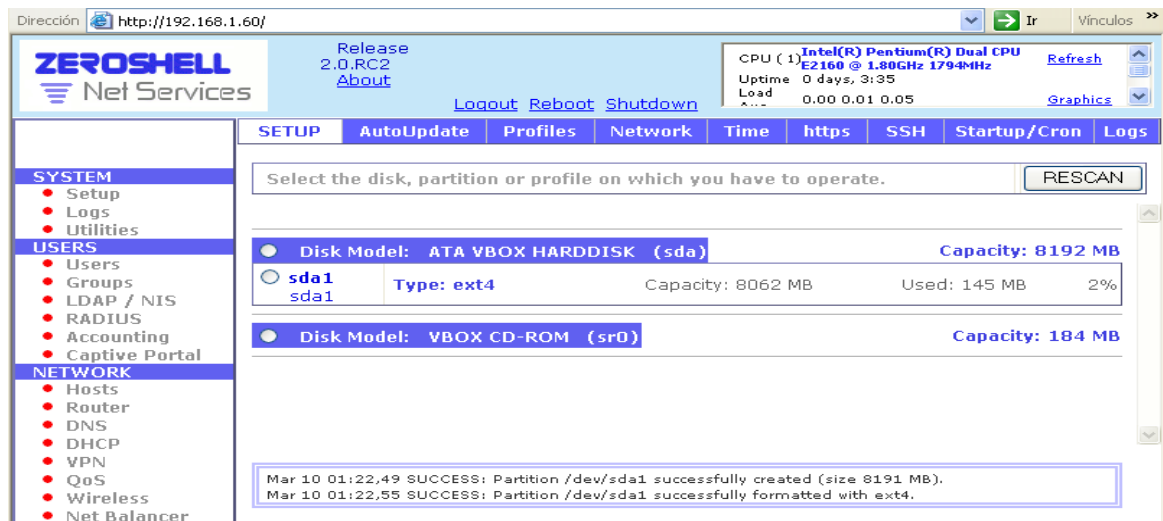
Figura 17. Creación de la partición



Una vez creada la partición, aparecerá la página *Profiles* con la nueva partición creada como se muestra en la figura 18.

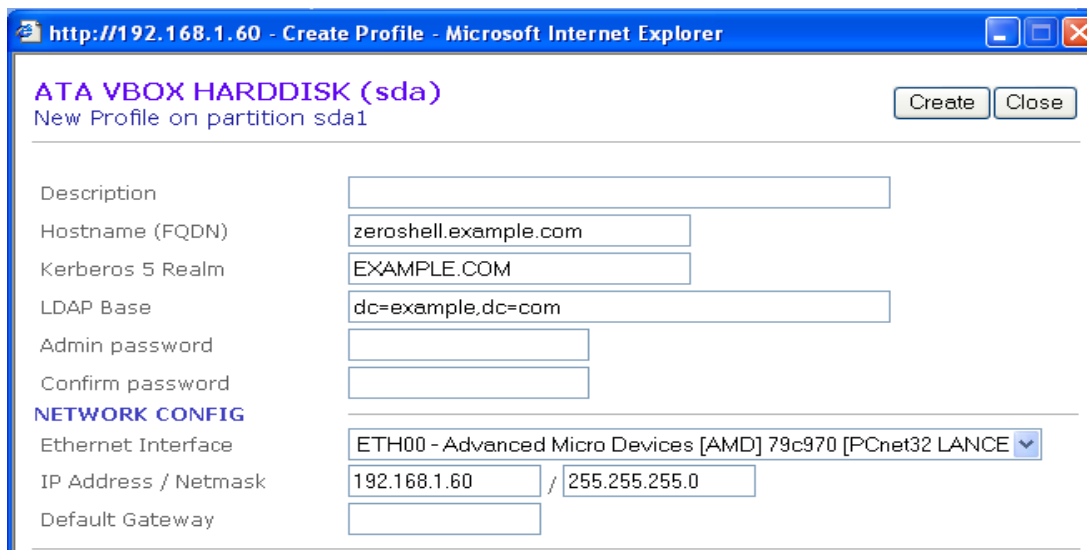


Figura 18. Página Profiles con la nueva partición creada.



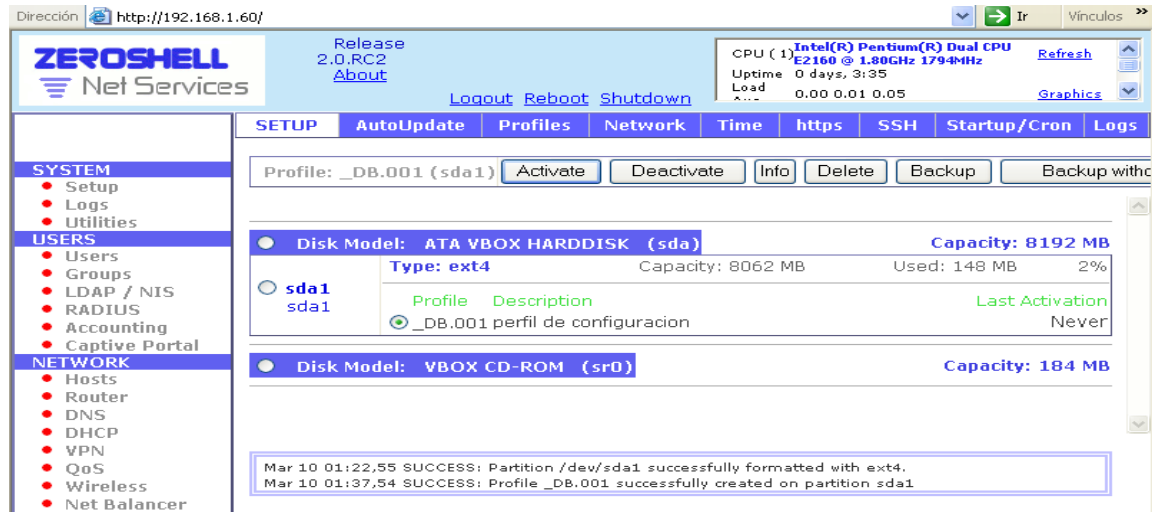
8.5.3. Para crear el perfil se selecciona la partición creada (sda1) y aparece un menú donde se debe seleccionar *Create Profile*, con lo cual aparece una ventana donde se debe suministrar unos datos necesarios como se muestra en la figura 19. Aquí se puede cambiar la contraseña de administrador del servidor Zeroshell.

Figura 19. Creación del perfil



8.5.4. Se ingresa los datos necesarios y se pulsa *Create* en la parte superior derecha. Se selecciona el perfil *\_DB.001* y se presiona *Activate* para que el perfil quede activo y funcionando como se observa en la figura 20.

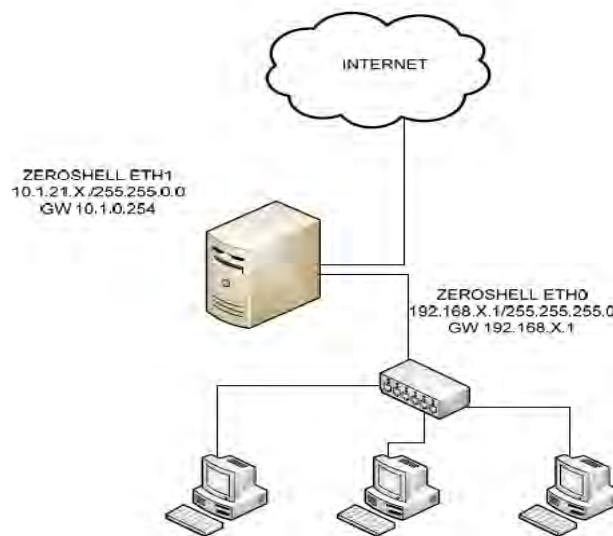
Figura 20. Activación del perfil.



Cuando se activa el perfil el sistema se reinicia con la configuración que se ha creado.

8.6. Se realiza la configuración de red como se muestra en la figura 21.

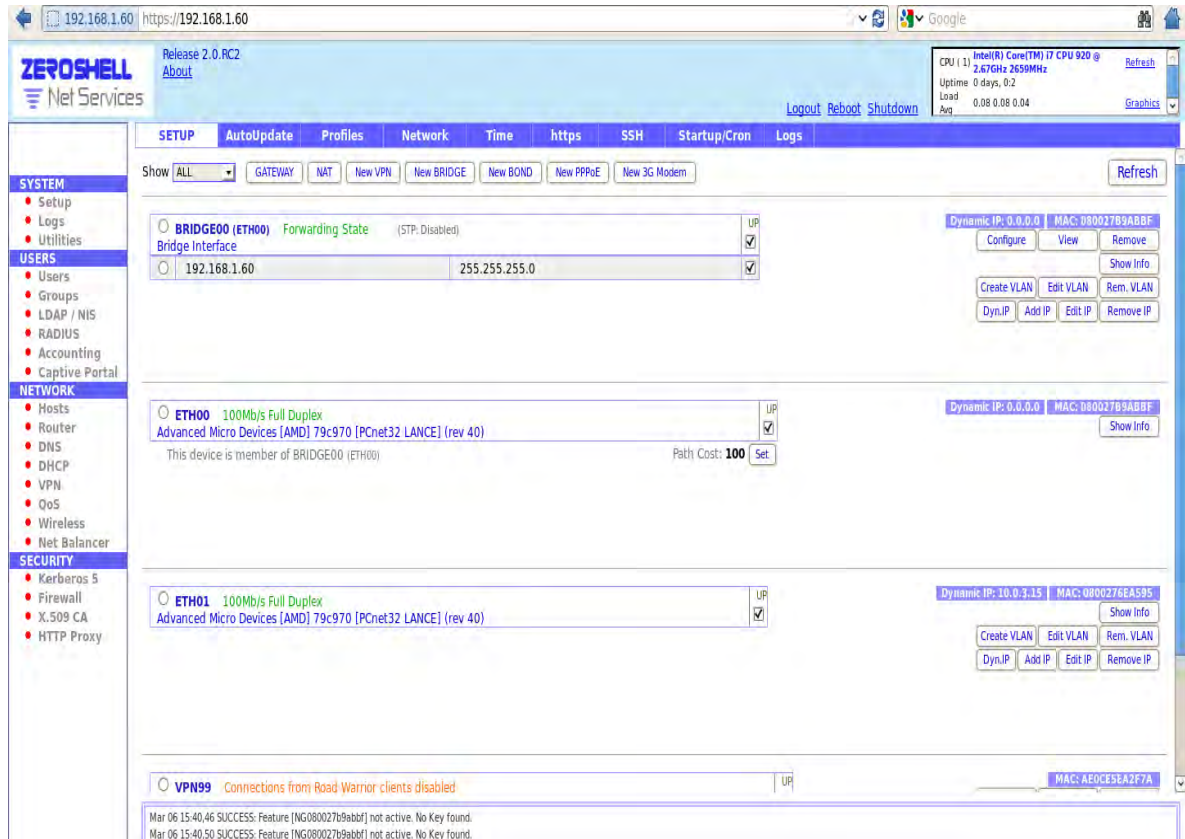
Figura 21. Esquema de red para el Zeroshell.



8.6.1. Se necesita activar dos interfaces de red, una que tenga salida a internet y otra con una dirección IP que conecte la red local. Para ello se ingresa a *Setup* y posteriormente en el menú superior se elige *Network*. Como se observa en la figura 22, ETH00 tiene configurada una dirección IP estática: 192.168.1.60, que es la que se comunica con la red local que se está manejando. Y ETH01 es la

interfaz que da salida a internet, se configura con DHCP y toma la dirección IP dinámica 10.0.3.15.

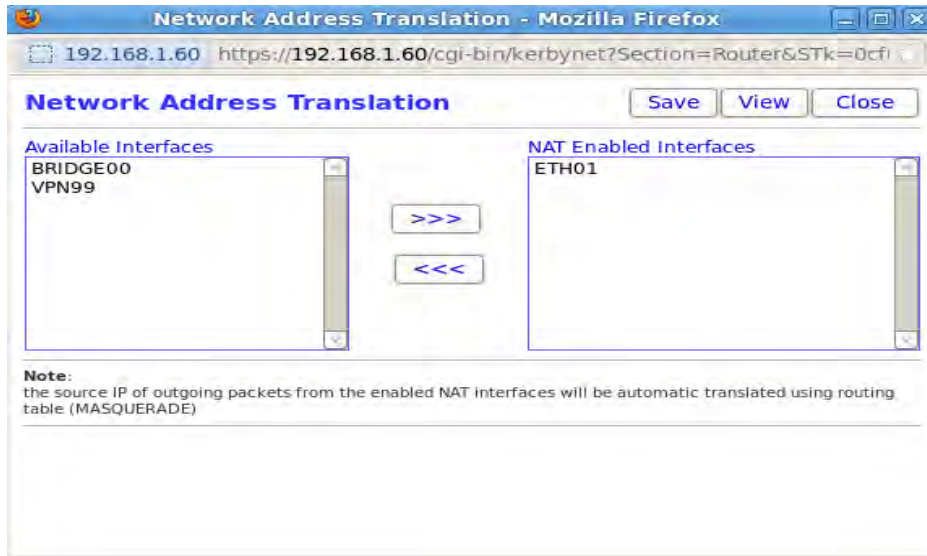
Figura 22. Network



**8.7. Configuración Servicio NAT:** Posteriormente en el menú del lado izquierdo de la interfaz principal del Zeroshell (figura 15) se accede a la configuración del *Router* para permitir darle salida de internet realizando NAT (Traducción de direcciones) entre la red interna y la red externa. Para configurar el servicio de NAT se ingresa en la parte superior al menú *NAT* donde aparece una pantalla que indica las interfaces de red del sistema; se selecciona la interface *ETH01* y se pasa a la ventana *NAT Enable Interfaces*, como se observa en la figura 23. Se guardan los cambios y se comprueba que desde la red local se pueda acceder a algún sitio de internet.

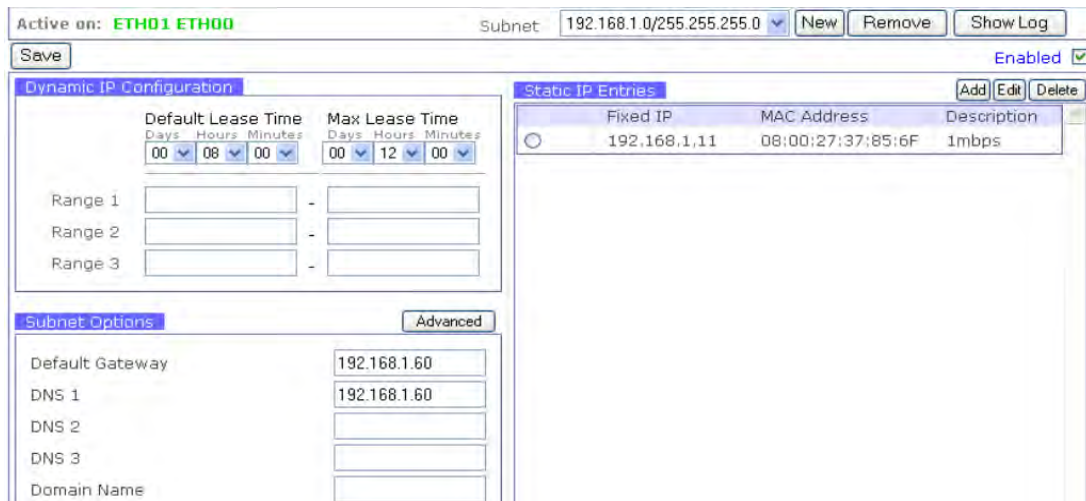
Hay que tener en cuenta que NAT utiliza IP Masquerade que es una técnica de traducción de muchos host a uno, es decir que permite a muchas direcciones IP privadas compartir simultáneamente una dirección IP pública.

Figura 23. NAT



**8.8.** Configuración servicio DHCP: Se accede al menú DHCP ubicado en la parte izquierda de la interfaz principal del Zeroshell. Se abre una ventana como se observa en la figura 24. En la parte derecha donde se encuentra la etiqueta “Static IP Entries”, se presiona el botón Add para ingresar la dirección MAC del equipo del usuario y la dirección IP que obtendrá este último. En Description se puede especificar el nombre del plan de ancho de banda que se le asigna al usuario. Se guardan los cambios y se prueba que esté funcionando el servicio DHCP.

Figura 24. Configuración DHCP



**8.9.** Creación de Usuarios: Para la creación de usuarios que van a ser los respectivos clientes del ISP se accede al menú izquierdo de la interfaz principal de

Zeroshell y se selecciona *Users*, como se muestra en la figura 25; en el menú superior se ingresa a *Add* para introducir los datos del usuario que se va a crear.

**Figura 25. Creación de Usuarios**

The screenshot shows the Zeroshell Net Services interface. The top navigation bar includes 'Logout', 'Reboot', and 'Shutdown'. The main menu on the left lists various system and network services. The 'USERS' section is active, showing a table of users:

Username	Group	Description	E-mail
admin	nobody	System Administrator	admin.labteleco@hotmail.com
falcao9	Dobleplay 1 Mega	Mac:00002211	rada9@madrid.com
jhorman.villanueva	Dobleplay 2 Megas	Mac:00:27:25:AF	jhorvi@hotmail.com
jona.delgado@hotmail.com	Dobleplay 1 Mega	Mac:00:27:25:AF	jona.delgado@hotmail.com
luis.villa	Dobleplay 1 Mega	Mac:00:27:25:AF	luis_villa@hotmail.com
Papo	Dobleplay 2 Megas	Mac:00:27:28:AB	papo@gmail.com
paulo17	Dobleplay 2 Megas	Mac:00:24:15:BC	paul17@america.com

**8.9.1.** Aparece un formulario como se observa en la figura 26 donde se introduce información importante del usuario como su nombre, apellido, número de identificación, correo electrónico, teléfono de ubicación.

**Figura 26. Formulario para la creación de un Usuario.**

The screenshot shows the 'Add' user form in Zeroshell. The form is titled 'Mac:00:27:25:AF (luis.villa)'. It contains the following sections:

- Account Information:** Username (luis.villa), UID (1130598323), Primary Group (Dobleplay 1 Mega), and GID (65535).
- User Information:** Firstname (Luis), Lastname (Villa), Organization (Calle 3B No 96-64), Description (Mac:00:27:25:AF), E-Mail (luis\_villa@hotmail.com), and Phone (4401020).
- RADIUS Accounting:** Expiration (04/05/2013), Accounting Class (FACTURACION), Credit (0.00 \$), Limits (-MB -h -Mb/s), Costs (0.00\$/MB 0.00\$/h), Password (masked), Authentication Protocol (Kerberos 5 and RADIUS (VLAN) checked).

Además de esto el formulario pide la creación de un *username* y *password* que sirven al usuario para autenticarse y poder hacer uso del servicio de internet; se escoge el grupo al cual va a pertenecer el usuario, es decir si va estar en los que solicitaron un ancho de banda de 1 Mbps o en los que solicitaron un ancho de banda de 2 Mbps, y se escoge el tipo de contabilización que se usa para la posterior facturación de los usuarios.

Se configura la fecha de corte de los servicios suministrados por el ISP, que en este caso son los primeros cinco días de cada mes y que deben actualizarse manualmente por el administrador del Zeroshell. Como protocolos de autenticación se seleccionan Kerberos 5 y Radius, protocolos que ya vienen seleccionados por defecto.

El formulario permite agregar información adicional en el campo *Description*, donde se puede ingresar la dirección MAC de la antena que le da la conexión inalámbrica al usuario, esto con el hecho de tener información de gestión y control por si el usuario reporta fallas en la prestación de los servicios por parte del ISP.

Para este diseño, los datos de los cuatro clientes que reciben el servicio por parte del ISP y que son introducidos a la base de datos del ZeroShell se muestran en el cuadro 5. A cada cliente se le crea un perfil de usuario con sus respectivos datos.

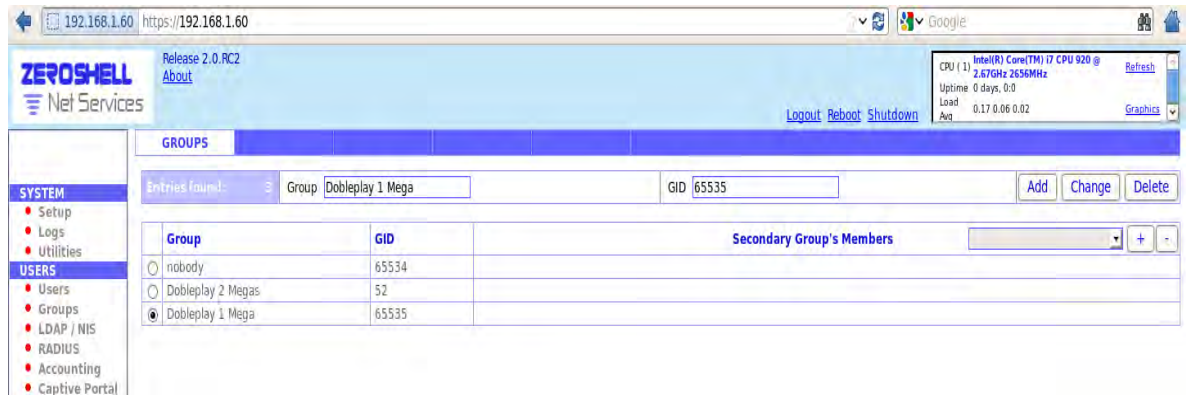
**Cuadro 14. Información de los Usuarios que adquieren los servicios del ISP**

	<b>Ciente 1</b>	<b>Ciente 2</b>	<b>Ciente 3</b>	<b>Ciente 4</b>
<b>Nombre</b>	Luis	Jhorman	Paulo	Jonathan
<b>Apellido</b>	Villa	Villanueva	Libreros	Delgado
<b>Dirección</b>	Calle 3B N° 96-64	Calle 4A N° 66-64	Av. 4N N° 35-46	Av. 4N N° 45-12
<b>Teléfono</b>	4401020	4402030	3305060	3307080
<b>E-Mail</b>	luis.villa@ hotmail.com	jhorvi@ hotmail.com	paulo.lib@ hotmail.com	<a href="mailto:jona.delgado@hotmail.com">jona.delgado@ hotmail.com</a>
<b>Nombre de Usuario</b>	luis.villa	jhorman.villanueva	paulo.libreros	jona.delgado
<b>CC</b>	1130598323	1131123478	1130984213	1130341234
<b>Passwd</b>	98323	23478	84213	41234

**8.10. Creación de grupo de Usuarios:** En el menú del lado izquierdo de la interfaz principal del Zeroshell (figura 15) se accede a *Groups* para obtener la interfaz de creación del grupo. En *Group* se ingresa el nombre que se le quiere dar al grupo y *GID* es el número de identificación del grupo; cuando se ingresan los respectivos

datos se presiona *Add* para finalizar la creación del grupo. En la figura 27 se observan dos grupos creados: Dobleplay 2 Megas y Dobleplay 1 Mega.

**Figura 27. Creación de los grupos de Usuarios.**



**8.11. Creación de la clase de contabilización:** En el menú del lado izquierdo de la interfaz principal del Zeroshell se accede a *Accounting* que presenta el consumo de los recursos de red por parte de los usuarios, como se visualiza en la figura 28. Se observa información como el tráfico descargado, el total de tiempo que ha estado conectado e información como costo y crédito si la cuenta que maneja el usuario es prepago y se le está cobrando por el tiempo que permanezca conectado o por la cantidad de tráfico descargado. Para esta ISP se maneja el tipo de cuenta Postpago, por ende estos valores (tráfico, tiempo, costo crédito) no importan mucho al administrador del Zeroshell.

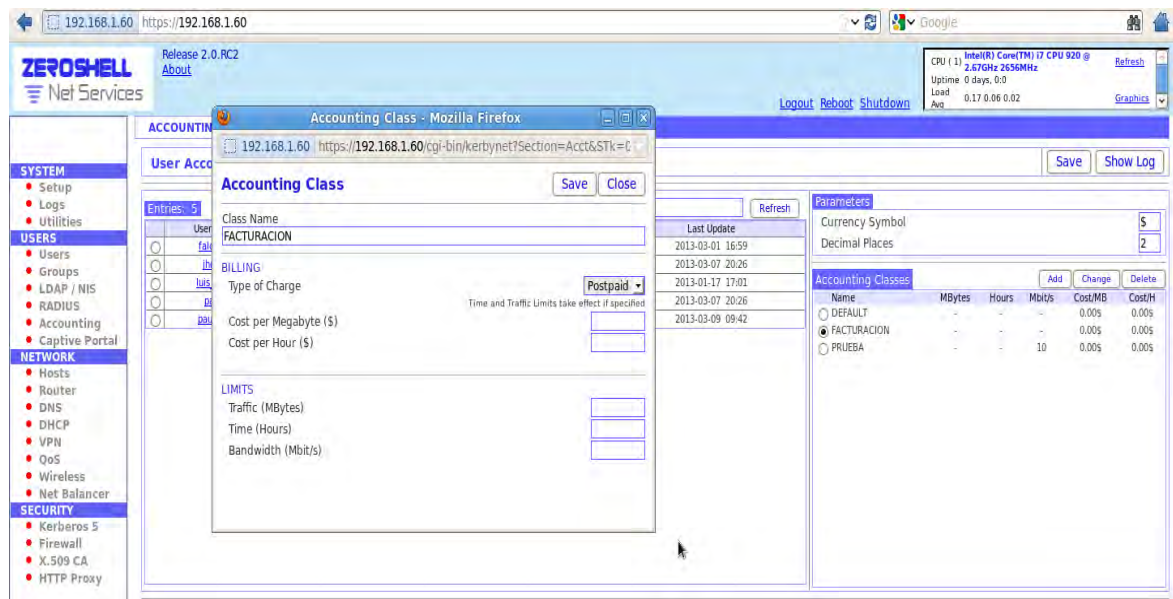
**Figura 28. Creación de la clase de contabilización.**



**8.11.1.** Para la creación de la clase de contabilización, se accede a la parte derecha a la sección de *Accounting Classes* y se presiona *Add*; sale una ventana como se observa en la figura 29 que solicita información como el nombre de la clase, para este caso se dio el nombre de FACTURACION, y el tipo de cuenta,

que la que se utiliza para el ISP es Postpago (Postpaid). Los otros campos como Costo por Megabyte y Costo por Hora se dejan vacíos ya que éstos se utilizan para el tipo de cuenta Prepago. La otra opción que se puede configurar son los límites de Tráfico, tiempo y ancho de banda; si a un determinado usuario se le especifica un límite de tráfico, cuando llegue a ese límite automáticamente se le suspende el servicio de internet. Estos valores no son necesarios para este ISP ya que el servicio de internet que se presta es ilimitado.

**Figura 29. Clase de cuenta**



**8.12. Creación del portal cautivo:** Se accede en el menú del lado izquierdo a *Captive Portal* donde muestra una interfaz como se observa en la figura 30.

**8.12.1.** En *Gateway* (menú superior) se activa la casilla donde dice *GW*, se selecciona la interface *ETH00*, que es la interface que conecta la red local y donde se quiere aplicar el portal cautivo. Se presiona *Save* para guardar los cambios realizados y de esta forma ya se tiene el portal cautivo configurado. Al activar el portal cautivo automáticamente se activa el servidor *Radius*, que es quien hace la autenticación de los usuarios. Cada vez que un usuario de la red local entre a un navegador se presenta una página de autenticación obligatoria como se observa en la figura 31, donde el usuario debe ingresar sus *Username* y *Password* para usar el servicio de internet.

**8.12.2.** Si la autenticación es correcta se podrá ver la ventana *popup* (ventana emergente), como se presenta en la figura 32, que muestra tiempo de conexión, cantidad de tráfico descargado y costo. Mientras esta ventana no se cierre el usuario podrá utilizar el servicio de internet.



Figura 30. Creación del Portal Cautivo.

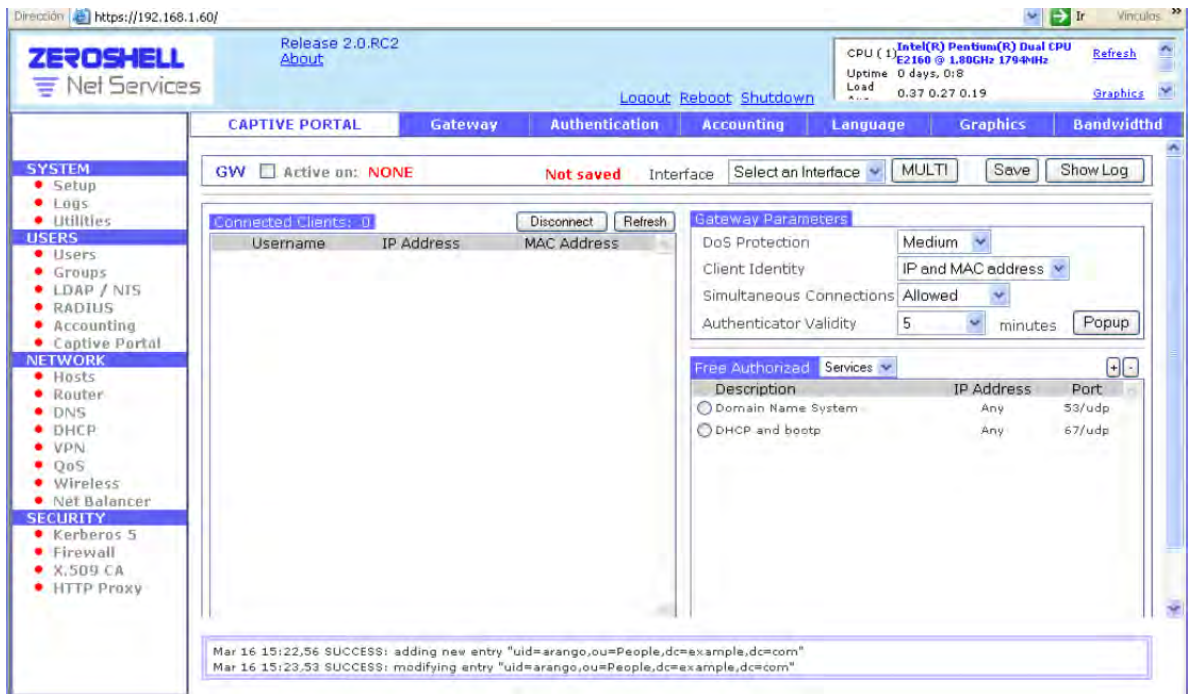


Figura 31. Pagina de autenticación.

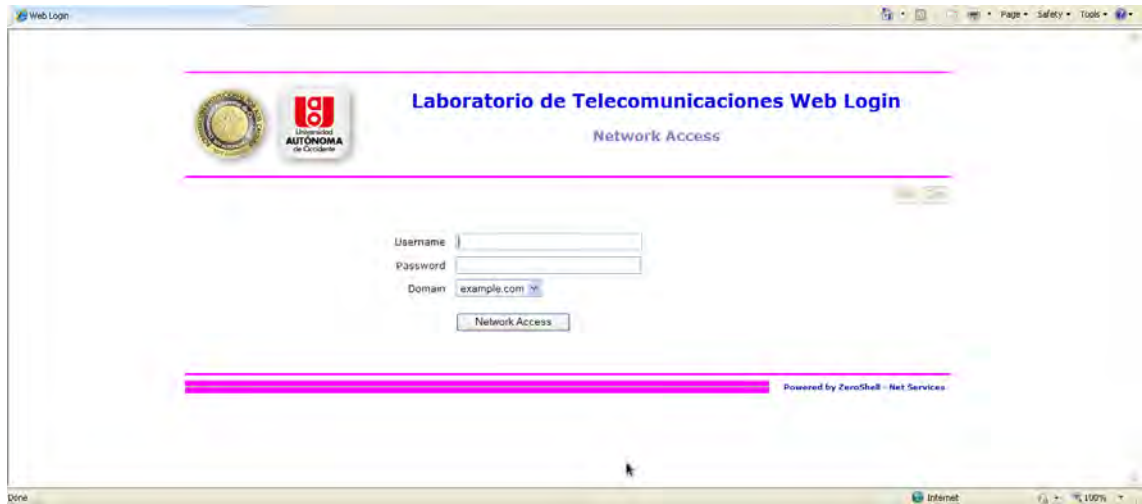
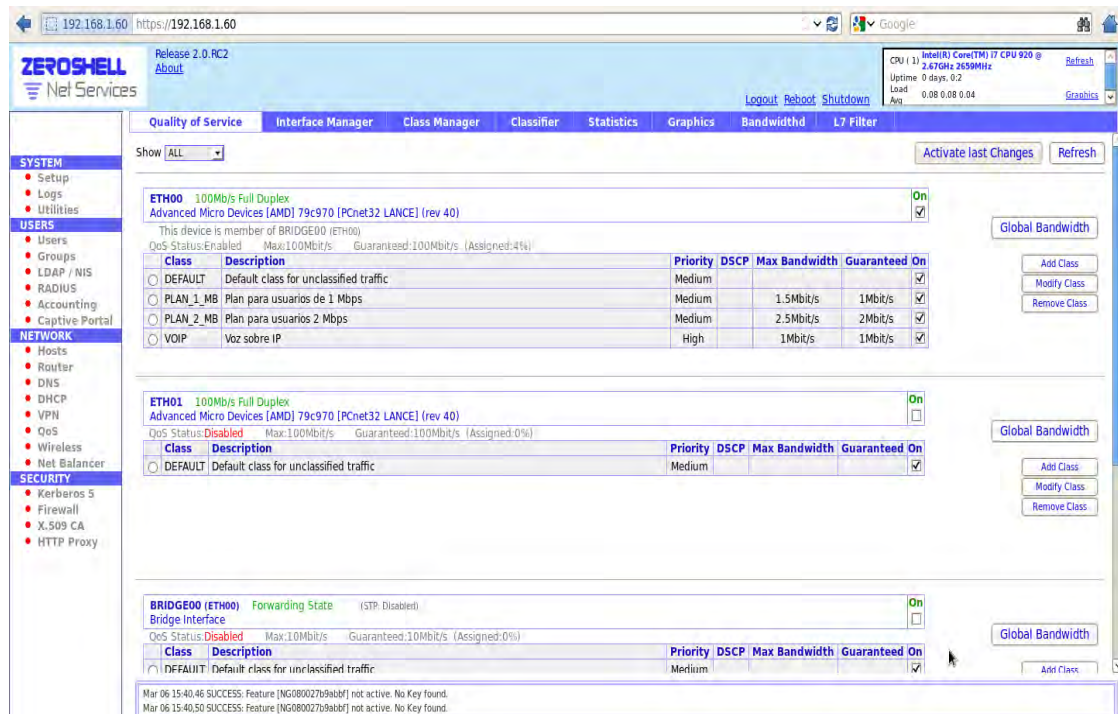


Figura 32. Ventana emergente que muestra datos sobre la conexión.



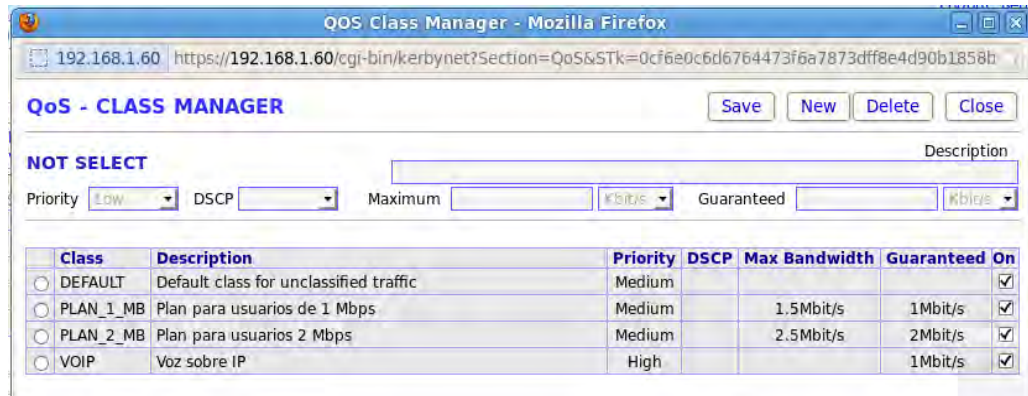
**8.13. QoS:** se accede a QoS en el menú del lazo izquierdo de la interfaz principal del Zeroshell; esta opción permite realizar QoS (Quality of Service) y gestión de ancho de banda en el tráfico de red que lo atraviesa. Es aquí donde se configura los diferentes planes de anchos de banda que el ISP va proveer a los diferentes usuarios. Para esto es necesario crear un cierto número de tipos de tráfico, con un respectivo rango de IP, a los que se les asignan los parámetros de calidad de servicio, prioridad, ancho de banda mínimo garantizado en caso de congestión de la red y el máximo ancho de banda cuando la red no esté congestionada.

Figura 33. Interfaz QoS



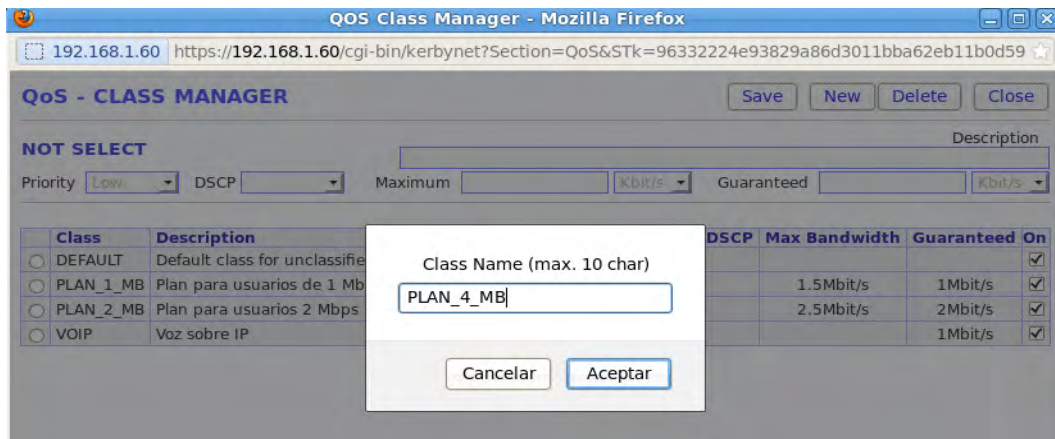
8.13.1. Se crean las diferentes clases de QoS ingresando en *Class Manager* que se encuentra en la parte superior del menú *QoS* (figura 33); al ingresar a *Class Manager* aparece una ventana como la que se observa en la figura 34.

Figura 34. Class Manager de la interfaz QoS



Para crear una nueva clase se presiona el botón *New* y aparece una ventana solicitando el nombre de la clase como se muestra en la figura 35; para este caso se dio el nombre de *PLAN\_4\_MB*.

Figura 35. Nombre de la clase que se va a crear



8.13.2. Al presionar aceptar se procede a llenar los datos adicionales como se observa en la figura 36. *Maximum* es el ancho de banda máximo que se puede alcanzar cuando no hay congestión y *Guaranteed* es el ancho de banda garantizado cuando la red se encuentra congestionada.

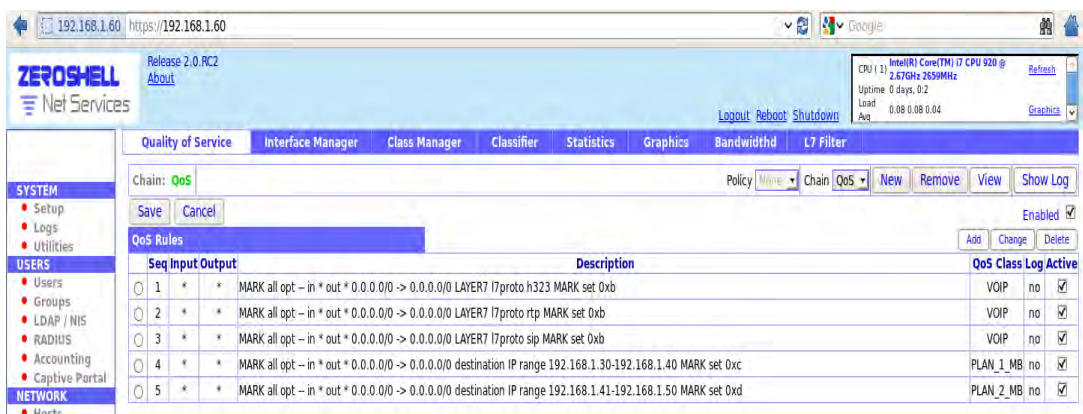
**Figura 36. Datos que se ingresan para la creación la clase**



Hasta ahora se han creado las diferentes clases de QoS, pero todavía no se ha especificado a que rango de IPs se desea aplicar la gestión del ancho de banda.

**8.13.3.** Se ingresa a la opción *Classifier* de la misma interfaz del QoS (figura 33) y se obtiene la ventana que se muestra en la figura 37. Se presiona el botón Add para insertar la regla que permita limitar el ancho de banda para un rango determinado de IP. En la ventana que aparece como se observa en la figura 38, en la sección de *Destination IP* se coloca el rango de IP al cual se le quiere limitar el ancho de banda. En la parte inferior en *TARGET CLASS* se escoge la clase de QoS, que ya trae configurado el valor de ancho de banda, en este caso de 1 Mbps. Se presiona *confirm* y posteriormente *Save* y de esta forma se tiene la regla QoS configurada. Se debe verificar que la regla quede activa.

**Figura 37. Classifier de la interfaz QoS.**



Se realiza la misma configuración anterior para los otros planes de ancho de banda con diferentes rangos de IP. Para este ISP se hizo la asignación de ancho de banda como se muestra en el cuadro 7.

**Figura 38. Configuración de la regla que limita el ancho de banda para determinado rango de IP.**

The screenshot shows the Mikrotik WinBox QoS configuration page. At the top, it says 'Apply to Routed and Bridged Packets' and 'Sequence 4'. The 'Packet Matching' section is expanded, showing the following fields: Input, Output, Source IP (\*), Destination IP (192.168.1.30-192.168.1.40), Fragments (with a checkbox for 'match only second and further fragments'), Packet Length, and Source MAC. Below this, there are sections for 'Protocol Matching' (set to ALL), 'Connection State' (with checkboxes for NEW, ESTABLISHED, RELATED, INVALID, UNTRACKED), 'IPTABLES Parameters', 'Time Matching', 'Layer 7 Filters', 'DiffServ' (set to DSCP), and 'Connection Limits' (Parallel connections per IP: more than; Traffic per connection: more than MB). At the bottom, the 'TARGET CLASS' is set to 'PLAN\_1\_MB'.

**8.13.4.** Se asignan las clases de QoS creadas a las interfaces de red, cuyo tráfico de salida se desea controlar. La interfaz que conecta a la red local en este ISP es la ETH00, por lo tanto es a la que se le agrega las clases de QoS, lo cual se hace desde el *Interface Manager* (figura 39) presionando el botón *Add Class* ubicado en la parte derecha de esta interfaz. Aparece una ventana con las diferentes clases que se desean agregar.

**Cuadro 7. Asignación de anchos de banda a rangos de IP.**

Ancho de banda	Rango de dirección IP	Dirección MAC
1 Mbps	192.168.1.101-192.168.1.150	A4:BA:DB:FB:92:62 00:1D:92:4A:C2:45
2 Mbps	192.168.1.151-192.168.1.200	00:1D:92:4A:A0:9E
4 Mbps	192.168.1.201-192.168.1.250	A4:BA:DB:FB:7C:23

**8.13.5.** Después de agregar las clases se guarda pulsando el botón *Activate last changes* ubicado en la parte superior derecha de la figura 39 y se verifica que las clases queden activas. De igual forma hay que activar el QoS para la interface ETH00 haciendo clic en el cuadro debajo de "On". Con la anterior configuración, QoS está trabajando para el tráfico de salida de la interfaz ETH00 y está realizando control de ancho de banda para la red local.

Figura 39. Interfaz QoS con las clases creadas.

The screenshot shows the ZeroShell web interface with the 'Quality of Service' section active. The interface is divided into three main sections for different network interfaces: ETH00, ETH01, and BRIDGE00. Each section displays the interface status, QoS status, and a table of configured classes.

**ETH00 Configuration:**

Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed	On
DEFAULT	Default class for unclassified traffic	Medium				<input checked="" type="checkbox"/>
PLAN_1_MB	Plan para usuarios de 1 Mbps	Medium		1.5Mbit/s	1Mbit/s	<input checked="" type="checkbox"/>
PLAN_2_MB	Plan para usuarios 2 Mbps	Medium		2.5Mbit/s	2Mbit/s	<input checked="" type="checkbox"/>
VOIP	Voz sobre IP	High		1Mbit/s	1Mbit/s	<input checked="" type="checkbox"/>

**ETH01 Configuration:**

Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed	On
DEFAULT	Default class for unclassified traffic	Medium				<input checked="" type="checkbox"/>

**BRIDGE00 Configuration:**

Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed	On
DEFAULT	Default class for unclassified traffic	Medium				<input checked="" type="checkbox"/>

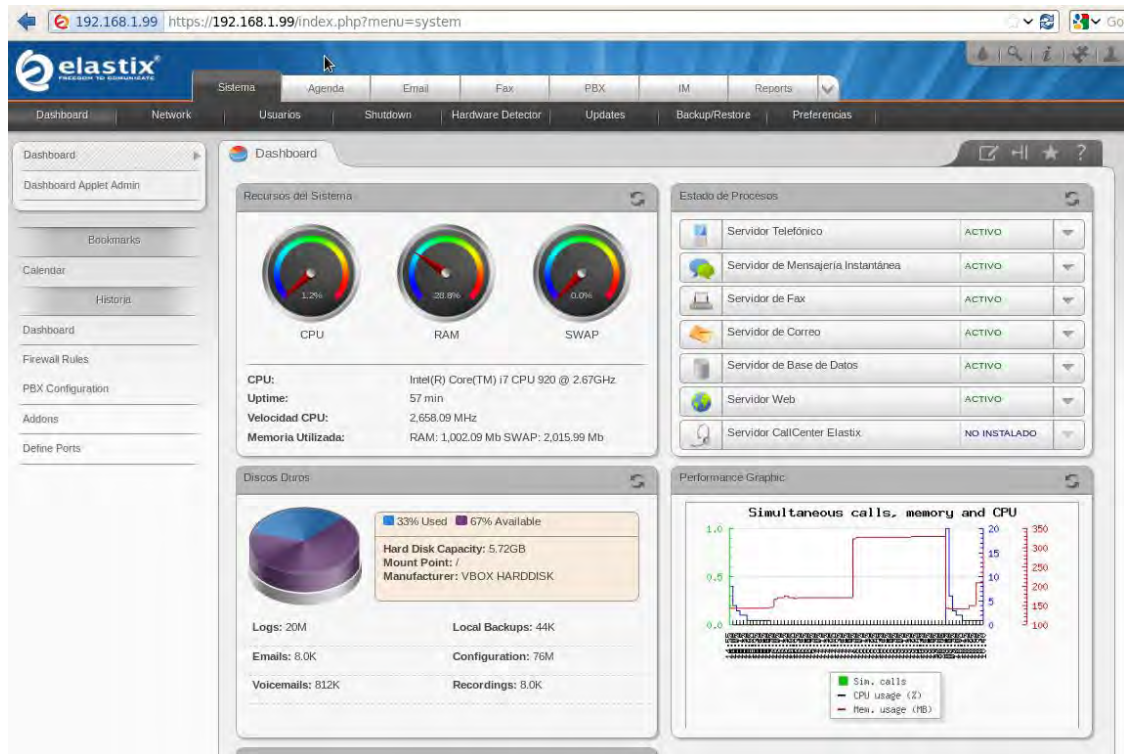
## 9. Configuración de la distribución Elastix

Se procede a continuación a configurar Elastix el cual genera el servicio de VoIP para realizar llamadas telefónicas. La distribución Elastix se instala en una máquina virtual en el software VirtualBox, tal como cualquier sistema operativo Linux.

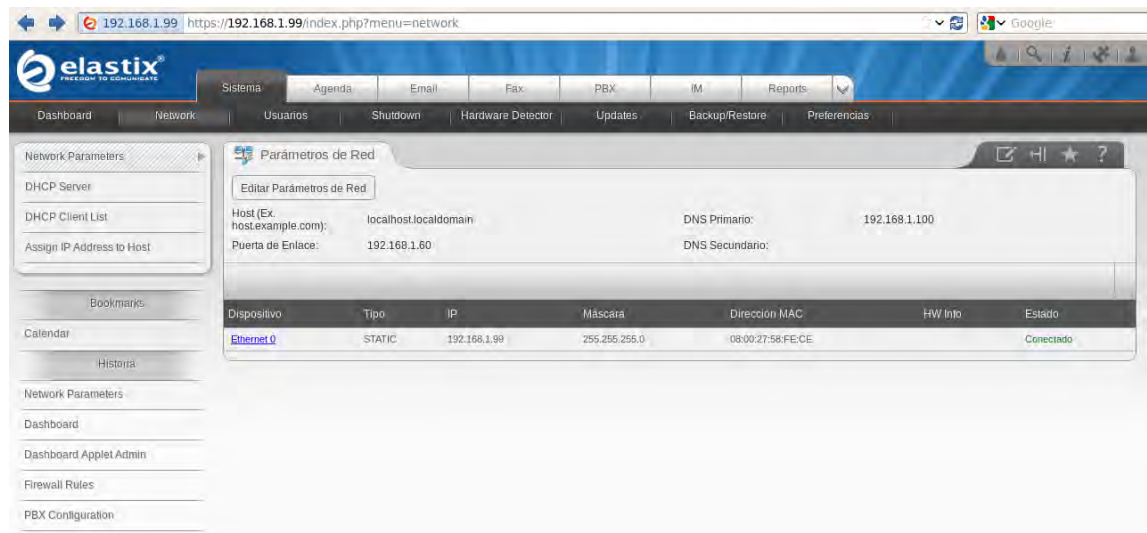
**9.1.** Se introduce en el browser o navegador de internet la dirección IP con la que se configuró el Elastix durante su instalación para ingresar a la interfaz web, que en este caso es 192.168.1.99. Se abre una ventana donde se introduce el usuario y la contraseña; para ingresar como administrador, el usuario es "admin" y la contraseña es "Autonoma2012", datos que se configuraron durante la instalación de esta distribución. Al ingresar se presenta la interfaz principal de Elastix como se muestra en la figura 40;

**9.2.** Se ingresa a la opción Network para configurar los parámetros de red: IP del Elastix, la puerta de enlace, el DNS Primario, entre otras características. Estos parámetros son importantes para establecer la conexión del Elastix con la red LAN. En este caso, la puerta de enlace se establece con la IP 192.168.1.60 que corresponde con la dirección IP con la que se configuró el ZeroShell y el DNS se establece con la IP 192.168.1.100 como se muestra en la figura 41.

**Figura 40. Pantalla de inicio de la interfaz web de Elastix**



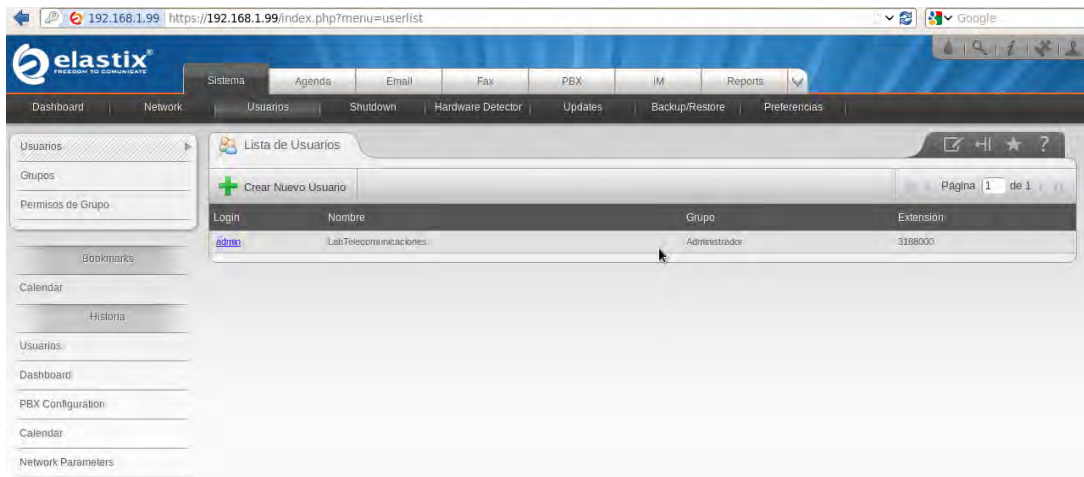
**Figura 41. Configuración de la opción Network**



**9.3.** En la opción de *Usuario* se establece el perfil de administración asignándole un nombre, un grupo y una extensión. Se pueden crear a demás usuarios que no tengan privilegios de administración. Para este caso, el nombre de administrador

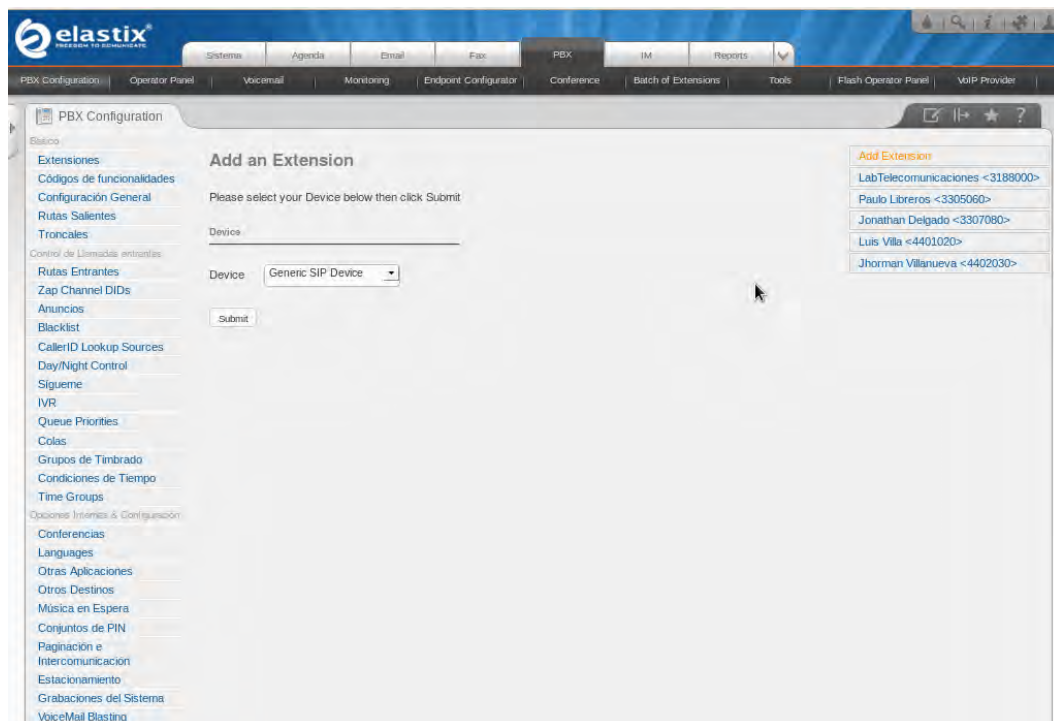
para el servidor de VoIP del ISP es LabTelecomunicaciones y se le asigna un número de extensión el cual es 3188000. Esta configuración se puede observar en la figura 42.

**Figura 42. Configuración de la opción Usuarios**



9.4. Se crean las extensiones de usuarios ingresando al menú *PBX* y seleccionando la opción *PBX Configuration*, como se observa en la figura 43.

**Figura 43. Creación de las extensiones de los usuarios**





En esta opción se adiciona las extensiones eligiendo primero el protocolo de VoIP que maneja el dispositivo de comunicación, que en este caso es SIP Genérico, y se da click en Submit. Se presenta una ventana en donde se ingresa los datos de la extensión: el número de la extensión, el nombre de la extensión y un número secreto en la sección *Device Options*, como se observa en la figura 44 y 45.

**Figura 44. Ingreso de datos para la Creación de las extensiones**

The screenshot shows the 'Add SIP Extension' form in the Elastix PBX Configuration interface. The form is divided into several sections:

- Add Extension:**
  - User Extension: 4401020
  - Display Name: Luis Villa
  - CID Num Alias: [Empty]
  - SIP Alias: [Empty]
- Extension Options:**
  - Outbound CID: [Empty]
  - Ring Time: Default
  - Call Waiting: Disable
  - Call Screening: Disable
  - Pinless Dialing: Disable
  - Emergency CID: [Empty]
- Assigned DID/CID:** [Empty]

On the right side, there is a list of existing extensions:

- Add Extension
- Lab Telecomunicaciones <3188000>
- Paulo Libreros <3305060>
- Jonathan Delgado <3307080>
- Jhorman Villanueva <4402030>

**Figura 45. Ingreso de datos para la creación de las extensiones (continuación)**

The screenshot shows the continuation of the 'Add SIP Extension' form, focusing on the 'Device Options' and 'Dictation Services' sections:

- Device Options:**
  - This device uses sip technology.
  - secret: 12345
  - dtmfmode: rfc2833
- Dictation Services:**
  - Dictation Service: Disabled
  - Dictation Format: Ogg Vorbis
  - Email Address: [Empty]
  - Language: [Empty]
  - Language Code: [Empty]

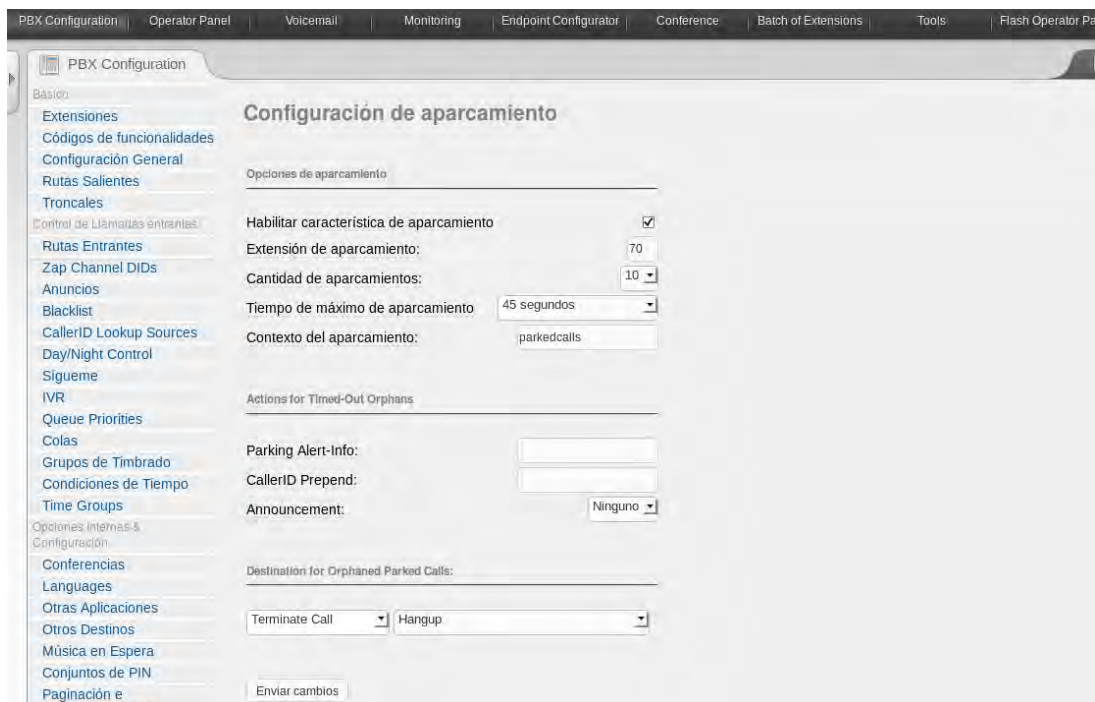
## 9.5. Configuración de los servicios para VoIP

Para la configuración de los servicios establecidos en la telefonía IP, se utilizan las funcionalidades que se encuentran en la opción *PBX Configuration* del menú *PBX*, ubicado en el lado izquierdo de la figura 43.

**9.5.1. Transferencia de Llamadas:** Por defecto, Elastix ya viene configurado con la funcionalidad de transferencia de llamadas. Para realizar esto solo se debe digitar desde el teléfono **##** seguido del número de la extensión a donde se va a transferir la llamada.

**9.5.2. Parqueo de Llamadas:** El parqueo de llamadas se realiza seleccionando la herramienta Estacionamiento, ubicado en la parte izquierda de la opción *PBX Configuration*. En la figura 46 se presenta los parámetros de este servicio. Los principales parámetros son: Habilitar las funcionalidades del parqueo de llamadas, la extensión del parqueo, el número de slots disponibles para el parqueo de llamadas, tiempo máximo en que permanece parqueada una llamada y el destino de una llamada cuando esta no puede ser parqueada. Por último se presiona el botón *Enviar Cambios* para guardar la configuración realizada.

**Figura 46. Parqueo de Llamadas en Elastix**



**9.5.3. Buzón de Voz:** La configuración del buzón de voz se realiza ya sea en el momento en que se crea las extensiones o ingresando a cada extensión ya

creada. En la figura 47 se observa los distintos parámetros para el uso del buzón de voz. Se utilizan dos parámetros los cuales son: Habilitar el servicio y la introducción de la contraseña para ingresar al buzón. Se establece la contraseña para cada uno de los 4 usuarios como los 4 últimos dígitos de la extensión correspondiente, por ejemplo la contraseña de Luis Villa es 1020 ya que su extensión es 4401020.

**Figura 47. Configuración del Buzón de Voz**

The screenshot shows a web interface for 'Voicemail & Directory' configuration. The settings are as follows:

- Status: Enabled (dropdown menu)
- Voicemail Password: 1020 (text input)
- Email Address: (empty text input)
- Pager Email Address: (empty text input)
- Email Attachment:  yes,  no
- Play CID:  yes,  no
- Play Envelope:  yes,  no
- Delete Voicemail:  yes,  no
- IMAP Username: (empty text input)
- IMAP Password: (empty text input)
- VM Options: (empty text input)
- VM Context: default (text input)

**9.5.4. Llamada en espera:** La configuración de la llamada en espera se realiza también en dos formas: en el momento en que se crea las extensiones o ingresando a cada extensión ya creada como se observa en la figura 48. Simplemente se habilita el *Call Waiting* y se presiona el botón *Enviar Cambios*, obteniendo finalmente el servicio en funcionamiento.

## 10. Configuración de teléfonos

Los teléfonos que los usuarios utilizan para realizar las llamadas y acceder al servicio de VoIP se presentan en el cuadro 8. En cada teléfono se configura los parámetros y se establece las conexiones pertinentes, teniendo en cuenta que los servicios ofrecidos por Elastix deben estar ejecutándose incluyendo las extensiones de cada usuario.

**Cuadro 8. Teléfonos de usuarios para acceder al servicio de VoIP**

Teléfonos	Cantidad	Marca	Modelo
Softphone	2	3CX	3CXPhone
Teléfono IP	1	Linksys Cisco	SPA921
Teléfono Análogo	1	Lucent	9101

**Figura 48. Configuración de la llamada en espera.**

Extension: 4401020

Delete Extension 4401020  
Add Gabcast Settings  
Add Follow Me Settings

Edit Extension

Display Name: Luis Villa  
CID Num Alias:  
SIP Alias:

Extension Options

Outbound CID:  
Ring Time: 10  
Call Waiting: Enable  
Call Screening: Disable  
Pinless Dialing: Disable  
Emergency CID:

Add Extension  
LabTelecomunicaciones <3188000>  
Paulo Libreros <3305060>  
Jonathan Delgado <3307080>  
Luis Villa <4401020>  
Jhorman Villanueva <4402030>

**10.1. Softphone:** Se descarga el softphone de forma gratuita de la página oficial de 3CX® al sistema operativo de Microsoft Windows. Al finalizar la instalación del programa, se puede ejecutar el softphone.

**10.1.1.** Se abre la ventana *Accounts* para ingresar el nombre y extensión de un usuario además de permitir visualizar las distintas cuentas creadas para el softphone como se muestra en la figura 49. En esta ventana se puede crear, editar y eliminar las cuentas de los usuarios; se selecciona la opción *New* para crear una nueva cuenta y aparece una ventana con los parámetros que se observan en la figura 50. Los principales parámetros que se configuran en esta ventana son el nombre de la cuenta de usuario, la identificación del usuario, el número de extensión, contraseña y la dirección IP del servidor PBX/SIP que corresponde a la IP del Elastix que en este caso es 192.168.1.99.

**Figura 49. Cuentas de usuario para el softphone.**

Accounts

Accounts

Manage SIP accounts

Active	Name	Domain	Caller ID
<input checked="" type="checkbox"/>	Jonathan D...	3307080@192.168....	Jonathan D...

New  
Edit  
Remove  
Soft keys

OK Cancel

**Figura 50. Parámetros para crear una cuenta de usuario**

The screenshot shows a Windows-style dialog box titled "Account settings". It has a close button (X) in the top right corner. The dialog is organized into several sections:

- Account name:** Jonathan Delgado
- Caller ID:** Jonathan Delgado
- Credentials:** Enter your SIP account credentials. Fields include Extension: 3307080, ID: 3307080, and Password: \*\*\*\*\*.
- My location:** Specify the IP of your PBX/SIP server. Two radio buttons are present: "I am in the office - local IP" (selected) with IP 192.168.1.99, and "I am out of the office - external IP" (unselected).
- Use 3CX Tunnel:** A checkbox that is checked. Below it, text reads "Eliminates firewall configuration. Requires 3CX Phone System for Windows". Fields include "Local IP of remote PBX:" (192.168.1.99) and "Tunnel password:" (\*\*\*\*\*).
- Use Outbound Proxy server:** A checkbox that is unchecked. Text below reads "Required by some VoIP Providers. Specify IP or name." with an empty text field.
- Perform provisioning from following URL:** A checkbox that is unchecked. Below it is a text field containing "http://".

At the bottom of the dialog are three buttons: "Advanced settings", "OK", and "Cancel".

Al finalizar esta configuración, el softphone pasa de un estado Not connected al estado On Hook y queda listo para poder efectuar las llamadas.

Como se estableció en el cuadro 8, se hace uso de dos softphone donde uno corresponde al usuario Jonathan Delgado con la extensión 3307080 y el otro corresponde al usuario Paulo Libreros con la extensión 3305060; en ambos casos se realiza el mismo procedimiento descrito anteriormente.

## 10.2 Teléfono IP

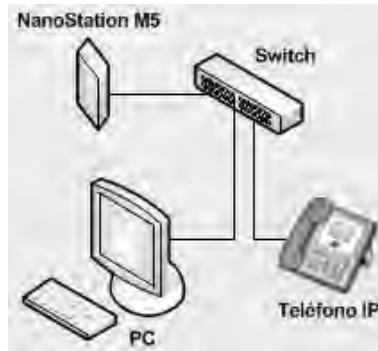
El teléfono IP se configura tanto en el portal web donde se establecen los parámetros de configuración como en el panel que presenta el teléfono físicamente.

**10.2.1.** Se realiza la conexión para el uso del teléfono se muestra en la figura 51. El teléfono IP y el PC se conectan en un switch junto al NanoStation M5 el cual realiza el enlace con la red inalámbrica.

**10.2.2.** Se establece en el panel del teléfono la dirección IP que este tendrá y su respectiva mascara, ingresando al menú *Network* que se encuentra presente en los ajustes del teléfono (*Setting*). Para configurar los otros parámetros, se ingresa

en el browser o navegador de internet la dirección IP con la que se configuró el teléfono y así entrar al portal web de Linksys, que en este caso es la IP 192.168.1.170.

**Figura 51. Conexión del teléfono IP**



**10.2.3.** Se ingresa a la interfaz web para la configuración del teléfono IP donde se encuentran todos los parámetros que actualmente tiene el teléfono IP como se observa en la figura 52.

**Figura 52. Pantalla de inicio de la interfaz web para el teléfono IP**

**SIPURA**  
technology, inc.

**Sipura Telephone Configuration**

**Info** System SIP Regional Phone Ext 1 User [User Login](#) [Basic](#) | [Advanced](#)  
[Personal Directory](#) [Call History](#)

**System Information**

DHCP:	Disabled	Current IP:	192.168.1.170
Host Name:	SipuraSPA	Domain:	192.168.1.99
Current Netmask:	255.255.255.0	Current Gateway:	0.0.0.0
Primary DNS:			
Secondary DNS:			

**Product Information**

Product Name:	SPA-921	Serial Number:	4M00H505046
Software Version:	4.1.10(b)	Hardware Version:	1.0.1(541f)
MAC Address:	00E08D3C65A	Client Certificate:	Installed
Licenses:	None		

**Phone Status**

Current Time:	1/1/2003 12:04:42	Elapsed Time:	00:04:42
Broadcast Pkts Sent:	0	Broadcast Bytes Sent:	0
Broadcast Pkts Recv:	567	Broadcast Bytes Recv:	42281
Broadcast Pkts Dropped:	0	Broadcast Bytes Dropped:	0
RTP Packets Sent:	0	RTP Bytes Sent:	0
RTP Packets Recv:	0	RTP Bytes Recv:	0
SIP Messages Sent:	46	SIP Bytes Sent:	21373
SIP Messages Recv:	0	SIP Bytes Recv:	0
External IP:			

**Ext 1 Status**

Registration State:	Not Registered	Last Registration At:	0/0/0 00:00:00
Next Registration In:	0 s	Message Waiting:	Yes
Mapped SIP Port:			

**Line 1 Call 1 Status**

Call State:	Idle	Tone:	None
Encoder:		Decoder:	
Type:		Remote Hold:	
Callback:		Peer Name:	
Peer Phone:		Duration:	
Packets Sent:		Packets Recv:	
Bytes Sent:		Bytes Recv:	
Decode Latency:		Jitter:	
Round Trip Delay:		Packets Lost:	
Packet Error:		Mapped RTP Port:	

Aquí se observa información del sistema, información del producto, status del teléfono, status de la extensión o en el status de la llamada en la línea 1; esta información presenta de forma general el rendimiento de las llamadas y el funcionamiento del teléfono.

**10.2.4.** Se introduce en el menú *System*, si se desea cambiar, la IP del teléfono de modo estático con su respectiva mascara; la información de este menú se observa en la figura 53. En el menú *Phone* se introduce el nombre del usuario y la cantidad de extensiones que se utiliza como se muestra en la figura 54.

**Figura 53. Menú System**

The screenshot shows the 'System' configuration menu. The navigation tabs at the top are 'Info', 'System' (selected), 'SIP', 'Regional', 'Phone', 'Ext 1', and 'User'. On the right, there are links for 'User Login', 'basic', 'advanced', 'Personal Directory', and 'Call History'. The main content area is divided into three sections:

- System Configuration:** Includes 'Enable Web Server' (set to 'yes') and 'User Password' (a text input field).
- Internet Connection Type:** Includes 'DHCP' (set to 'no'), 'Static IP' (192.168.1.170), 'NetMask' (255.255.255.0), and 'Gateway' (empty).
- Optional Network Configuration:** Includes 'HostName' (empty), 'Domain' (192.168.1.99), 'Primary DNS' (empty), 'Secondary DNS' (empty), 'DNS Query Mode' (set to 'Parallel'), 'Syslog Server' (empty), 'Debug Server' (empty), and 'Debug Level' (set to '0').

**Figura 54. Menú Phone**

The screenshot shows the 'Phone' configuration menu. The navigation tabs at the top are 'Info', 'System', 'SIP', 'Regional', 'Phone' (selected), 'Ext 1', and 'User'. On the right, there are links for 'User Login', 'basic', 'advanced', 'Personal Directory', and 'Call History'. The main content area is divided into several sections:

- General:** Includes 'Station Name' (Luis Villa) and 'Voice Mail Number' (101).
- Line Key 1:** Includes 'Extension' (1) and 'Short Name' (\$USER).
- Ring Tone:** Lists ten ring tones (Ring1 to Ring10) with their respective configurations, such as 'n=Classic-1;w=3;c=1' for Ring1 and 'n=Office;w=4;c=1' for Ring10.
- Audio Input Gain (dB):** Includes 'Handset Input Gain' (0) and 'Speakerphone Input Gain' (0).

**10.2.5.** Se habilita la línea telefónica en el menú *Ext 1*, se introduce la dirección IP del servidor Elastix en el parámetro Proxy, se introduce la información del usuario como el nombre, la extensión y una contraseña, y se selecciona el códec con el que va a trabajar el teléfono IP. El usuario asignado para este teléfono IP es Luis Villa que presenta la extensión 4401020, como se muestra en la figura 55.

**Figura 55. Menú Ext 1**

Section	Parameter	Value
General	Line Enable:	yes
NAT Settings		
NAT Mapping Enable:	no	
NAT Keep Alive Enable:	no	
SIP Settings		
SIP Port:	5060	
SIP Debug Option:	none	
Call Feature Settings		
Message Waiting:	yes	
Default Ring:	10	
Mailbox ID:		
Proxy and Registration		
Proxy:	192.168.1.99	
Register:	yes	
Make Call Without Reg:	yes	
Register Expires:	3600	
Ans Call Without Reg:	yes	
Subscriber Information		
Display Name:	Luis Villa	
User ID:	4401020	
Password:	*****	
Use Auth ID:	yes	
Auth ID:	4401020	
Audio Configuration		
Preferred Codec:	G729a	
Use Pref Codec Only:	no	
Silence Supp Enable:	no	
DTMF Tx Method:	Auto	

Al finalizar la configuración, el teléfono IP queda listo para efectuar llamadas.

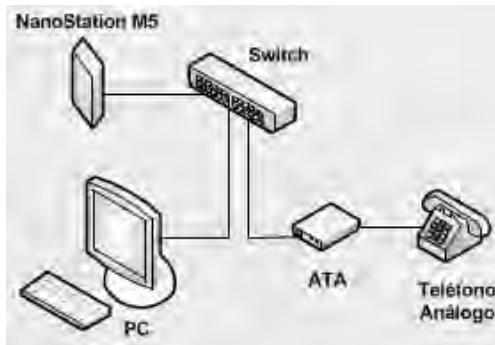
### 10.3. Teléfono Análogo

El teléfono análogo realiza una comunicación en redes PSTN y no sobre IP. Por lo tanto, para que este teléfono realice llamada sobre protocolo IP, se debe utilizar un ATA en donde se efectúe todas las configuraciones para acceder al servicio de VoIP.

**10.3.1.** Se realiza la conexión para el uso del teléfono análogo como se presenta en la figura 56. El teléfono se enlaza al ATA y este último se conecta a un switch junto al PC y el NanoStation M5 encargado de efectuar el enlace inalámbrico. El ATA que se implementa es de marca Linksys Cisco, modelo PAPT2, el cual contiene dos puertos RJ-45 para teléfonos análogos y un puerto RJ-45 para una conexión Ethernet.



**Figura 56. Conexión para uso del teléfono análogo**



**10.3.2.** Se realiza la configuración para utilizar el teléfono en el ATA, donde se manejan dos opciones: Uno es la configuración de los parámetros utilizando el teléfono al entrar a un menú de voz e ingresar una serie de códigos establecidos en el manual del ATA; la segunda configuración se realiza directamente en la interfaz web al ingresar la IP del ATA en el browser. En la primera configuración es donde se asigna la dirección IP del ATA para poder ingresar a la interfaz web.

**10.3.3.** Para configurar el ATA en la interfaz web, se ingresa con la IP 192.168.1.171 en el browser y se presenta una ventana de inicio que muestra toda la información del sistema, información del producto y status del sistema, que se muestra en la figura 57.

**Figura 57. Interfaz web del ATA**

La interfaz web del ATA Linksys muestra la configuración de voz y el estado del sistema. El título de la página es "Voice" y el modelo es "PAP2". La versión de firmware es 3.1.15(LS).

Info	System	SIP	Regional	Line 1	Line 2	User 1	User 2
Basic View (switch to advanced view) <span style="float: right;">User Login</span>							
<b>System Information</b>	DHCP: Disabled	Current IP: 192.168.1.171					
	Host Name: LinksysPAP	Domain:					
	Current Netmask: 255.255.255.0	Current Gateway: 192.168.1.60					
	Primary DNS:						
	Secondary DNS:						
<b>Product Information</b>	Product Name: PAP2T	Serial Number: FL100K223576					
	Software Version: 3.1.15(LS)	Hardware Version: 0.3.5					
	MAC Address: 687F74575637	Client Certificate: Installed					
	Customization: Open						
<b>System Status</b>	Current Time: 1/1/2003 12:10:27	Elapsed Time: 00:10:27					
	Broadcast Pkts Sent: 0	Broadcast Bytes Sent: 0					
	Broadcast Pkts Recv: 1458	Broadcast Bytes Recv: 101146					
	Broadcast Pkts Dropped: 0	Broadcast Bytes Dropped: 0					
	RTP Packets Sent: 0	RTP Bytes Sent: 0					
	RTP Packets Recv: 0	RTP Bytes Recv: 0					
	SIP Messages Sent: 114	SIP Bytes Sent: 59508					
	SIP Messages Recv: 0	SIP Bytes Recv: 0					
	External IP:						

**10.3.4.** En el menú *System* se ingresa todos los datos relacionados a la red como la dirección IP, la máscara, la puerta de enlace y se deshabilita DHCP. La información de este menú se presenta en la figura 58.

**Figura 58. Menú System**

The screenshot shows the 'System' configuration page for a 'Phone Adapter with 2 Ports for Voice-Over-IP'. The page is divided into several sections:

- System Configuration:** Includes 'Enable Web Server' (set to 'yes') and 'User Password' (empty field).
- Internet Connection Type:** Includes 'DHCP' (set to 'no'), 'Static IP' (192.168.1.171), 'NetMask' (255.255.255.0), and 'Gateway' (192.168.1.60).
- Optional Network Configuration:** Includes 'HostName', 'Domain', 'Primary DNS', 'Secondary DNS', 'DNS Query Mode' (set to 'Parallel'), 'Syslog Server', 'Debug Server', and 'Debug Level' (set to 0).

At the bottom, there are 'Save Settings' and 'Cancel Settings' buttons. The Cisco Systems logo is visible in the bottom right corner.

**10.3.5.** En el menú Line 1 se configura los parámetros y características referente a las llamadas.

Se habilita la línea para que las llamadas entren en funcionamiento, se introduce la IP del servidor Elastix en la opción Proxy y el nombre del usuario con su respectiva extensión; el usuario asignado para este teléfono análogo es Jhorman Villanueva que presenta la extensión 4403040 como se observa en la figura 59.

Al finalizar la configuración, el teléfono análogo queda listo para efectuar llamadas. Como ya se tiene la configuración de cada uno de los teléfonos ya se pueden ejecutar llamadas entre cada uno de estos para verificar el funcionamiento de los servicios.

## 11. Configuración del VoIPMonitor

Se procede a configurar el VoIPmonitor que registra las medidas de QoS de las llamadas. El programa VoIPmonitor se instala en Centos 6 a partir de los paquetes de instalación que se encuentran en su página oficial (<http://www.voipmonitor.org/>).

**11.1.** Se introduce en el browser la dirección <http://localhost/voipmonitor> para ingresar a la interfaz web del VoIP monitor, en donde aparece una ventana de autenticación para ingresar al portal web. Se ingresa con el nombre de usuario "admin" y la contraseña "admin", que son valores que ya vienen por defecto.

Figura 59. Menu Line 1

The screenshot shows the configuration interface for a voice line. The main title is 'Voice' and the sub-header is 'Phone Adapter with 2 Ports for Voice-Over-IP'. The page is organized into a sidebar with categories: SIP Settings, Proxy and Registration, Subscriber Information, Supplementary Service Subscription, and Audio Configuration. The main content area is titled 'Line 1' and contains the following settings:

- SIP Settings:** Line Enable (yes), SIP Port (5060).
- Proxy and Registration:** Proxy (192.168.1.99), Register (yes), Make Call Without Reg (yes), Register Expires (3600), Ans Call Without Reg (yes).
- Subscriber Information:** Display Name (Jhorman Villanuev), User ID (4403040), Password (\*\*\*\*\*), Use Auth ID (yes), Auth ID (4403040).
- Supplementary Service Subscription:** Call Waiting Serv (yes), Block ANC Serv (yes), Dist Ring Serv (yes), Cfwd All Serv (yes), Cfwd Busy Serv (yes), Cfwd No Ans Serv (yes), Cfwd Sel Serv (yes), Cfwd Last Serv (yes), Block Last Serv (yes), Accept Last Serv (yes), DND Serv (yes), CID Serv (yes), CWCD Serv (yes), Call Return Serv (yes), Call Back Serv (yes), Three Way Call Serv (yes), Three Way Conf Serv (yes), Attn Transfer Serv (yes), Unattn Transfer Serv (yes), MWI Serv (yes), VMWI Serv (yes).
- Audio Configuration:** Preferred Codec (G711u), Silence Supp Enable (no), Use Pref Codec Only (no), FAX CED Detect Enable (yes), DTMF Tx Method (Auto).

En la figura 60 se observa el portal de inicio *CDR* donde se visualiza distintas informaciones referentes a las llamadas realizadas. El *CDR* muestra las características de las llamadas tanto del origen como del destino, información referente al protocolo RTP y algunas medidas de QoS que puedan interesar al personal que administra la red.

En la parte izquierda de la figura 60 se ubica las distintas opciones para visualizar y configurar las llamadas registradas en el servicio de VoIP. Se puede obtener registro en tiempo real de las llamadas, gráficas estadísticas, reportes de QoS, resumen de la llamada, alertas, etc.

**11.2.** La opción *Active Call* permite monitorear las llamadas en tiempo real, ya que las otras opciones arrojan información cuando se ha finalizado la llamada. En la figura 61 se observa que se está realizando una llamada desde el usuario Paulo Libreros con extensión 3305060 hacia el usuario Jonathan Delgado con extensión 3307080; se visualiza además las direcciones IP de ambos usuarios.

Figura 60. Portal de inicio CDR

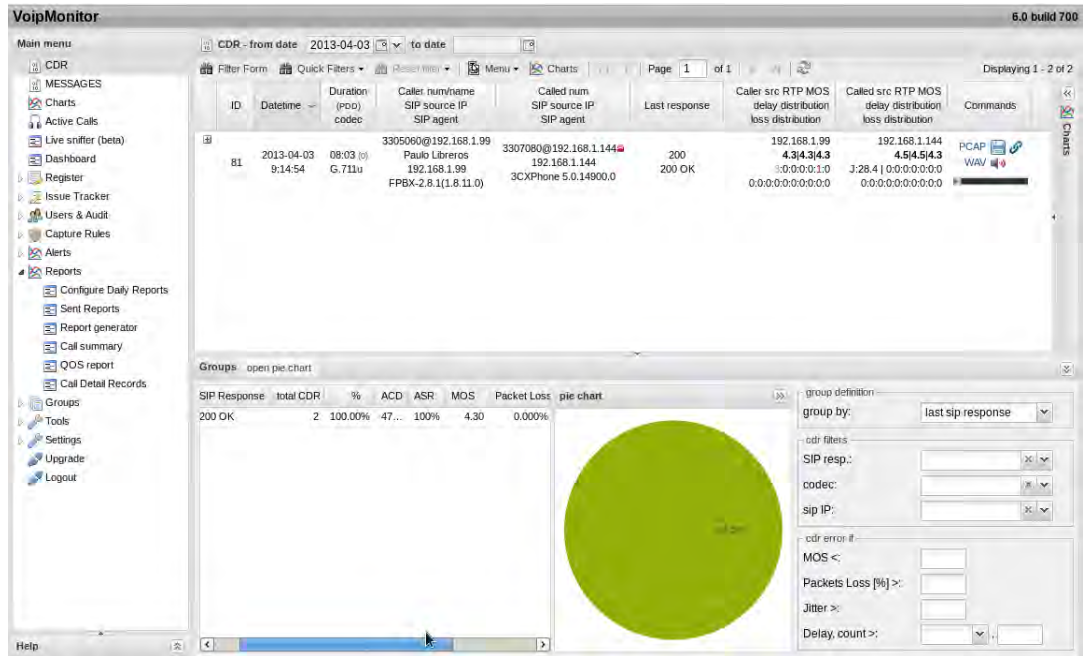
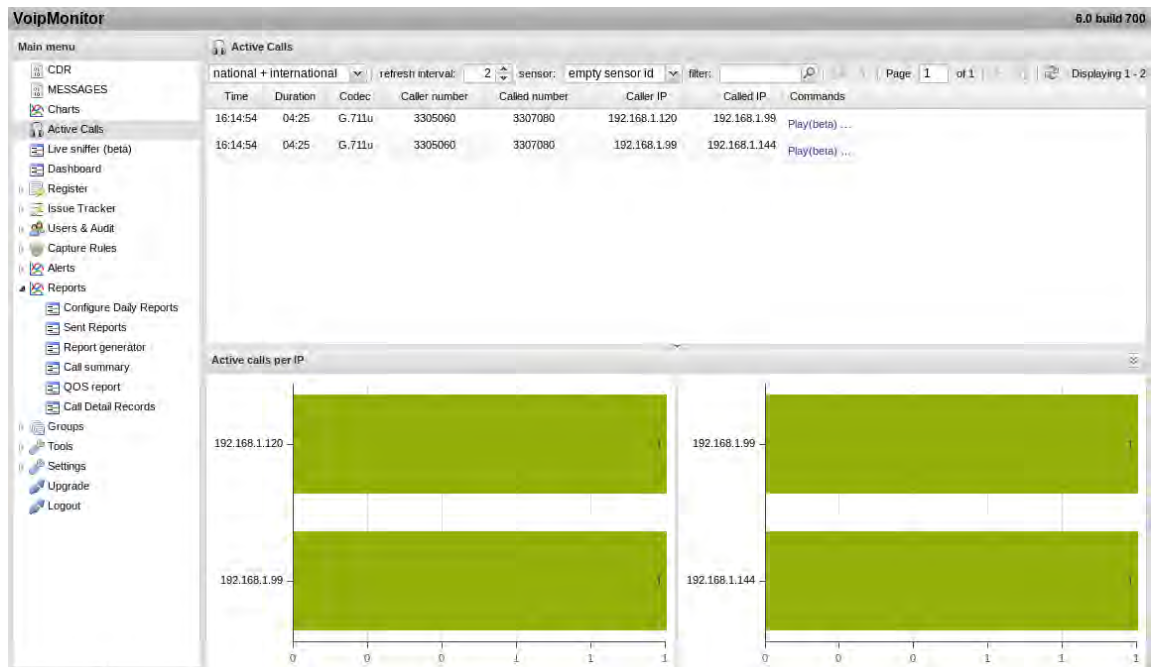


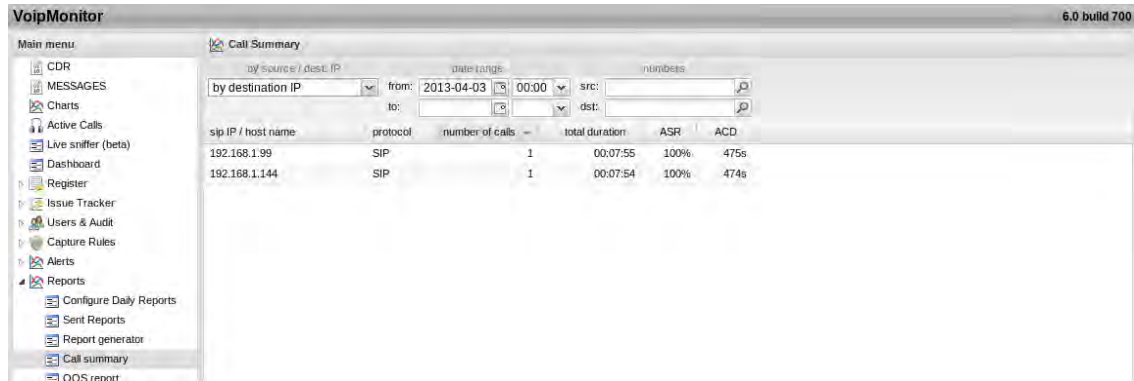
Figura 61. Monitoreo de llamadas en tiempo real.



11.3. Al finalizar la llamada, se puede observar el resumen de esta en la opción *Call Summary*, que se encuentra dentro de *Reports*. En esta opción se visualiza las distintas características que presentó la llamada, ya sea en el usuario fuente

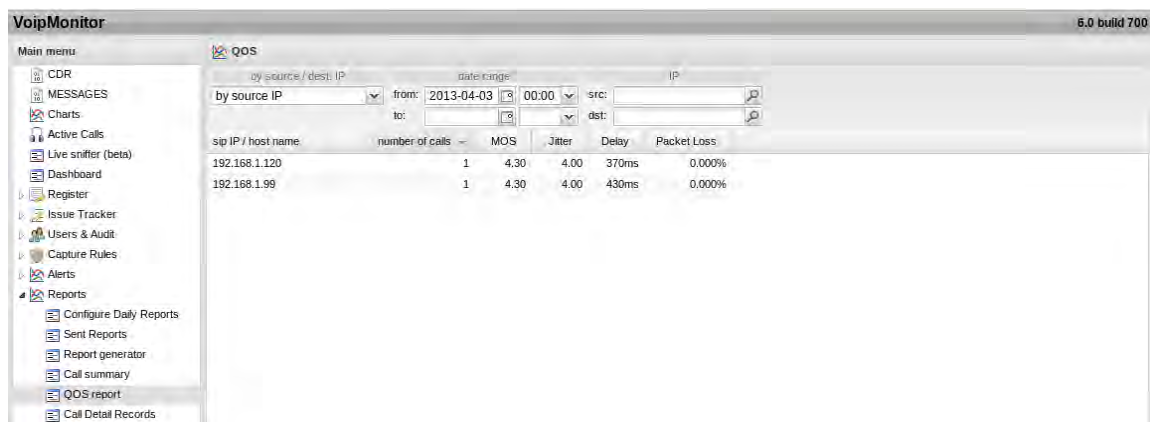
representado con la IP 192.168.1.120 o en el usuario destino representado con la IP 192.168.1.144; se debe seleccionar el usuario destino o el usuario fuente para ver las propiedades de cada uno. Esta ventana se muestra en la figura 62.

**Figura 62. Resumen de llamada para el usuario destino.**



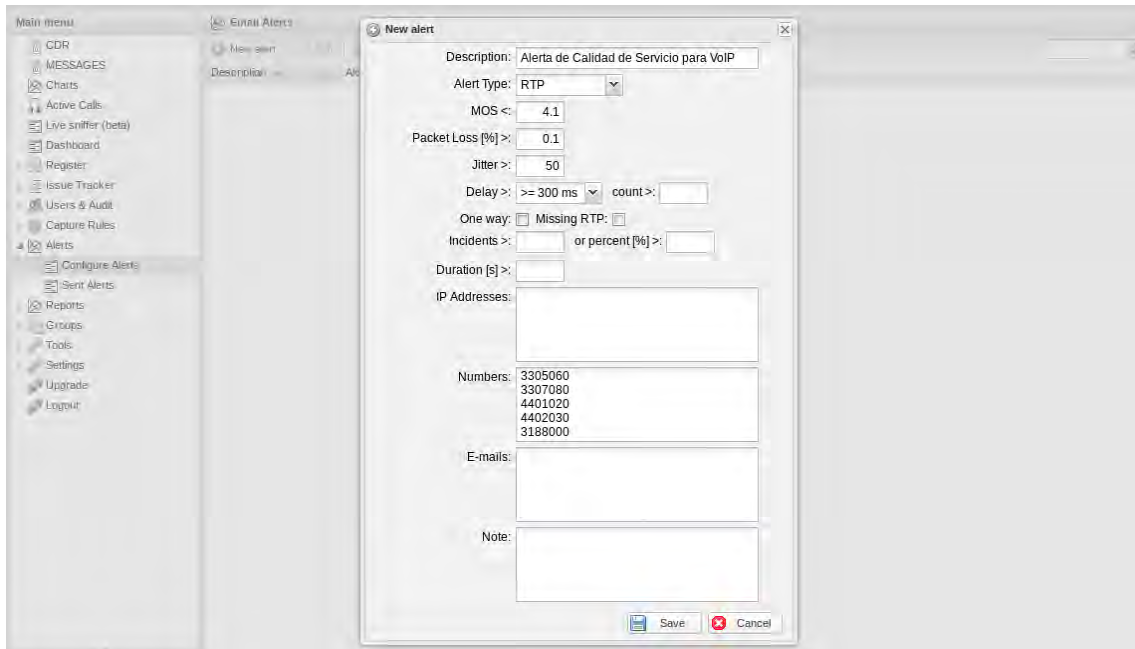
**11.4.** Las mediciones de QoS de la llamada realizada se observan en la opción *QoS Report*, donde se encuentran las mediciones correspondientes al Jitter, Latencia o Delay, MOS y pérdida de paquetes. En la figura 63 se muestra las medidas para el usuario fuente con IP 192.168.1.120. De igual forma se puede seleccionar al usuario destino con IP 192.168.1.144 para observar sus medidas de QoS.

**Figura 63. Medición de QoS para el usuario fuente.**



**11.5.** Para ingresar las alarmas correspondientes a las mediciones de QoS, en caso que se sobrepase un valor máximo y se presente errores de comunicación, se utiliza la opción *Configure Alerts* que se encuentra dentro de *Alerts*. Se crea una nueva alerta y se introducen los valores máximos correspondientes al Jitter, perdida de paquetes, latencia y MOS como se observa en la figura 64.

**Figura 64. Creación de Alertas para mediciones de QoS.**



## 12. NOTA

- Este manual de usuario se basa en el proyecto de grado “Diseño e implementación de un ISP con acceso inalámbrico para soportar servicios de internet y telefonía IP en el laboratorio de telecomunicaciones de la Universidad Autónoma de Occidente” realizado por Jhorman A. Villanueva y Luis H. Villa.
- Si se realiza esta implementación en una localidad geográfica, se debe realizar los estudios y análisis correspondientes al espectro de frecuencia, ruido y otros factores que influyen en el espacio, ya que la implementación de este proyecto se realizó en un medio cerrado donde solo se presentó 2 frecuencias en la banda de 5 GHz correspondientes al Wifi de la universidad y no se presentó un nivel de ruido que afectara la comunicación. El diseñador debe conocer esta información para configurar los parámetros correspondientes a las antenas y así poder implementar el enlace inalámbrico sin que se presente inconvenientes.
- Para la instalación del Voipmonitor es necesario que descarguen la guía de la comunidad oficial ([www.voipmonitor.org](http://www.voipmonitor.org)) ya que es un poco tediosa su configuración. Se debe descargar de igual forma una licencia que expira a los 30 días, la cual pueden renovar inscribiéndose nuevamente a la comunidad o adquiriéndola por una suma de dinero.

- Es necesario que los estudiantes que quieran entender la arquitectura de red de un ISP y los procedimientos que se llevan a cabo para prestar los servicios, tengan un conocimiento sobre TCP/IP y tecnología inalámbrica.
- La conexión de Internet que toma este ISP se realiza por un canal no dedicado, ya que pertenece a la red de la Universidad Autónoma de Occidente y por ende se presentan varias restricciones de accesibilidad a algunas páginas, producto del servidor Proxy, o restricciones de velocidad para realizar descargas en programas P2P.