



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

**CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y  
COMUNICACIÓN DE DATOS**

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE INGENIERÍA EN ELECTRÓNICA, REDES Y  
COMUNICACIÓN DE DATOS**

**TEMA: ESTUDIO COMPARATIVO DE LOS PROTOCOLOS  
NSTREME Y NV2 PARA UN ENLACE INALÁMBRICO A 2.4GHZ  
Y 5.8 GHZ**

**AUTORES: BONILLA FERNÁNDEZ, PAÚL ANDRÉS  
REYES AGUIRRE, FELIPE DANIEL**

**DIRECTOR: DR. ESPINOSA ORTIZ, NIKOLAI DANIEL**

**SALGOLQUÍ**

**2015**



**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**  
**INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS**

**CERTIFICACIÓN**

Certifico que el trabajo de titulación. *“ESTUDIO COMPARATIVO DE LOS PROTOCOLOS NSTREME Y NV2 PARA UN ENLACE INALÁMBRICO A 2.4GHZ Y 5.8GHZ”*, realizado por los señores Paúl Andrés Bonilla Fernández y Felipe Daniel Reyes Aguirre, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores Paúl Andrés Bonilla Fernández y Felipe Daniel Reyes Aguirre para que lo sustenten públicamente.

Sangolquí, 9 de diciembre de 2015

  
\_\_\_\_\_  
Dr. Nikolai Daniel Espinosa Ortiz PhD.  
DIRECTOR





**DEPARTAMENTO DE ELECTRICA Y ELECTRONICA  
INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS**

**AUTORÍA DE RESPONSABILIDAD**

PAÚL ANDRÉS BONILLA FERNÁNDEZ, con cédula de identidad N° 0201605649 y FELIPE DANIEL REYES AGUIRRE, con cédula de identidad N° 1003698964 declaramos que este trabajo de titulación ***"ESTUDIO COMPARATIVO DE LOS PROTOCOLOS NSTREME Y NV2 PARA UN ENLACE INALÁMBRICO A 2.4GHZ Y 5.8GHZ"*** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 9 de diciembre de 2015

Paúl Andrés Bonilla Fernández

C.C. 0201605649

Felipe Daniel Reyes Aguirre

C.C. 1003698964



**DEPARTAMENTO DE ELÉCTRICA Y ELECTRONICÆ**  
**INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS**

**AUTORIZACIÓN**

PAÚL ANDRÉS BONILLA FERNÁNDEZ y FELIPE DANIEL REYES AGUIRRE, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***“ESTUDIO COMPARATIVO DE LOS PROTOCOLOS NSTREME Y NV2 PARA UN ENLACE INALÁMBRICO A 2.4GHZ Y 5.8GHZ*** cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 9 de diciembre de 2015

  
\_\_\_\_\_  
Paúl Andrés Bonilla Fernández

C.C. 0201605649

  
\_\_\_\_\_  
Felipe Daniel Reyes Aguirre

C.C. 1003698964

## **DEDICATORIA**

A mi madre Esthela Fernández, por darme la vida, creer en mí y porque siempre me apoyaste dándome tu voz de aliento para poder salir adelante en los momentos difíciles que atravesé. Mami gracias por darme una carrera para mi futuro y por brindarme tu amor.

A mi padre Jaime Bonilla, por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien.

A mis hermanos por siempre apoyarme en cada decisión que tomo, y por estar a mi lado en cada momento.

Paúl Andrés Bonilla Fernández

Quiero dedicar este trabajo toda mi familia, en especial a mi mami y mi ñaña por educarme con mucho amor y dedicación, y sobre todo por su apoyo incondicional ya que han sido el pilar fundamental en los cuales me apoyado para llegar a cumplir este objetivo.

También quiero dedicar este esfuerzo a mis sobrinito Adrián Ismael y Paúl Ignacio porque han llegado para colmar de mucha felicidad a mí y a toda mi familia.

Felipe Daniel Reyes Aguirre

## **AGRADECIMIENTO**

A mis profesores, Ing. Christian Vega y Dr. Nikolai Espinosa quienes nos guiaron y ayudaron para que este proyecto pueda concluir satisfactoriamente.

A mi familia en general, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

Paúl Andrés Bonilla Fernández

Quiero agradecer a todos los que hicieron posibles que este sueño se convierta en realidad en especial a toda mi familia, amigos y profesores de la Universidad de las Fuerzas Armadas-ESPE

Un agradecimiento muy sincero al Ing. Christian Vega y al Dr. Nikolai Espinosa por los conocimientos que me impartieron durante toda la carrera y sobre todo por ayuda incondicional y desinteresa con lo cual no hubiese sido posible concluir este ciclo.

Felipe Daniel Reyes Aguirre

## INDICE GENERAL

CERTIFICACIÓN DE TUTORÍA .....	ii
AUTORÍA DE RESPONSABILIDAD .....	iii
AUTORIZACIÓN DE PUBLICACIÓN .....	iv
DEDICATORIA .....	v
AGRADECIMIENTO .....	vi
INDICE GENERAL.....	vii
INDICE DE TABLAS .....	xiii
INDICE DE CUADROS.....	xv
INDICE DE FIGURAS.....	xvi
RESUMEN.....	xxv
ABSTRACT .....	xxvi
GLOSARIO DE TERMINOS.....	xxvii
CAPITULO I.....	1
INTRODUCCIÓN .....	1
1.1    Antecedentes. ....	1
1.2    Justificación e Importancia.....	3
1.3    Objetivos. ....	3
1.3.1    Objetivo General. ....	3
1.3.2    Específicos. ....	4
CAPITULO II .....	5
MARCO TEÓRICO.....	5
2.1    Redes Inalámbricas.....	5

2.1.1	Aplicaciones para Redes Inalámbricas.....	5
2.2	Estándares IEEE 802.11 (a, b, g, n, ac).....	5
2.2.1	IEEE 802.11a .....	6
2.2.2	IEEE 802.11b.....	6
2.2.3	IEEE 802.11g.....	6
2.2.4	IEEE 802.11n.....	6
2.2.5	IEEE 802.11ac.....	7
2.3	Acceso Múltiple por Detección de Portadora con Evasión de Colisiones. ....	7
2.3.1	Funcionamiento.....	8
2.3.2	Características de CSMA/CA .....	11
2.4	Acceso Múltiple por División de Tiempo .....	12
2.4.1	Funcionamiento.....	12
2.4.2	Características .....	14
2.5	Ancho de Banda .....	15
2.5.1	Tasa de Transferencia .....	16
2.6	Retardo en la Transmisión.....	17
2.7	Antenas.....	18
2.7.1	Parámetros de una Antena.....	18
2.7.2	Zona de Fresnel.....	21
2.8	Protocolo Nstreme .....	22
2.8.1	Funcionalidad y Características .....	22
2.8.2	Compatibilidad y Coexistencia entre otros Protocolos Inalámbricos .....	24
2.9	Protocolo Nv2.....	24
2.9.1	Funcionalidad y Características .....	25



2.9.2	Compatibilidad y Coexistencia entre otros Protocolos Inalámbricos .....	26
2.10	Diferencias entre Nv2 y Nstreme .....	27
CAPITULO III .....		28
ENLACE INALÁMBRICO.....		28
3.1	Topología De La Red .....	28
3.1.1	Topología del Enlace a 2.4Ghz .....	28
3.1.2	Topología del Enlace de 5.8Ghz .....	29
3.2	Inspección técnica de las radio bases .....	30
3.3	Estudio de Factibilidad del enlace con PTP LinkPlanner .....	33
3.3.1	Configuración de un Enlace de Radio Frecuencia en LinkPlanner.....	34
3.3.2	Reporte de Instalación.....	36
3.4	Criterios de Elección de los Equipos.....	42
3.5	Características de los Equipos .....	44
3.5.1	Router Mikrotik RB433AH.....	44
3.5.2	Router Inalámbrico Mikrotik SXT 5HnD .....	47
3.5.3	Antena HyperLink Technologies HG2424G .....	51
3.6	Soporte de los Protocolo Nstreme y Nv2 en Equipos Mikrotik.....	56
3.6.1	Formas de Ingresar a RouterOS Mikrotik.....	56
3.6.2	Direccionamiento IP en RouterOS.....	57
3.6.3	Configuración de la interface Wireless .....	58
3.6.4	Sección General .....	59
3.6.5	Sección Wireless .....	59
3.6.6	Sección Data Rates.....	69
3.6.7	Sección Advanced.....	70

- 3.6.8 Sección HT.....71
- 3.6.9 Sección WDS (Sistema de Distribución Wireless).....72
- 3.6.10 Sección Nstream.....72
- 3.6.11 Sección Tx Power .....73
- 3.6.12 Sección Current Tx Power .....74
- 3.6.13 Sección Status. ....74
- 3.6.14 Sección Traffic .....75
- CAPITULO IV.....76
- GESTIÓN E IMPLEMENTACIÓN DE SERVICIOS DE RED.....76
- 4.1 Instalación del Sistema Operativo Centos 7 en VMWare .....76
- 4.2 Configuración del servidor VSFTP .....83
- 4.3 Configuración del servidor NFS.....90
- 4.4 Configuración del servidor SMB .....93
- 4.5 Instalación y configuración de la central de VoIP Trixbox en VMWare.....96
  - 4.5.1 Instalación de la herramienta ZOIPER .....102
  - 4.5.2 Configuración de la herramienta ZOIPER .....103
- 4.6 Habilidad de Internet sobre la red .....106
- 4.7 Obtención de los parámetros del enlace inalámbrico para el estudio comparativo..
  - .....114
  - 4.7.1 Pruebas de conectividad por medio del comando ping en la frecuencia de 2.4GHz con el protocolo Nstreme.....114
  - 4.7.2 Prueba de conectividad por medio del comando ping en la frecuencia de 5.8GHz con el protocolo Nstreme.....116
  - 4.7.3 Prueba de conectividad por medio del comando ping en la frecuencia de 2.4GHz con el protocolo Nv2 .....117

4.7.4	Prueba de conectividad por medio del comando ping en la frecuencia de 5.8GHz con el protocolo Nv2 .....	118
4.7.5	Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 2.4GHz con el protocolo Nstreme .....	119
4.7.6	Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 5.8GHz con el protocolo Nstreme .....	121
4.7.7	Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 2.4GHz con el protocolo Nv2.....	122
4.7.8	Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 5.8GHz con el protocolo Nv2.....	123
4.7.9	Obtención de datos por medio de la tabla <i>Registration</i> .....	125
4.7.10	Elección de las frecuencias menos saturadas a través de la herramienta <i>Frequency Usage</i> .....	126
4.8	Activación del protocolo SNMP en equipos Mikrotik, Windows y Centos 7	126
4.9	Gestión de la red por medio de la herramienta The Dude.....	129
4.9.1	Gestión en el enlace de 2.4GHZ con The Dude.....	130
4.9.2	Gestión en el enlace de 5.8GHZ con The Dude.....	131
4.10	Gestión de la red por medio de la herramienta LANState PRO.....	133
4.10.1	Gestión en el enlace de 2.4GHZ con LANState PRO.....	134
4.10.2	Gestión en el enlace de 5.8GHZ con LANState PRO.....	136
4.11	Gestión de la red por medio de la herramienta PRTG.....	138
4.11.1	Gestión en el enlace de 2.4GHz con PRTG Network Monitor .....	139
4.11.2	Gestión en el enlace de 5.8 GHz con PRTG Network Monitor .....	142
CAPITULO V.....		144
ANALISIS DE RESULTADOS .....		144

5.1	Análisis de resultados para el enlace inalámbrico a 2.4GHz.....	144
5.1.1	Análisis de resultados para el enlace a inalámbrico 2.4GHz variando la banda .....	144
5.1.2	Análisis de resultados para el enlace inalámbrico a 2.4GHz variando el ancho de canal .....	151
5.1.3	Análisis de resultados para el enlace inalámbrico a 2.4GHz variando la frecuencia .....	158
5.2	Análisis de resultados para el enlace a 5.8 GHz.....	165
5.2.1	Análisis de resultados para el enlace a 5.8 GHz variando la banda .....	165
5.2.2	Análisis de resultados para el enlace a 5.8 GHz variando en ancho de canal	172
5.2.3	Análisis de resultados para el enlace a 5.8 GHz variando la frecuencia..	179
CAPITULO VI.....		186
CONCLUSIONES Y RECOMENDACIONES.....		186
6.1	Conclusiones .....	186
6.2	Recomendaciones .....	188
REFERENCIAS BIBLIOGRÁFICAS .....		190

## INDICE DE TABLAS

Tabla 1. Anchos de banda por tecnología.....	16
Tabla 2. Tabla de direccionamiento IP del enlace de 2.4GHz.....	29
Tabla 3. Tabla de Direccionamiento IP del enlace de 2.4GHz.....	30
Tabla 4. Potencia de transmisión de la tarjeta Wireless.....	50
Tabla 5. Potencia de recepción de la tarjeta Wireless.....	51
Tabla 6. Especificaciones Eléctricas.....	53
Tabla 7. Especificaciones mecánicas.....	53
Tabla 8. Carga de viento.....	53
Tabla 9. Características del patrón de irradiación vertical.....	54
Tabla 10. Características del patrón de irradiación horizontal.....	55
Tabla 11. Banda vs. Tasa de transmisión promedio a 2.4GHz.....	144
Tabla 12. Banda vs. Tasa de Recepción Promedio a 2.4GHz.....	145
Tabla 13. Banda vs. Tiempo de respuesta a 2.4GHz.....	146
Tabla 14. Banda vs. CCQ Tx a 2.4GHz.....	147
Tabla 15. Banda vs. CCQ Rx a 2.4GHz.....	148
Tabla 16. Banda vs. Tasa de transmisión a 2.4GHz.....	149
Tabla 17. Banda vs. Tasa de Recepción a 2.4GHz.....	150
Tabla 18. Ancho de Canal vs. Tasa de Transmisión Promedio a 2.4GHz.....	151
Tabla 19. Ancho de canal vs. Tasa de recepción promedio a 2.4GHz.....	152
Tabla 20. Ancho de Canal vs. Tiempo de Respuesta a 2.4GHz.....	153
Tabla 21. Ancho de Canal vs. CCQ Tx a 2.4GHz.....	154
Tabla 22. Ancho de Canal vs. CCQ Rx a 2.4GHz.....	155
Tabla 23. Ancho de Canal vs. Tasa de Transmisión a 2.4GHz.....	156
Tabla 24. Ancho de Canal vs. Tasa de Recepción a 2.4GHz.....	157
Tabla 25. Frecuencia vs. Tasa de Transmisión Promedio a 2.4GHz.....	158
Tabla 26. Frecuencia vs. Tasa de Recepción Promedio a 2.4GHz.....	159
Tabla 27. Frecuencia vs. Tiempo de Respuesta a 2.4GHz.....	160
Tabla 28. Frecuencia vs. CCQ Tx a 2.4GHz.....	161
Tabla 29. Frecuencia vs. CCQ Rx a 2.4GHz.....	162

Tabla 30. Frecuencias vs. Tasa de Transmisión a 2.4GHz .....	163
Tabla 31. Frecuencia vs. Tasa de Recepción a 2.4GHz .....	164
Tabla 32. Banda vs. Tasa de Transmisión Promedio a 5.8GHz.....	165
Tabla 33. Banda vs. Tasa de Recepción Promedio a 5.8GHz.....	166
Tabla 34. Banda vs. Tiempo de Respuesta a 5.8GHz .....	167
Tabla 35. Banda vs. CCQ Tx a 5.8GHz.....	168
Tabla 36. Banda vs. CCQ Rx a 5.8GHz.....	169
Tabla 37. Banda vs. Tasa de Transmisión a 5.8GHz .....	170
Tabla 38. Banda vs. Tasa de Recepción a 5.8GHz .....	171
Tabla 39. Ancho de Canal vs. Tasa de Transmisión Promedio a 5.8GHz .....	172
Tabla 40. Ancho de Canal vs. Tasa de Recepción Promedio a 5.8GHz .....	173
Tabla 41. Ancho de Canal vs. Tiempo de Respuesta a 5.8GHz.....	174
Tabla 42. Ancho de Canal vs. CCQ Tx a 5.8GHz .....	175
Tabla 43. Ancho de Canal vs. CCQ Rx a 5.8GHz .....	176
Tabla 44. Ancho de Canal vs. Tasa de Transmisión a 5.8GHz.....	177
Tabla 45. Ancho de Canal vs. Tasa de Recepción a 5.8GHz.....	178
Tabla 46. Frecuencia vs. Tasa de Transmisión a 5.8GHz.....	179
Tabla 47. Frecuencia vs. Tasa de Recepción Promedio a 5.8GHz .....	180
Tabla 48. Frecuencia vs. Tiempo de Respuesta a 5.8GHz.....	181
Tabla 49. Frecuencia vs. CCQ Tx A 5.8GHz .....	182
Tabla 50. Frecuencia vs. CCQ Rx a 5.8GHz .....	183
Tabla 51. Frecuencia vs. Tasa de Transmisión a 5.8GHz.....	184
Tabla 52. Frecuencia vs. Tasa de Transmisión a 5.8GHz.....	185

## INDICE DE CUADROS

Cuadro 1. Resumen del enlace AMAGUAÑA-ESPE.....	37
Cuadro 2. Configuración del enlace.....	39
Cuadro 3. Notas de instalación para la estación AMAGUAÑA.....	40
Cuadro 4. Notas de instalación para la estación ESPE .....	41
Cuadro 5. Especificaciones técnicas del router RB433AH.....	45
Cuadro 6. Especificaciones técnicas del router SXT 5HnD .....	48
Cuadro 7. Indicadores LED de la potencia de señal inalámbrica .....	49
Cuadro 8. Especificaciones técnicas de la antena del SXT5HnD.....	51
Cuadro 9. Opciones del parámetro <i>Mode</i> .....	60
Cuadro 10. Opciones del parámetro <i>Wireless Protocol</i> .....	64

## INDICE DE FIGURAS

Figura 1. Flujograma del funcionamiento de CSMA/CA .....	8
Figura 2. Funcionamiento de tres fases de CSM/CA .....	10
Figura 3. Funcionamiento de TDMA .....	13
Figura 4. Trama de TDMA .....	14
Figura 5. Patrones de irradiación. a) isotrópico, b) direccional, c) omnidireccional .....	19
Figura 6. Zona de Fresnel. ....	21
Figura 7. Topología de red del enlace a 2.4GHz.....	28
Figura 9. Vista satelital de la estación ESPE .....	30
Figura 10. Coordenadas de la estación ESPE .....	31
Figura 11. Estación ESPE .....	31
Figura 12. Vista satelital de la estación AMAGUAÑA .....	32
Figura 13. Coordenadas de la estación AMAGUAÑA.....	32
Figura 14 Estación AMAGUAÑA.....	33
Figura 15. Opción <i>New Network Site</i> .....	34
Figura 16. Configuración de la estación AMAGUAÑA en PTP LinkPlanner .....	35
Figura 17. Configuración de la estación ESPE en PTP LinkPlanner.....	35
Figura 18. Opción <i>New Link</i> .....	35
Figura 19. Opción <i>Installation Report PDF</i> .....	36
Figura 20. Mapa de red .....	37
Figura 21. Mapa de altimetría. ....	38
Figura 22. Características de los equipos Mikrotik.....	43
Figura 23. Router RB433AH .....	44
Figura 24. Router SXT 5HnD .....	47
Figura 25. Puerto LAN 1 del router SXT5HnD.....	49
Figura 26. Indicadores LED de la potencia de la señal inalámbrica.....	50
Figura 27. Antena HyperLink Technologies HG2414G .....	52
Figura 28. Polaridad vertical y horizontal.....	52
Figura 29. Patrón de irradiación vertical.....	54



Figura 30. Patrón de irradiación horizontal.....	55
Figura 31. Ingreso al RouterOS a través web browser.....	56
Figura 32. Ingreso a RouterOS a través de Winbox.....	57
Figura 33. Direccionamiento IP en RouterOS .....	57
Figura 34. Configuración de direcciones IP en las interfaces en RouterOS .....	58
Figura 35. Activación de la interface <i>Wireless</i> en RouterOS.....	58
Figura 36. Sección <i>General</i> .....	59
Figura 37. Sección <i>Wireless</i> .....	59
Figura 38. Configuración del parámetro <i>Mode</i> .....	60
Figura 39. Configuración del parámetro <i>Band</i> .....	61
Figura 40. Configuración del parámetro <i>Channel Width</i> .....	61
Figura 41. Configuración del parámetro <i>Frecuency</i> .....	62
Figura 42. Configuración del parámetro <i>SSID</i> .....	62
Figura 43. Configuración del parámetro <i>Scan List</i> .....	63
Figura 44. Configuración del parámetro <i>Wireless Protocol</i> .....	63
Figura 45. Configuración del parámetro <i>Security Profile</i> .....	65
Figura 46. Configuración del parámetro <i>Frecuency Mode</i> .....	65
Figura 47. Configuración del parámetro <i>Country</i> .....	66
Figura 48. Configuración del parámetro <i>Antenna Gain</i> .....	66
Figura 49. Configuración del parámetro <i>DFS Mode</i> .....	67
Figura 50. Configuración del parámetro <i>Proprietary Extensions</i> .....	67
Figura 51. Configuración de los parámetros <i>Default AP Tx Rate</i> y <i>Default Client Tx Rate</i> .....	68
Figura 52. Configuración del parámetro <i>Multicast Helper</i> .....	68
Figura 53. Sección <i>Data Rates</i> .....	69
Figura 54. Sección <i>Advanced</i> .....	71
Figura 55. Sección <i>HT</i> .....	72
Figura 56. Sección <i>WDS</i> .....	72
Figura 57. Sección <i>Nstreme</i> .....	73
Figura 58. Sección <i>Tx Power Mode</i> .....	73

Figura 59. Sección <i>Current Power</i> .....	74
Figura 60. Sección <i>Status</i> .....	75
Figura 61. Sección <i>Traffic</i> .....	75
Figura 62. Asistente de una nueva máquina virtual .....	76
Figura 63. Fuente de instalación del sistema operativo Centos7 en VMWare .....	77
Figura 64. Creación de un usuario en VMWare .....	77
Figura 65. Configuración del nombre de la máquina virtual .....	78
Figura 66. Configuración del tamaño del disco duro de la máquina virtual .....	78
Figura 67. Personalización de la máquina virtual .....	79
Figura 68. Configuración de la memoria RAM de la máquina virtual .....	79
Figura 69. Configuración del procesador de la máquina virtual .....	80
Figura 70. Configuración de la tarjeta de red de la máquina virtual .....	80
Figura 71. Configuración del usuario de Centos 7 .....	81
Figura 72. Instalación de Centos 7 .....	81
Figura 73. Configuración del idioma de Gnome .....	82
Figura 74. Configuración del teclado en Gnome .....	82
Figura 75. Configuración de la dirección IP en Centos 7 .....	83
Figura 76. Ingreso como usuario root .....	84
Figura 77. Instalación del paquete vsftpd .....	84
Figura 78. Ingreso al archivo vsftpd.conf .....	84
Figura 79. Configuración de acceso en el archivo vsftpd.conf .....	85
Figura 80. Configuración de descarga, conexión y logs en el archivo vsftpd.conf .....	85
Figura 81. Activación de la lista de usuarios en el archivo vsftpd.conf .....	86
Figura 82. Configuración de puertos en el archivo vsftpd.conf .....	86
Figura 83. Activación del soporte SSL/TLS en el archivo vsftpd.conf .....	87
Figura 84. Creación del archivo chroot_list .....	87
Figura 85. Creación del certificado y firma digital .....	88
Figura 86. Creación de usuarios vsftp .....	88
Figura 87. Activación del servicio vsftp .....	88
Figura 88. Prueba de funcionamiento del servidor vsftp .....	89

Figura 89. Prueba de funcionamiento del servidor vsftp a través de Wireshark.....	89
Figura 90. Instalación del paquete nfs-utils .....	90
Figura 91. Creación del directorio compartido del servidor NFS.....	90
Figura 92. Configuración del archivo exports.conf .....	91
Figura 93. Inicialización del servicio NFS.....	91
Figura 94. Creación del directorio compartido en el cliente NFS.....	91
Figura 95. Exploración de puntos de montaje.....	91
Figura 96. Montaje del directorio compartido del servidor NFS .....	92
Figura 97. Comprobación del montaje del directorio compartido .....	92
Figura 98. Prueba de funcionamiento del servidor NFS por medio de Wireshark .....	92
Figura 99. Instalación de los paquetes SMB.....	93
Figura 100. Ingreso al archivo smb.conf.....	93
Figura 101. Configuración de los clientes con acceso al servidor SMB.....	93
Figura 102. Configuración de los logs del servidor SMB.....	94
Figura 103. Configuración del directorio compartido del servidor SMB .....	94
Figura 104. Creación del directorio compartido .....	94
Figura 105. Permisos para el directorio compartido .....	95
Figura 106. Inicialización del servicio SMB.....	95
Figura 107. Verificación del funcionamiento de SMB en un equipo Windows .....	95
Figura 108. Prueba de funcionamiento del servidor SMB a través de Wireshark .....	96
Figura 109. Asignación de espacio de disco duro para Trixbox .....	96
Figura 110. Selección de teclado en Trixbox.....	97
Figura 111. Selección de la zona horaria en Trixbox.....	97
Figura 112. Creación del usuario en Trixbox.....	98
Figura 113. Instalación finalizada de Trixbox .....	98
Figura 114. Acceso A Trixbox.....	98
Figura 115. Configuración de la interface ether0.....	99
Figura 116. Reinicio del servidor Trixbox.....	99
Figura 117. Inicio de Trixbox .....	99
Figura 118. Autenticación en Trixbox .....	100

Figura 119. Estado del sistema Trixbox.....	100
Figura 120. Configuración de PBX en Trixbox .....	101
Figura 121. Tipos de dispositivos en Trixbox.....	101
Figura 122. Configuración de extensiones en Trixbox .....	101
Figura 123. Zoiper Setup.....	102
Figura 124. Licencia Zoiper .....	102
Figura 125. Selección de Componentes Zoiper .....	102
Figura 126. Finalización de la instalación de Zoiper .....	103
Figura 127. Ajustes Zoiper.....	103
Figura 128. . Creación Cuenta en Zoiper .....	104
Figura 129. Tipo de Cuenta Zoiper .....	104
Figura 130. Credenciales Zoiper .....	105
Figura 131. Registro de cuenta SIP .....	105
Figura 132. Prueba de funcionamiento de la central de VoIP con Wireshark .....	105
Figura 133. Opción <i>Addresses</i> .....	106
Figura 134. Añadir una nueva dirección IP .....	107
Figura 135. Configuración de una dirección IP .....	107
Figura 136. Activación de la interface wlan .....	108
Figura 137. Sección <i>Wireless</i> .....	108
Figura 138. Escaneo de la red ESPE.....	109
Figura 139. Sección <i>DCHP Client</i> .....	109
Figura 140. Creación del cliente DHCP.....	110
Figura 141. Elección de la interface DHCP Client .....	110
Figura 142. Sección <i>DNS</i> .....	111
Figura 143. Activación del servicio DNS .....	111
Figura 144. Sección <i>Firewall</i> .....	112
Figura 145. Crear una nueva regla NAT.....	112
Figura 146. Enmascaramiento de direcciones IP .....	113
Figura 147. Sección <i>Routes</i> .....	113
Figura 148. Creación de una ruta por defecto .....	114

Figura 149. Ping desde ESPE hasta AMAGUAÑA a 2.4GHz con Nstreme .....	115
Figura 150. Ping desde AMAGUAÑA hasta ESPE a 2.4GHz con Nstreme .....	115
Figura 151. Ping desde ESPE hasta AMAGUAÑA a 5.8GHz con Nstreme.....	116
Figura 152. Ping desde AMAGUAÑA hasta ESPE a 5.8GHz con Nstreme .....	117
Figura 153. Ping desde ESPE hasta AMAGUAÑA a 2.4GHz con Nv2.....	117
Figura 154. Ping desde AMAGUAÑA hasta ESPE a 2.4GHz con Nv2.....	118
Figura 155. Ping desde ESPE hasta AMAGUAÑA A 5.8GHz con Nv2 .....	118
Figura 156. Ping desde AMAGUAÑA hasta ESPE A 5.8GHz con Nv2 .....	119
Figura 157. Prueba con Btest desde ESPE hasta AMAGUAÑA a 2.4GHz con Nstreme .....	120
Figura 158. Prueba con Btest desde AMAGUAÑA hasta ESPE a 2.4GHz con Nstreme .....	120
Figura 159. Prueba con Btest desde ESPE hasta AMAGUAÑA a 5.8GHz con Nstreme .....	121
Figura 160. Prueba con Btest desde AMAGUAÑA hasta ESPE a 5.8GHz con Nstreme .....	122
Figura 161. Prueba con Btest desde ESPE hasta AMAGUAÑA a 2.4GHz con Nv2....	122
Figura 162. Prueba con Btest desde AMAGUAÑA hasta ESPE a 2.4GHz con Nv2....	123
Figura 163. Prueba con Btest desde ESPE hasta AMAGUAÑA a 5.8GHz con Nv2....	124
Figura 164. Prueba con Btest desde AMAGUAÑA hasta ESPE a 5.8GHz con Nv2....	125
Figura 165. Tabla <i>Registration</i> .....	126
Figura 166. <i>Frequency Usage</i> para los enlaces a 2.4GHz y 5.8GHz .....	126
Figura 167. Menú Principal.....	127
Figura 168. Habilitación SNMP en RouterOS .....	128
Figura 169. Habilitación SNMP en Windows.....	128
Figura 170. Habilitación SNMP en Centos 7 .....	129
Figura 171. Descubrimiento de dispositivos con The Dude .....	130
Figura 171. Topología del enlace a 2.4GHz con The Dude.....	130
Figura 173. Comportamiento del router ESPE .....	131
Figura 174. Comportamiento del router AMAGUAÑA .....	131

Figura 174. Topología de red del enlace a 5.8GHz con The Dude.....	132
Figura 176. Comportamiento del router ESPE A 5.8GHz.....	132
Figura 177. Comportamiento del router AMAGUAÑA A 5.8GHz.....	133
Figura 178. Descubrimiento de dispositivos con LANState PRO.....	134
Figura 179. Topología de red a 2.4GHz con LANState PRO.....	134
Figura 180. Lista de dispositivos a 2.4GHz.....	135
Figura 181. Ancho de banda del router AMAGUAÑA a 2.4GHz.....	135
Figura 182. Ancho de banda del router ESPE a 2.4GHz.....	136
Figura 183. Topología de red a 5.8GHz con LANState PRO.....	136
Figura 184. Lista de dispositivos a 5.8GHz.....	137
Figura 185. Ancho de banda del router AMAGUAÑA a 5.8GHz.....	137
Figura 186. Ancho de banda del router ESPE a 5.8GHz.....	138
Figura 187. Inicio PRTG.....	139
Figura 188. Selección de Grupo.....	139
Figura 189. Nombre e Identificadores de Grupo.....	140
Figura 190. Sensores Enlace 2.4GHz.....	140
Figura 191. Trafico Wlan1 Amaguaña en 2.4GHz.....	141
Figura 192. Trafico Wlan1 ESPE en 2.4GHz.....	141
Figura 193. Sensores Enlace 5.8GHz.....	142
Figura 194. Sensor Ping Amaguaña en 5.8GHz.....	142
Figura 195. Sensor Ping ESPE en 5.8GHz.....	143
Figura 196. Banda vs. Tasa de transmisión promedio a 2.4GHz.....	144
Figura 197. Banda vs. Tasa de Recepción Promedio a 2.4GHz.....	145
Figura 198. Banda vs. Tiempo de respuesta a 2.4GHz.....	146
Figura 199. Banda vs. CCQ Tx a 2.4GHz.....	147
Figura 200. Banda vs. CCQ Rx a 2.4GHz.....	148
Figura 201. Banda vs. Tasa de transmisión a 2.4GHz.....	149
Figura 202. Banda vs. Tasa de Recepción a 2.4GHz.....	150
Figura 203. Ancho de Canal vs. Tasa de Transmisión Promedio a 2.4GHz.....	151
Figura 204. Ancho de canal vs. Tasa de recepción promedio a 2.4GHz.....	152

Figura 205. Ancho de Canal vs. Tiempo de Respuesta a 2.4GHz .....	153
Figura 206. Ancho de Canal vs. CCQ Tx a 2.4GHz .....	154
Figura 207. Ancho de Canal vs. CCQ Rx a 2.4GHz.....	155
Figura 208. Ancho de Canal vs. Tasa de Transmisión a 2.4GHz .....	156
Figura 209. Ancho de Canal vs. Tasa de Recepción a 2.4GHz .....	157
Figura 210. Frecuencia vs. Tasa de Transmisión Promedio a 2.4GHz .....	158
Figura 211. Frecuencia vs. Tasa de Recepción Promedio a 2.4GHz .....	159
Figura 212. Frecuencia vs. Tiempo de Respuesta a 2.4GHz .....	160
Figura 213. Frecuencia vs. CCQ Tx a 2.4GHz .....	161
Figura 214. Frecuencia vs. CCQ Rx a 2.4GHz .....	162
Figura 215. Frecuencia vs. Tasa de Transmisión a 2.4GHz.....	163
Figura 216. Frecuencia vs. Tasa de Recepción a 2.4GHz.....	164
Figura 217. Banda vs. Tasa de Transmisión Promedio a 5.8GHz .....	165
Figura 218. Banda vs. Tasa de Recepción Promedio a 5.8GHz .....	166
Figura 219. Banda vs. Tiempo de Respuesta a 5.8GHz.....	167
Figura 220. Banda vs. CCQ Tx a 5.8GHz.....	168
Figura 221. Banda vs. CCQ Rx a 5.8GHz .....	169
Figura 222. Banda vs. Tasa de Transmisión a 5.8GHz.....	170
Figura 223. Banda vs. Tasa de Recepción a 5.8GHz .....	171
Figura 224. Ancho de Canal vs. Tasa de Transmisión Promedio a 5.8GHz.....	172
Figura 225. Ancho de Canal vs. Tasa de Recepción Promedio a 5.8GHz.....	173
Figura 226. Ancho de Canal vs. Tiempo de Respuesta a 5.8GHz .....	174
Figura 227. Ancho de Canal vs. CCQ Tx a 5.8GHz.....	175
Figura 228. Ancho de Canal vs. CCQ Rx a 5.8GHz.....	176
Figura 229. Ancho de Canal vs. Tasa de Transmisión a 5.8GHz .....	177
Figura 230. Ancho de Canal vs. Tasa de Recepción a 5.8GHz .....	178
Figura 231. Frecuencia vs. Tasa de Transmisión Promedio a 5.8Ghz.....	179
Figura 232. Frecuencia vs. Tasa de Recepción a 5.8GHz.....	180
Figura 233. Frecuencia vs. Tiempo de Respuesta a 5.8GHz .....	181
Figura 234. Frecuencia vs. CCQ Tx a 5.8GHz .....	182

Figura 235. Frecuencia vs. CCQ Rx a 5.8Ghz.....	183
Figura 236. Frecuencia vs. Tasa de Transmisión a 5.8GHz.....	184
Figura 237. Frecuencia vs. Tasa de Recepción a 5.8GHz.....	185



## **RESUMEN**

La proliferación de redes inalámbricas debido a su flexibilidad y movilidad, y la necesidad de ofertar mejores servicios para las tecnologías de la información y comunicación hacen que constantemente se busque nuevas alternativas de conectividad; por lo que empresas como Mikrotik han enfocado sus esfuerzos en el desarrollo de nuevas alternativas que permitan obtener enlaces inalámbricos más eficientes. En el presente proyecto se elabora un estudio comparativo entre los protocolos inalámbricos propietarios de Mikrotik Nstreme y Nv2 para un enlace a 2.4GHz y 5.8GHz. Este estudio es realizado en un ambiente totalmente real, para lo que se implementó un enlace inalámbrico de aproximadamente 10 kilómetros, el cual cuenta con los servicios de Internet, voz sobre IP y transferencia de datos con la implementación de diferentes servidores, lo que se verifica si estos protocolos pueden soportar redes convergentes. Para obtener valores que permitan realizar la comparativa de estos dos protocolos se utiliza herramientas como Btest, The Dude, PRTG y LANState PRO. El estudio comparativo se enfoca en valores como: tasas de transferencia, tiempo de respuesta en la transmisión y calidad del enlace.

### **Palabras Claves:**

**MIKROTIK**

**NSTREME**

**NV2**

## **ABSTRACT**

The proliferation of wireless networks for its flexibility and mobility, and the need to offer better services for information and communication technologies constantly make new connectivity alternatives be sought; so companies like Mikrotik have focused their efforts on developing new technologies that enable more efficient wireless links. In this project, a comparative study of owner's wireless protocols Mikrotik Nv2 Nstreme for a link to 2.4GHz and 5.8GHz is made. This study is conducted in a fully realistic environment, so a wireless link of about 10 kilometers which features internet services, voice over IP and data transfer with the implementation of different servers with implemented it checks whether these protocols can support converged networks. For obtain values that allow comparative of these two protocols tools as Btest , The Dude, PRTG and LanState PRO is used. The comparative study focuses on values such as transfer rate, delay in transmission and quality link

**Key Words:**

**MIKROTIK**

**NSTREME**

**NV2**

## GLOSARIO DE TERMINOS

<b>ARP</b>	Es un protocolo que permite obtener una dirección lógica a partir de una dirección física
<b>BTEST</b>	Herramienta de Mikrotik para realizar pruebas de ancho de banda en enlaces inalámbricos
<b>CCK</b>	Esquema de modulación usado en redes inalámbricas IEEE 802.11b
<b>CCQ</b>	Es la calidad de conexión del cliente; un valor porcentual que muestra la eficacia del uso de ancho de banda.
<b>CENTOS</b>	Es un sistema operativo para la comunidad empresarial basado en el kernel GNU/Linux.
<b>CSMA/CA</b>	Protocolo de acceso al medio por detección de portadora con evasión de colisiones, el cual es usado en red inalámbricas.
<b>DHCP</b>	Protocolo que permite a los clientes de una red IP obtener los parámetros de configuración de manera automática
<b>DNS</b>	Protocolo que permite asociar un nombre de dominio con una dirección IP
<b>GNU/LINUX</b>	Termino utilizado para referirse al sistema operativo GNU con núcleo o kernel libre Linux
<b>IEEE</b>	Instituto de ingenieros eléctricos y electrónicos.
<b>IP</b>	Protocolo de comunicación de datos digitales clasificado en la capa de red del modelo OSI
<b>MIKROTIK</b>	Empresa dedicada al desarrollo de soluciones para la interconectividad de redes

<b>NFS</b>	Sistema de archivos de red para compartir información entre un servidor y los nodos clientes
<b>NSTREME</b>	Protocolo inalámbrico desarrollado por Mikrotik que utiliza TDMA para acceder al medio compartido
<b>NV2</b>	Protocolo Nstreme versión 2. Es la versión mejorada del protocolo Nstreme
<b>OFDM</b>	Método de multiplexación que utiliza un conjunto de ondas portadoras que transmite información en diferentes frecuencias.
<b>OSI</b>	Modelo de referencia para los protocolos de red
<b>POLLING</b>	Forma de control en redes de área local en donde una unidad central de procesamiento controla la transmisión de datos de cada cliente.
<b>PRTG</b>	Herramienta de monitorización de redes desarrollado por la empresa PAESSLER
<b>QAM</b>	Modulación de amplitud en cuadratura. Técnica que transporta dos señales diferentes mediante la modulación en amplitud y fase de la señal portadora.
<b>ROUTEROS</b>	Sistema operativo con el cual se administran los equipos creados por Mikrotik
<b>SMB</b>	Protocolo de red que permite compartir recursos entre nodos con sistema operativo Windows
<b>SNMP</b>	Protocolo de la capa de aplicación que permite el intercambio de información de administración entre los nodos de la red
<b>SSL</b>	Protocolo que permite el intercambio de información de forma segura. Utiliza claves de cifrado.

<b>TCP</b>	Protocolo de control de transmisión. Permite la conexión en la red de computadoras
<b>TDMA</b>	Protocolo de acceso al medio compartido por división de tiempo. Cada nodo tiene un tiempo determinado para realizar una transmisión
<b>THE DUDE</b>	Herramienta gratuita para la gestión de redes desarrollado por Mikrotik.
<b>TLS</b>	Protocolo criptográfico que permite tener comunicaciones seguras dentro de una red.
<b>TRIXBOX</b>	Distribución del sistema operativo GNU/Linux basado en Centos que funciona como una central telefónica
<b>TTL</b>	Tiempo de vida. Indica cuantos nodos puede pasar un paquete antes de ser descartado
<b>VSFTP</b>	Protocolo de transmisión de archivos muy seguro. Se lo denomina seguro debido a que envía la información encriptada
<b>WINBOX</b>	Herramienta grafica con la cual se puede ingresar y configurar el sistema operativo RouterOS
<b>WLAN</b>	Red de área local inalámbrica
<b>ZOIPER</b>	Herramienta que emula un teléfono convencional o IP en una computadora

# CAPITULO I

## INTRODUCCIÓN

### 1.1 Antecedentes.

En los últimos años se ha verificado la proliferación de redes inalámbricas. Esto se debe a varias razones, como el estilo de vida actual, la necesidad de mantener conectividad a redes locales o internet de forma constante, el soporte a la movilidad, mayor flexibilidad, etc. (Universidad Politecnica de Valencia, 2010)

La aparición de las redes inalámbricas ofrece muchas ventajas además de las referidas anteriormente. Entre ellas están la compatibilidad con las redes cableadas ya existentes, la facilidad de instalación, la reducción en los costes, la sencillez de administración, su escalabilidad, la capacidad de atravesar barreras físicas, etc. (Universidad Politecnica de Valencia, 2010)

En nuestra era han surgido los adictos a la información: gente que necesita estar todo el tiempo en línea. Para estos usuarios móviles, el cable de par trenzado, el cable coaxial y la fibra óptica no son útiles. Ellos necesitan obtener datos para sus computadoras laptop, notebook, de bolsillo, de mano o de reloj pulsera sin estar limitados a la infraestructura de comunicaciones terrestre. Para estos usuarios, la comunicación inalámbrica es la respuesta. (Tanenbaum, 2003)

En el futuro se aspira tener dos medios de comunicación: de fibra óptica e inalámbrica. Por lo tanto todos los aparatos fijos como computadoras, teléfonos, faxes, etc, se conectarán con fibra óptica; y todos los aparatos móviles usarán comunicación inalámbrica. (Tanenbaum, 2003)

Sin embargo, la comunicación inalámbrica también tiene ventajas para los dispositivos fijos en ciertas circunstancias. Por ejemplo, si es difícil tender fibras hasta un

edificio debido al terreno (montañas, selvas, pantanos, etc.), podría ser preferible un sistema inalámbrico. Vale la pena mencionar que la comunicación digital inalámbrica moderna comenzó en las islas de Hawái, en donde partes considerablemente grandes del océano Pacífico separaban a los usuarios, y el sistema telefónico era inadecuado. (Tanenbaum, 2003)

Desde la existencia de las redes inalámbricas muchas empresas de desarrollo han enfocado sus esfuerzos para crear métodos y protocolos que permitan mejor la interconectividad de los enlaces inalámbricos, una de estas empresas es Mikrotik.

Mikrotik es una empresa letona, que fue fundada en 1995 para desarrollar routers y sistemas Wireless ISP. Mikrotik ahora ofrece hardware y software para la conexión a internet en la mayoría de los países del mundo. (Mikrotik, 2013)

La experiencia en la industria de hardware de PC estándar y sistemas de enrutamiento permitió en 1997 crear el sistema de software RouterOS que proporciona una amplia estabilidad, control y flexibilidad para todo tipo de interfaces de datos y enrutamiento. (Mikrotik, 2013)

En el año 2002 se decidió a realizar su propio hardware, y nació la marca RouterBOARD. Existen distribuidores en la mayor parte del mundo, y clientes probablemente en todos los países del planeta. La empresa se encuentra en Riga, la capital de Letonia y cuenta con 80 empleados. (Mikrotik, 2013)

Existen dos protocolos de transporte de datos inalámbricos desarrollados por la empresa Mikrotik; Nstream y Nv2, que al utilizar la tecnología de acceso al medio TDMA (Acceso Múltiple por división de tiempo) tienen algunas ventajas con relación a los protocolos que utilizan CSMA/CA (Acceso múltiple por detección de portadora con evasión de colisión).

## **1.2 Justificación e Importancia.**

Desde finales de la década de los 90 ha surgido un gran interés por el uso de redes inalámbricas, esta demanda se ha seguido incrementando debido a la aparición de muchos dispositivos inalámbricos de gran movilidad y portabilidad como: teléfonos inteligentes, tablets y laptops.

Existe gran demanda de los enlaces inalámbricos gracias a que las tecnologías de nueva generación en redes inalámbricas como los estándares IEEE 802.11n, IEEE 80.11ac e IEEE 802. 11e permiten altas tasas de transferencia y mejora el rendimiento de la red.

En la actualidad la marca de equipos Mikrotik, se ha posicionado como una de las primeras opciones dentro de las empresas que proveen comunicaciones inalámbricas debido a la versatilidad de sus opciones de configuración, robustez en sus equipos y bajo costo de implementación.

Mikrotik provee dentro de su sistema operativo RouterOS, dos alternativas propietarias para la transmisión de flujo de datos inalámbricamente como son: NStream y NV2 (NStream Versión 2). Sin embargo una de las debilidades de esta marca de equipos es la falta de difusión en la información, razón por la cual se ve justificado el desarrollo del presente proyecto de fin de carrera, que implica el análisis, estudio, armado de trama, pruebas de ancho de banda utilizable, pruebas de estrés en ambos protocolos para las frecuencias en las que Mikrotik desarrolla tarjetas Wireless que son 2.4 GHz y 5.8 GHz.

## **1.3 Objetivos.**

### **1.3.1 Objetivo General.**

Diseñar e implementar un enlace de comunicaciones inalámbricas en frecuencias no licenciadas en 2.4GHz y 5.8GHz utilizando los protocolos de transmisión propietarios de la marca Mikrotik como son Nstream y Nv2, realizando además una comparativa de las funcionalidades y mejoras entre ambos protocolos.



### **1.3.2 Específicos.**

1.3.1.1 Comprender y analizar el funcionamiento de los protocolos Nstream y Nv2 a 2.4Ghz y 5.8GHz.

1.3.1.2 Implementar y configurar un enlace de comunicaciones inalámbrico entre la Universidad de las Fuerzas Armadas-ESPE y el cerro Amaguaña.

1.3.1.3 Comparar el funcionamiento de los protocolos Nstream y Nv2 a 2.4Ghz y 5.8GHz.

1.3.1.4 Realizar el análisis de las pruebas de funcionamiento y desempeño de los protocolos Nstream y Nv2.

## CAPITULO II

### MARCO TEÓRICO

#### **2.1 Redes Inalámbricas.**

Una red inalámbrica se define como una red que permite comunicar distintos dispositivos sin la necesidad de utilizar una conexión por cable; sino mediante la propagación de ondas electromagnéticas. Además, las redes inalámbricas facilitan el acceso a dispositivos remotos los cuales pueden estar a pocos metros de distancia como a varios kilómetros.

##### **2.1.1 Aplicaciones para Redes Inalámbricas.**

###### **2.1.1.1 Aplicaciones Punto a Punto.**

Los dispositivos de red inalámbrica punto a punto permiten tener muchas aplicaciones como por ejemplo trasladar servicios de internet, líneas telefónicas, o extensiones de conmutador, monitoreo de alarmas y sistemas de video vigilancia.

###### **2.1.1.2 Aplicaciones Punto – Multipunto.**

Las aplicaciones punto-multipunto permiten ahorrar hasta un 50% de recursos al compartir entre varias instalaciones relativamente lejanas; entre las más comunes se puede enfatizar algunas como: servicio de internet, servidores de trabajo como: web, correo electrónico, impresión, archivos, etc., líneas telefónicas, o incluso interconectar conmutadores telefónicos, análogos e híbridos para lograr comunicar sucursales, dependencias u organismos.

#### **2.2 Estándares IEEE 802.11 (a, b, g, n, ac).**

El estándar IEEE 802.11 comprende la parte de control de acceso al medio (MAC) y la capa física (PHY) para la implementación de la red de área local de comunicación inalámbrica (WLAN), el cual puede operar en las bandas de frecuencia de 2.4; 3; 6; 5 y

60 GHz. El estándar y los cambios constituyen la base de los productos de red inalámbricos que utilizan la marca gratuita WiFi.

### **2.2.1 IEEE 802.11a**

Este estándar trabaja en la banda de los 5 GHz y puede transmitir hasta 54 megabits por segundo. Utiliza OFDM, que es una técnica de codificación eficiente que divide la señal de radio en varias sub señales para después alcanzar un receptor. Con esto se logra reducir la interferencia entre señales.

### **2.2.2 IEEE 802.11b**

Es un estándar que posee una velocidad máxima de 11 megabits por segundo por lo cual es un estándar muy lento y menos costoso. Inicialmente 802.11b fue el estándar más popular debido a su costo, pero debido a estándares más rápidos este ha perdiendo popularidad. Esta norma transmite en la banda de frecuencia de 2.4 GHz, utiliza código complementario (CCK).

Los dispositivos que operan en el rango de 2.4 GHz, por ejemplo, pueden ser hornos de microondas, dispositivos Bluetooth, monitores de bebés, teléfonos inteligentes, y algunos equipos de radioaficionados.

### **2.2.3 IEEE 802.11g**

El estándar IEEE 802.11g transmite a 2.4 GHz como 802.11b pero a mayor velocidad. Similar a 802.11a; 802.11g es de transmisión más rápida, porque utiliza OFDM en vez de CCK. Funciona a una velocidad de bits de la capa física máxima de 54 megabits por segundo exclusivo de códigos de corrección de errores, o alrededor de 22 megabits por segundo de rendimiento promedio.

### **2.2.4 IEEE 802.11n**

Este es el estándar más reciente y se ha convirtiendo en uno de los más utilizados en los últimos años. 802.11n mejora significativamente la velocidad y alcance. Por

ejemplo, aunque 802.11g transmite teóricamente 54 megabits de datos por segundo, sólo alcanza velocidades reales de aproximadamente 24 megabits por segundo debido a la congestión de la red. 802.11n, sin embargo, puede transmitir de hasta 140 megabits por segundo. Para lo cual se utiliza múltiples señales y antenas inalámbricas en vez de una, esta tecnología se llama MIMO.

### **2.2.5 IEEE 802.11ac**

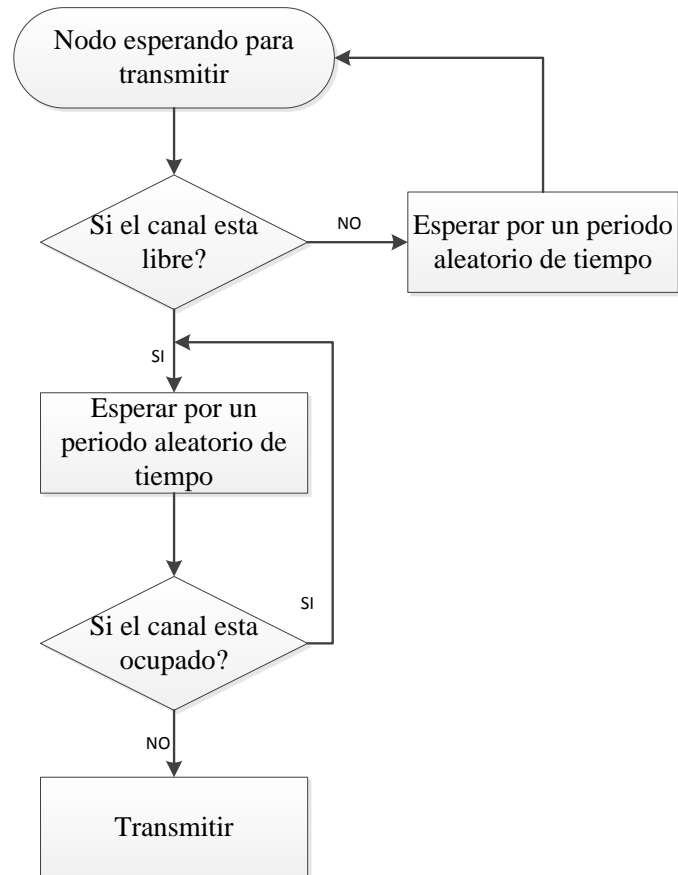
IEEE 802.11ac añade anchos de banda de canal de 80 MHz y 160 MHz con dos canales de 160 MHz contiguos y no contiguos de asignación de canal flexible. Se añade modulación de orden superior en forma de 256 modulaciones de amplitud en cuadratura (QAM), proporcionando una mejora adicional de 33 por ciento en tasa de datos. Una duplicación adicional de la velocidad de datos se logra aumentando el número máximo de flujos espaciales a ocho.

IEEE 802.11ac introduce una nueva tecnología revolucionaria para soportar múltiples transmisiones de enlace descendente concurrentes, que se conoce como "múltiple-usuario, múltiple-entrada, múltiple-salida" (MU-MIMO). Mediante el uso de la tecnología de antena inteligente, MU-MIMO permite un uso más eficiente del espectro, una mayor capacidad del sistema y latencia reducida apoyando hasta cuatro transmisiones de usuarios simultáneos. Esto es particularmente útil para dispositivos cliente con un número limitado de antenas, tales como teléfonos inteligentes y tabletas.

### **2.3 Acceso Múltiple por Detección de Portadora con Evasión de Colisiones.**

El acceso múltiple por detección de portadora con evasión de colisión (CSMA/CA), es un método de acceso al medio físico que es usado, por lo general en redes inalámbricas, el cual utiliza la detección de la portadora, para que un dispositivo conectado al medio físico detecte si éste se encuentra libre o no. Este método evita que existan colisiones de paquetes transmitiendo solo cuando el canal este libre, para esto, el dispositivo que desea transmitir un paquete espera un tiempo aleatorio corto, y si tras ese

tiempo el canal aún está libre se procede a la transmisión, evitando de esta manera que se produzca una colisión. CSMA/CA opera en la capa de datos del modelo OSI.



**Figura 1. Flujograma del funcionamiento de CSMA/CA**

## 2.3.1 Funcionamiento

### 2.3.1.1 Función de Coordinación Distribuida

El estándar IEEE 802.11 para WLAN define una función de coordinación distribuida (DCF) para compartir el acceso al medio a través del protocolo CSMA/CA. Un nodo escucha el canal antes de la transmisión para poder determinar si alguien más está transmitiendo, si el canal está libre comienza la transmisión.

Cuando el nodo receptor recibe un paquete, se envía un acuse de recibo denominado ACK después de un corto intervalo de tiempo desde que se recibió el paquete. Si el nodo transmisor no recibe un ACK, el paquete se considera perdido y se dispone una nueva retransmisión.

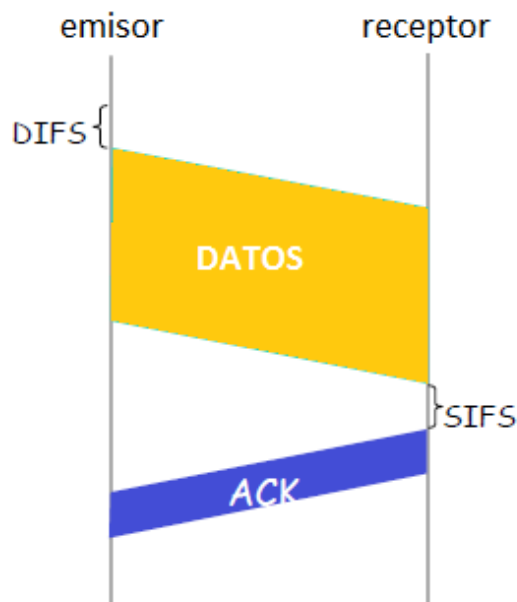
Para realizar la transmisión, el medio es censado, y si se encuentra libre se espera un intervalo de tiempo denominado DIFS (DCF Inter-Frame Space). Si el medio está ocupado el nodo aplaza su transmisión hasta el final de la transmisión actual y luego se espera un intervalo DIFS adicional y se genera un tiempo de retardo de envío (backoff) de manera aleatoria escogido en un intervalo  $[0, W - 1]$  donde  $W$  se denomina ventana de retardo de envío o ventana de contienda (CW).

El temporizador de retardo de envío comienza a reducir su tiempo siempre y cuando el medio sea censado para saber si se encuentra libre; si en ese tiempo se detecta una transmisión, el temporizador se detiene y se reanuda nuevamente el conteo cuando se detecta que el canal está nuevamente inactivo. Cuando el temporizador llega a 0, la estación transmite paquete.

Si dos o más nodos realizan el decremento de su temporizador de retardo de envío al mismo tiempo se produce una colisión, para evitar esta situación, el CW se duplica para cada retransmisión hasta que alcanza un valor máximo.

Cuando se recibe un paquete correctamente, el nodo de destino espera un intervalo de tiempo denominado SIFS (Short inter-Frame Space) inmediatamente después de que la recepción se ha completado y transmite un ACK de regreso hacia el nodo de origen confirmando la recepción del paquete.

Si el nodo de origen no recibe un ACK debido a errores de colisión o de transmisión, se reactiva el temporizador de retardo, después de que el canal permanece inactivo durante un intervalo extendido IFS (EIFS)



**Figura 2. Funcionamiento de tres fases de CSM/CA**

**Fuente: (Universidad de Navarra, 2013)**

### 2.3.1.2 Detección de Portadora en Redes Inalámbricas

La detección de portadora se realiza de dos maneras, la primera, mediante la detección física de la portadora por medio de la actividad en la interfaz inalámbrica, y la segunda, a través, de la detección de la portadora virtual que se realiza por el método de acceso RTS/CTS.

El método de acceso RTS/CTS permite que tanto los clientes inalámbricos como los Access Point (AP) intercambian las tramas de control RTS (Ready to send) y CTS (Clear to Send).

Cuando un cliente desea enviar datos, primero evalúa si el medio está libre; si lo está, se envía una trama RTS al AP solicitando el acceso dedicado durante un periodo específico. El AP recibe dicha trama, y si está libre envía al cliente inalámbrico una trama

CTS con la misma duración. Todos los demás dispositivos que observan la trama CTS permiten que el nodo transmisor realice el envío de datos. Para implementar la detección de portadora virtual, cada nodo envía información de duración en la cabecera de los paquetes RTS y CTS.

La información de duración indica la cantidad de tiempo que se debe reservar en el medio para la transmisión de los datos y la posterior devolución del paquete ACK. Las estaciones que se encuentran en el mismo conjunto de servicios básicos BSS (Basic Services Set), utilizan esta información para actualizar su vector de asignación de red, denominado NAV, que representa la cantidad de tiempo que tiene para acceder al medio, de esta manera cada nodo aprenderá cuanto tiempo debe utilizar para la transmisión de sus datos.

### **2.3.1.3 Esquema del Temporizador de Retardo Exponencial**

El temporizador de retardo (backoff) es escogido uniformemente en el rango  $[0, W - 1]$ , después de cada transmisión infructuosa; la ventana de retardo de envío duplica su tamaño hasta un valor máximo.

Una vez que el tamaño de la ventana de retardo de envío alcanza su máximo valor, se mantendrá en dicho valor hasta que se vuelva a restablecer. El valor de  $W$  se restablecerá después de cada transmisión exitosa, o cuando un contador de reintento de transmisión llegue a su límite.

### **2.3.2 Características de CSMA/CA**

- El protocolo de acceso al medio CSMA/CA es de tipo determinístico, esto quiere decir que cada nodo tiene asegurada su oportunidad de transmisión, siguiendo un criterio de rotación.
- CSMA/CA es un protocolo de acceso al medio de tres frases: escucha para ver si el medio está libre, transmite el dato, y espera un paquete de reconocimiento por parte del nodo receptor.



- CSMA/CA es un protocolo de la capa de acceso al medio del modelo OSI que es utilizado en redes LAN inalámbricas, ya en este tipo de redes es más probable que existan colisiones.
- El protocolo CSMA/CA asegura que los mensajes sean recibidos correctamente, sin embargo, debido a las dos transmisiones, la primera para enviar datos, y la segunda, para el envío del acuse de recibo; se pierde algo de eficiencia.

## **2.4 Acceso Múltiple por División de Tiempo**

El acceso múltiple por división de tiempo denominado TDMA es un método de acceso al medio compartido, el cual divide un único canal de comunicación en segmentos o ranuras de tiempo (slots), donde cada dispositivo de la red consigue uno o más segmentos, durante el cual se puede transmitir o recibir datos. TDMA permite dar servicios de alta calidad en la transmisión de voz y datos. (ALEGSA, 2009) .

TDMA fue especificado inicialmente entre los años 1988 y 1989 por el estándar IS-54, y ahora es definido en el estándar IS-13x de la EIA/TIA. Actualmente la compañía letona Mikrotik, está utilizando este tipo de acceso al medio para sus protocolos inalámbricos Nstream y Nv2.

### **2.4.1 Funcionamiento**

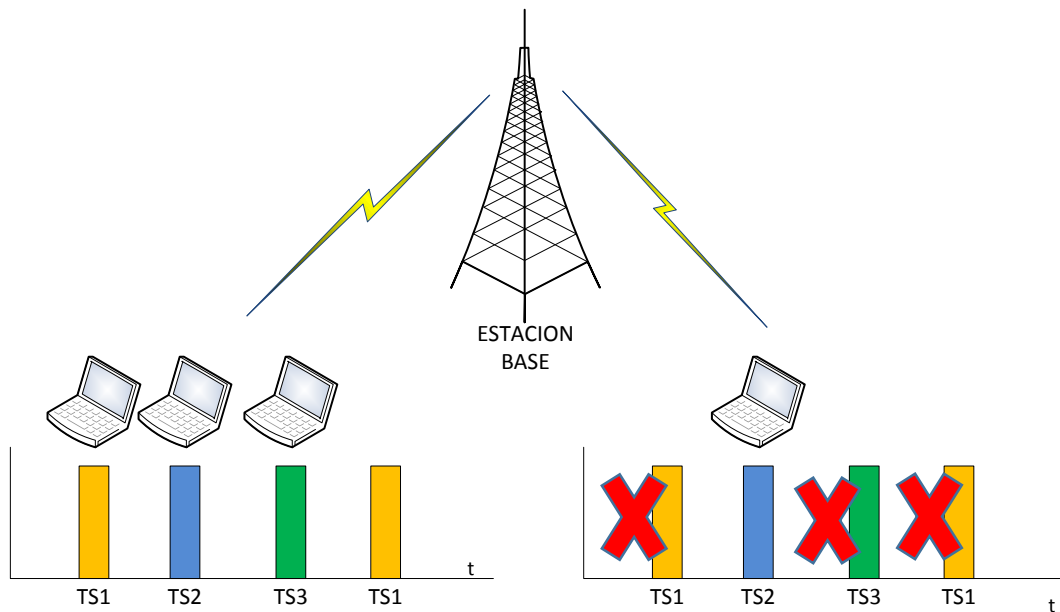
La técnica de acceso al medio por división de tiempo (TDMA) es utilizada en señales digitales, la cual logra una apariencia de continuidad en la asignación y uso de recursos frecuenciales, que realmente están compartidos temporalmente entre varios usuario.

Por lo tanto, se tiene una sola frecuencia de transmisión compartida, en que cada usuario tiene un determinado tiempo de transmisión, y cuando este tiempo termina, se da paso a la transmisión del siguiente usuario, haciendo de esta manera que el acceso sea sucesivo.

Es un sistema que aunque el usuario tenga la apariencia de tener un único canal siempre disponible, en realidad el recurso se va alternando a una velocidad lo

suficientemente alta como para que el usuario no note esta particularidad, por lo que es necesario la utilización de memoria adicional para almacenar los datos de transmisión hasta que al usuario le sea asignado un tiempo de transferencia.

Los sistemas que utilizan este método de acceso al medio deben poseer un mecanismo capaz de reconocer a cada uno de sus usuarios, así como de sincronización, que permita que cada nodo sea capaz de determinar el momento en que le toca acceder al recurso.



**Figura 3. Funcionamiento de TDMA**

**Fuente: (Sedin Escalona, 2004)**

TDMA se organiza en torno a tramas con una duración temporal  $T_t$ , siendo esta una sucesión de N cantidad de intervalos de tiempo asignados a cada terminal, por lo tanto, el tiempo que cada nodo tiene para acceder al medio será:  $T = T_t/N$ .

En este tiempo T el terminal deberá transmitir toda la información almacenada en memoria, en forma de un tren de bits denominado burst. Se debe tomar en cuenta que no todo el tiempo asignado al nodo se utiliza para la transmisión del burst, ya que la circuitería del transmisor necesita un tiempo para aumentar su nivel de potencia al adecuando; de la misma manera, al finalizar la transmisión se necesita un espacio de

tiempo para disminuir la potencia del transmisor a cero y evitar la interferencia con la siguiente comunicación.

Al momento de realizar la transmisión de datos, TDMA coloca una cabecera o tara al tren de bits a transmitir que se define de la siguiente manera:

$$B_b, \text{ bits total del burst} = B_o + B_i$$

$$B_o, \text{ bits de cabecera o tara} = B_{fa} + B_{co} + B_g$$

Donde:

$B_{fa}$ , es el formato de acceso TDMA

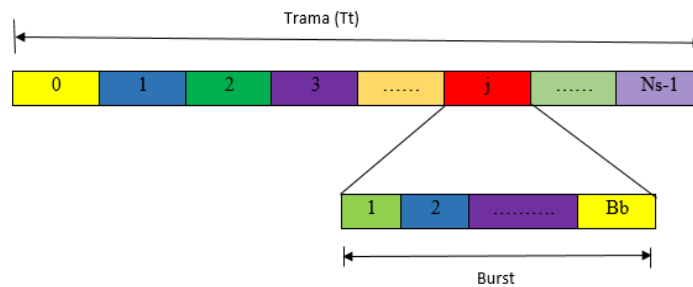
$B_{co}$ , codificación de canal

$B_g$ , Guarda

$$B_i, \text{ bit de información por trama} = v_c + T_t$$

Donde:

$v_c$ , velocidad de la fuente



**Figura 4. Trama de TDMA**

**Fuente: (Sedin Escalona, 2004)**

### 2.4.2 Características

- TDMA necesita una estricta sincronización de acceso para evitar colisiones de paquetes durante la transmisión en el enlace ascendente, y que cada terminal obtenga la información que corresponda en el enlace descendente.

- TDMA necesita que la información sea digitalizada, independientemente de que se transmita video, voz o datos.
- TDMA necesita establecer mecanismo que permitan a las estaciones bases recibir sus slots de tiempo independientemente de la distancia que se encuentre con respecto a sus emisores y receptores
- Se necesita establecer un límite de la duración de cada trama, para evitar el excesivo retraso al momento de acceder al medio.
- Todos los sistemas que utilizan TDMA para acceder al medio compartido necesitan algún medio de almacenamiento de información, en donde se pueda recopilar el tren de bits hasta esperar su tiempo de transmisión.

## **2.5 Ancho de Banda**

El término ancho de banda es la cantidad máxima de información o de datos que se consigue enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda es un factor clave a la hora de diseñar y analizar el desempeño de una red de datos. El ancho de banda está limitado por el tipo de medio de transmisión (cable de cobre, fibra óptica, etc.) y por la tecnología utilizada (xDSL, GPON, etc.).

El ancho de banda en los sistemas digitales se mide en bits por segundo (bps), pero, debido al gran avance en tecnologías de transmisión de datos se suele utilizar múltiplos de bits por segundo como los kilobits por segundo (kbps) o megabits por segundo (Mbps).

El ancho de banda queda limitado por el tipo de medio de transmisión y por las tecnologías de transmisión utilizadas, tanto en redes LAN, MAN y WAN. Las diferencias físicas en las formas en que se transmite la información por los diferentes medios, generan las limitaciones en la capacidad que cada medio tiene para transportar información.

**Tabla 1.****Anchos de banda por tecnología.**

<b>TECNOLOGIA</b>	<b>ANCHO DE BANDA</b>
Modem por teléfono	56 Kbps
ADSL Lite	1.5 Mbps
T1/DS1	1.544 Mbps
Ethernet	10 Mbps
Inalámbrico 802.11b	11 Mbps
T3/DS3	44.736 Mbps
Inalámbrico 802.11g	54 Mbps
Ethernet rápido	100 Mbps
OC3	155 Mbps
Inalámbrico 802.11n	600 Mbps
OC12	622 Mbps
Gigabit Ethernet	1 Gbps
OC48	2.5 Gbps
OC192	9.6 Gbps
Ethernet 10 Gigabits	10 Gbps

**Fuente: (Acevedo, 2012)**

### 2.5.1 Tasa de Transferencia

La tasa de transferencia es la medida real del ancho de banda en un momento determinado, en una ruta específica al transmitirse un conjunto específico de datos; por lo general, la tasa de transferencia es mucho menor que el ancho de banda máximo que el medio de transmisión soporta. La tasa de transferencia este determinado por los siguientes factores:

- Dispositivos de red
- Topología de la red
- Cantidad de usuarios en la red
- Tipos de datos que se transfiere
- Cantidad de usuarios simultáneos en la red
- Equipos terminales.

## 2.6 Retardo en la Transmisión.

El retardo en la transmisión o latencia es la suma de todos los retardos temporales que se producen durante la transmisión de información dentro de una red de datos. La latencia generalmente es produce por los siguientes factores:

- Demora en la propagación de los paquetes en el medio de transmisión.
- Mal estado de los medios de transmisión.
- Tamaño de los paquetes.
- Tamaño de los buffer o memoria en los equipos de conectividad.
- La cantidad de equipos de red intermediarios que existan entre el emisor y receptor
- Protocolos que controlan la transmisión.

Dependiendo del medio de transmisión que se utilice se obtendrá diferentes valores de latencia, es así que la fibra óptica puede tener una latencia casi nula, sin embargo, el cable de par trenzado puede llegar a tener hasta el triple de latencia de la fibra óptica. Incluso con el mismo tipo medio de transmisión se puede generar diferentes latencias, dependiendo del estado físico del medio.

Los buffer o memoria en algunas ocasiones también producen retardo, debido a que al tener paquetes de envío que superan al tamaño de la memoria se produce un cuello de botella haciendo que el retardo aumente en la red.

Una red de datos posee una variedad de equipos de red interconectados entre sí, y cada uno de estos equipos produce un tiempo de retardo debido al procesamiento que se realiza en cada uno de ellos, por lo tanto mientras un paquete tiene que atravesar menos equipos de red, la latencia se reducirá.

Los diferentes protocolos que se utilizan para la transmisión de datos también producen retardos, debido a que el proceso de verificación de datos y el establecimiento de la comunicación requiere de un tiempo. Algunos protocolos como TCP también poseen dentro de su cabecera algunos campos para la verificación de errores como el checksum lo cual produce algún tiempo de retardo adicional.

## 2.7 Antenas

Una antena es un sistema conductor metálico que permite radiar y recibir ondas electromagnéticas hacia el espacio libre; se lo puede considerar como un transductor porque convierte las ondas electromagnéticas en pulsos eléctricos y viceversa.

Una antena es un dispositivo reciproco pasivo; reciproco porque las características de transmisión y recepción son las mismas, y pasivo porque no puede amplificar la señal.

En los sistemas de comunicación las antenas son muy utilizadas para realizar enlaces a largas distancia.

### 2.7.1 Parámetros de una Antena

#### 2.7.1.1 Patrón de Radiación

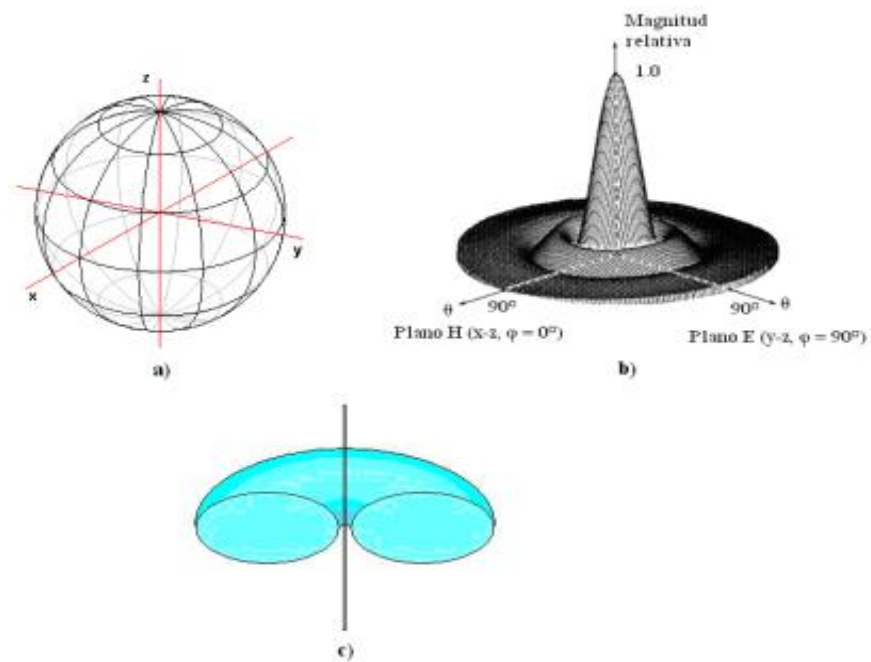
El parámetro de radiación es la representación gráfica en dos o tres dimensiones de la energía que irradia la antena. En el patrón de radiación en dos dimensiones existen dos planos sobre los cuales se grafica la representación de la energía de irradiación de la antena; el plano Azimutal y el plano de elevación. El plano azimutal es considerado como el plano horizontal y está relacionado con el ángulo  $\phi$ , mientras que el plano de elevación o plano vertical está relacionado con el ángulo  $\theta$ .

Los parámetros más significativos del patrón de radiación son:

- Dirección de apuntamiento.- Es el punto donde se produce la máxima radiación.
- Lóbulo principal.-Es el área del patrón de radiación rodeada por regiones con relativa alta intensidad
- Lóbulos secundarios.- Son lóbulos de menor intensidad energética que el lóbulo principal
- Ancho de haz.- Es la dirección en la que la potencia radiada se comprime a la mitad.
- Relación de lóbulo principal a secundario (SLL).- Es el cociente en dB entre el valor máximo del lóbulo principal y el valor máximo del lóbulo secundario.

Existen tres tipos de patrones de irradiación que son:

- Patrón Isotrópico.- Patrón que muestra que una antena irradia en todas las direcciones con la misma potencia, caso ideal (figura 5a).
- Patrón Direccional.- Patrón de radiación que muestra que la energía puede irradiar hacia el plano azimutal, plano de elevación o ambos (figura 5b)
- Patrón Omnidireccional.- Representa un patrón no direccional en un plano, y direccional en el otro (figura 5c).



**Figura 5. Patrones de irradiación. a) isotrópico, b) direccional, c) omnidireccional**

**Fuente: (Aquino, 2008)**



### **2.7.1.2 Tamaño**

El tamaño de una antena está relacionado estrictamente a la frecuencia. Cada frecuencia equivale a una longitud de onda, dicha longitud determina el tamaño de la antena; a mayor frecuencia la longitud de onda es menor, por lo tanto el tamaño de la antena se reduce y viceversa.

### **2.7.1.3 Polaridad**

La polaridad de una antena se refiere a la forma en que están colocadas ya sea en una torre de telecomunicaciones o en un mástil. Las ondas electromagnéticas poseen un campo eléctrico que se desplaza en sentido vertical, y un campo magnético que se desplaza en sentido horizontal. Para determinar la polaridad de una antena se toma como referencia al campo eléctrico. Se debe tomar en cuenta que para realizar un enlace inalámbrico es necesario que las antenas tengan la misma polaridad.

### **2.7.1.4 Directividad**

La directividad se refiere a las zonas en donde la antena irradia la mayor potencia. La directividad de una antena se lo puede observar en el patrón de irradiación, que es propio de cada antena. Según la directividad existen las antenas omnidireccionales; las cuales irradian la misma potencia en todas las direcciones; y las antenas direccionales, las cuales concentran su mayor potencia hacia una determinada dirección.

### **2.7.1.5 Ganancia**

La ganancia de una antena se refiere a la relación entre la mayor potencia irradiada en una dirección determinada, con relación a la potencia que irradia una antena isotrópica. La ganancia viene expresada en decibelios [db].

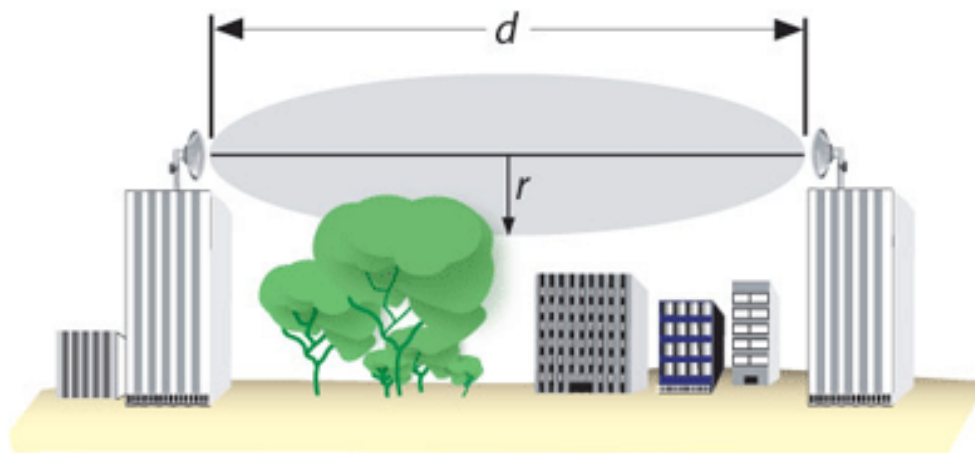
### **2.7.1.6 Impedancia**

La impedancia de una antena es la relación entre la tensión y la corriente en sus terminales; la impedancia se lo simboliza con un número complejo en donde la parte real representa la resistencia de la antena, y la parte imaginaria es la reactancia.

### 2.7.2 Zona de Fresnel

Para realizar un enlace inalámbrico de alta frecuencia es necesario que exista línea de vista; es decir que debe existir un camino limpio, sin obstáculos, entre la antena emisora y receptora.

La zona de Fresnel son elipsoides concéntricos que rodean a la línea de vista. Las ondas electromagnéticas emitidas por una antena pueden reflejarse en la superficie de estos elipsoides antes de incidir en la antena receptora, haciendo que exista un desfase al momento de la recepción.



**Figura 6. Zona de Fresnel.**

**Fuente: (Mundo Teleco, 2014)**

La primera zona de Fresnel abarca hasta un desfase de  $180^\circ$ ; la segunda zona comprende hasta  $360^\circ$  de desfase por lo que el segundo elipsoide contiene al primero.

Las posibles reflexiones que se pueden dar en el borde de la primera zona de Fresnel pueden causar atenuación puesto que la onda reflejada llegaría en oposición de fase a la antena receptora, por lo tanto durante la planificación del radioenlace se debe tomar en cuenta que no debe haber obstrucción que sobrepase el 40% de la primera zona de Fresnel.

Para el cálculo de la zona de Fresnel se utiliza la siguiente fórmula:

$$r = 17.32 \sqrt{\frac{d}{4f}}$$

Dónde: r, es el radio de la primera zona de Fresnel

d, distancia entre las antenas en kilómetros

f, es la frecuencia de transmisión en GHz

## **2.8 Protocolo Nstreme**

Nstreme es un protocolo para redes inalámbricas desarrollado y patentado por la marca Mikrotik, el cual es utilizado en redes punto a punto y punto-multipunto. Este protocolo posee un pequeño encabezado de trama, lo que permite una alta velocidad de transmisión y limita el retardo, por lo que se lo puede utilizar en enlaces de larga distancia. Es compatible con los chips Atheros 802.11a/b/g/n; en los modelos AR5211 y AR5212 únicamente.

Nstreme utiliza el método de acceso al medio TDMA (Acceso al Medio por División de Tiempo), corrigiendo, de esta manera, el inconveniente del nodo oculto y haciendo más eficiente el uso del canal, mejorando el rendimiento y la latencia, principalmente en redes punto-multipunto

### **2.8.1 Funcionalidad y Características**

#### **2.8.1.1 Funcionalidad**

El protocolo Nstreme utiliza el método de acceso al medio llamado TDMA, por lo que es necesario determinar la unidad central de procesamiento o Access Point Nstreme, este dispositivo realizará la segmentación de tiempo para que cada cliente pueda tener su

espacio para la transmisión, tanto de downlink (datos enviados desde el AP a los clientes) como de uplink (datos enviados desde los clientes al AP)

El AP Nstreme generará una agenda de transmisión para cada cliente; con lo que se evitará la interferencia al momento de la transmisión. Nstreme es soportado por dispositivos Mikrotik que posean RouterOS con licencia de nivel 3 en adelante.

El AP Nstreme posee un slot de tiempo que no es usado por los clientes que ya están conectados, este tiempo sirve para que nuevos clientes realicen la registración y se puedan conectar a la red Nstreme.

Nstreme puede operar en los siguientes modos:

- Modo Punto a Punto.- El modo punto a punto se refiere a que se tiene solo dos estaciones, la una que hará de Access Point y la otra de cliente.
- Modo Punto a Punto de radio dual.- El protocolo puede ser usado con dos antenas en el mismo sitio, la una para transmitir y la otra para recibir de manera simultánea, lo que permite una conexión de manera más rápida y eficiente. A esta modificación del protocolo se lo conoce como Nstreme dual.
- Modo Punto-Multipunto.-En este modo, el AP Nstreme hace una consulta constante hacia los clientes para crear un sincronismo de transmisión y de esta manera evitar colisiones, este método se denomina polling de cliente.

### **2.8.1.2 Características**

- Nstreme posee una forma de control para el acceso de los clientes denominado polling, según el cual cada Access Point (AP) pide, de acuerdo con su agenda de programación determinada a cada puesto de trabajo conectado a la red, si ha de enviar alguna información.
- El polling de cliente reduce los tiempos de acceso al medio, porque la tarjeta de red del cliente no tiene que censar el medio (aire) cada vez que necesita transmitir datos. El polling o sondeo se encarga de ello.

- Posee un ajuste dinámico, dependiendo del tipo de tráfico y el uso de recursos
- Nstreme posee muy baja sobrecarga de encabezado en su trama lo que permite velocidades de datos muy altas
- No posee degradación de velocidad en enlaces de larga distancia
- Soporte WDS(Sistema de distribución Wireless )

### **2.8.2 Compatibilidad y Coexistencia entre otros Protocolos Inalámbricos**

El protocolo Nstreme y sus diferentes variantes son incompatible con otros protocolos inalámbricos, incluyendo a los que trabajan con TDMA.

Los dispositivos 802.11 no podrán reconocer ni conectarse con un AP Nstreme. Los equipos RouterOS que tengan el soporte para el protocolo Nstreme, con licencia de nivel 3 en adelante, verán los AP por medio del comando SCAN, pero sólo se conectarán a ellos cuando estén debidamente configurados como clientes Nstream.

## **2.9 Protocolo Nv2**

Nv2 es un protocolo inalámbrico desarrollado por Mikrotik que permite trabajar con los chips inalámbricos Atheros 802.11. Nv2 utiliza el protocolo de acceso al medio TDMA en lugar de CSMA/CA, usado en los dispositivos 802.11.

TDMA corrige el inconveniente del nodo oculto y hace más eficiente el uso del canal, mejorando el rendimiento y la latencia, principalmente en redes punto-multipunto.

Nv2 es soportado por los chips Atheros 802.11n y demás chipsets 802.11a/b/g partiendo desde el AR5212, pero no soportado en AR5210 ni en ningún otro chipset anterior al AR5211. Esto significa que ambos (802.11n y dispositivos estándar) pueden formar parte de la misma red sin la necesidad de actualizar el hardware para implementar Nv2. (Mikrotik, 2010)

## **2.9.1 Funcionalidad y Características**

### **2.9.1.1 Funcionalidad**

El acceso al medio en redes inalámbricas que utilizan Nv2 es controlado por el Access Point Nv2, el cual se encarga de dividir el tiempo en períodos de tamaño fijo denominados slots de tiempo, los cuales son dinámicamente fraccionados en segmentos de downlink (datos enviados desde el AP a los clientes) y uplink (datos enviados desde los clientes al AP), utilizando el estado de colas en el AP y clientes. El tiempo de uplink es fragmentado entre los clientes conectados, teniendo en cuenta sus requerimientos de ancho de banda. Al inicio de cada ciclo, el AP transmite su agenda de transmisión (schedule), la cual muestra a los clientes cuando pueden transmitir y que cantidad de tiempo pueden utilizar.

Con la finalidad de permitir que los nuevos clientes puedan conectarse al AP, éste fija periódicamente un tiempo de enlace ascendente para los "clientes no especificados". Este intervalo de tiempo se utiliza para que los nuevos clientes puedan comenzar la registración; después el AP realiza un retardo de propagación entre él mismo y el cliente con lo cual inicia periódicamente la programación de tiempo de enlace ascendente para que el cliente pueda completar la registración y recibir datos.

En cuanto a calidad de servicio (QoS), Nv2 diseño un número variable de colas de prioridad incluidas por defecto, lo que conlleva a que también se puede ajustar a las políticas de QoS con las reglas de firewall o información de prioridad propagada a través de la red empleando VLAN o MPLS.

### **2.9.1.2 Características**

En la versión 5.0rc1, Nv2 tiene las siguientes características:

- Acceso al medio por TDMA
  - Soporte WDS (Sistema de Distribución Wireless)
  - Soporte de QoS con un numero variable de colas de prioridad

Desde la versión 5.0rc2:

- Encriptación de datos

Desde la versión 5.0rc3:

- Características de autenticación de RADIUS

Desde la versión 5.0rc4:

- Se insertaron algunos campos estadísticos olvidados

Características que aún no tiene Nv2:

- Políticas de acceso al medio controladas por el administrador
- Sincronismo entre los AP Nv2

### **2.9.2 Compatibilidad y Coexistencia entre otros Protocolos Inalámbricos**

Nv2 no es compatible con cualquier otro protocolo inalámbrico, ya sea que esté relacionado con TDMA o cualquier otro tipo, incluyendo Motorola Canopy, Airmax Ubiquiti y la práctica TDMA de FreeBSD; por lo tanto sólo los dispositivos que soporten y tengan habilitado el protocolo Nv2 podrán tener conectividad.

Los demás dispositivos 802.11 no reconocerán ni podrán conectarse a un AP Nv2. Los equipos RouterOS que tengan el soporte para el protocolo Nv2 desde la versión 5.0rc1 en adelante, verán los AP Nv2 por medio del comando SCAN, pero sólo se conectarán a ellos cuando estén debidamente configurados.

Debido a que Nv2 no utiliza la tecnología CSMA/CA, puede interferir con cualquier otra red en el mismo canal; otras redes pueden perturbar a la red Nv2, porque cualquier otra señal es considerada como ruido.

Puntos clave acerca de la compatibilidad y la coexistencia:

- Sólo los dispositivos RouterOS podrán formar parte en redes Nv2.
- Sólo los dispositivos RouterOS verán el AP Nv2 al realizar el escaneo.

- Una red Nv2 interferirá a otras redes si se encuentran el mismo canal.
- Una red Nv2 puede verse afectada en su rendimiento por cualquier otra red en el mismo canal, ya sea Nv2 o no.
- Un dispositivo con habilitado con Nv2 no se conectará a cualquier otra red basada en TDMA.

### **2.10 Diferencias entre Nv2 y Nstreme**

- Reducción del encabezado de polling.- El AP Nv2 en vez de sondear a cada cliente, transmite su agenda de asignación de tiempos por broadcast, de esta manera se evita la pérdida de tiempo en el sondeo de cada cliente individual, dejando más tiempo para la transmisión de datos reales. Esto mejora el rendimiento, especialmente en configuraciones punto a multipunto.
- Reducción del retardo de propagación del encabezado.- Nv2 no sondea a cada cliente individualmente, lo que permite crear una agenda basada en la distancia estimada a los clientes (retardo de propagación) con lo que se obtiene un uso de canal más efectivo. Esto también mejora el rendimiento, especialmente en configuraciones punto a multipunto. (Mikrotik, 2010)
- Nv2 posee más control sobre la latencia, sobrecarga reducida, tamaños de período ajustable y características de QoS que permite un mayor control sobre la latencia en la red.

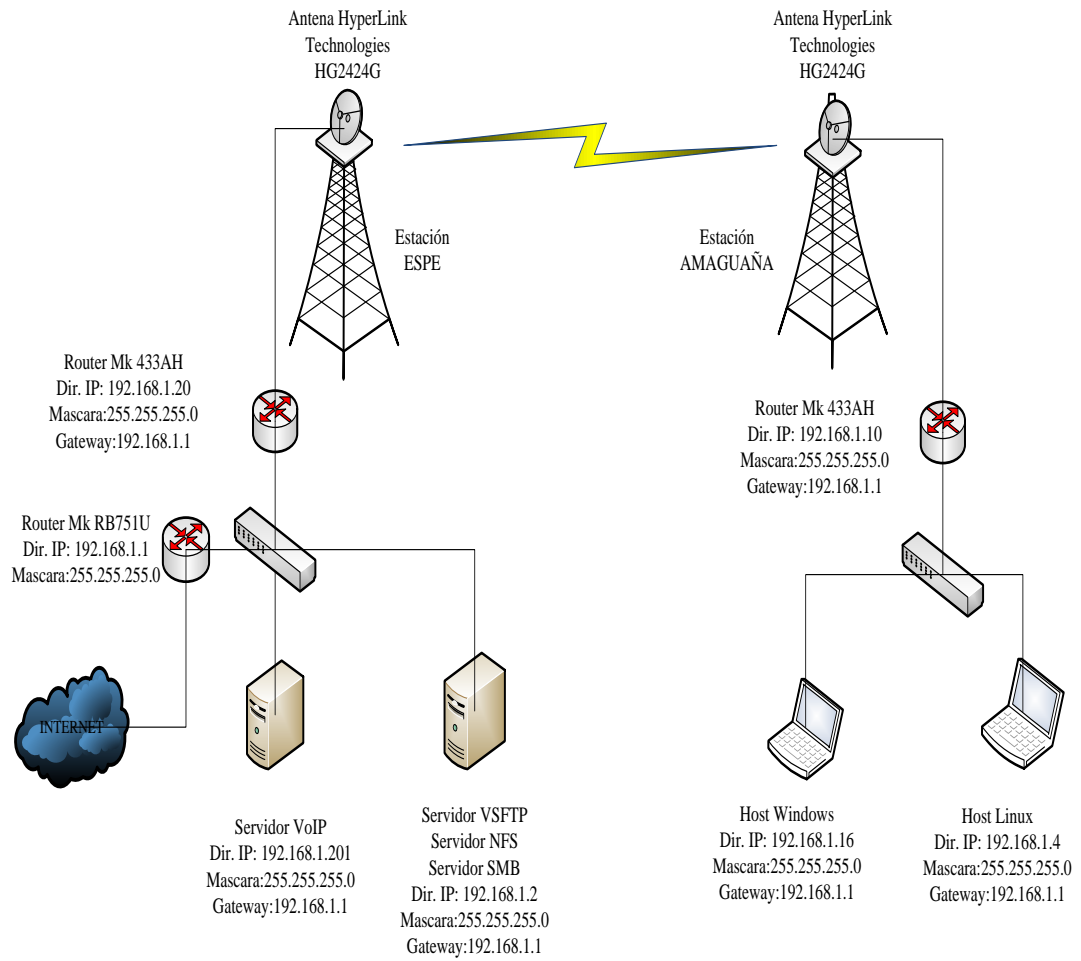


## CAPITULO III

### ENLACE INALÁMBRICO

#### 3.1 Topología De La Red

##### 3.1.1 Topología del Enlace a 2.4Ghz



**Figura 7. Topología de red del enlace a 2.4GHz**

Tabla 2.

Tabla de direccionamiento IP del enlace de 2.4GHz

Nombre	Interface	Dirección IP	Mascara	Gateway
<b>RB-INTERNET</b>	Ether 1	192.168.1.1	255.255.255.0	N/A
<b>RB-ESPE</b>	Bridge wireless-ether1	192.168.1.20	255.255.255.0	N/A
<b>RB-AMAGUAÑA</b>	Bridge wireless-ether1	192.168.1.10	255.255.255.0	N/A
<b>Servidor 1</b>	NIC	192.168.1.201	255.255.255.0	192.168.1.1
<b>Servidor 2</b>	NIC	192.168.1.2	255.255.255.0	192.168.1.1
<b>Host 1</b>	NIC	192.168.1.16	255.255.255.0	192.168.1.1
<b>Host 2</b>	NIC	192.168.1.4	255.255.255.0	192.168.1.1

### 3.1.2 Topología del Enlace de 5.8Ghz

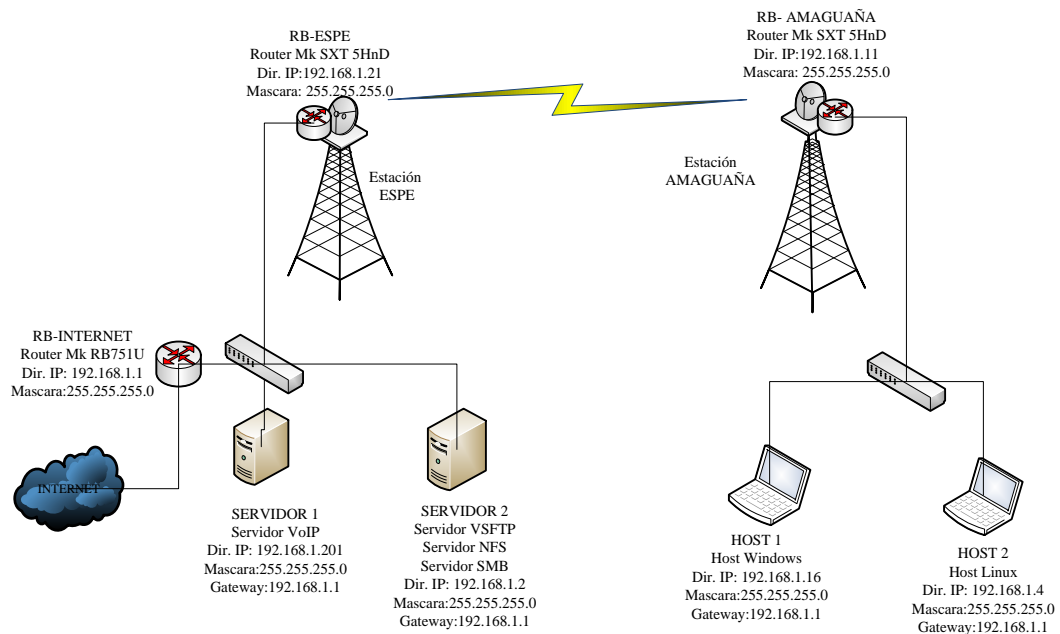


Figura 8. Topología del enlace 5.8GHz

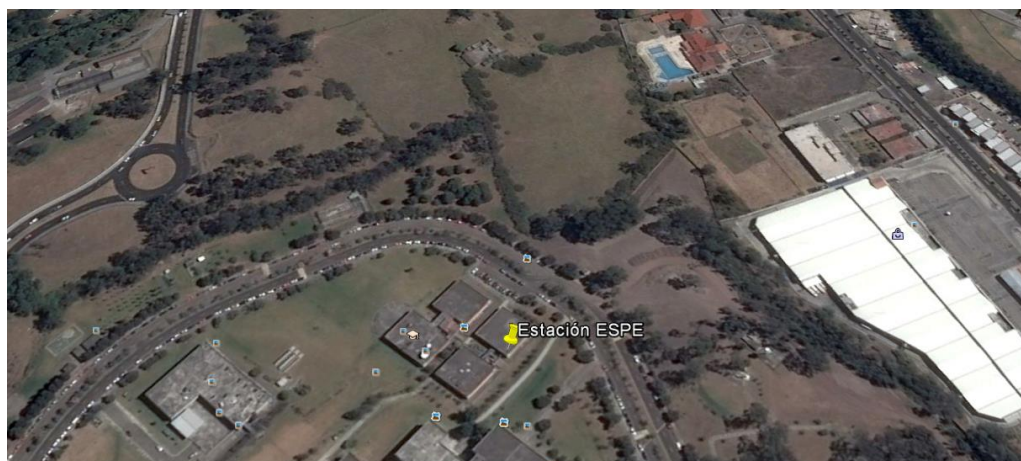
Tabla 3.

Tabla de Direccionamiento IP del enlace de 2.4GHz


Nombre	Interface	Dirección IP	Mascara	Gateway
<b>RB-INTERNET</b>	Ether 1	192.168.1.1	255.255.255.0	N/A
<b>RB-ESPE</b>	Bridge wireless-ether1	192.168.1.21	255.255.255.0	N/A
<b>RB-AMAGUAÑA</b>	Bridge wireless-ether1	192.168.1.11	255.255.255.0	N/A
<b>Servidor 1</b>	NIC	192.168.1.201	255.255.255.0	192.168.1.1
<b>Servidor 2</b>	NIC	192.168.1.2	255.255.255.0	192.168.1.1
<b>Host 1</b>	NIC	192.168.1.16	255.255.255.0	192.168.1.1
<b>Host 2</b>	NIC	192.168.1.4	255.255.255.0	192.168.1.1

### 3.2 Inspección técnica de las radio bases

La radio base ESPE se encuentra ubicada en la provincia de Pichincha en el cantón Sangolquí dentro de la Universidad de las Fuerzas Armadas-ESPE. Como se muestra en las figuras 9 y 10, la estación se encuentra en las coordenadas: latitud:  $0^{\circ}18'44.44''S$  y longitud  $78^{\circ}26'44.06''O$ ; a una altitud de 2500 metros sobre el nivel del mar.



**Figura 9. Vista satelital de la estación ESPE**

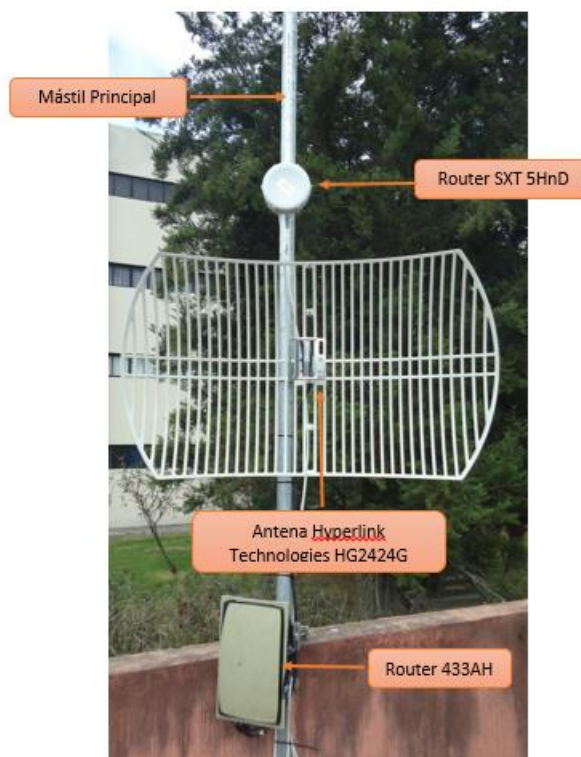
Nombre:  

Latitud:

Longitud:

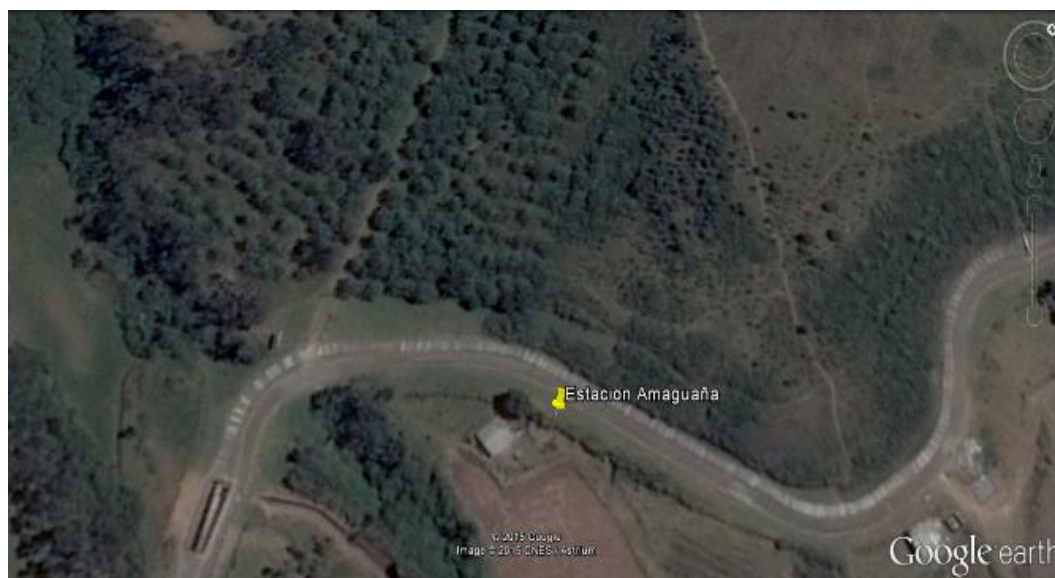
**Figura 10. Coordenadas de la estación ESPE**

En la estación ESPE se ha instalado un mástil de 1.5 pulgadas de diámetro y 2 metros de altura en la terraza del edificio de los laboratorios de Electrónica, en donde se tiene colocada la antena Hyperlink Technologies HG2424G con su respectiva grilla y los routers Mikrotik SXT 5HnD y RB433AH. El router RB433AH ha sido introducido en una caja metálica para exteriores, para evitar que los agentes externos lo dañen. Los equipos se encuentran instalados a una altura de 10 metros.



**Figura 11. Estación ESPE**

La radio base Amaguaña se encuentra ubicada en la provincia de Pichincha en el lado occidental del cantón Amaguaña; como se muestra en las figuras 12 y 13, la estación se encuentra situada en las coordenadas: latitud:  $0^{\circ}20'51.10''S$ ; y longitud  $78^{\circ}31'4.02''O$ , a una altitud de 3006 metros sobre el nivel del mar.

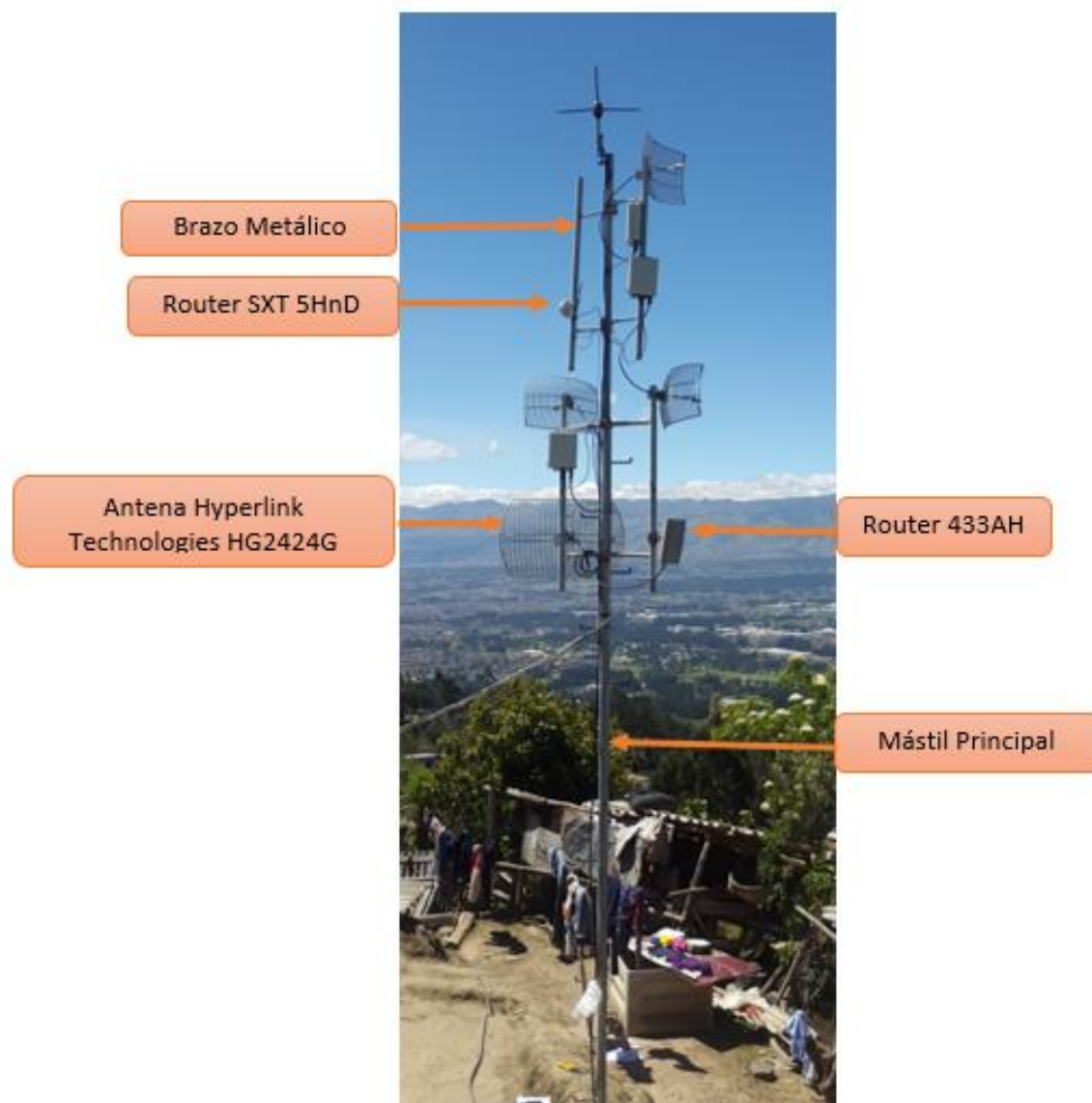


**Figura 12. Vista satelital de la estación AMAGUAÑA**

Nombre:	<input type="text" value="Rep. Amaguaña"/>	
Latitud:	<input type="text" value="2°29'35.91\"/>	
Longitud:	<input type="text" value="76°35'2.33\"/>	

**Figura 13. Coordenadas de la estación AMAGUAÑA**

En la estación AMAGUAÑA se tiene un mástil principal de 3 pulgadas de diámetro y 10 metros de altura; anclados al mástil principal se tiene 4 brazos metálicos de 1 pulgada de diámetro, en donde se tiene colocada la antena Hyperlink Technologies HG2424G con su respectiva grilla y los router Mikrotik SXT 5HnD y RB433AH. El router 433AH ha sido introducido en una caja metálica para exteriores, para evitar que los agentes externos lo dañen.



**Figura 14 Estación AMAGUAÑA**

### **3.3 Estudio de Factibilidad del enlace con PTP LinkPlanner**

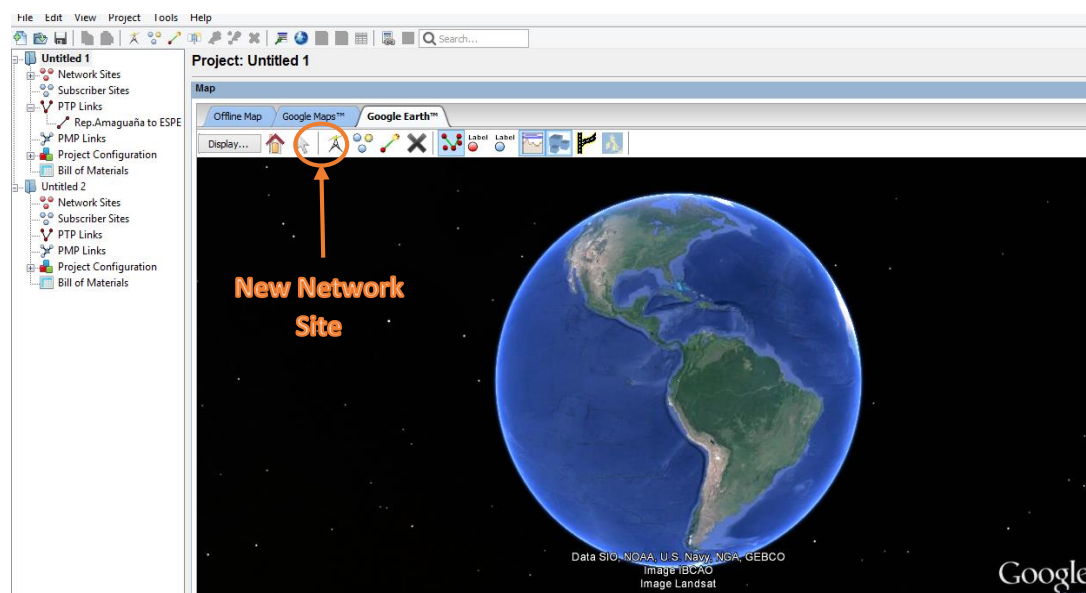
LinkPlanner es una herramienta diseñada por Cambium Networks que permite realizar estudios de factibilidad de enlaces de radio frecuencia (RF) punto a punto y punto-



multipunto, basados en la geografía, distancia, altura de la antena, potencia de transmisión, entre otros factores. LinkPlanner permite diseñar de manera rápida y fácil enlaces inalámbricos con un despliegue óptimo; está disponible para plataformas Windows y MacOS.

### 3.3.1 Configuración de un Enlace de Radio Frecuencia en LinkPlanner

Para realizar un estudio de factibilidad de un enlace inalámbrico, es necesario crear un nuevo proyecto e ingresar los datos de ubicación de cada una de las estaciones de transmisión, para lo cual se escoge, en la barra de herramientas, la opción *New Network Site* (Nuevo sitio de red).



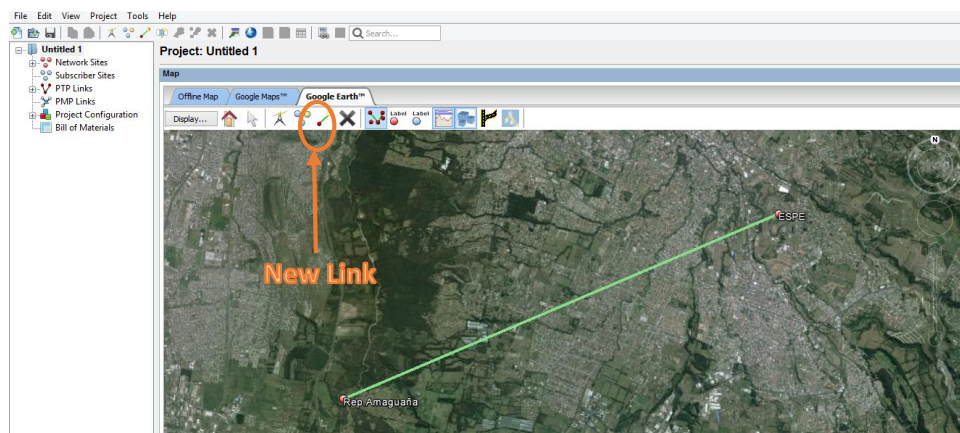
**Figura 15. Opción *New Network Site***

Al momento de crear una nueva estación de transmisión, es necesario ingresar los datos de longitud, latitud, el nombre de la estación y la altura de la torre, además, opcionalmente una descripción de la estación. En las figuras 16 y 17 se ilustra cómo se configura las dos radio bases que se utilizarán para la elaboración de este proyecto.

**Figura 16. Configuración de la estación AMAGUAÑA en PTP LinkPlanner**

**Figura 17. Configuración de la estación ESPE en PTP LinkPlanner**

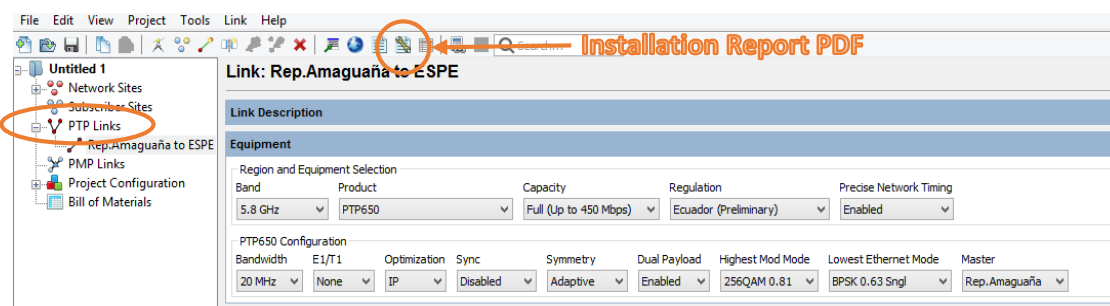
Una vez creada las dos estaciones de transmisión se procede a enlazarlas por medio de la opción *New Link* (nuevo enlace), para que de esta manera LinkPlanner pueda hacer los respectivos cálculos de factibilidad.



**Figura 18. Opción *New Link***



Con la opción *PTP Link* (enlace punto a punto) se puede configurar los diferentes parámetros del enlace como: banda de transmisión; país de regulación, ancho de canal entre otros. Una vez ingresado todos los parámetros se puede generar un reporte con todos los resultados obtenidos, escogiendo la opción *Installation Report PDF* (reporte de instalación)

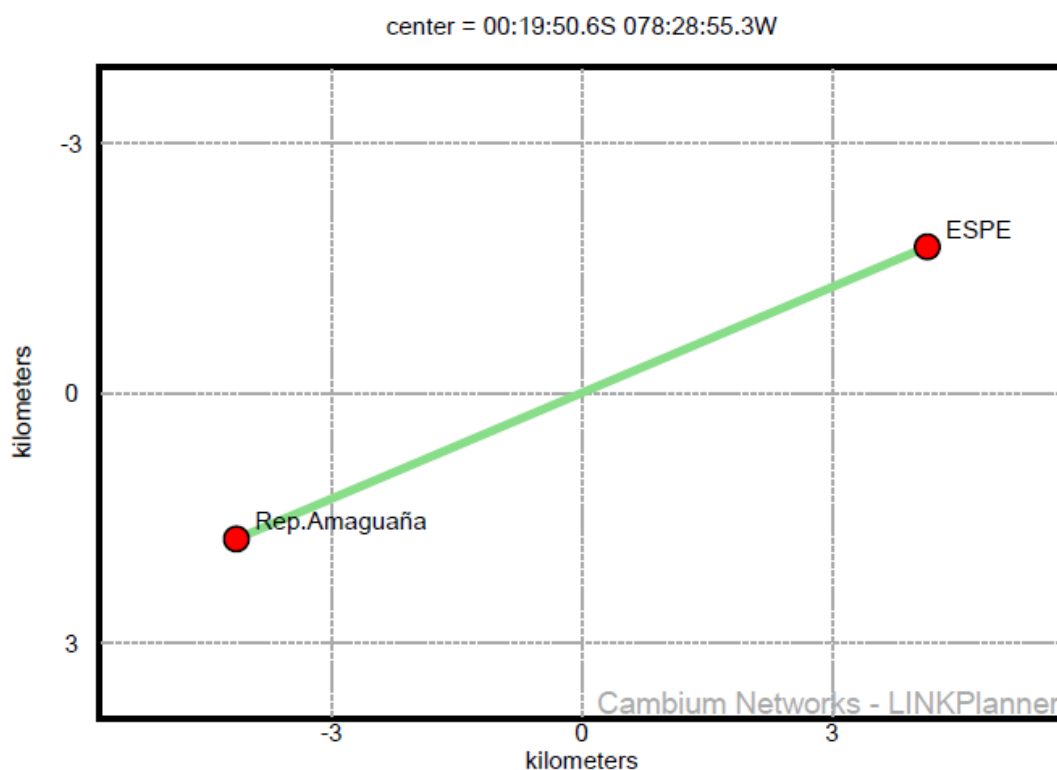


**Figura 19. Opción *Installation Report PDF***

### 3.3.2 Reporte de Instalación.

El reporte de instalación que genera LinkPlanner permite obtener información útil al momento de instalar los equipos de radio frecuencia; este reporte indica parámetros como: si existe, o no, línea de vista, zona de Fresnel, ángulo azimutal y ángulo de elevación, distancia del enlace, entre otros. Estos parámetros son muy importante porque permiten una fácil instalación y asegura el rendimiento del enlace inalámbrico. El reporte generado por esta herramienta es el siguiente:

En la figura 20 se puede apreciar el mapa de red el cual indica la posición del centro del enlace *ESPE-Rep. Amaguaña*, además de la ubicación de una estación con respecto a la otra.



**Figura 20. Mapa de red**

En la cuadro 1 se ilustra un resumen del enlace que se va a instalar. Se debe tomar en cuenta que LinkPlanner es un software dedicado a equipos Motorola, por lo que se ha utilizado como referencia el dispositivo PTP650 porque posee características similares a los equipos Mikrotik que se van a utilizar.

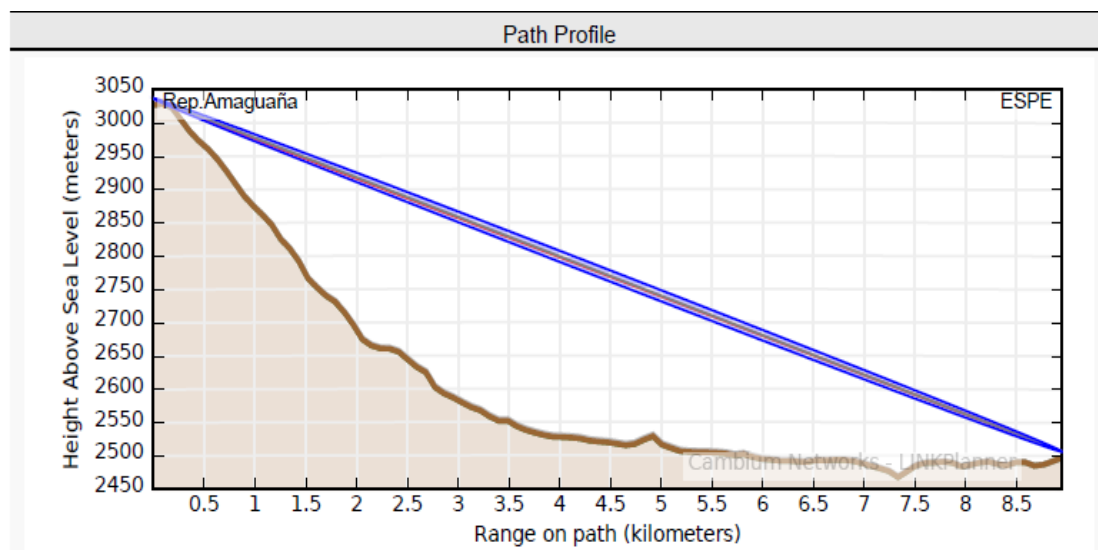
**Cuadro 1.**

**Resumen del enlace AMAGUAÑA-ESPE**

RESUMEN	
<b>Nombre del Enlace</b>	Rep. Amaguaña-ESPE
<b>Tipo De Enlace</b>	Con línea de vista
<b>Tipo De Equipo</b>	PTP650
<b>Obstrucción Máxima</b>	0 metros

<b>Distancia del Enlace</b>	8.943 kilómetros
<b>Pérdida en el Trayecto del Espacio Libre</b>	126.73 dB
<b>Exceso de Perdidas</b>	0.55 dB
<b>Rendimiento esperado para un Usuario IP</b>	Aproximadamente 443.62 Mbps asumiendo la serie de equipos PTP-650 que ejecuta el software 650-01-40
<b>Banda De Frecuencia</b>	5.8 Ghz (5725 To 5850 Mhz)
<b>Ancho de Canal</b>	45 Mhz

La figura 21 muestra que efectivamente, existe línea de vista entre las dos radio bases, y que la zona de Fresnel no posee ninguna obstrucción, esto debido a que existe una diferencia de desnivel entre las radio bases de aproximadamente 500m.



**Figura 21. Mapa de altimetría.**

En la cuadro 2 se muestra los parámetros que se toman en cuenta para el diseño del enlace de radio frecuencia; entre los mas importantes se encuentra la capacidad máxima que los equipos pueden trabajar, y cuál de los nodos actuará como maestro y cuál como esclavo

## Cuadro 2.

### Configuración del enlace

<b>CONFIGURACIÓN DEL ENLACE</b>	
<b>Capacidad</b>	Full (Hasta 450 Mbps)
<b>Temporizador</b>	Deshabilitado
<b>Ancho De Banda</b>	45MHz
<b>E1/T1</b>	Ninguno
<b>Optimización</b>	IP
<b>Sincronización</b>	Deshabilitado
<b>Simetría</b>	Adaptable
<b>Carga Dual</b>	Habilitado
<b>Nodo Master</b>	Rep. Amaguaña
<b>Nodo Esclavo</b>	ESPE

En el cuadro 3 se muestra todos los parámetros necesarios que se deben tomar en cuenta al realizar la instalación de los equipos en la estación Rep.Amaguaña, tanto para el enlace a 2.4GHz como para 5.8GHz.

**Cuadro 3.****Notas de instalación para la estación AMAGUAÑA**

<b>NOTAS DE INSTALACION PARA LA ESTACION AMAGUAÑA</b>	
<b>Variante de Plataforma</b>	Antena Integrada
<b>Altura de la Antena</b>	10.0 metros
<b>Tipo De Antena</b>	Antena de polarización dual
<b>Orientación hacia ESPE</b>	67,10 ° Norte 70.15 ° desde el norte magnético
<b>Declinación Magnética</b>	3.06 ° W ± 0,31 ° se debe cambiar 0,16°W por año
<b>Ángulo de Inclinación de la Antena</b>	-3.4° de declinación
<b>Nombre del Enlace</b>	Rep. Amaguaña-ESPE
<b>Sitio Del Enlace</b>	Amaguaña
<b>Latitud</b>	00:20:47.3S
<b>Longitud</b>	078:31:08.5W
<b>Altitud</b>	3037 Metros
<b>Interfaz TDM</b>	Ninguna
<b>Modo Maestro-Esclavo</b>	Maestro
<b>Cargador Dual</b>	Habilitado
<b>Modo de Optimización del Enlace</b>	Trafico IP
<b>Modo de Sincronización TDD</b>	Deshabilitado

<b>Banda De Regulación</b>	44 - 5.8 GHz
<b>Ancho de Canal</b>	45MHz
<b>Enlace Simétrico</b>	Adaptable
<b>Potencia de Transmisión Máxima</b>	27 dBm
<b>Modo/ Rango</b>	Auto 0 a 40 Kilómetros
<b>Predicción de Potencia Recibida</b>	-54 dBm $\pm$ 5 Db
<b>Predicción de Paquetes Perdidos</b>	127.33 Db $\pm$ 5.17 Db

En cuadro 4 se muestra todos los parámetros necesarios que se deben tomar en cuenta al realizar la estación de los equipos en la estación ESPE como la ubicación geográfica de los equipos y la altura de la antena

#### **Cuadro 4.**

##### **Notas de instalación para la estación ESPE**

<b>NOTAS DE INSTALACION PARA LA ESTACION ESPE</b>	
<b>Variante de Plataforma</b>	Antena Integrada
<b>Altura de la Antena</b>	10.0 metros
<b>Tipo De Antena</b>	Antena de polarización dual
<b>Orientación hacia Rep.Amaguaña</b>	247.10° Norte 250.21° desde el norte magnético
<b>Declinación Magnética</b>	3.11 ° W $\pm$ 0,31 ° se debe cambiar 0,16°W por año
<b>Ángulo de Inclinación de la Antena</b>	3.4° de declinación

<b>Nombre del Enlace</b>	Rep. Amaguaña-ESPE
<b>Sitio Del Enlace</b>	ESPE
<b>Latitud</b>	00:18:54.0S
<b>Longitud</b>	078:26:42.1W
<b>Altitud</b>	2507 Metros
<b>Interfaz TDM</b>	Ninguna
<b>Modo Maestro-Esclavo</b>	Esclavo
<b>Cargador Dual</b>	Habilitado
<b>Modo de Optimización del Enlace</b>	Trafico IP
<b>Modo de Sincronización TDD</b>	Deshabilitado
<b>Banda De Regulación</b>	44 - 5.8 GHz
<b>Ancho de Canal</b>	45MHz
<b>Enlace Simétrico</b>	Adaptable
<b>Potencia de Transmisión Máxima</b>	27 dBm
<b>Modo/ Rango</b>	Auto 0 a 40 Kilómetros
<b>Predicción de Potencia Recibida</b>	-54 dBm $\pm$ 5 Db
<b>Predicción de Paquetes Perdidos</b>	127.33 Db $\pm$ 5.17 Db

### 3.4 Criterios de Elección de los Equipos

Una vez que se ha realizado el estudio de factibilidad, y se ha comprobado que si es posible la implementación del enlace inalámbrico se procede a escoger los equipos a utilizar; se ha optado por manejar la gama media de dispositivos Mikrotik.

Se ha escogido el router RB433AH para el enlace a 2.4GHz, ya que al tener ranuras de expansión miniPCI se adapta de manera sencilla a la antena Hyperlink Technologies HG2424G; y soporta un flujo de tráfico inalámbrico considerable debido a su procesador y capacidad de memoria. Este dispositivo posee el sistema operativo RouterOS con licencia nivel 4 la cual permite configurar el router como un AP y asegura el soporte necesario para la configuración de los protocolos Nstreme y Nv2

Para la implementación del enlace a 5.8GHz se ha escogido el router inalámbrico SXT 5HnD; este dispositivo trae integrada en su placa la antena, permitiendo una fácil instalación al ser un equipo pequeño y portable; además de tener una carcasa para exteriores. Si bien es cierto que solo posee la licencia de nivel 3, es suficiente para el proyecto a implementar porque este nivel de licencia si soporta los protocolos Nstreme y Nv2 para un enlace punto a punto.

Otras características de los equipos que se van a utilizar se describen en la figura 22; y se los profundiza a continuación.

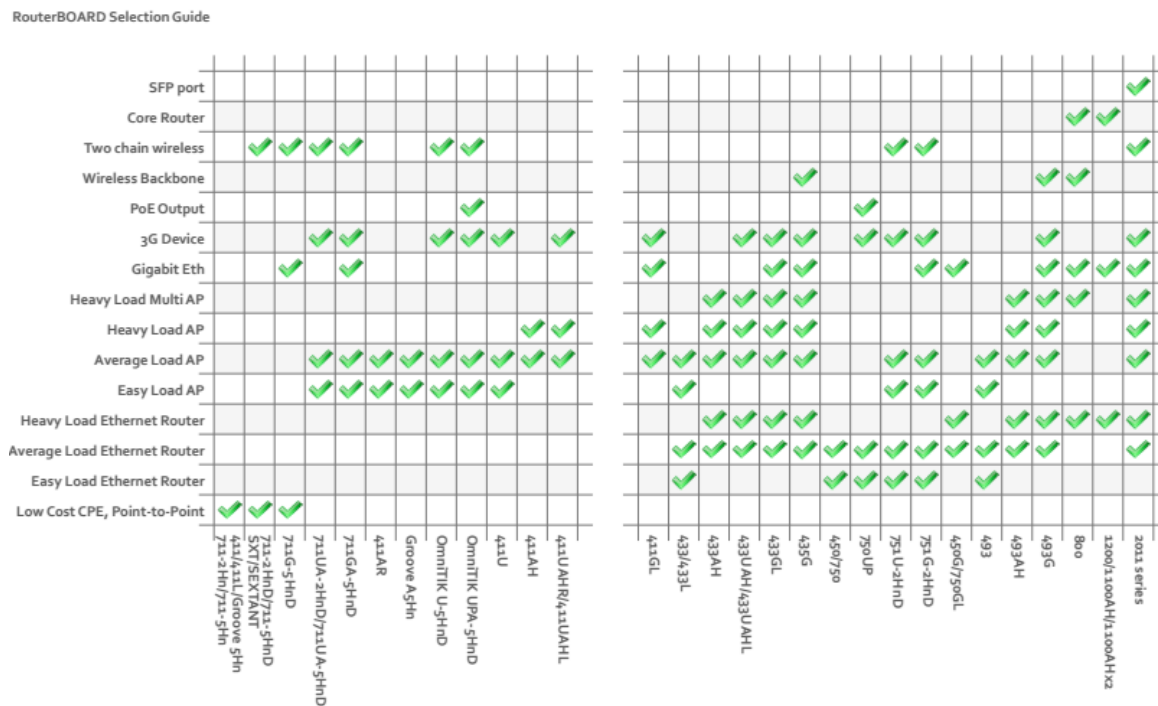


Figura 22. Características de los equipos Mikrotik.

Fuente: (Mikrotik, 2010)

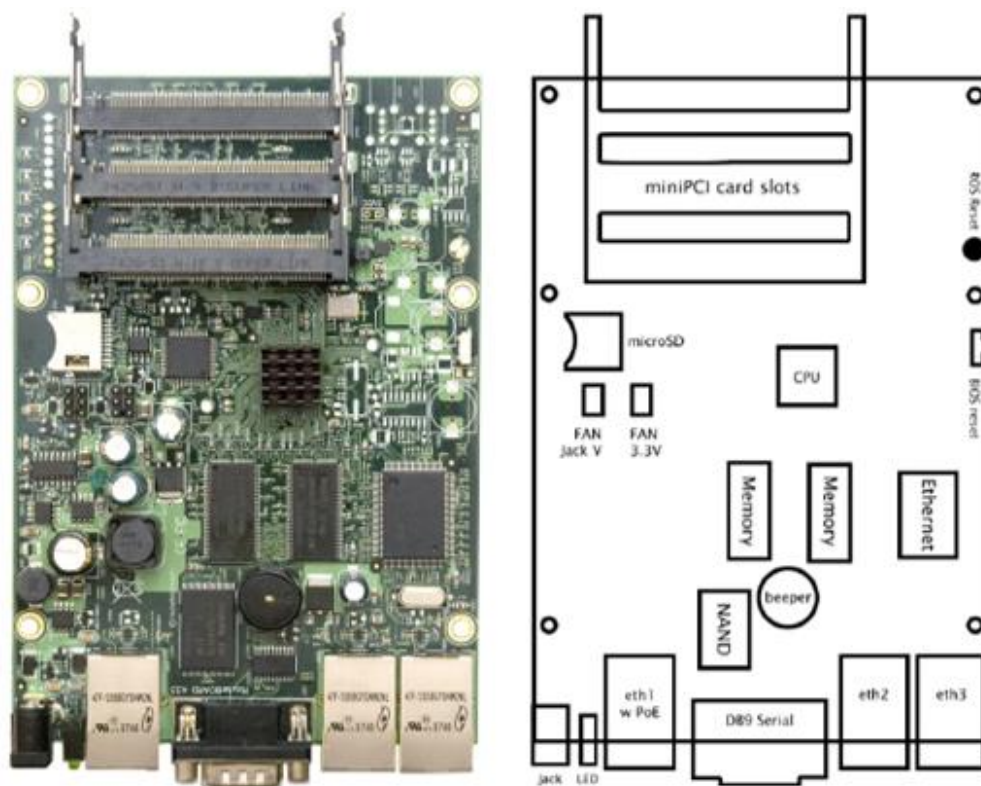


### 3.5 Características de los Equipos

#### 3.5.1 Router Mikrotik RB433AH

El router Mikrotik RB433AH es un dispositivo de enrutamiento que posee tres ranuras mini PCI y tres puertos Ethernet, con lo que se puede obtener un sin número de opciones de conectividad. El router Mikrotik RB433AH es la versión mejorada del modelo estándar RB433

A diferencia del modelo estándar, el RB433AH posee mayor capacidad en memoria RAM, un procesador Atheros AR7161 de 680MHz y una tarjeta MicroSD que permite la posibilidad de agregar mayor capacidad de almacenamiento de memoria para la implementación de Webproxy, logs (registros) y máquinas virtuales para Metarouter.



**Figura 23. Router RB433AH**

**Fuente:** (RouterBoard, 2015)

**Cuadro 5.****Especificaciones técnicas del router RB433AH**

<b>RouterBOARD RB433AH</b>	
<b>CPU</b>	Atheros AR7161 680MHz
<b>Memoria</b>	Memoria interna de 128MB DDR SDRAM
<b>Gestor de Arranque</b>	RouterBOOT
<b>Almacenamiento de Datos</b>	Chip de memoria NAND de 64MB
<b>Ethernet</b>	Tres puertos de 100 Mbit/s, Fast Ethernet con Auto MDI/X
<b>Ranura MiniPCI</b>	Tres ranuras MINIPCI tipo IIIB
<b>Puerto Serial</b>	Puerto serial asincrono DB9 RS232C
<b>LEDs</b>	LEDs de alimentación y usuario
<b>Localizador</b>	Existente
<b>Fuente de Poder</b>	Alimentación a través de Ethernet: 10-28V DC Conector :10-28V DC
<b>Control de Ventilador</b>	Dos ventiladores DC con sensor de rotación y con conmutacion automatica (Corriente de salida maxima: 500mA)
<b>Dimensiones</b>	105 mm x 150 mm (4.13 pulgadas x 5.91 pulgadas)
<b>Peso</b>	140 g
<b>Temperatura</b>	Funcionamiento: Desde -20 °C hasta + 65 °C (-4 °F a 149 °F)
<b>Humedad</b>	Opreacion hasta un 70% de humedad relativa (sin condensación)
<b>Consumo de Energia</b>	Aproximadamente 3W sin tarjetas de ampliación, máximo 25W (18W para tarjetas de expansión)
<b>Licencia RouterOS</b>	Nivel 4

**Fuente:** (RouterBoard, 2015)

**3.5.1.1 Hardware del router Mikrotik RB433AH**

- **Memoria Interna.-** El RB433 está equipado con una memoria interna SDRAM de 64 MB, mientras que el modelo RB433AH posee una memoria interna SDRAM de 128 MB

- **Dispositivos de almacenamiento NAND.-** El RB433AH está equipado con un chip de memoria no volátil de tipo NAND de 64 MB.
- **Ranura de Expansión MiniPCI.-** La placa RB433AH tiene tres ranuras MiniPCI de tipo IIIA de 3.3V. También acepta tarjetas estándar MiniPCI de tipo IIIB. Estas ranuras han sido probadas para funcionar con tarjetas de alta potencia Ubiquiti SR2 garantizando una refrigeración adecuada.
- **Puerto LAN1 con PoE.-** Este puerto FastEthernet es reconocido como la primera interfaz LAN. Es compatible con PoE. La placa acepta la entrada de tensión de 10 a 28 V DC.
- **Puerto LAN2.-** Este puerto FastEthernet es reconocido como la segunda interfaz LAN. Este puerto no es compatible con alimentación por Ethernet..
- **Puerto LAN 3.-** Este puerto FastEthernet es reconocido como la tercera interfaz LAN. Este puerto no es compatible con alimentación por Ethernet.

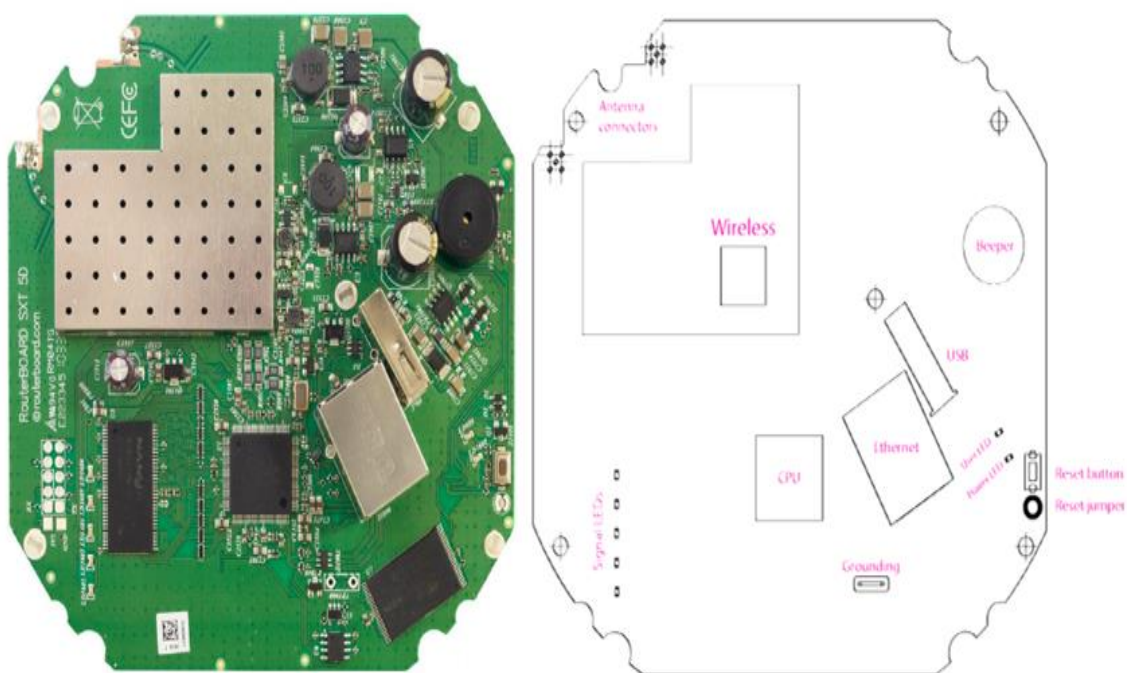
Todos los cables de red hechos a las especificaciones EIA/TIA 568A/B funcionarán correctamente. Se debe tomar en cuenta que se puede utilizar cable directo o cable cruzado para conectar a otros dispositivos de red gracias a Auto-MDIX.

- **Puerto serial DB9.-** El puerto serie asíncrono DB9 macho de estándar RS232C se puede usar para la configuración inicial, o para la fijación de un módem o cualquier otro dispositivo serie RS232. TxD (pin 3) de este puerto tiene una fuente de -5V DC cuando está inactivo.
- **Ventiladores.-** Se puede conectar hasta dos ventiladores a la placa RouterBOARD, pero sólo puede funcionar uno de ellos a la vez. Los ventiladores recibirán la misma tensión que la propia placa. Se puede dañar los ventiladores si la tensión de entrada de la placa está fuera del rango de funcionamiento de los ventiladores.
- **Indicador LED de alimentación.-** LED que se enciende cuando se enciende la placa RB433AH.
- **Indicador LED de usuario.-** El LED de usuario se puede programar a elección. Se ilumina por defecto cuando la placa se inicia, y se apaga cuando el gestor de arranque ejecuta el kernel.

### 3.5.2 Router Inalámbrico Mikrotik SXT 5HnD

El dispositivo inalámbrico SXT 5HnD es una unidad para exteriores, que permite realizar enlaces inalámbricos punto a punto y punto multipunto. SXT 5HnD es un dispositivo inalámbrico de alta velocidad, de bajo costo, que funciona en la banda de 5GHz.

Este dispositivo soporta la tecnología IEEE 802.11n y los protocolos propietarios Nstream y Nv2 que trabajan con TDMA, con lo que se puede alcanzar una tasa de transferencia real de 200Mbps. Posee una interface FastEthernet 10/100 y una interface Wireless asociada a una antena de polarización doble de 16dBi.



**Figura 24. Router SXT 5HnD**

**Fuente:** (RouterBoard, 2015)

**Cuadro 6.****Especificaciones técnicas del router SXT 5HnD**

<b>RouterBOARD SXT 5HnD</b>	
<b>CPU</b>	AR7241 400MHz.
<b>Memoria</b>	Memoria interna de 32MB DDR SDRAM.
<b>Gestor de Arranque</b>	RouterBOOT
<b>Almacenamiento de Datos</b>	Chip de memoria NAND de 64MB
<b>Ethernet</b>	Un puerto 10/100 con Auto MDI/X/
<b>Wireless</b>	Construido en 5GHz para 802.11a/n 2x2 MIMO
<b>Antena</b>	Antena 2x2 MIMO de polarización dual
<b>Proteccion ESD</b>	Porteccion electrostática (ESD) de 15kV en cada puerto RF y ethernet.
<b>Ranura MiniPCI</b>	No tiene
<b>Puerto Serial</b>	No tiene
<b>LEDs</b>	LEDs de alimetación y usuario; 5 LEDs para monitoreo wireless.
<b>Extras</b>	Localizador, boton de reinicio, puerto USB 2.0, monitor de voltaje, monitor de temperatura.
<b>Fuente de Poder</b>	Alimentación a través de Ethernet: 8-30V DC
<b>Dimensiones</b>	140 mm x 140 mm x 56 mm
<b>Peso</b>	265 g
<b>Temperatura</b>	Funcionamiento: Desde -30 °C hasta + 80 °C
<b>Consumo de Energia</b>	Maximo 5W
<b>Licencia RouterOS</b>	Nivel 3

**Fuente:** (RouterBoard, 2015)

**3.5.2.1 Hardware del router Inalámbrico Mikrotik SXT 5HnD**

- **Puerto LAN 1 con PoE.-** El puerto LAN 1 es compatible con PoE (Power over Ethernet). La tarjeta acepta una entrada de voltaje entre 8V a 30V DC. El fabricante sugiere utilizar altos voltajes de energía (que se encuentren dentro del rango) durante

largos periodos de tiempo para mejorar la eficiencia; a menor energía, las ondas electromagnéticas se pierden durante el trayecto. Se debe tomar en cuenta que se puede utilizar cable directo o cable cruzado para conectar a otros dispositivos de red gracias a Auto-MDIX.



**Figura 25. Puerto LAN 1 del router SXT5HnD**

**Fuente:** (RouterBoard, 2015)

- **Indicadores LEDs.-** Indicador LED de encendido indica que el dispositivo esta, o no, activo, este LED se encuentra dentro del case o caja protectora para exteriores. El indicador LED de usuario se puede programar a elección. Se ilumina por defecto cuando la placa se inicia, y se apaga cuando el gestor de arranque ejecuta el kernel. El router SXT 5HnD posee, adicional, 5 LEDs que indican la potencia de la señal inalámbrica de la siguiente manera:

#### Cuadro 7.

#### Indicadores LED de la potencia de señal inalámbrica

LED	ESTADO	SEÑAL WIRELESS
<b>LD1602</b>	Encendido	Si un cliente está conectado al AP (usualmente $\geq -89$ dBm)
<b>LD1603</b>	Encendido	Señal $\geq -82$ dBm
<b>LD1604</b>	Encendido	Señal $\geq -75$ dBm
<b>LD1605</b>	Encendido	Señal $\geq -68$ dBm
<b>LD1606</b>	Encendido	Señal $\geq -62$ dBm

**Fuente:** (RouterBoard, 2015)



**Figura 26. Indicadores LED de la potencia de la señal inalámbrica**

**Fuente:** (RouterBoard, 2015)

- **Tarjeta Wireless 802.11a/n 5GHz.-** SXT 5HnD tiene incorporado un dispositivo inalámbrico 802.11a /n de 5GHz basado en el chipset AR9280, el cual viene conectado directamente a la antena del equipo. El dispositivo Wireless proporciona las siguientes características:

**Tabla 4.**

**Potencia de transmisión de la tarjeta Wireless**

PROTOCOL O	TASA DE TRANSMISION	POTENCIA DE TRANSMISION (Tx)
<b>802.11a</b>	6 Mbit/s	26 dBm
	54 Mbit/s	22 dBm
<b>802.11n</b>	MCS0/8 20MHz	25 dBm
	MCS0/8 40MHz	25 dBm
	MCS7/15 20MHz	19 dBm
	MCS7/15 40MHz	18 dBm

**Fuente:** (RouterBoard, 2015)

**Tabla 5.****Potencia de recepción de la tarjeta Wireless**

PROTocol	TASA DE TRANSMISION	SENSIBILIDAD DE RECEPCIÓN (Rx)
<b>802.11<sup>a</sup></b>	6 Mbit/s	-96 dBm
	54 Mbit/s	-80 dBm
<b>802.11n</b>	MCS0/8 20MHz	-96 dBm
	MCS0/8 40MHz	-92 dBm
	MCS7/15 20MHz	-77 dBm
	MCS7/15 40MHz	-74 dBm

**Fuente:** (RouterBoard, 2015)

- **Antena.-** El equipo SXT 5HnD posee una antena de doble polarización de tipo PCB (antena en circuito impreso), la cual tiene las siguientes características:

**Cuadro 8.****Especificaciones técnicas de la antena del SXT5HnD**

CARACTERISTICA	DESCRIPCION
<b>Tipo</b>	Antena de 5GHz de doble polarización
<b>Rangos de Frecuencias</b>	5.17 -5.825 GHz
<b>Ganancia</b>	16 +- 2dBi
<b>WSWR Máximo</b>	1.7:1
<b>Polarización</b>	Dual ( Polarización vertical y horizontal)
<b>Aislamiento Puerto a Puerto</b>	-35dB

**Fuente:** (RouterBoard, 2015)

**3.5.3 Antena HyperLink Technologies HG2424G**

La antena HyperLink Technologies HG2424G posee un reflector tipo grilla, la cual provee una ganancia de 24dBi, con un ancho de haz de 8 grados; fue ideada para aplicaciones direccionales de largo alcance. Puede ser polarizada tanto vertical como horizontalmente; además de tener un riel que permite inclinar la antena de manera precisa.

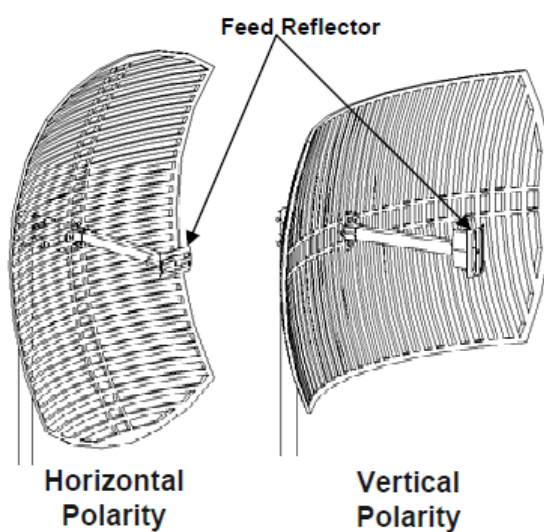




**Figura 27. Antena HyperLink Technologies HG2414G**

**Fuente:** (CyberService, 2013)

La grilla reflectora está construida de una aleación de magnesio resistente, ligero y a prueba de óxido. Posee un revestimiento con protección UV para asegurar mayor durabilidad y conservar la estética. Al ser el reflector de tipo grilla se minimiza la carga del viento.



**Figura 28. Polaridad vertical y horizontal**

**Fuente:** (CyberService, 2013)

### 3.5.3.1 Especificaciones técnicas de la antena Hyperlink Technologies HG2424G

En las tablas que se muestran a continuación se especifican cada uno de los parámetros eléctricos, mecánicos, carga de viento y parámetros de irradiación de la antena HyperLink Technologies.

**Tabla 6.**

#### Especificaciones Eléctricas

ESPECIFICACIONES ELECTRICAS	
Frecuencia	2400-2500MHz
Ganancia	24dBi
Ancho de Haz (-3dbi)	8 grados
Impedancia	50 Ohm
Maxima Entrada de Potencia	50 watts
VSWR	< 1.5:1 (promedio)

**Fuente:** (CyberService, 2013)

**Tabla 7.**

#### Especificaciones mecánicas

ESPECIFICACIONES MECANICAS	
Peso	4.8 lb.
Dimensiones de la Grilla	100.3cm X 59.7cm
Ancho de Haz (-3dbi)	8 grados
Impedancia	50 Ohm
Maxima Entrada de Potencia	50 watts
VSWR	< 1.5:1 (promedio)

**Fuente:** (CyberService, 2013)

**Tabla 8.**

#### Carga de viento

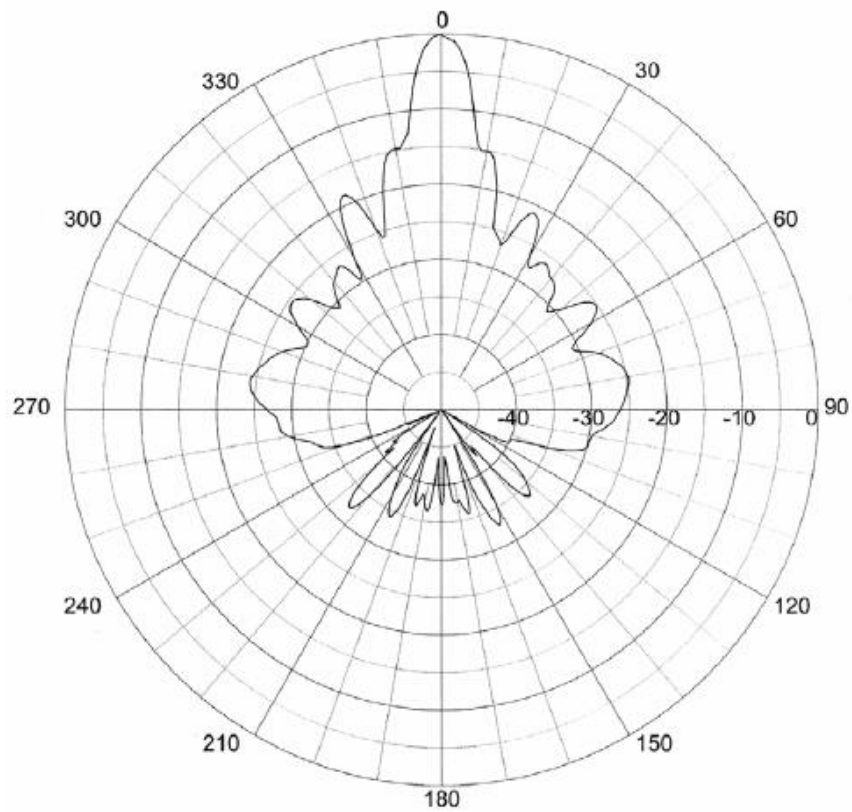
CARGA DE VIENTO	
VELOCIDAD DEL VIENTO (Km/h)	CARGA-PESO
60	16.4 lb.
90	36.3 lb.
120	63.8 lb.
150	97.0 lb.
180	147.0 lb.
210	195.5 lb.

**Fuente:** (CyberService, 2013)

**Tabla 9.****Características del patrón de irradiación vertical**

PATRON DE IRRADIACION VERTICAL	
<b>Ganancia</b>	24.25 dBi
<b>Frecuencia</b>	2 GHz
<b>10db BW</b>	12.2 grados
<b>3db BW</b>	6.8 grados

**Fuente:** (CyberService, 2013)

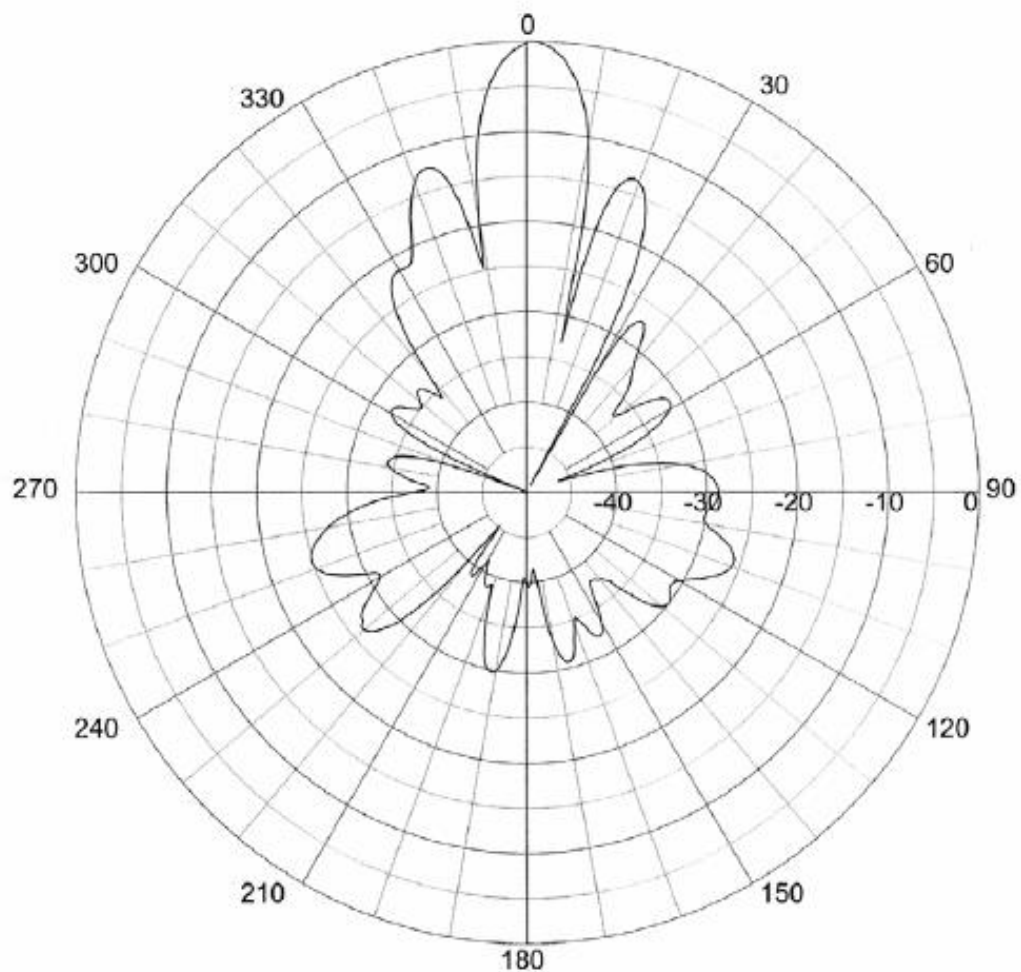
**Figura 29. Patrón de irradiación vertical**

**Fuente:** (CyberService, 2013)

**Tabla 10.****Características del patrón de irradiación horizontal**

PATRON DE IRRADIACION HORIZONTAL	
<b>Ganancia</b>	24.38 dBi
<b>Frecuencia</b>	2.4 GHz
<b>10db BW</b>	17.5 grados
<b>3db BW</b>	10 grados

**Fuente:** (CyberService, 2013)

**Figura 30. Patrón de irradiación horizontal**

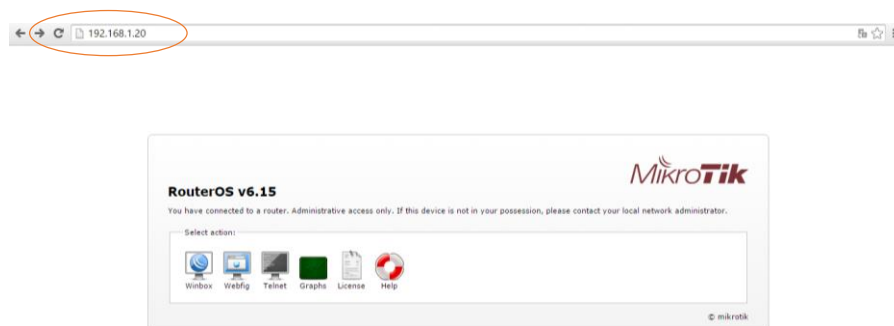
**Fuente:** (CyberService, 2013)

### 3.6 Soporte de los Protocolo Nstreme y Nv2 en Equipos Mikrotik

#### 3.6.1 Formas de Ingresar a RouterOS Mikrotik.

Mikrotik ofrece algunas maneras de ingresar a la configuración de un dispositivo, a través de Web browser, puerto serial o puerto de consola RS-232, telnet, ssh y la más conocida, a través de Winbox.

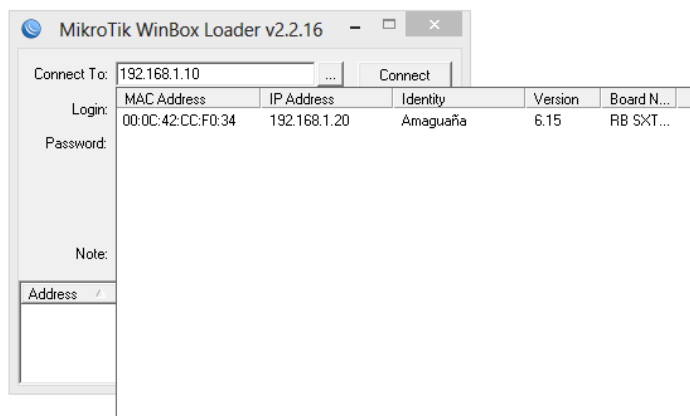
El ingreso por Web browser puede ser usado cuando el router ya tiene algunos parámetros previamente configurados. Proporciona una manera intuitiva de conectarse a un router únicamente colocando la dirección IP asignada al router en el navegador web.



**Figura 31. Ingreso al RouterOS a través web browser**

La manera más popular de ingresar a la configuración de un dispositivo Mikrotik, y la que se utilizará para la elaboración de este proyecto, es por medio de Winbox. Winbox es una interfaz gráfica propietaria de Mikrotik que permite acceder al router a través de la dirección IP (capa 3 OSI) o MAC (capa 2 OSI).

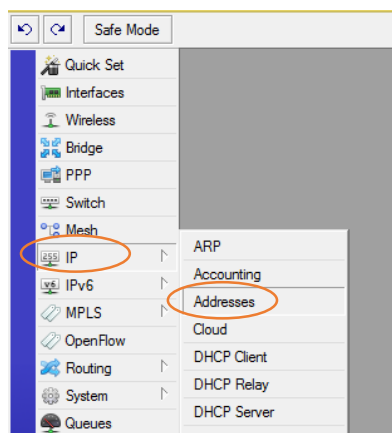
Para ingresar por medio de Winbox, se debe abrir la aplicación y en la sección *Connect to* (conectar con) se escoge la dirección IP o MAC del dispositivo al que se va a acceder. (Figura 32)



**Figura 32. Ingreso a RouterOS a través de Winbox.**

### 3.6.2 Direccionamiento IP en RouterOS

Una vez que se ingresa a la configuración del equipo por medio de Winbox y antes de realizar la configuración de la interfaz inalámbrica es necesario identificarla con una dirección IP, esto se lo puede realizar opción *IP*, en la sección *Addresses* (Direcciones).



**Figura 33. Direccionamiento IP en RouterOS**

Una vez escogido la sección *Addresses* a parecerá una ventana en donde se ingresara la dirección IP con su respectiva mascara de subred y se escogerá la interface a la cual se le asignará dicha interface.

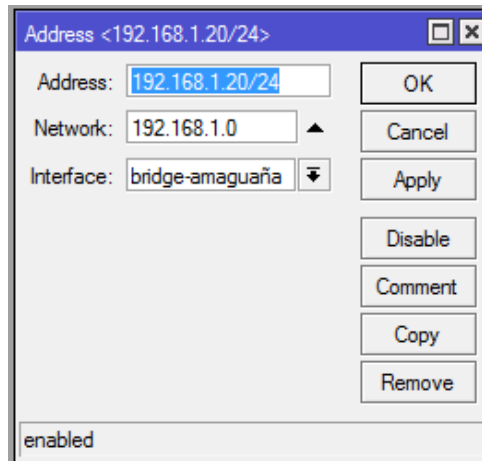


Figura 34. Configuración de direcciones IP en las interfaces en RouterOS

### 3.6.3 Configuración de la interface Wireless

Para la configuración de la interface inalámbrica se escoge la opción *Wireless* (inalámbrico) y se activa la interface wlan2 con la opción *enable* (habilitar). Una vez que se habilita la interface se ingresa a ella en donde se podrá configurar todos los parámetros requeridos.

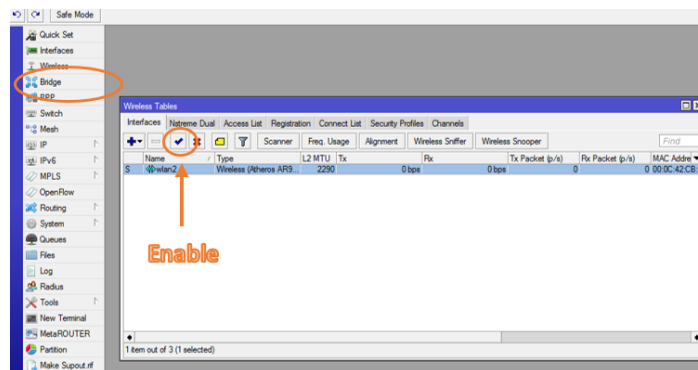
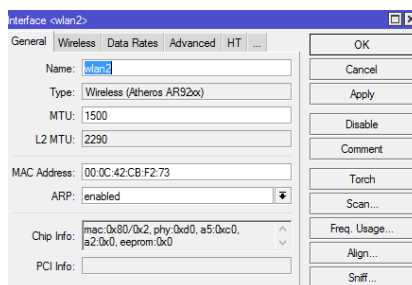


Figura 35. Activación de la interface *Wireless* en RouterOS

### 3.6.4 Sección General

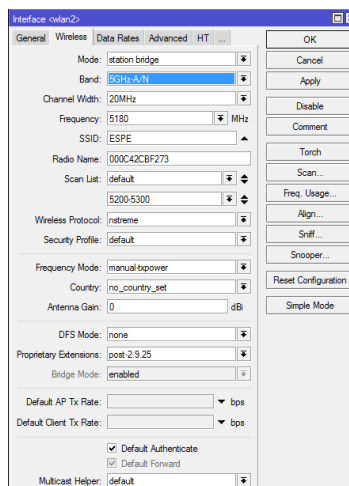
La sección *General* se puede configurar el nombre de la interface Wireless, el MTU (unidad máxima de transferencia), la dirección MAC, el tipo de chipset y el protocolo ARP (protocolo de resolución de direcciones).



**Figura 36. Sección General**

### 3.6.5 Sección Wireless

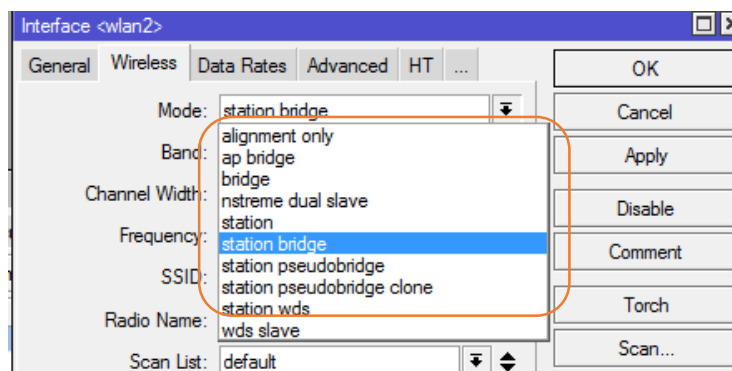
La sección *Wireless* es la más importante para la configuración porque aquí se establece todos los parámetros que permiten el levantamiento del enlace inalámbrico. De estas configuraciones depende el buen rendimiento de la red.



**Figura 37. Sección Wireless**



El primer parámetro que se debe configurar en la sección Wireless, es el *Mode* (modo); este parámetro tiene diferentes opciones que se explican en el cuadro 9. Los diferentes modos se activan dependiendo del nivel de licencia.



**Figura 38. Configuración del parámetro *Mode***

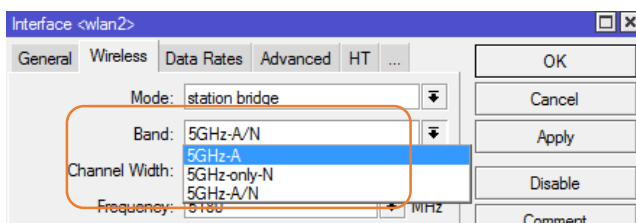
#### Cuadro 9.

#### Opciones del parámetro *Mode*

OPCIONES DEL PARAMETRO MODE		
<b>Modos Station</b>	station	Modo station básico. Escanea y se conecta con un AP
	station-wds	Igual que station pero crea un enlace WDS con el AP. El AP también debe ser configurado con WDS
	station-pseudobridge	Igual que station, pero además, llevar a cabo la traducción de direcciones MAC. Permite que la interface sea un bridge
	station-pseudobridge-clone	Igual que station psuedobridge pero usa la dirección station-bridge-clone-mac para conectarse con el AP
<b>Modos AP</b>	ap-bridge	Punto de acceso básico
	bridge	Igual que ap-bridge, pero limita la asociación con un solo cliente
	wds-slave	Igual que ap-bridge, pero escanea un AP con el mismo SSID y establece un enlace WDS
<b>Modos Especiales</b>	alignment-only	Pone la interface un modo continuo de transmisión, útil para apuntar a la antena remota
	nstreme-dual-slave	Permite que la interface sea usada en modo nstreme-dual

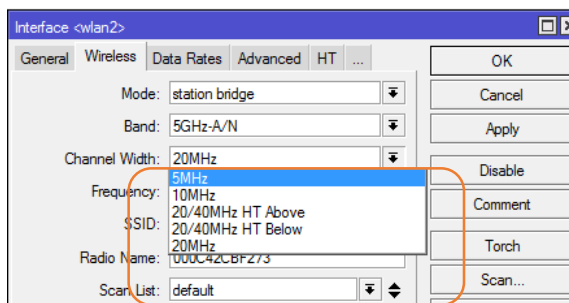
Fuente: (Mikrotik, 2010)

El parámetro *band* (banda) permite escoger la banda de frecuencia en la que va a trabajar el enlace inalámbrico y el tipo de protocolo IEEE 802.11. Mikrotik trabaja en las bandas 5GHz (802.11 a/n/ac) y 2.4GHz (802.11 b/g/n). Esta opción se seleccionara basadas en la capacidad soportada por los routers y clientes.



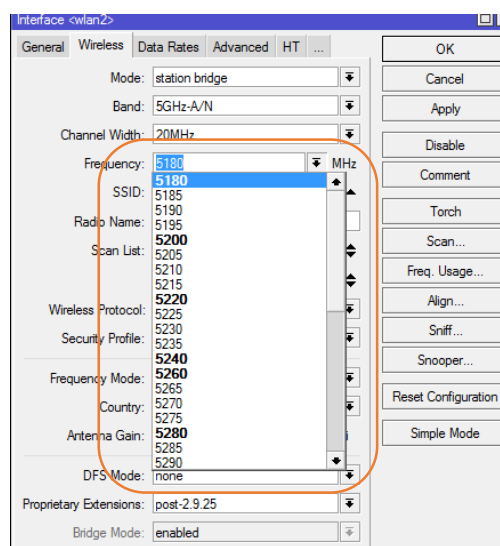
**Figura 39. Configuración del parámetro *Band***

La opción *Channel Width* (ancho de canal) permite escoger el ancho de canal con el que va a trabajar el enlace de radio frecuencia. Permite tener anchos de canal de 20MHz, 10MHz, 5Mhz; además de las opciones *20/40MHz HT Above* y *20/40MHz HT Below*, con lo que se consigue aumentar 20MHz por encima o debajo del canal. Esta extensión permite utilizar un espectro de 40MHz en dispositivos IEEE 802.11n con lo que se consigue aumentar el rendimiento.



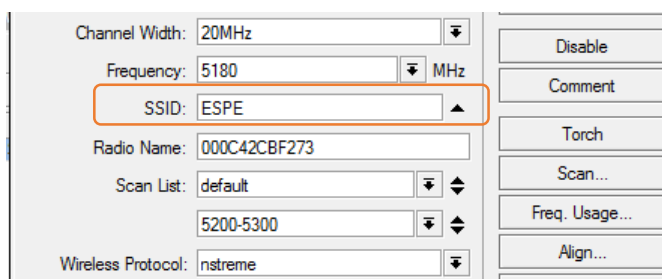
**Figura 40. Configuración del parámetro *Channel Width***

La opción *frequency* (frecuencia) permite escoger la frecuencia en la que transmitirá el enlace inalámbrico. Se debe escoger una frecuencia que no se encuentre saturada, ya que al usar bandas libres (2.4GHz y 5GHz), diferentes usuarios pueden estar utilizando dichas frecuencia. Para la elección correcta de la frecuencia, Winbox posee una herramienta denominada *Frequency Usage* (uso de la frecuencia), la cual indica la cantidad de saturación y ruido de cada una de las frecuencias.



**Figura 41. Configuración del parámetro *Frequency***

El *SSID* (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de dicha red. El código consiste en un máximo de 32 caracteres, que por lo general son alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.



**Figura 42. Configuración del parámetro *SSID***

El valor por defecto (*default*) en la opción *Scan List* (Lista de escaneo) indica todos los canales seleccionados en la opción *band* que pueden ser soportadas por la tarjeta y permitidas por las secciones *country* (país) y *frequency-mode* (modo de frecuencia). Si se especifica frecuencias adicionales en *Scan List*, se tomará en cuenta las frecuencias configuradas en las anteriores secciones y las ingresadas manualmente.

The screenshot shows the configuration interface for a wireless interface. The 'Scan List' dropdown menu is highlighted with an orange box and is currently set to 'default'. Other visible parameters include Frequency: 5180 MHz, SSID: ESPE, Radio Name: 000C42CBF273, Scan List: default, Frequency Range: 5200-5300, Wireless Protocol: nstreme, and Security Profile: default. On the right side, there are buttons for Comment, Torch, Scan..., Freq. Usage..., Align..., and Sniff...

**Figura 43. Configuración del parámetro *Scan List***

A partir de la versión de RouterOS 5.0rc1, y con licencia superior a la del nivel 2 se ha introducido un nuevo parámetro, *Wireless-protocol* (protocolo inalámbrico). Esta opción permite controlar cual protocolo inalámbrico se utilizará. Se debe tomar en cuenta que este parámetro está relacionado con el rol de la interfaz (AP o cliente). En cuadro 10 se pone a consideración posibles valores que puede tomar la sección *Wireless-protocol*.

The screenshot shows the configuration interface for a wireless interface. The 'Wireless Protocol' dropdown menu is open, showing a list of options: 802.11, any, nstreme (highlighted in blue), nv2, nv2 nstreme, and unspecified. Other visible parameters include Band: 5GHz-A/N, Channel Width: 20MHz, Frequency: 5180 MHz, SSID: ESPE, Radio Name: 000C42CBF273, Scan List: default, Frequency Range: 5200-5300, Security Profile: any, Frequency Mode: nv2 nstreme, Country: nv2 nstreme 802.11, and Antenna Gain: 0 dBi. On the right side, there are buttons for Apply, Disable, Comment, Torch, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., Reset Configuration, and Simple Mode.

**Figura 44. Configuración del parámetro *Wireless Protocol***

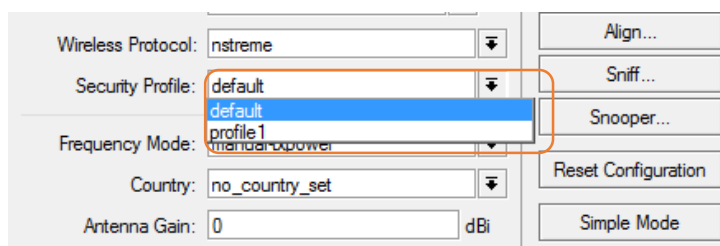
Cuadro 10.

Opciones del parámetro *Wireless Protocol*

VALOR	AP	CLIENTE
<b>unspecified</b>	Establece redes 802.11 o nstreme basadas en parámetros antiguos de nstreme	Conecta redes 802.11 o nstreme basadas en parámetros antiguos de Nstreme
<b>any</b>	Lo mismo que unspecified	Escanea todas las redes, sin importar el protocolo y se conecta usando el protocolo de la red seleccionada.
<b>802.11</b>	Establece una red 802.11	Se conecta solo a redes 802.11
<b>nstreme</b>	Establece una red nstreme	Se conecta solo a redes Nstreme
<b>Nv2</b>	Establece una red Nv2	Se conecta sólo a redes Nv2
<b>Nv2-nstreme-802.11</b>	Establece una red Nv2	Escanea redes Nv2, si encuentra una adecuada, se conecta; de lo contrario escanea redes Nstreme, si encuentra una red apropiada se conecta, por último escanea redes 802.11 y si encuentra una apropiada, se conecta.
<b>Nv2-nstreme</b>	Establece redes Nv2	Escanea redes Nv2, si encuentra una red adecuada - se conecta, de lo contrario escanea redes Nstreme y si encuentra una apropiada se conecta

Fuente: (Mikrotik, 2010)

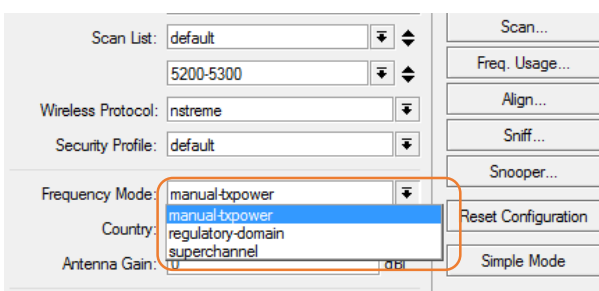
La opción *Security Profile* (perfil de seguridad) permite tener una mayor seguridad en el acceso al enlace inicial. Aquí se acogerá un perfil o *profile* que se configura en la opción *Security Profiles*. No se recomienda usar por ningún motivo una conexión inalámbrica sin *security profile* ya que se deja propenso a un ataque o infiltración al enlace.



**Figura 45. Configuración del parámetro *Security Profile***

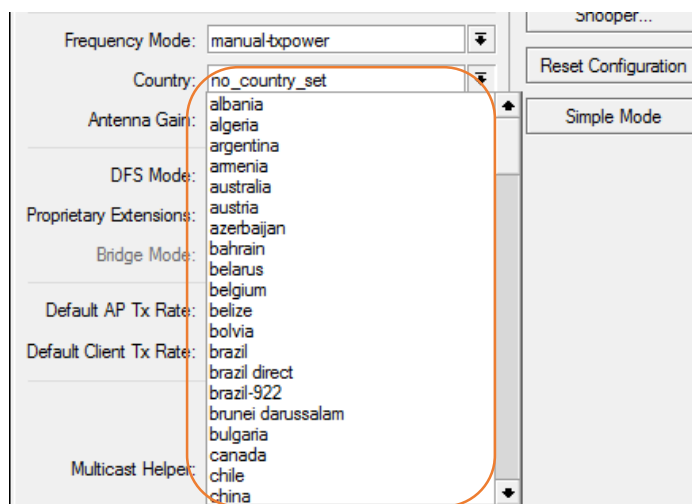
*Frequency Mode* permite elegir el modo en el cual el router va a trabajar, respetando las siguientes limitaciones:

- *Regulatory-domain*: Esta sección limita los canales usados y potencia Tx, basados en las regulaciones del país; estas regulaciones se configuran en el parámetro *country*
- *Manual-txpower*: Es igual que *Regulatory-domain* pero sin restricción de la potencia Tx.
- *Superchannel*: Ignorará todas las restricciones.



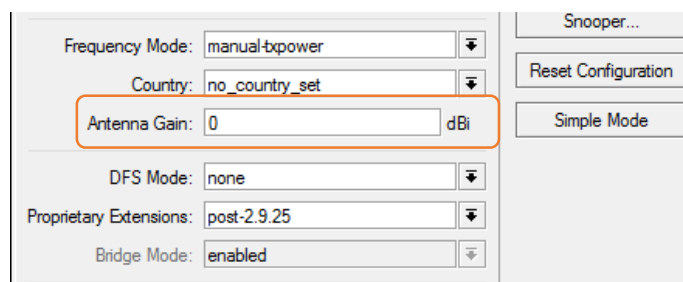
**Figura 46. Configuración del parámetro *Frequency Mode***

El parámetro *country* se enfoca en la frecuencia y potencias de transmisión, reguladas y limitadas por cada país. Cuando se usa la opción *no\_contry\_set* (ningún país configurado) se usa los parámetros de frecuencia y potencia según los canales aprobados por la FCC (Comisión Federal de Comunicaciones).



**Figura 47. Configuración del parámetro *Country***

El parámetro *Antenna Gain* (ganancia de la antena) es usado para calcular la máxima potencia de transmisión dependiendo de la regulación de cada país.



**Figura 48. Configuración del parámetro *Antenna Gain***

*DSF Mode* (Selección Dinámica de Frecuencia) tiene las siguientes opciones:

- *None*: Deshabilita DSF.
- *No-radar-detect*: Selecciona el menor canal de *scan-list*. En el modo *wds-slave* no tiene efecto.
- *Radar-detect*: Selecciona el menor canal de *scan-list* y lo usa si detecta una frecuencia durante los próximos 60 segundos. Este ajuste depende de las regulaciones de cada país.

The screenshot shows the RouterOS configuration interface for a wireless network. The 'DFS Mode' dropdown menu is open, showing options: 'none', 'no radar detect', 'radar detect', and 'enabled'. The 'Proprietary Extensions' dropdown menu is also open, showing options: 'none', 'radar detect', and 'enabled'. The 'Bridge Mode' dropdown menu is set to 'enabled'. Other visible settings include 'Country: no\_country\_set', 'Antenna Gain: 0 dBi', 'Default AP Tx Rate: bps', 'Default Client Tx Rate: bps', 'Default Authenticate: checked', and 'Default Forward: checked'. Buttons for 'Reset Configuration' and 'Simple Mode' are also visible.

**Figura 49. Configuración del parámetro *DFS Mode***

RouterOS incluye información propietaria en el argumento *proprietary-extensions* (extensiones propietarias) sobre elementos de control de trama. Los parámetros de control son los siguientes:

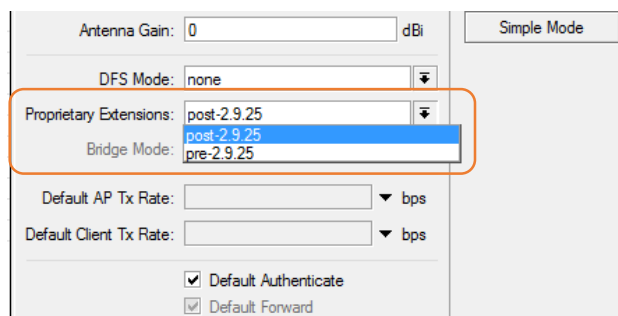
- *Pre-2.9.25*: Es el método más antiguo, pero puede operar con las versiones más recientes de RouterOS. Es incompatible con algunos clientes como los basados en Centrino.
- *Post-2.9.25*: Es una manera estandarizada de incluir información acerca del proveedor de la marca.

The screenshot shows the RouterOS configuration interface for a wireless network. The 'Proprietary Extensions' dropdown menu is open, showing options: 'post-2.9.25', 'post-2.9.25', and 'pre-2.9.25'. The 'Bridge Mode' dropdown menu is set to 'pre-2.9.25'. Other visible settings include 'Frequency Mode: manual-tpower', 'Country: no\_country\_set', 'Antenna Gain: 0 dBi', 'DFS Mode: none', 'Default AP Tx Rate: bps', and 'Default Client Tx Rate: bps'. Buttons for 'Snooper...', 'Reset Configuration', and 'Simple Mode' are also visible.

**Figura 50. Configuración del parámetro *Proprietary Extensions***



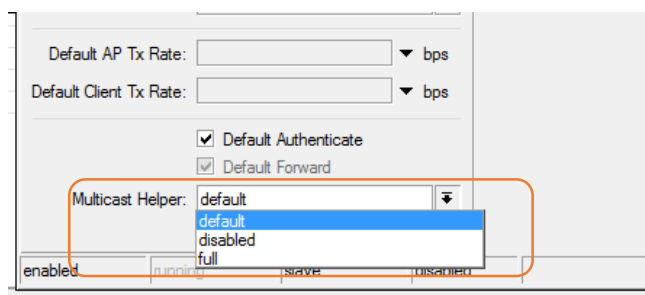
Los parámetros *Default AP Tx Rate* (tasa de transferencia por defecto del AP) y *Default Client Tx Rate* (tasa de transferencia por defecto del cliente) permiten definir manualmente la tasa de transferencia tanto del cliente como el AP.



**Figura 51. Configuración de los parámetros *Default AP Tx Rate* y *Default Client Tx Rate***

La opción *Multicast Helper* permite configurar el envío de paquetes multicast con una dirección MAC de destino unicast. Este parámetro solo debe ser configurado en el punto de acceso y los clientes deben ser especificados en modo *station-bridge* (estación puente). Se tiene las siguientes opciones:

- *Disabled*: Deshabilita el helper y envía paquetes multicast con una dirección MAC de destino multicast.
- *Full*: Todas las direcciones de destino MAC de paquetes multicast con cambiadas a direcciones MAC unicast.
- *Default*: Esta opción esta deshabilitada. Puede cambiar en futuras versiones de RouterOS.



**Figura 52. Configuración del parámetro *Multicast Helper***

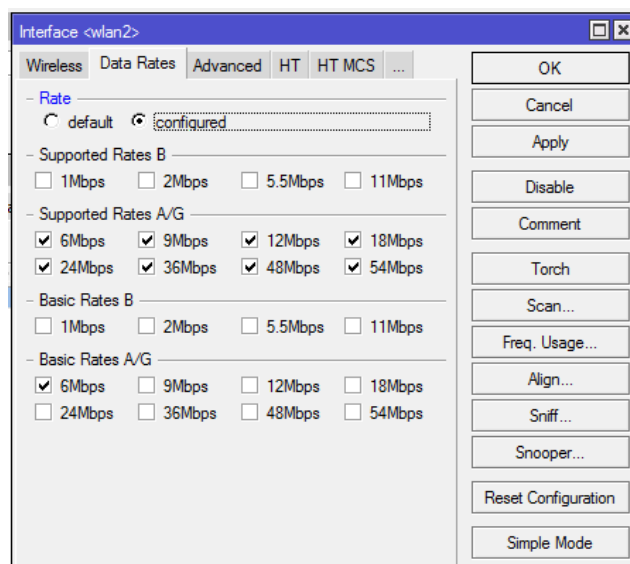
### 3.6.6 Sección Data Rates

En esta sección se puede configurar las diferentes tasas de velocidad de transmisión en el enlace dependiendo del tipo de protocolo IEEE 802.11 que se vaya a utilizar. Las *data rates* (tasas de transferencia) son soportados según el estándar usado como se muestra a continuación:

- 802.11b: 1 1 11Mbps
- 802.11 a/g: 6 a 54Mbps
- 802.11n: 6 a 300Mbps

Existen dos tipos de tasas de transferencia que se puede configurar en RouterOS, estas son:

- *Basic-rates*: Tasas de velocidad mínima que un cliente debería soportar al momento de conectarse al AP. Para que haya comunicación entre el cliente y el AP, los dos deben estar configurados con el mismo *data rate*.
- *Supported-rates*: Tasas de velocidad que un cliente puede llegar a soportar.

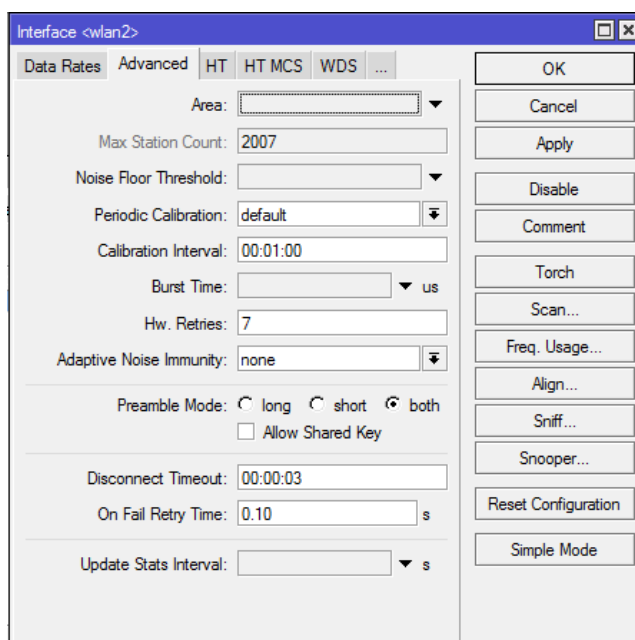


**Figura 53. Sección Data Rates**

### 3.6.7 Sección Advanced

En esta sección se puede configurar parámetros avanzados del enlace inalámbrico, entre los que se encuentran:

- *Area*: Identifica el grupo de redes inalámbricas. Este valor es anunciado por el AP
- *Max station count* : Máximo de clientes que se pueden asociar al AP.
- *Noise floor threshold*: Umbral de ruido. Esta propiedad solo es efectiva para tarjetas Atheros AR5211
- *Periodic Calibration*: Habilita una calibración periódica. Este valor depende del tipo de tarjeta Wireless, y es solo efectiva en el chipset Atheros.
- *Calibration Interval*: Se configura el lapso de tiempo para la calibración periódica.
- *Burst Time*: Tiempo en microsegundo que serán usados para enviar datos sin interrupciones. Se debe tomar en cuenta que ningún otro equipo podrá transmitir datos cuando se encuentra activo el *Burst Time*. Está disponible para las tarjetas AR5000 y AR5001X.
- *Hw-retries*: Número de veces que se vuelve a reenviar una trama antes de que se considere como una transmisión fallida.
- *Adaptative noise immunity*: Inmunidad a ruido adaptativo. Esta propiedad es solo efectiva en tarjetas Atheros.
- *Preamble mode*: Permite configurar el tamaño de la cabecera de la trama. Esta opción es habilitada para IEEE802.11b.
- *Disconnect timeout*: Tiempo que se espera para declarar al enlace como desconectado. Se mide desde el tercer envío fallido.
- *On fail retry time*: Es el tiempo que se debe esperar para reintentar la conexión.
- *Update start interval*: Frecuencia de solicitud por parte de los clientes de actualización de señales de potencia y CCQ.

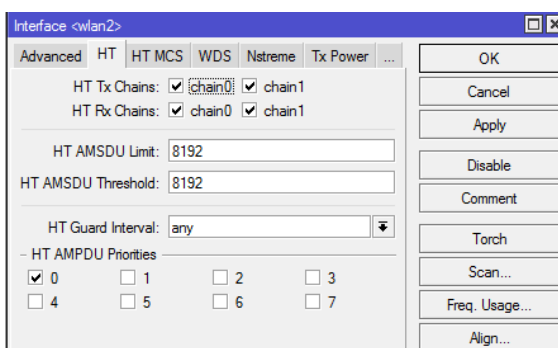


**Figura 54. Sección *Advanced***

### 3.6.8 Sección HT

En esta sección se puede configurar parámetros relacionados con las antenas. Se puede escoger cuantas antenas se van a utilizar para la transmisión y recepción. Otros parámetros configurables son los siguientes:

- *HT AMSDU Limit*: Máximo AMSDU (característica de IEEE802.11 e/n que envía varios paquetes en una transmisión simple) que el dispositivo puede negociar, puede aumentar significativamente el rendimiento, pero consume capacidad de procesamiento.
- *HT AMSDU threshold*: Máximo tamaño de trama que incluye AMSDU.
- *HT guard interval*: Intervalo de guarda o espera.
- *HT AMPDU Priorities*: Prioridad de los paquetes con AMPDU.

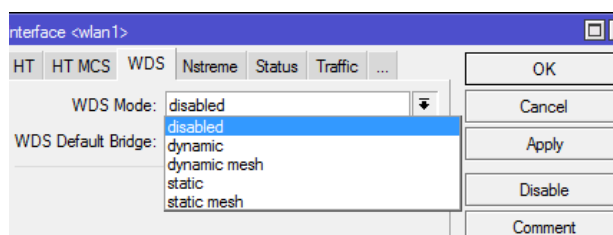


**Figura 55. Sección HT**

### 3.6.9 Sección WDS (Sistema de Distribución Wireless)

El Sistema de Distribución Inalámbrico permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11, por lo que una red puede ser ampliada mediante múltiples puntos de acceso sin la necesidad de un cable troncal.

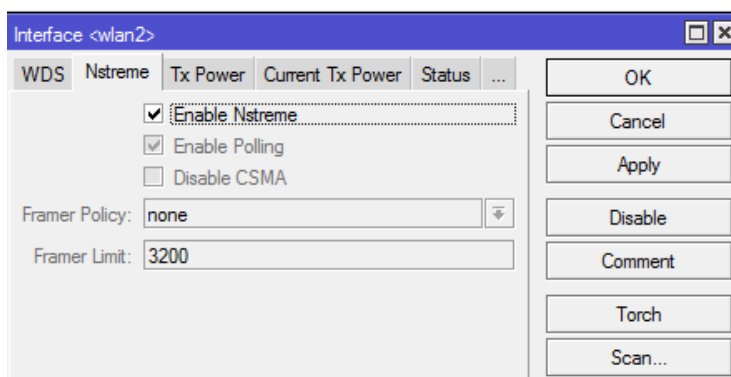
En esta sección se puede configurar modo dinámico, estático, el bridge WDS, el costo y el rango del costo.



**Figura 56. Sección WDS**

### 3.6.10 Sección Nstream

En esta sección se puede configurar parámetros de Nstream, como habilitar o no el polling, el límite y las políticas de la trama, entre otros. Se debe activar Nstream siempre y cuando en el parámetro *Wireless protocol* se encuentre configurado con este protocolo

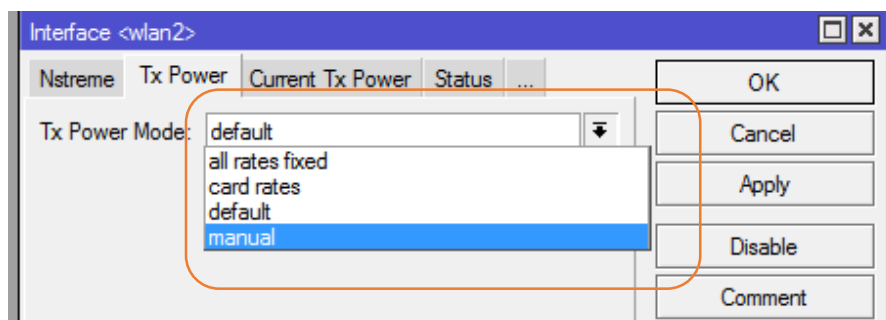


**Figura 57. Sección *Nstreme***

### 3.6.11 Sección Tx Power

En esta sección permite configurar los diferentes modos de configuración de la potencia de transmisión; entre los que se encuentran:

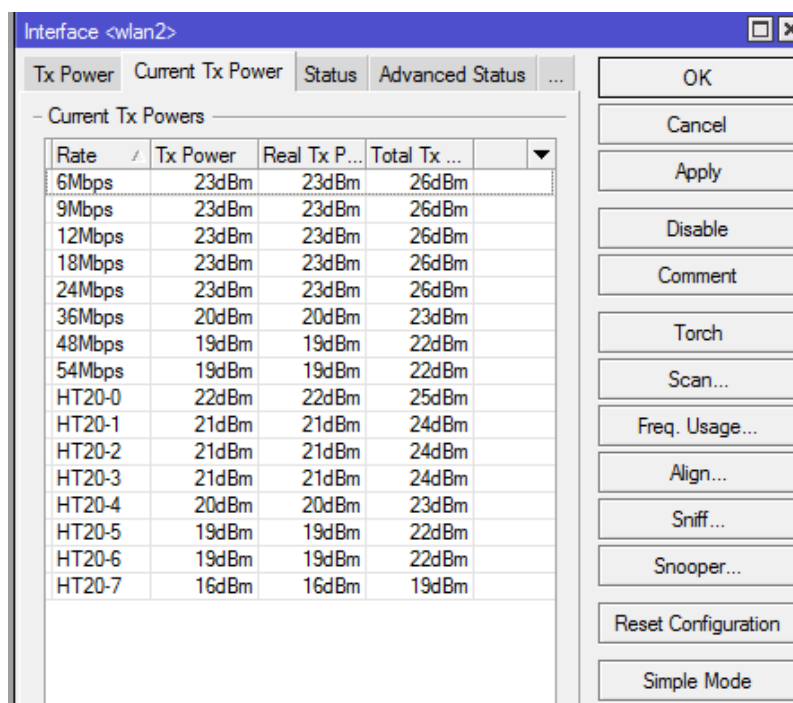
- *Default*: Usa valores configurados y guardados en la tarjeta.
- *Card rate*: Usa la potencia de transmisión definida en el parámetro *tx-power*.
- *All rate fixed*: Usa la misma potencia de transmisión las relacionadas con las tasa de transferencia. Puede dañar las tarjetas si se transmite un valor superior al que pueden soportar.
- *Manual table*: Define una potencia de transmisión para cada tasa de transmisión por separado.



**Figura 58. Sección *Tx Power Mode***

### 3.6.12 Sección Current Tx Power

Esta sección indica diferentes parámetros acerca de la potencia de transmisión del router. Entre las que se puede encontrar son: tasa de transmisión, potencia de transmisión, potencia real de transmisión, y potencia total.

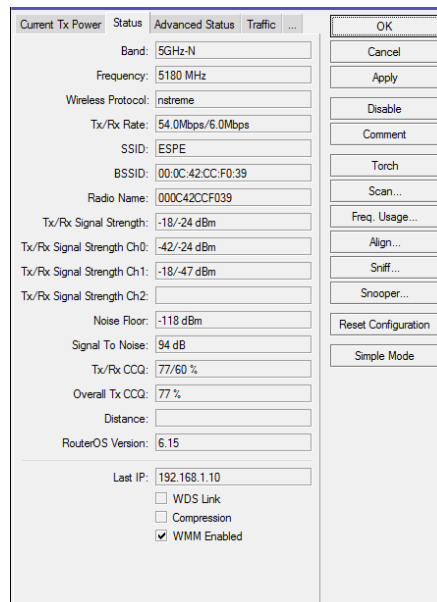


Rate	Tx Power	Real Tx P...	Total Tx ...
6Mbps	23dBm	23dBm	26dBm
9Mbps	23dBm	23dBm	26dBm
12Mbps	23dBm	23dBm	26dBm
18Mbps	23dBm	23dBm	26dBm
24Mbps	23dBm	23dBm	26dBm
36Mbps	20dBm	20dBm	23dBm
48Mbps	19dBm	19dBm	22dBm
54Mbps	19dBm	19dBm	22dBm
HT20-0	22dBm	22dBm	25dBm
HT20-1	21dBm	21dBm	24dBm
HT20-2	21dBm	21dBm	24dBm
HT20-3	21dBm	21dBm	24dBm
HT20-4	20dBm	20dBm	23dBm
HT20-5	19dBm	19dBm	22dBm
HT20-6	19dBm	19dBm	22dBm
HT20-7	16dBm	16dBm	19dBm

Figura 59. Sección *Current Power*

### 3.6.13 Sección Status.

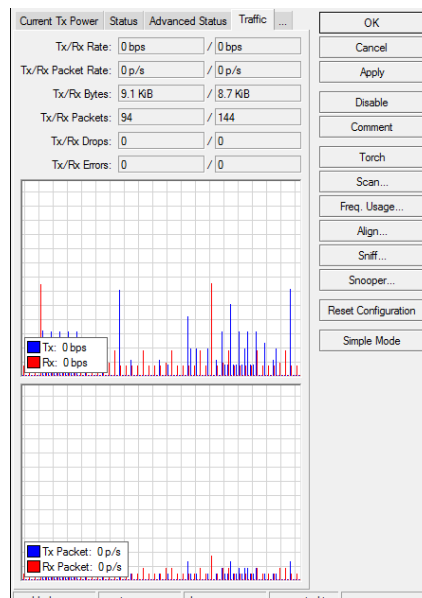
En esta sección se muestra de manera detallada los parámetros que permiten obtener una idea clara acerca del rendimiento del enlace como el CCQ (Calidad de Conexión del Cliente), ruido, potencia de transmisión y recepción, entre otros.



**Figura 60. Sección *Status***

### 3.6.14 Sección *Traffic*

Muestra gráficamente la tasa de transmisión y recepción que tiene la interface inalámbrica en tiempo real.



**Figura 61. Sección *Traffic***



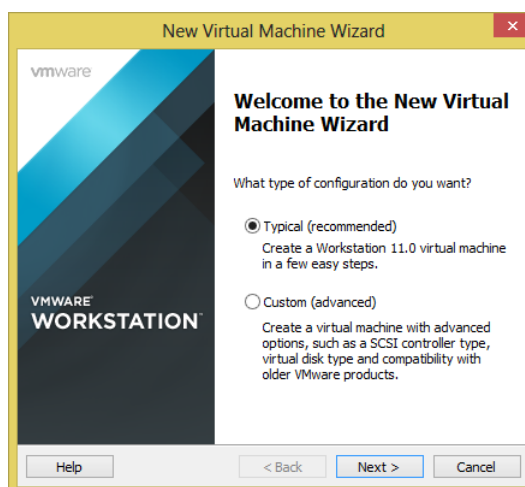
## CAPITULO IV

### GESTIÓN E IMPLEMENTACIÓN DE SERVICIOS DE RED

#### 4.1 Instalación del Sistema Operativo Centos 7 en VMWare

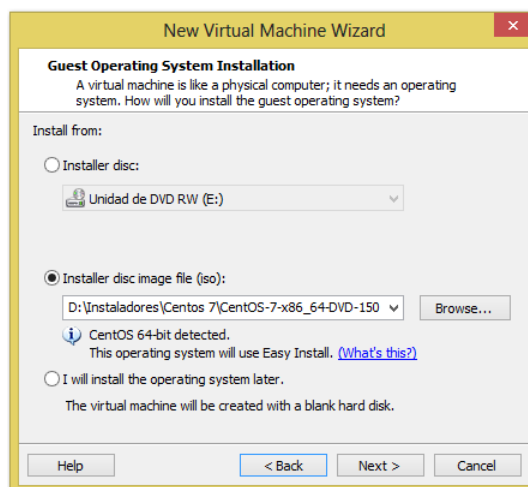
VMWare es un software que permite la virtualización. Un sistema virtualizado por software es una herramienta que simula un sistema físico con unas características de hardware determinado. Cuando se ejecuta el simulador, se proporciona un ambiente de ejecución similar a todos los efectos de un computador físico con CPU, memoria RAM, tarjeta de red, conexión USB, disco duro, tarjeta gráfica, entre otros. Un virtualizador permite ejecutar varios sistemas físicos con diferentes sistemas operativos en un mismo equipo de hardware.

Para crear una nueva máquina virtual en VMWare se escoge el apartado *File* (archivo) y a continuación *New Virtual Machine* (nueva máquina virtual), en este punto aparecerá un asistente de configuración en el cual se podrá escoger la creación de una máquina virtual típica o una personalizada, para este proyecto se escogerá una instalación típica.



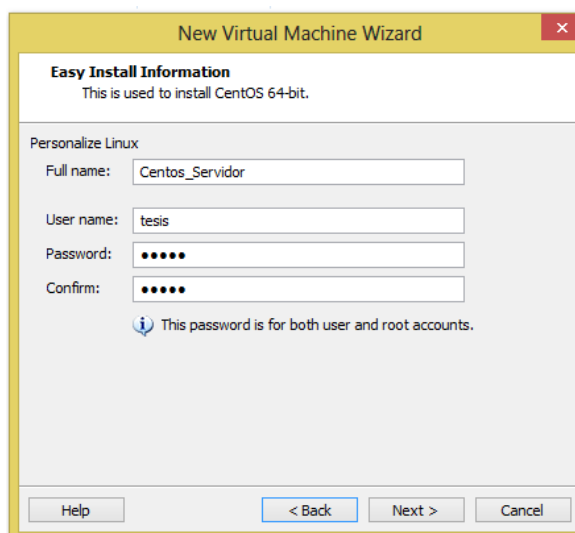
**Figura 62. Asistente de una nueva máquina virtual**

El siguiente paso del asistente de instalación es escoger la fuente de instalación del nuevo sistema operativo, se tiene las opciones de instalación a través de un disco por medio de una imagen iso; se escogerá la opción de la imagen iso ya que se descargó previamente el archivo de instalación del sistema operativo Centos 7.



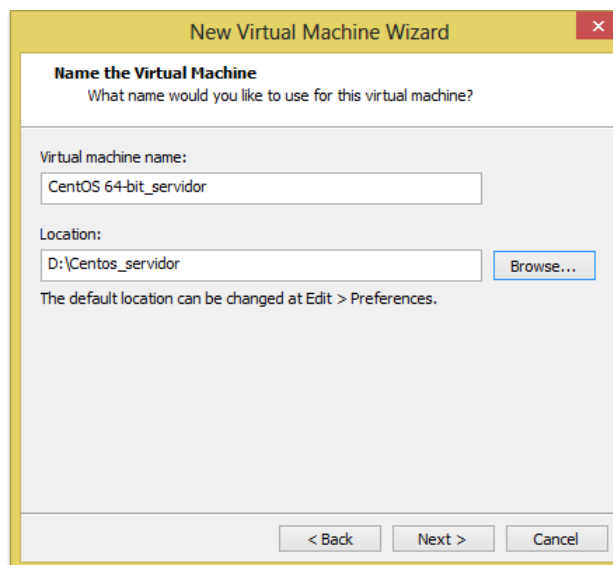
**Figura 63. Fuente de instalación del sistema operativo Centos7 en VMWare**

A continuación se procede a nombrar y a crear un nuevo usuario del sistema operativo Centos 7 con su respectiva clave de acceso.



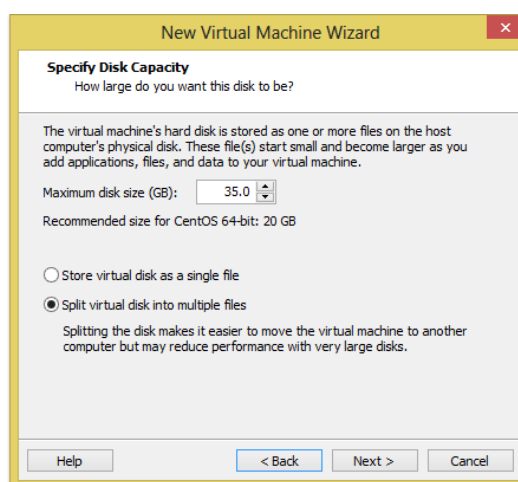
**Figura 64. Creación de un usuario en VMWare**

En la siguiente ventana se procede a nombrar y a escoger la dirección donde la nueva máquina virtual será instalada. Para este caso se escogió el disco local D.



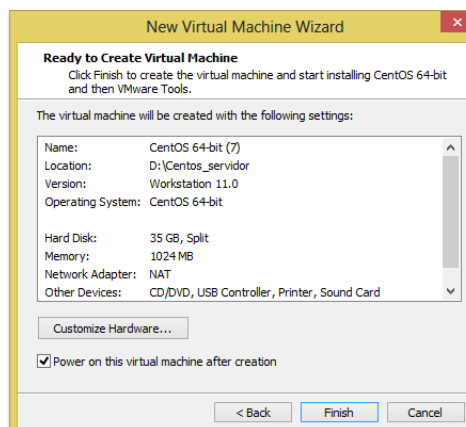
**Figura 65. Configuración del nombre de la máquina virtual**

Una vez configurado el nombre y la ruta de instalación de la nueva máquina virtual, se escogió el tamaño del disco duro que se reservará para la máquina virtual. Este parámetro se lo debe escoger dependiendo de la capacidad del equipo físico, se recomienda un mínimo de 20GB para el sistema operativo Centos 7.



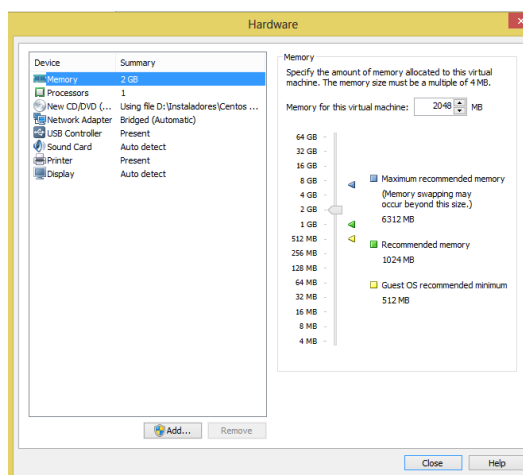
**Figura 66. Configuración del tamaño del disco duro de la máquina virtual**

A continuación se realizará la personalización del hardware de la máquina virtual, para esto se escoge la opción *Customize Hardware* (personalización del hardware), si no se personaliza el hardware VMWare configura los parámetros con los valores por defecto. En esta sección también se puede escoger la opción de encender la nueva máquina virtual una vez finalizada la creación.



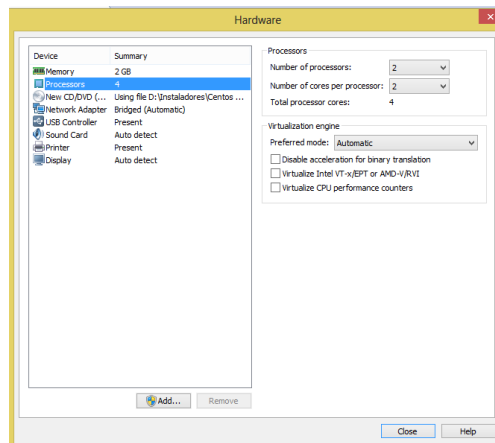
**Figura 67. Personalización de la máquina virtual**

Si se escoge la opción de personalización el hardware se comienza configurando la cantidad de memoria RAM, este parámetro dependerá en su totalidad de la cantidad de memoria que se tenga en el equipo físico. Para Centos 7 se recomienda un mínimo de 1GB de memoria RAM.



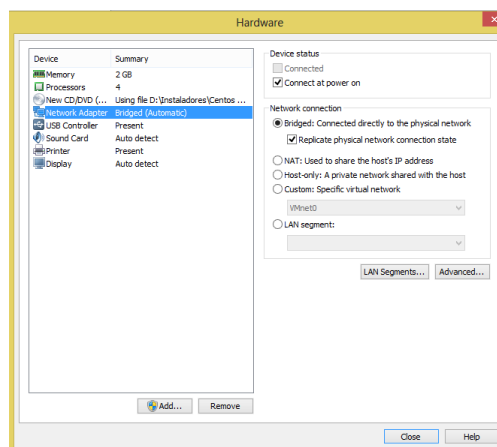
**Figura 68. Configuración de la memoria RAM de la máquina virtual**

Otro parámetro importante del hardware es el procesador, VMWare permite escoger la cantidad de procesadores y de núcleos que utilizará la máquina virtual. Para este proyecto se ha configurado dos procesadores con dos núcleos cada uno con lo que se obtiene 4 núcleos de procesador en total.



**Figura 69. Configuración del procesador de la máquina virtual**

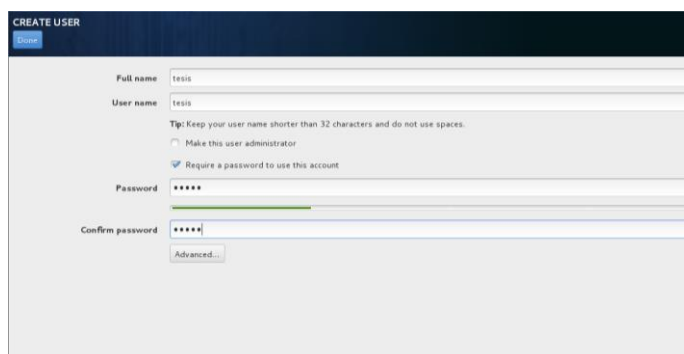
Por último se procede a configurar la tarjeta de red; se tiene las opciones de bridge (puente), NAT (traducción de direcciones de red), host-only (solo un host) y custom (personalizado). Para este proyecto se utiliza la opción bridge porque permite realizar una réplica del estado de conexión de la tarjeta de red del equipo físico. Una vez terminado este procedimiento se da por finalizada la creación de la máquina virtual.



**Figura 70. Configuración de la tarjeta de red de la máquina virtual**

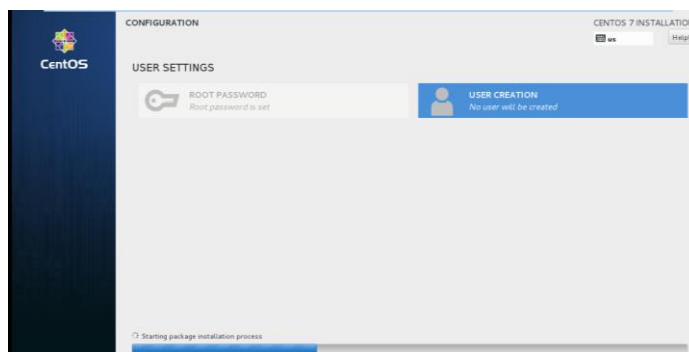
Una vez creada la máquina virtual se procede a instalar el sistema operativo Centos 7. Centos es un sistema operativo de código abierto basado en el kernel de GNU/Linux, es una distribución clon de Red Hat Enterprise Linux (RHEL) que fue lanzado el 14 de mayo de 2004. Ofrece un software de clase empresarial gratuito muy robusto, fácil de instalar y utilizar, por lo que es muy usado en nuestro medio. Desde la versión 5, cada versión recibe un soporte de diez años, por lo que la actual versión 7 recibirá las siguientes actualizaciones el 30 de junio de 2024.

Una vez que se arranca la máquina virtual aparecerá un el asistente de instalación grafico de Centos denominado Anaconda. Este asistente permite configurar el nombre de usuario y además la clave del súper usuario root.



**Figura 71. Configuración del usuario de Centos 7**

Después de que se ha configurado los diferentes usuarios Anaconda procederá a realizar la instalación del sistema operativo Centos 7.



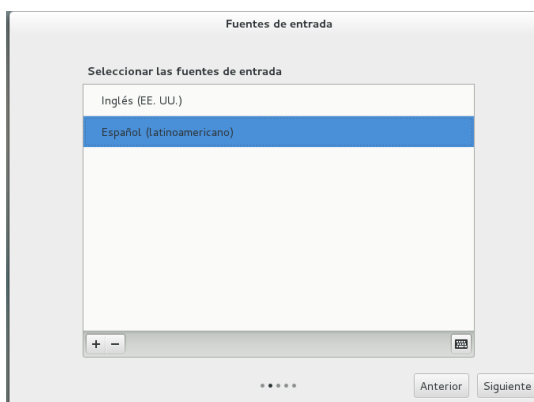
**Figura 72. Instalación de Centos 7**

Después de terminada la instalación se procede a ingresar con el usuario que se creó anteriormente y se configura el escritorio Gnome. Gnome es una interface gráfica de escritorio muy intuitiva y de fácil manejo que permite manipular de manera óptima el sistema Centos. El primer paso es escoger el idioma en el cual va a funcionar el escritorio Gnome.



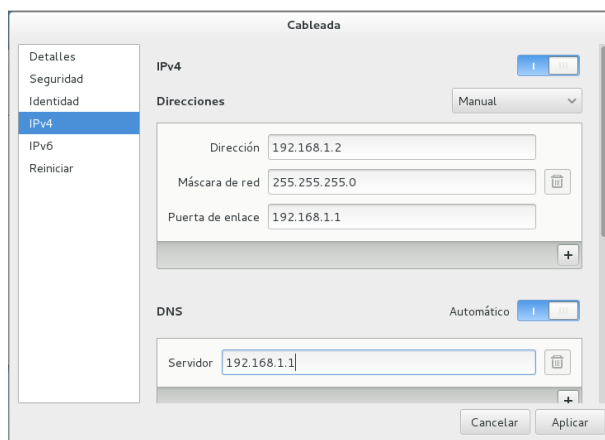
**Figura 73. Configuración del idioma de Gnome**

El siguiente paso es escoger el idioma del teclado, por lo que se escogerá el idioma latinoamericano. Este parámetro depende del teclado que posea el equipo físico. Por lo general existe una confusión entre el teclado latinoamericano y el teclado español, si el signo @ está en la letra Q es un teclado latinoamericano, y si está en el numero 2 es un teclado español.



**Figura 74. Configuración del teclado en Gnome**

Por último se procede a activar la interface de red y se ingresa en la pestaña *configuración*, en donde se procede a configurar la dirección IP, máscara, puerta de enlace y DNS.



**Figura 75. Configuración de la dirección IP en Centos 7**

#### 4.2 Configuración del servidor VSFTP

El protocolo de transferencia de archivos (FTP) es uno de los protocolos más utilizados en internet porque permite la transferencia de grandes bloques de datos a través de redes TCP/IP. Utiliza el puerto 20 y 21 exclusivamente TCP; el 20 es utilizado para transferir datos desde el cliente hacia el servidor y el 21 se lo utiliza para enviar órdenes desde el cliente hacia el servidor.

La variante de FTP que se utilizará para la elaboración de este proyecto es VSFTP (Very Secure FTP) debido a que es un protocolo que se caracteriza por no tener ninguna falla de seguridad conocida. VSFTP utiliza los protocolos SSL (Secure Layer Socket) y TLS (Transport Layer Security) que permite el envío de datos de una manera cifrada por lo que hace que el servidor VSFTP sea uno de los más seguros que se conoce.

El primer paso para crear un servidor VSFTP es ingresar al terminal y autenticarse como súper usuario *root*, porque de esta manera se podrá realizar todos los cambios que sean necesarios.



```
[tesis@localhost ~]$ su root
Contraseña:
[root@localhost tesis]#
```

**Figura 76. Ingreso como usuario root**

Para la creación del servidor VSFTP es necesario instalar el demonio de este servidor conocido como vsftpd, para esto se ejecuta el comando *yum install vsftpd* en el terminal.

```
[root@localhost tesis]# yum install vsftpd
Complementos cargados:fastestmirror, langpacks
base | 3.6 kB 00:00
extras | 3.4 kB 00:00
updates | 3.4 kB 00:00
(1/4): base/7/x86_64/group_gz | 154 kB 00:07
(2/4): extras/7/x86_64/primary_db | 87 kB 00:09
(3/4): updates/7/x86_64/primary_db | 4.0 MB 01:34
(4/4): base/7/x86_64/primary_db | 5.1 MB 01:34
Loading mirror speeds from cached hostfile
* base: mirror.uta.edu.ec
* extras: mirror.uta.edu.ec
* updates: mirror.uta.edu.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete vsftpd.x86_64 0:3.0.2-9.el7 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package      Arquitectura  Versión      Repositorio  Tamaño
=====
Instalando:
vsftpd      x86_64        3.0.2-9.el7  base         165 k
```

**Figura 77. Instalación del paquete vsftpd**

Al momento de instalar el demonio del servidor vsftp se crea automáticamente un archivo de configuración denominado *vsftpd.conf*, en este archivo se realiza todas las configuraciones necesarias para el buen funcionamiento del servidor vsftp. Para abrir este archivo se usa el comando vim seguido de su ubicación.

```
[root@localhost tesis]# vim /etc/vsftpd/vsftpd.conf
```

**Figura 78. Ingreso al archivo vsftpd.conf**

Una vez ingresado al archivo se procede a editarlo. En la figura 79 se puede observar las configuraciones necesarias para evitar que usuarios anónimos puedan ingresar al servidor, pero que si lo puedan hacer usuarios locales del sistema, además se

da permiso de lectura, escritura y ejecución (rwx) al usuario root; de lectura y escritura al grupo de usuario locales y a usuarios remotos (rw) por lo que se tiene una umask de 022.

```
#Evitar usuarios anonimos
anonymous_enable=NO
#permitir ingresar usuarios locales
local_enable=YES
#escribir sobre archivo en el servidor
write_enable=YES
#usuario root con permisos de rwx
local_umask=022
```

**Figura 79. Configuración de acceso en el archivo vsftpd.conf**

Las siguientes líneas permiten enviar algún tipo de mensaje desde el servidor hacia los usuarios, realizar descargas de archivos desde y hacia el servidor; el servidor se conectará por medio del puerto 20 de forma segura y se crearán logs de información hacia una ruta definida.

```
#permitir mensajes hacia usuarios
dirmessage_enable=YES
# Activar logging para uploads/downloads.
xferlog_enable=YES
# Hacer seguro el puerto de transferencia 20.
connect_from_port_20=YES
#generar logs o registros de actividad hacia /var/log/xferlog
xferlog_file=/var/log/xferlog
xferlog_std_format=YES
```

**Figura 80. Configuración de descarga, conexión y logs en el archivo vsftpd.conf**

De manera predeterminada, todos los usuarios que utilicen el servidor vsftp podrán acceder hacia los directorios de los otros usuarios, por seguridad, se debe configurar para que el usuario solo pueda acceder a su directorio, por lo tanto se debe activar las opciones que se muestran en la figura 81; se debe tomar en cuenta que el archivo `/etc/vsftd/chroot_list` contiene los nombres de usuarios del servidor.

```
# se conectaran usuarios que se esten
# en la lista chroot_list y usuarios locales
chroot_local_user=YES
chroot_list_enable=YES
# ubicacion de chroot_list
chroot_list_file=/etc/vsftpd/chroot_list
```

**Figura 81. Activación de la lista de usuarios en el archivo vsftpd.conf**

Las configuraciones que se muestran en la figura 82 permiten solo aceptar direccionamiento IPv4, darle un nombre al servidor, por seguridad es preferible usar un puerto efímero (10021) para escuchar a los clientes en vez del puerto 21, habilitar un rango de puertos pasivos de reserva, y por último se configura la dirección IP del servidor.

```
# escuchar ipv4
listen=YES
#escuchar ipv6
listen_ipv6=NO
#nombre del servidor
pam_service_name=vsftpd
#habiliar lista de usuarios
userlist_enable=YES
#utilizar TCP
tcp_wrappers=YES
#puerto de escucha
listen_port=10021
#habilitar pueros pasivos
pasv_enable=YES
pasv_min_port=30300
pasv_max_port=30309
#direccion IP del servidor
pasv address=192.168.1.2
```

**Figura 82. Configuración de puertos en el archivo vsftpd.conf**

Par aque sea un servidor ftp seguro es necesario activar algun metodo de encriptacion, en la figura 83 se puede observar que se ha habilitado el soporte SSL/TLS, se prefirira ssl\_tlsv1, y se muestra las rutas donde se almacenaran los certificados y la firma digital.

```
# Habilita el soporte de TLS/SSL
ssl_enable=YES
# # Se prefiere TLSv1 sobre SSLv2 y SSLv3
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# # Rutas del certificado y firma digital
rsa_cert_file=/etc/pki/tls/certs/vsftpd.crt
rsa_private_key_file=/etc/pki/tls/private/vsftpd.key
```

### Figura 83. Activación del soporte SSL/TLS en el archivo vsftpd.conf

Una vez que se ha realizado la edición del archivo vsftpd.conf se procede a crear un nuevo registro denominado chroot\_list, para lo cual se utiliza el comando vim. En este archivo se introducirá los nombres de los usuarios remotos que tendrán permitido el acceso al servidor.

```
[root@localhost vsftpd]# vim chroot_list
```

### Figura 84. Creación del archivo chroot\_list

Para que el servidor ftp se convierta en un servidor ftp muy seguro (vsftp) se necesita crear un certificado y una firma digital, para esto se va hacia el directorio /etc/pki/tls, y una vez allí se ejecuta el comando *openssl req -sha256 -x509 -nodes -days 1825 -newkey rsa:4096 \*, una vez ejecutado dicho comando se procede a llenar una serie de requerimientos para la generación del certificado digital como país, provincia, ciudad, nombre de usuario y correo electrónico.

```

[root@localhost vsftpd]# cd /etc/pki/tls/
[root@localhost tls]# openssl req -sha256 -x509 -nodes -days 1825 -newkey rsa:4096 \
> -keyout private/vsftpd.key \
> -out certs/vsftpd.crt
Generating a 4096 bit RSA private key
..++
.....++
writing new private key to 'private/vsftpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:EC
State or Province Name (full name) []:PICHINCHA
Locality Name (eg, city) [Default City]:QUITO
Organization Name (eg, company) [Default Company Ltd]:ESPE
Organizational Unit Name (eg, section) []:DEEE
Common Name (eg, your name or your server's hostname) []:tesis
Email Address []:tesis@espe.ec

```

**Figura 85. Creación del certificado y firma digital**

A continuación se procede a crear, tanto en el servidor como en cada uno de los clientes los usuarios con sus respectivas claves de acceso.

```

[root@localhost home]# useradd clienteuno
[root@localhost home]# passwd clienteuno
Cambiando la contraseña del usuario clienteuno.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: todos los símbolos de autenticación se actualizaron con éxito.

```

**Figura 86. Creación de usuarios vsftp**

Terminada la configuración de todos los parámetros del servidor vsftp se procede a activarlo a través del siguiente comando.

```

[root@localhost home]# systemctl start vsftpd

```

**Figura 87. Activación del servicio vsftp**

Para ingresar al servidor desde un usuario remoto se utiliza el comando *stp usuario@ip\_servidor*, una vez dentro del servidor, se puede descargar un archivo desde el servidor hacia el host de usuario con el comando *get*, y para subir un archivo hacia el servidor se utiliza el comando *put*.

```
[clienteuno@localhost ~]$ sftp clienteuno@192.168.1.2
clienteuno@192.168.1.2's password:
Connected to 192.168.1.2.
sftp> put archivoup
Uploading archivoup to /home/clienteuno/archivoup
archivoup          100%   0   0.0KB/s   00:00
sftp> get archivoup
Fetching /home/clienteuno/archivoup to archivoup
```

**Figura 88. Prueba de funcionamiento del servidor vsftp**

Wireshark es un analizador de protocolos creado en 1998 utilizado para la solución de problemas en redes de comunicaciones porque permite examinar datos en una red en tiempo real. Wireshark incluye un completo lenguaje que admite filtrar los protocolos y posee la habilidad de mostrar el flujo reconstruido de la sesión TCP. Es un software libre que se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles incluyendo Linux, Solaris, NetBSD, Android, Mac OS así como en Microsoft Windows.

En la figura 89 se puede comprobar que efectivamente los paquetes vsftp se están enviado a través de la red de manera encriptada por medio de los protocolos TLS y SSL, además se puede observar que también se encuentra encriptada la dirección IP del servidor, para evitar algún ataque de terceros.

No.	Time	Source	Destination	Proto	Length	Info
2989	142.12397400	192.168.1.36	192.168.1.16	TLSv1.2	85	Encrypted Alert
3035	144.02273500	192.168.1.36	192.168.1.16	TLSv1.2	361	Client Hello
3036	144.02273700	192.168.1.16	192.168.1.36	TLSv1.2	1183	Server Hello, Certificate, Server Hello Done
3038	144.02614700	192.168.1.36	192.168.1.16	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3043	144.03213600	192.168.1.16	192.168.1.36	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
3044	144.03564000	192.168.1.36	192.168.1.16	TLSv1.2	85	Encrypted Alert
3077	144.72801500	64.233.167.91	192.168.1.4	TLSv1.2	1182	[TCP Retransmission] Certificate
3079	144.73007100	192.168.1.4	64.233.167.91	TLSv1.2	228	Client Key Exchange, Change Cipher Spec, Hello Request
3129	144.83700900	64.233.167.91	192.168.1.4	TLSv1.2	1180	Certificate
3131	144.84108700	192.168.1.4	64.233.167.91	TLSv1.2	228	Client Key Exchange, Change Cipher Spec, Hello Request
3447	147.83488200	192.168.1.4	64.233.167.91	TLSv1.2	131	Application Data
4407	201.99602700	192.168.1.36	192.168.1.16	SSLV2	102	Client Hello
4421	202.01627600	192.168.1.36	192.168.1.16	SSLV3	194	Client Hello
4422	202.01650100	192.168.1.16	192.168.1.36	SSLV3	1178	Server Hello, Certificate, Server Hello Done
4423	202.01839500	192.168.1.36	192.168.1.16	SSLV3	394	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4426	202.02710600	192.168.1.16	192.168.1.36	SSLV3	129	Change Cipher Spec, Encrypted Handshake Message
4429	202.02827700	192.168.1.36	192.168.1.16	SSLV3	91	Encrypted Alert
4439	202.04674500	192.168.1.36	192.168.1.16	TLSv1	269	Client Hello
4440	202.04701500	192.168.1.16	192.168.1.36	TLSv1	1183	Server Hello, Certificate, Server Hello Done

**Figura 89. Prueba de funcionamiento del servidor vsftp a través de Wireshark**

### 4.3 Configuración del servidor NFS

NFS (Network File Service) es un protocolo de la capa de aplicación que permite compartir archivos y directorios en sistemas Linux de manera transparente entre diferentes anfitriones a través de una red TCP/IP, es utilizado para sistemas de archivos distribuidos.

NFS fue creado en el año de 1984 por Sun Microsystems, funciona a través de los protocolos de nivel de presentación XDR (Xternal Data Representation) y del nivel de sesión ONC RPC (Open Network Computing Remote Procedure Call). Se debe tomar en cuenta que este sistema de archivos solo debe funcionar en una red LAN bajo un firewall y listas de control de acceso porque este protocolo no poseen ningún tipo de encriptación.

Para configurar el servidor NFS en Centos 7 se debe ingresar al terminal como super usuario e instalar el demonio de NFS llamdo nfs-utils.

```
[tesis@localhost ~]$ su root
Contraseña:
[root@localhost tesis]# yum install nfs-utils
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: centos.brisanet.com.br
* extras: centos.brisanet.com.br
* updates: centos.brisanet.com.br
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete nfs-utils.x86_64 1:1.3.0-0.8.el7 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package           Arquitectura  Versión                Repositorio  Tamaño
=====
Instalando:
nfs-utils          x86_64       1:1.3.0-0.8.el7       base         362 k
=====
Resumen de la transacción
=====
Instalar 1 Paquete
```

**Figura 90. Instalación del paquete nfs-utils**

Se debe crear un directorio en donde se encontraran todos los archivos que se van a compartir en la red, por lo que se utilizara el comando:

```
[root@localhost etc]# mkdir /home/nfs
```

**Figura 91. Creación del directorio compartido del servidor NFS**

El archivo */etc/exports.conf* permite otorgar permisos de acceso a los equipos de diferentes redes que van a consumir la información, además provee premisos para solo lectura o también modificación de documentos. En este archivo se designa el directorio compartido, la dirección IP de red en que se va a compartir archivos y se da permisos de lectura y escritura (rw).

```
/home/nfs/ 192.168.1.0/24(rw, sync, no_root_squash)
```

### Figura 92. Configuración del archivo exports.conf

Desde pues de que se ha proporcionado, al servidor NFS, los permisos de acceso correspondientes, muy importante para la integridad y confidencialidad de los datos, se procede a arrancar con el servicio. Con esto se da por finalizado la configuración del servidor.

```
[root@localhost etc]# systemctl start nfs
```

### Figura 93. Inicialización del servicio NFS

En el cliente también es preciso instalar y arrancar el servicio NFS, la instalación y arranque se lo realiza de la misma manera que en el servidor, además, se debe crear un nuevo directorio, el cual se montará sobre el directorio compartido creado en el servidor.

```
[root@localhost clienteuno]# mkdir /home/clientenfs
```

### Figura 94. Creación del directorio compartido en el cliente NFS

Una buena práctica para saber si el servidor está compartiendo algún directorio es utilizar el comando *showmount -e* seguido de la dirección IP del servidor, el cual permitirá verificar los directorios que el equipo está dispuesto a compartir.

```
[root@localhost clienteuno]# showmount -e 192.168.1.2
Export list for 192.168.1.2:
/home/nfs 192.168.1.0/24
```

### Figura 95. Exploración de puntos de montaje



Una vez comprobado los directorios de compartición del servidor se procede a realizar el montaje de la carpeta creada en el cliente sobre la del servidor. Para este propósito se utiliza el comando: `mount -t nfs IP_servidor /directorio_servidor /directorio_cliente`

```
[root@localhost clienteuno]# mount -t nfs 192.168.1.2:/home/nfs /home/clientenfs
```

### Figura 96. Montaje del directorio compartido del servidor NFS

El comando `df -h` permite mostrar todos los montajes que se han realizado en algún dispositivo, por lo tanto es de gran utilidad para verificar si el montaje NFS fue realizado correctamente. Cuando se ha verificado que el montaje es exitoso ya se puede compartir archivos entre directorios de los diferentes equipos.

```
[root@localhost clienteuno]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        38G   7.0G   31G   19% /
devtmpfs         905M   0   905M   0% /dev
tmpfs            914M  480K   913M   1% /dev/shm
tmpfs            914M   8.9M   905M   1% /run
tmpfs            914M   0   914M   0% /sys/fs/cgroup
/dev/sda1        297M  111M  186M   38% /boot
/dev/sr0         54M   54M   0  100% /run/media/clienteuno/CDROM
/dev/sr1         4.1G   4.1G   0  100% /run/media/clienteuno/CentOS 7 x86_64
192.168.1.2:/home/nfs  33G   4.1G   29G   13% /home/clientenfs
```

### Figura 97. Comprobación del montaje del directorio compartido

Por medio del sniffer Wireshark se puede comprobar que efectivamente está corriendo el protocolo NFS a través de la red, además de que se puede concluir que el intercambio de archivos se lo está realizando entre el host 192.168.1.4 y el servidor 192.168.1.2

No.	Time	Source	Destination	Protocol	Length	Info
3161	170.131607000	192.168.1.4	192.168.1.2	NFS	110	V4 NULL Call (Reply In 3163)
3163	170.132807000	192.168.1.2	192.168.1.4	NFS	94	V4 NULL Reply (Call In 3161)
3165	170.133103000	192.168.1.4	192.168.1.2	NFS	266	V4 Call (Reply In 3166) SETCLIENTID
3166	170.134349000	192.168.1.2	192.168.1.4	NFS	130	V4 Reply (Call In 3165) SETCLIENTID
3167	170.134414000	192.168.1.4	192.168.1.2	NFS	186	V4 Call (Reply In 3168) SETCLIENTID_CONFIRM
3168	170.135131000	192.168.1.2	192.168.1.4	NFS	114	V4 Reply (Call In 3167) SETCLIENTID_CONFIRM
3171	170.135296000	192.168.1.4	192.168.1.2	NFS	194	V4 Call (Reply In 3173) PUTROOTFH   GETATTR
3173	170.136710000	192.168.1.2	192.168.1.4	NFS	278	V4 Reply (Call In 3171) PUTROOTFH   GETATTR
3174	170.136859000	192.168.1.4	192.168.1.2	NFS	198	V4 Call (Reply In 3175) GETATTR FH: 0x62d40c52
3175	170.138267000	192.168.1.2	192.168.1.4	NFS	162	V4 Reply (Call In 3174) GETATTR
3176	170.138395000	192.168.1.4	192.168.1.2	NFS	202	V4 Call (Reply In 3177) GETATTR FH: 0x62d40c52
3177	170.139055000	192.168.1.2	192.168.1.4	NFS	178	V4 Reply (Call In 3176) GETATTR
3178	170.139116000	192.168.1.4	192.168.1.2	NFS	198	V4 Call (Reply In 3179) GETATTR FH: 0x62d40c52
3179	170.139831000	192.168.1.2	192.168.1.4	NFS	162	V4 Reply (Call In 3178) GETATTR
3180	170.139881000	192.168.1.4	192.168.1.2	NFS	202	V4 Call (Reply In 3181) GETATTR FH: 0x62d40c52
3181	170.140613000	192.168.1.2	192.168.1.4	NFS	178	V4 Reply (Call In 3180) GETATTR
3182	170.140667000	192.168.1.4	192.168.1.2	NFS	198	V4 Call (Reply In 3183) GETATTR FH: 0x62d40c52
3183	170.141394000	192.168.1.2	192.168.1.4	NFS	142	V4 Reply (Call In 3182) GETATTR
3184	170.141662000	192.168.1.4	192.168.1.2	NFS	198	V4 Call (Reply In 3185) GETATTR FH: 0x62d40c52
3185	170.142218000	192.168.1.2	192.168.1.4	NFS	162	V4 Reply (Call In 3184) GETATTR

### Figura 98. Prueba de funcionamiento del servidor NFS por medio de Wireshark

#### 4.4 Configuración del servidor SMB

El protocolo SMB (Server Message Block) trabaja en la capa de presentación del modelo OSI; dicho protocolo fue creado en 1985 por la compañía IBM, también se lo conoce como CIFS (Common Internet File System), después de ser renombrado por Microsoft en 1998. Trabaja a través del protocolo NetBios y permite el intercambio de archivos a través de la red TCP/IP entre dispositivos Linux y Windows.

Para crear un servidor SMB en Centos 7 se requiere instalar los demonios: samba, samba-client, samba-common-tools y samba-winbind-clients.

```
[root@localhost home]# yum install samba samba-client samba-common-tools s
amba-winbind-clients
Complementos cargados:fastestmirror, langpacks
base | 3.6 kB | 00:00
extras | 3.4 kB | 00:00
updates | 3.4 kB | 00:00
(1/2): extras/7/x86_64/primary_db | 88 kB | 00:33
(2/2): updates/7/x86_64 8% [= ] 6.6 kB/s | 356 kB | 09:39
(2/2): updates/7/x86_64/primary_db
```

**Figura 99. Instalación de los paquetes SMB**

Cuando ya se ha instalado todos los demonios necesarios se creará automáticamente un archivo de configuración llamado `smb.conf`, este archivo se encuentra en la dirección `/etc/samba`. Para abrir dicho archivo se utiliza el comando `vim`.

```
[root@localhost tesis]# vim /etc/samba/smb.conf
```

**Figura 100. Ingreso al archivo `smb.conf`**

En la figura 101 se muestra las primeras líneas de configuración del archivo `smb.conf`, en las que se establece el grupo de trabajo, el tipo de codificación (UTF-8), el nombre del anfitrión (servidor), los hosts que tendrán permitido ingresar al servidor SMB y adicionalmente alguna descripción.

```
workgroup = tesis
# descripción
server string = Samba Server Version %v
#formato de codificación
unix charset = UTF-8
#nombre del anfitrión
netbios name = tesis
# redes que permiten acceso al servidor
hosts allow = 127.0.0.1 192.168.1.0/24
```

**Figura 101. Configuración de los clientes con acceso al servidor SMB**

El servidor SMB permite crear logs o registros, estos registros son archivos en donde se almacenaran todos los cambios que se han hecho en el equipo, en las siguientes líneas se configurará la ruta en donde se guardarán estos registros y su tamaño máximo por archivo.

```
# logs o registros
log file = /var/log/samba/log.%m
# maximo tamaño de archivo de log
max log size = 50
```

**Figura 102. Configuración de los logs del servidor SMB**

Para finalizar la configuración del archivo *smb.conf* se procede a establecer los parámetros para el directorio compartido, en este apartado se describe la ruta del directorio, permisos de creación de archivos y directorios, accesos de usuarios por medio de un web browser y de manera simultánea, y permisos de escritura e impresión.

```
[carpeta_compartida]
#comentario
comment = Carpeta compartida SAMBA
#ruta del directorio compartido
path = /home/samba
#se puede ingresar via web browser
browseable = yes
#acceso como usuario invitado
guest ok = yes
guest only = yes
#permisos para la creacion de archivos
create mode = 0777
#permisos para la creacion de directorios
directory mode = 0777
#permite acceder mas de una persona a la vez
share modes =yes
#permite escribir sobre archivos compartidos
writable = yes
#permite impresion de archivos compartidos
printable = yes
```

**Figura 103. Configuración del directorio compartido del servidor SMB**

Ya terminada la configuración del archivo *smb.conf* se procede a crear el directorio compartido con el nombre y la ruta que se especificó previamente, esto se lo realiza por medio del comando *mkdir*.

```
[tesis@localhost ~]$ cd /home
[tesis@localhost home]$ mkdir samba
```

**Figura 104. Creación del directorio compartido**

A continuación se procede a dar permisos de lectura, escritura y ejecución al nuevo directorio compartido, por medio del comando *chmod* y también se especifica el grupo de trabajo al cual pertenecerá el directorio, a través del comando *chown*.

```
[root@localhost home]# chmod 777 /home/samba  
[root@localhost home]# chown tesis:tesis /home/samba
```

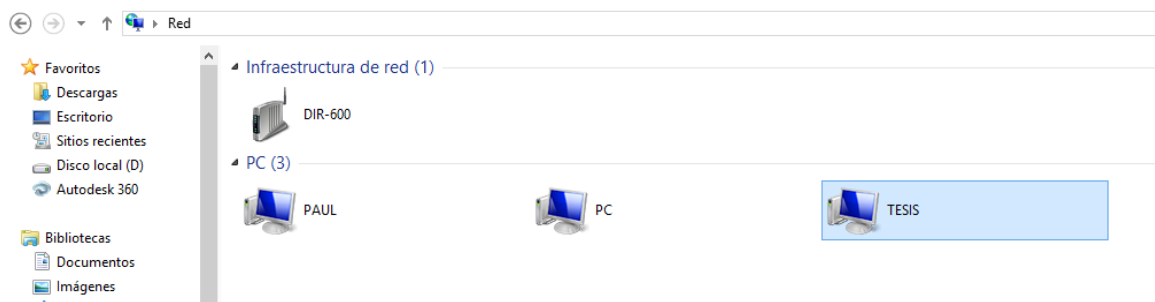
**Figura 105. Permisos para el directorio compartido**

Para dar por finalizado la configuración del servidor SMB se procede a levantar los servicios *smb* y *nmb*.

```
[root@localhost home]# systemctl start smb  
[root@localhost home]# systemctl start nmb
```

**Figura 106. Inicialización del servicio SMB**

Para comprobar que el servidor SMB está funcionando de manera adecuada, en un host con sistema operativo Windows se debe dirigirse hacia el apartado de red y aquí aparecerá de manera automática un dispositivo con el nombre del servidor, ingresando a este dispositivo se podrá observar el directorio compartido que se configuro anteriormente.



**Figura 107. Verificación del funcionamiento de SMB en un equipo Windows**

Por medio de Wireshark se puede comprobar que efectivamente está corriendo el protocolo SMB en la red LAN, en donde el equipo con dirección IP 192.168.1.2 es el servidor SMB y el dispositivo 192.168.1.16 es el host Windows

Io.	Time	Source	Destination	Protocol	Length	Info
138	7.75310900	192.168.1.16	192.168.1.255	BROWSEF	216	Get Backup List Request
140	7.75456000	192.168.1.2	192.168.1.16	BROWSEF	222	Get Backup List Response
234	10.0391520	192.168.1.16	192.168.1.2	SMB	213	Negotiate Protocol Request
255	10.0604320	192.168.1.16	192.168.1.2	SMB	191	Negotiate Protocol Request
256	10.0691970	192.168.1.2	192.168.1.16	SMB	217	Negotiate Protocol Response
257	10.0696180	192.168.1.16	192.168.1.2	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATE
258	10.0707430	192.168.1.2	192.168.1.16	SMB	300	Session Setup AndX Response, NTLMSSP_CHALLENGE, Er
259	10.0709570	192.168.1.16	192.168.1.2	SMB	238	Session Setup AndX Request, NTLMSSP_AUTH, User: \
260	10.0722460	192.168.1.2	192.168.1.16	SMB	156	Session Setup AndX Response
261	10.0724420	192.168.1.16	192.168.1.2	SMB	134	Tree Connect AndX Request, Path: \\TESIS\IPC\$
262	10.0737430	192.168.1.2	192.168.1.16	SMB	114	Tree Connect AndX Response
264	10.0738710	192.168.1.16	192.168.1.2	LANMAN	181	NetServerEnum2 Request, workstation, server, SQL s
265	10.0744940	192.168.1.2	192.168.1.16	LANMAN	176	NetServerEnum2 Response

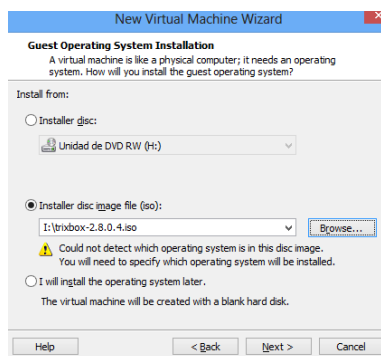
**Figura 108. Prueba de funcionamiento del servidor SMB a través de Wireshark**

#### 4.5 Instalación y configuración de la central de VoIP Trixbox en VMWare.

Trixbox es un sistema operativo GNU/Linux, basado en Centos, que actúan como una central telefónica (PBX), permite interconectar teléfonos dentro de una compañía y conectarlos a la red convencional. Al ser un software de código abierto admite crear nuevas funcionalidades, además de soportar VoIP con lo que se obtiene ahorros significativos en los costes de llamadas internacionales porque estas se realizan vía internet.

Por medio de Trixbox se puede crear extensiones, envíos de mensajes de voz, emails, llamadas para conferencias, menús interactivos de voz y distribución automáticas de llamadas. Utiliza los protocolos SIP, H.323, IAX, IAX2 y MGCP.

Al ser una variante de Centos, la instalación de Trixbox en VMware se lo realiza de la misma como muestra en el apartado 4.1, cargando la imagen iso del sistema operativo y reservando un mínimo de 20GB de disco duro.



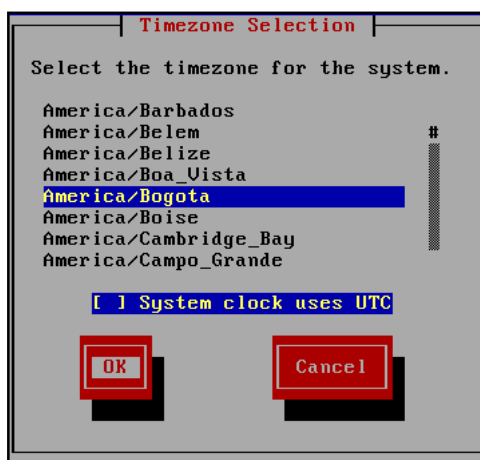
**Figura 109. Asignación de espacio de disco duro para Trixbox**

Una vez creada la máquina virtual Trixbox y luego de la detección de los componentes del sistema, se escoge el tipo de teclado. Para lo cual se selecciona el más apropiado, por ejemplo “Latinoamericano”, luego con la tecla Tab se selecciona *OK*.



**Figura 110. Selección de teclado en Trixbox**

A continuación se procede a elegir la zona horaria, para este caso se elige la opción: “América/Guayaquil”.



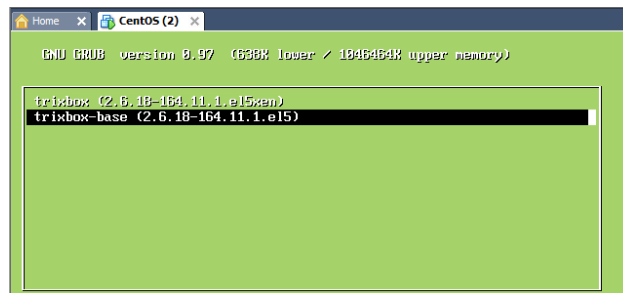
**Figura 111. Selección de la zona horaria en Trixbox**

El sistema operativo Trixbox, por seguridad, pedirá ingresar una contraseña para el súper usuario root y su respectiva confirmación.



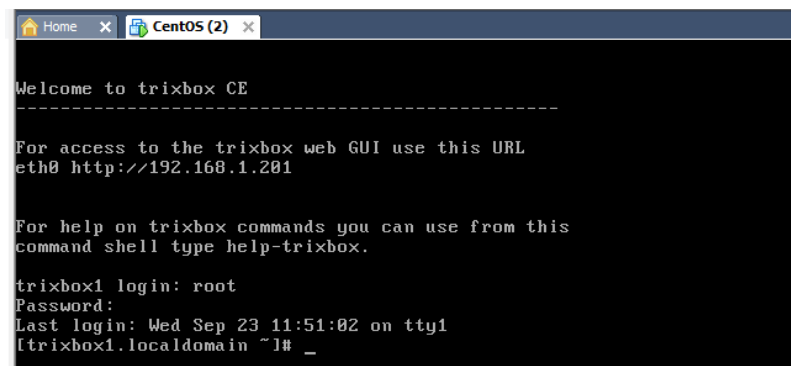
**Figura 112. Creación del usuario en Trixbox**

Una vez terminada la instalación del sistema operativo se espera que se reinicie el equipo, y se comprueba que Trixbox se haya instalado correctamente.



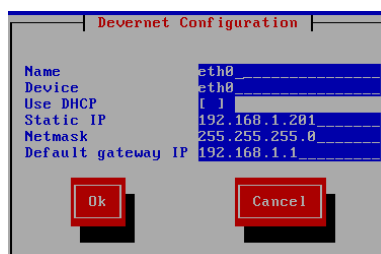
**Figura 113. Instalacion finalizada de Trixbox**

A continuación se procede a acceder al servidor ingresando el nombre de usuario root y su respectiva contraseña, el cual fue asignado al momento de la instalación



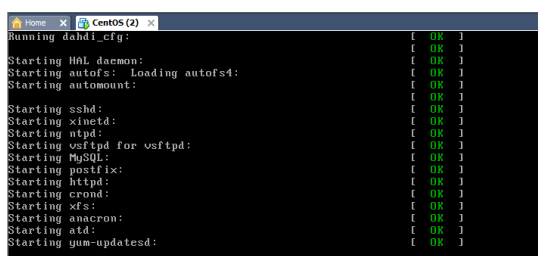
**Figura 114. Acceso A Trixbox**

Ahora para configurar la red se procede a cambiar dirección IP, para ello se utiliza el comando *system-config-network*, a continuación se elige: *edit devices*, *eth0* y se añade la dirección IP, en este caso se usará como ejemplo la dirección 192.168.1.201.



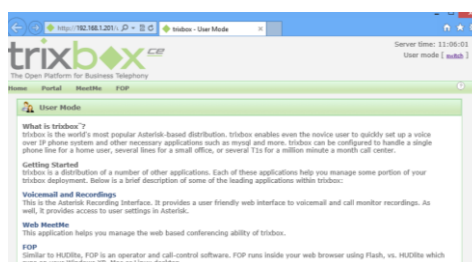
**Figura 115. Configuración de la interface ether0**

Una vez configurados estos parámetros, se selecciona *OK* para terminar; y para que los cambios sean efectivos se reinicia el servicio de red con el comando *service network restart*.



**Figura 116. Reinicio del servidor Tribox**

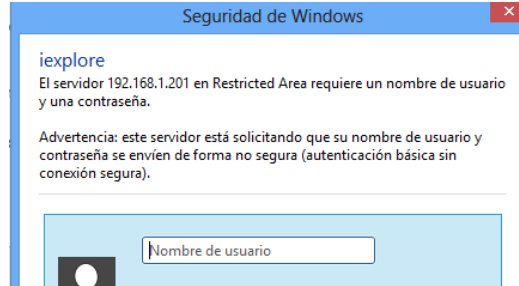
Ahora se procede a abrir un navegador Web y se ingresa la dirección IP del servidor: <http://192.168.1.201> y se verá una imagen similar a la que se muestra en la figura 117.



**Figura 117. Inicio de Tribox**

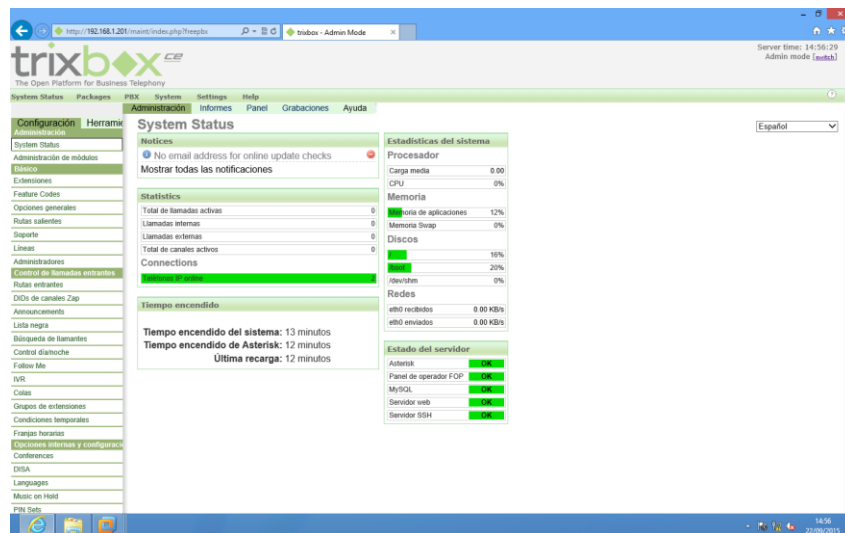


En la parte superior derecha se debe escoger la opción *switch* para cambiar de usuario común a administrador, el usuario es *maint* y el password es *password*



**Figura 118. Autenticación en Trixbox**

Una vez que se autenticado el usuario de administración, aparece el estado del sistema y sus diferentes opciones.



**Figura 119. Estado del sistema Trixbox**

Se elige la opción *PBX Settings* la cual permitirá configurar las extensiones del servidor de voz sobre IP. Las extensiones se refiere a cada uno de los usuarios que van a utilizar el servicio



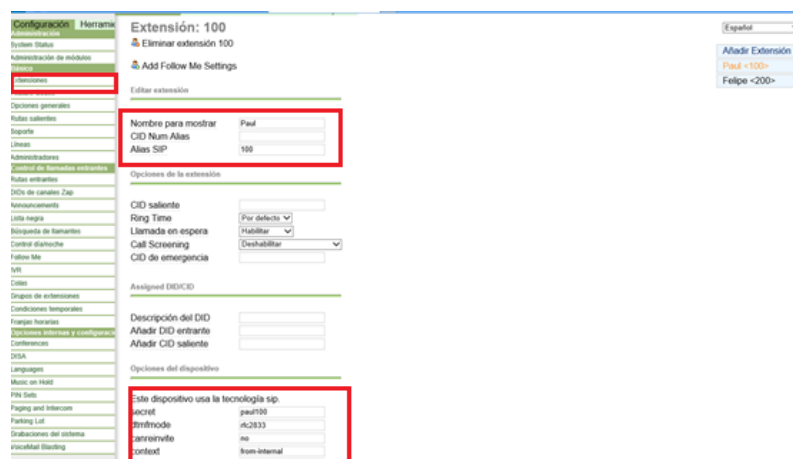
**Figura 120. Configuración de PBX en Trixbox**

Una vez que se ingresó a la configuración de PBX se elige la opción *Extensiones* y se selecciona el tipo de dispositivo que se va a añadir.



**Figura 121. Tipos de dispositivos en Trixbox**

Ya seleccionado el dispositivo se procede a llenar los campos: Nombre para mostrar, Alias SIP y secret que son los más importantes para la creación de extensiones.

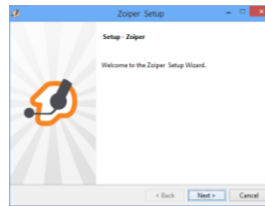


**Figura 122. Configuración de extensiones en Trixbox**

#### 4.5.1 Instalación de la herramienta ZOIPER

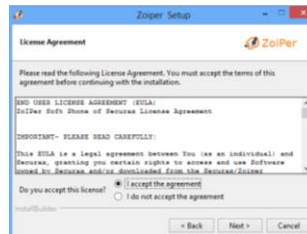
Zoiper es una aplicación gratuita que emula un teléfono que permite realizar llamadas desde un computador a otros que tengan instalado un software igual o similar o hacia teléfonos fijos o celulares en cualquier país del mundo.

Una vez descargado el instalador de Zoiper se procede hacer doble clic sobre el archivo .exe y de inmediato aparecerá la siguiente ventana.



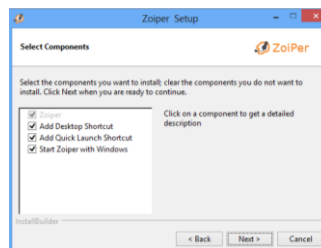
**Figura 123. Zoiper Setup**

En esta parte se selecciona *I accept the agreement* y después se da clic en *Next*.



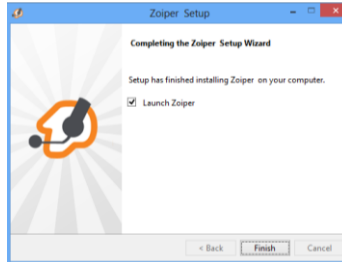
**Figura 124. Licencia Zoiper**

Aquí se selecciona los componentes necesarios para la instalación y después se da clic en *Next*.



**Figura 125. Selección de Componentes Zoiper**

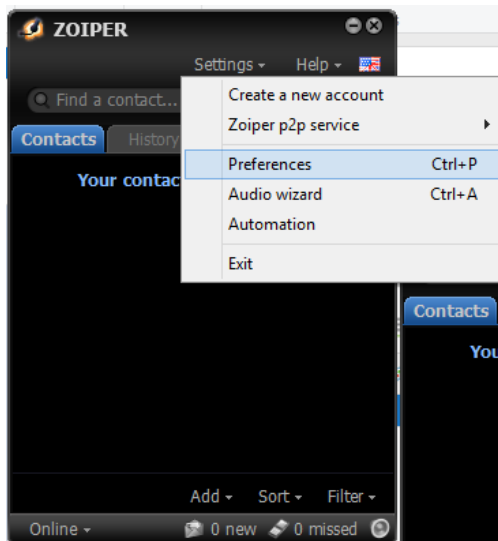
Una vez que se realizó todos los pasos anteriores se puede observar que ya está instalado el programa Zoiper.



**Figura 126. Finalización de la instalación de Zoiper**

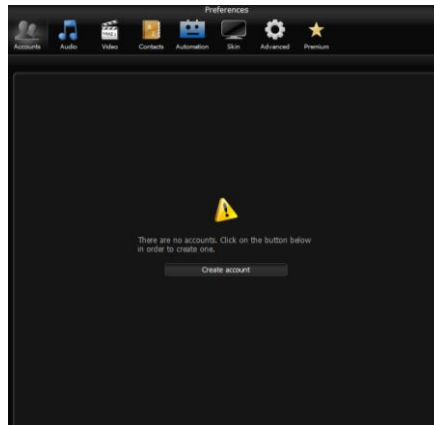
#### 4.5.2 Configuración de la herramienta ZOIPER

Para configurar las extensiones en Zoiper se escoge la opción *Settings* y se elige *Preferences*.



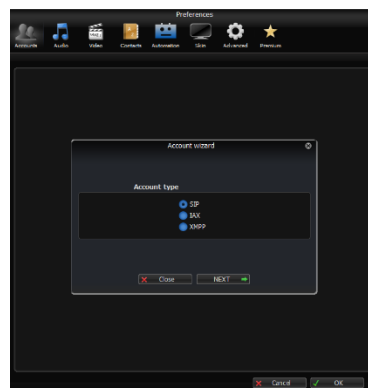
**Figura 127. Ajustes Zoiper**

Una vez que se accedió a la opción *Preferences* aparece la ventana como la que se muestra en la figura 128, en donde se a crear una extensión para lo cual se selecciona *Create account*



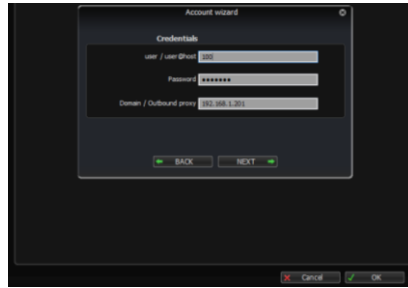
**Figura 128. . Creación Cuenta en Zoiper**

Ahora se procede a seleccionar el tipo de cuenta que se va a utilizar para que se conecte con el servidor de telefonía IP, en este caso se utilizara la cuenta con protocolo SIP.



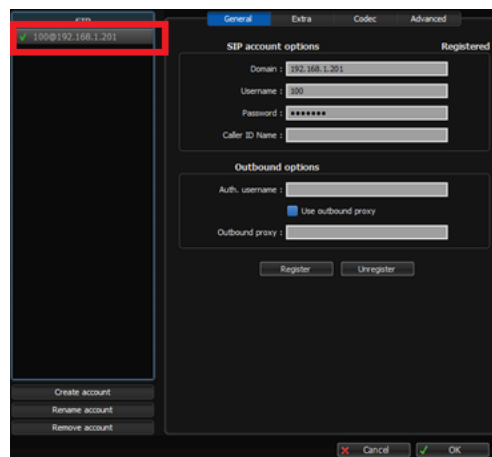
**Figura 129. Tipo de Cuenta Zoiper**

A continuación se ingresa los datos que antes ya se configuraron en Trixbox por ejemplo en *user* (usuario) se escribe el Alias SIP, en *password* se escribe la clave y en *domain* (dominio) se escribe la dirección IP del servidor.



**Figura 130. Credenciales Zoiper**

Y por último se observa que los datos que se ingresó anteriormente están correctos y que la cuenta SIP ya está registrada en el servidor



**Figura 131. Registro de cuenta SIP**

Para realizar la verificación del funcionamiento del servicio de VoIP en la red se utiliza la herramienta Wireshark con la que se determina que existe transferencia de paquetes SIP entre el servidor 192.168.1.201 y el cliente 192.168.1.16

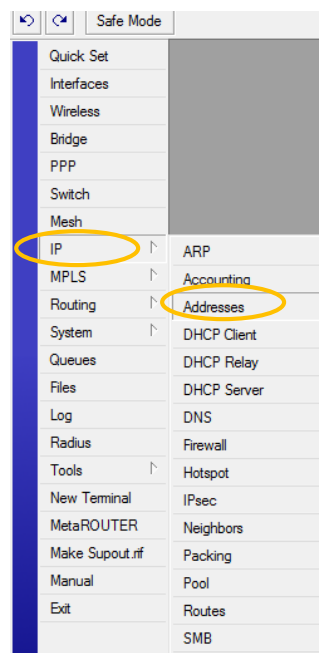
No.	Time	Source	Destination	Protocol	Length	Info
122	4.06475200	192.168.1.16	192.168.1.201	SIP	735	Request: SUBSCRIBE sip:200@192.168.1.201;transpo
123	4.06664900	192.168.1.201	192.168.1.16	SIP	481	Request: ACK sip:200@192.168.1.16:63519
124	4.06714700	192.168.1.201	192.168.1.16	SIP	518	Status: 501 Method Not Implemented
125	4.06714700	192.168.1.201	192.168.1.16	SIP	586	Status: 401 Unauthorized
128	4.10417600	192.168.1.16	192.168.1.201	SIP	907	Request: SUBSCRIBE sip:200@192.168.1.201;transpo
129	4.10506800	192.168.1.201	192.168.1.16	SIP	507	Status: 489 Bad Event
140	4.21503100	192.168.1.16	192.168.1.201	SIP/XML	991	Request: PUBLISH sip:200@192.168.1.201;transport
141	4.21511500	192.168.1.16	192.168.1.201	SIP	735	Request: SUBSCRIBE sip:200@192.168.1.201;transpo
143	4.21675000	192.168.1.201	192.168.1.16	SIP	518	Status: 501 Method Not Implemented
144	4.21761200	192.168.1.201	192.168.1.16	SIP	586	Status: 401 Unauthorized
147	4.22434400	192.168.1.16	192.168.1.201	SIP	907	Request: SUBSCRIBE sip:200@192.168.1.201;transpo
148	4.22524700	192.168.1.201	192.168.1.16	SIP	507	Status: 489 Bad Event
3940	33.35717400	192.168.1.201	192.168.1.16	SIP	667	Request: OPTIONS sip:200@192.168.1.16:63519;rins
3942	33.36295600	192.168.1.16	192.168.1.201	SIP	709	Status: 200 OK

**Figura 132. Prueba de funcionamiento de la central de VoIP con Wireshark**

#### 4.6 Habilitación de Internet sobre la red

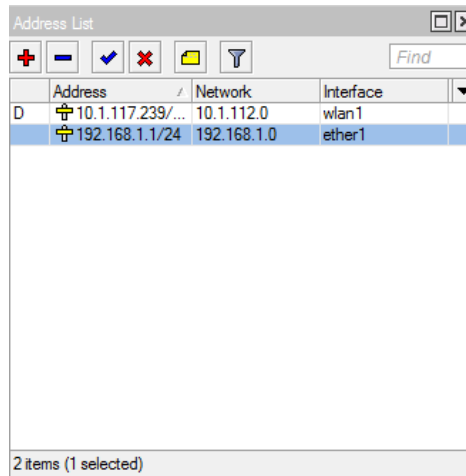
Para habilitar el servicio de internet sobre la red LAN se utilizará un router Mikrotik RB751U, el cual servirá de puerta de enlace predeterminada para los dispositivos de usuario final. Por medio de la interface inalámbrica que posee este dispositivo se procederá a conectarse a la red la Universidad de las Fuerzas Armadas “ESPE” y a su vez hacia internet.

La primera configuración requerida para el router Mikrotik es asignar una dirección IP a una de las interfaces fastethernet, para lo cual se debe ingresar al sistema operativo RouterOS por medio de la herramienta Winbox, y una vez allí se escoge la opción *IP* y a continuación *Addresses*.(direcciones)



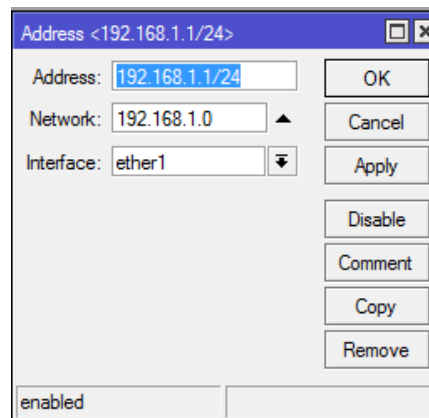
**Figura 133. Opción *Addresses***

Ya escogida la opción *Addresses* aparecerá una ventana denominada Address List (lista de direcciones) en donde se procede a añadir una nueva dirección IP, para lo cual se escoge la opción *Add (+)*.



**Figura 134. Añadir una nueva dirección IP**

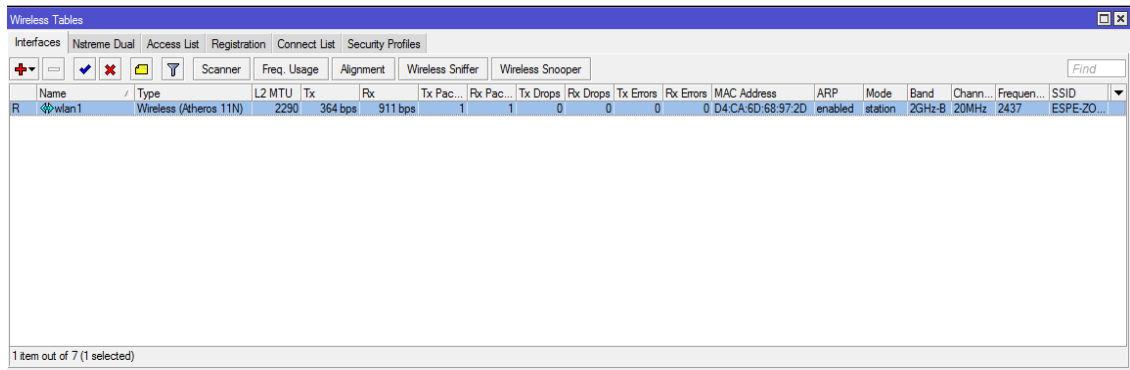
A continuación aparecerá una ventana en la que se procede a asignar una dirección IP con su respectiva máscara, la dirección de red y la interface a la cual le pertenecerá dicha dirección IP; para este caso será ether1.



**Figura 135. Configuración de una dirección IP**

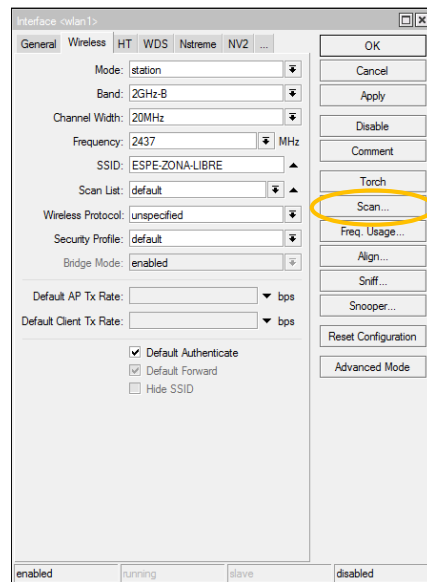
Una vez que se ha realizado la configuración de la interface fastethernet se procede a la configuración de la interface WLAN, para lo cual se escoge la opción Wireless, dentro del menú principal, y a continuación se activa la interface escogiendo la opción *enable* (habilitar) (✓).





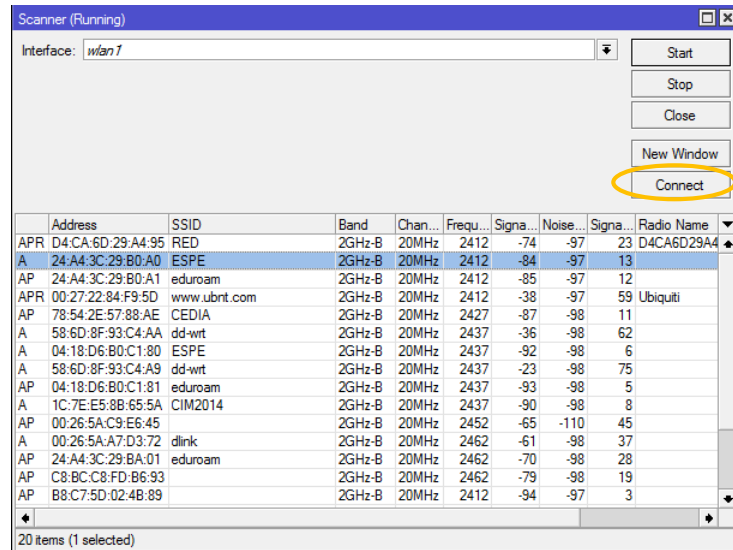
**Figura 136. Activación de la interface wlan**

Escogiendo la opción *wlan1* aparecerá una ventana de configuración de la interface inalámbrica. Debido a que este equipo funcionará como estación no se requiere configurar ningún parámetro, sino que escogiendo la opción *Scan* (escanear), el equipo empezará a buscar las redes inalámbricas a las que se pueda anclar, y automáticamente establecerá los parámetros que sean necesarios.



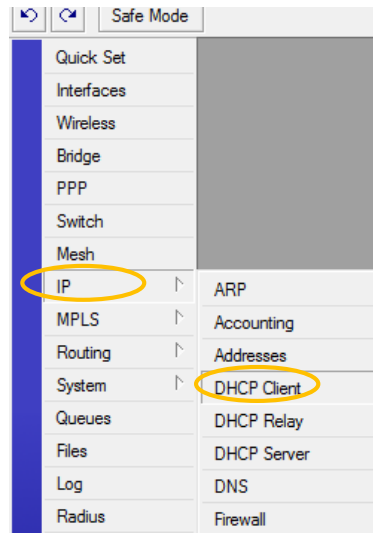
**Figura 137. Sección Wireless**

Ya escogida la opción *Scan* aparecerá una ventana con todas las redes que se encuentren disponibles al momento, se escoge una de ellas, que en este caso es la red con el SSID ESPE y se procede a conectarse por medio de la opción *Connect*. (conectar)



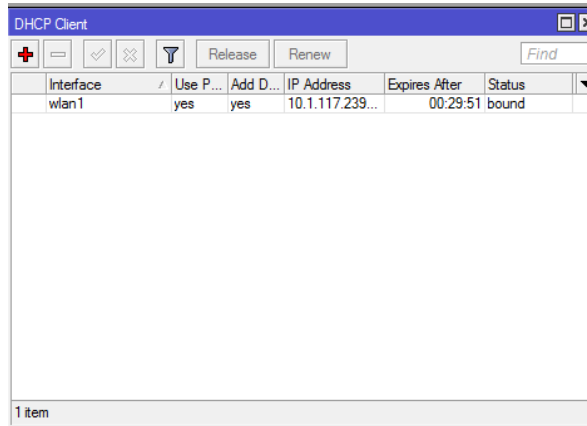
**Figura 138. Escaneo de la red ESPE**

La red ESPE asigna las direcciones IP automáticamente por medio del protocolo DHCP (Dynamic Host Configuration Protocol), por lo que es necesario que la interface *wlan1* se convierta en cliente DHCP, para lo cual en el menú inicial se escoge la opción *IP*, y a continuación *DHCP Client* (cliente DHCP).



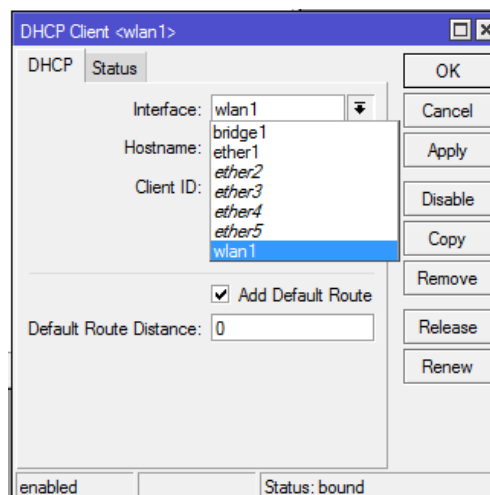
**Figura 139. Sección *DCHP Client***

Dentro de la ventana DHCP Client, por medio de la opción *Add (+)*, se procede a crear un nuevo cliente DHCP el cual obtendrá automáticamente una dirección IP que es provista por un servidor DHCP.



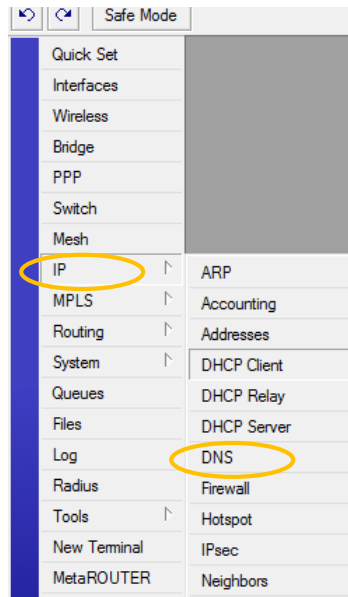
**Figura 140. Creación del cliente DHCP**

Una vez que se crea un nuevo cliente DHCP es preciso determinar cuál interface va a recibir una dirección IP automáticamente, para este caso en concreto será la interface wlan1.



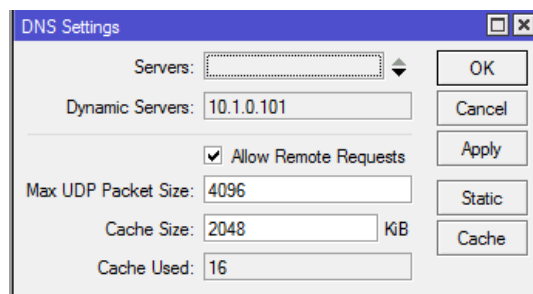
**Figura 141. Elección de la interface DHCP Client**

Para poder tener un correcto acceso hacia internet, es necesario activar el protocolo DNS (Domain Name System), el cual permite traducir la dirección IP de un sitio web en un nombre de dominio. Para poner en funcionamiento este protocolo, en Winbox, se escoge la opción *IP* y después *DNS*.



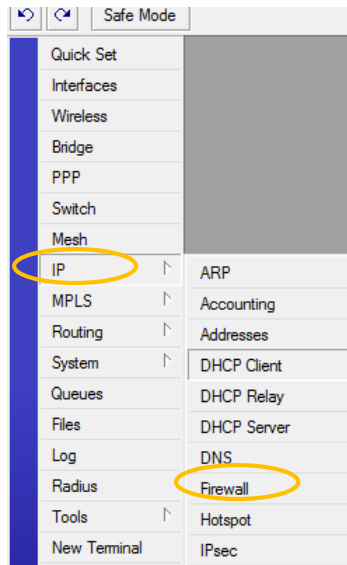
**Figura 142. Sección DNS**

Una vez que se ha ingresado en el apartado DNS, se debe activar la opción *Allow Remote Request* (permitir solicitud remota) con lo que permite hacer una réplica del servidor DNS hacia los equipos de usuario final que se encuentran dentro de la LAN.



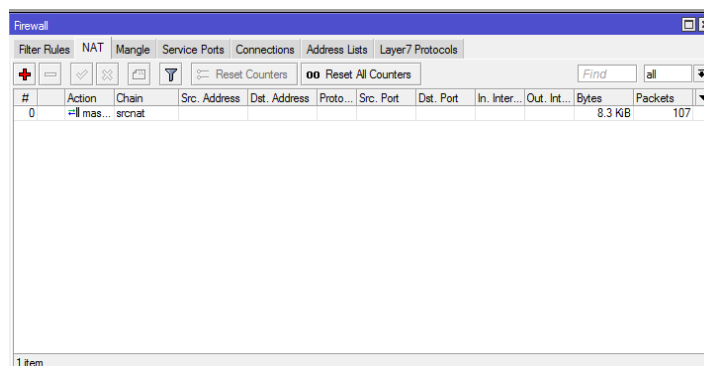
**Figura 143. Activación del servicio DNS**

Los equipos de una red LAN están configurados con direcciones IP privadas, mientras que dentro del internet el direccionamiento IP es público; por esta razón se necesita utilizar *NAT* (Network Address Translation), esta técnica permite traducir las dirección IP privadas hacia una dirección IP pública. Para activar NAT en RouterOS se escoge la opción *IP* y después *Firewall* (Contrafuegos).



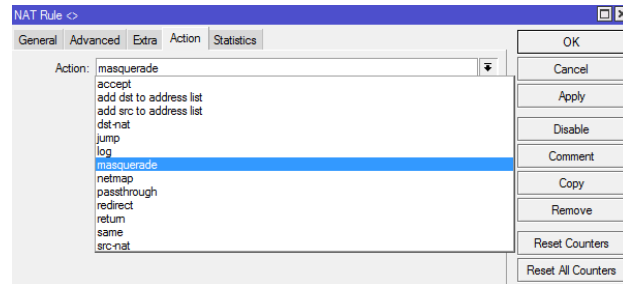
**Figura 144. Sección Firewall**

Dentro de la opción Firewall se escoge la pestaña *NAT* y por medio de la opción *Add (+)*, se crea una nueva regla de NAT.



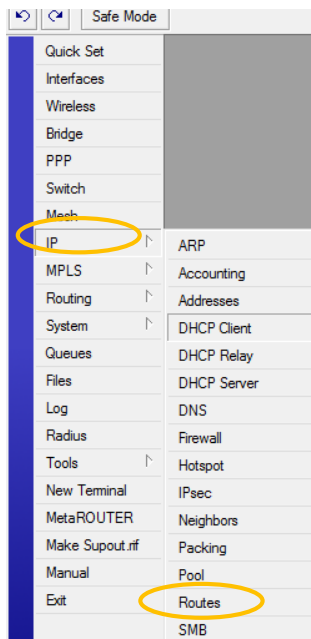
**Figura 145. Crear una nueva regla NAT**

Dentro de la regla de *NAT* se escoge la pestaña *Action* (acción) y a continuación *masquerade* (enmascaramiento). Esta opción permitirá enmascarar todas las direcciones IP privadas de la red LAN en una sola dirección IP pública que fue asignada a la interface wlan1 por medio del protocolo DHCP.



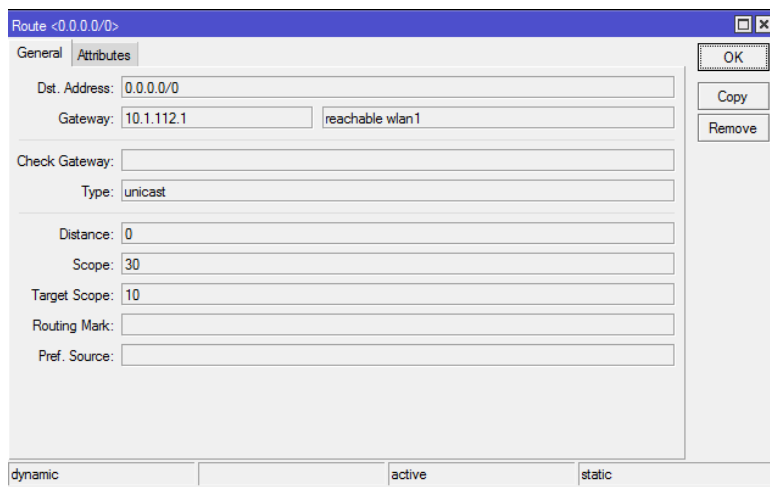
**Figura 146. Enmascaramiento de direcciones IP**

Para finalizar la configuración del router Mikrotik RB751U se debe crear una ruta estática por defecto, la cual permitirá enrutar los paquetes desde y hacia los equipos que se encuentran dentro de la red LAN, para lo cual se escoge *IP* y luego *Routes* (rutas).



**Figura 147. Sección Routes**

En la lista de rutas se crea una nueva ruta por medio de *Add (+)*, donde se configura la ruta por defecto (0.0.0.0) y la dirección del siguiente salto o a su vez la interface de salida del router.

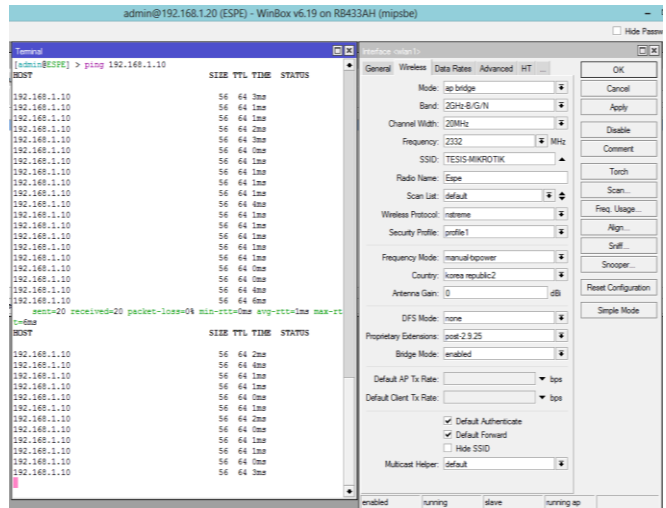


**Figura 148. Creación de una ruta por defecto**

## **4.7 Obtención de los parámetros del enlace inalámbrico para el estudio comparativo**

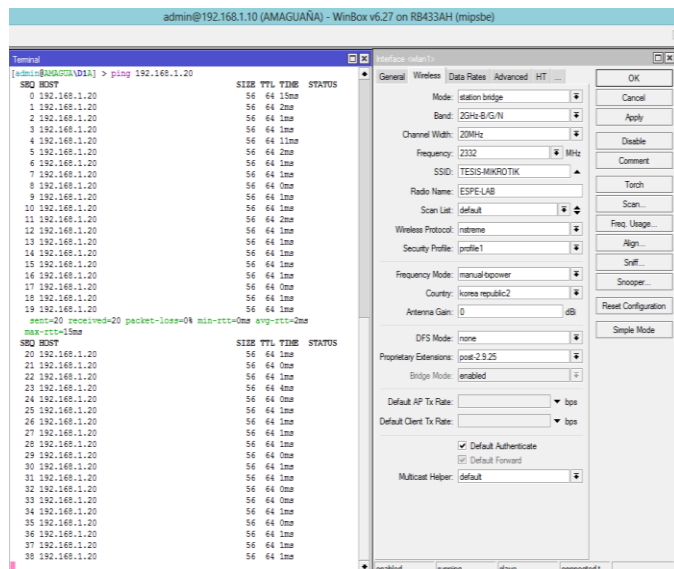
### **4.7.1 Pruebas de conectividad por medio del comando ping en la frecuencia de 2.4GHz con el protocolo Nstreme**

En la figura 149 se puede apreciar la prueba de conectividad realizada por medio del comando ping en el enlace a 2.4GHz utilizando el protocolo Nstreme, entre el router Mikrotik RB433AH ubicado en la estación ESPE con dirección IP 192.168.1.20 y el ubicado en la estación AMAGUAÑA con dirección IP 192.168.1.10; este comando además de confirmar la conectividad, también permite observar los tiempos de propagación de los paquetes.



**Figura 149. Ping desde ESPE hasta AMAGUAÑA a 2.4GHz con Nstreme**

Por medio del comando ping, el cual fue ejecutado desde el equipo Mikrotik RB433 ubicado en la estación AMAGUAÑA con dirección IP 192.168.1.10 se puede comprobar la conectividad con el equipo ubicado en la estación ESPE con dirección IP 192.168.1.20, en el enlace a 2.4GHZ utilizando el protocolo Nstreme; el comando ping utiliza el protocolo de la capa de red ICMP (Internet Control Message Protocol)

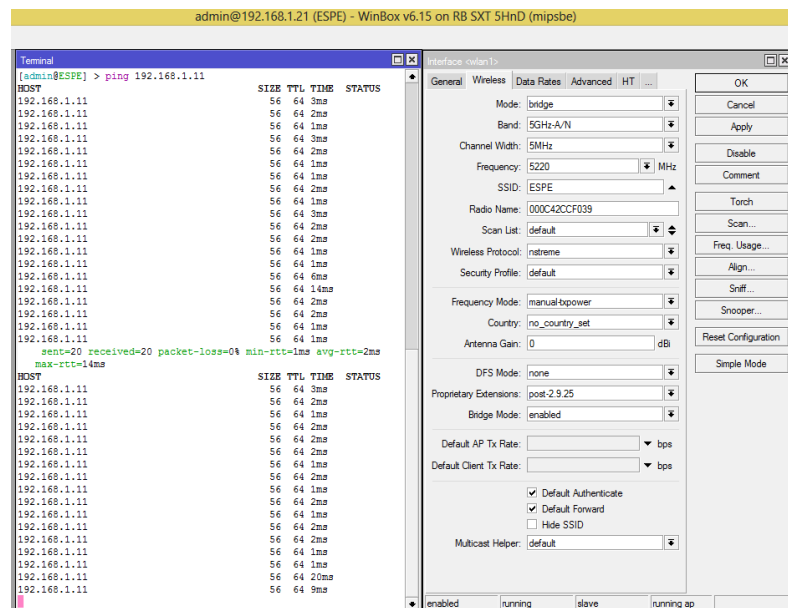


**Figura 150. Ping desde AMAGUAÑA hasta ESPE a 2.4GHz con Nstreme**



#### 4.7.2 Prueba de conectividad por medio del comando ping en la frecuencia de 5.8GHz con el protocolo Nstreme

El comando ping permite comprobar la conectividad entre dos dispositivos de red, por lo que se ha ejecutado este comando en el terminal de Winbox del equipo SXT5HnD ubicado en la estación ESPE con dirección IP 192.168.1.21 hacia el dispositivo ubicado en AMAGUAÑA el cual posee la dirección IP 192.168.1.11; de esta manera se confirma que el enlace a 5.8GHz usando el protocolo Nstreme está funcionando correctamente.



**Figura 151. Ping desde ESPE hasta AMAGUAÑA a 5.8GHz con Nstreme**

Para comprobar la conectividad del enlace de 5.8GHz con el protocolo Nstreme se ha ejecutado el comando ping entre el equipo Mikrotik SXT5HnD de la estación AMAGUAÑA que tiene configurado la dirección IP 192.168.1.11 y el ubicado en la estación ESPE con dirección IP 192.168.1.21.

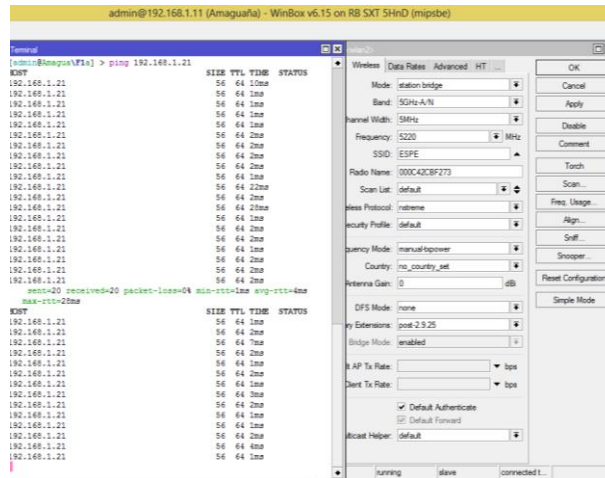


Figura 152. Ping desde AMAGUAÑA hasta ESPE a 5.8GHz con Nstreme

#### 4.7.3 Prueba de conectividad por medio del comando ping en la frecuencia de 2.4GHz con el protocolo Nv2

Se ha ejecutado el comando ping desde el equipo con dirección IP 192.168.1.20, el cual está ubicado en la estación ESPE hacia la dirección 192.168.1.10, que es la dirección del dispositivo RB433AH que se encuentra en la estación AMAGUAÑA; de esta manera se puede comprobar la conectividad del enlace a 2.4GHz con el protocolo Nv2

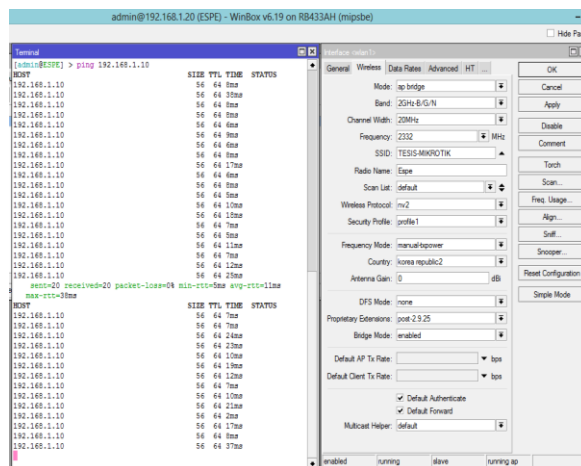
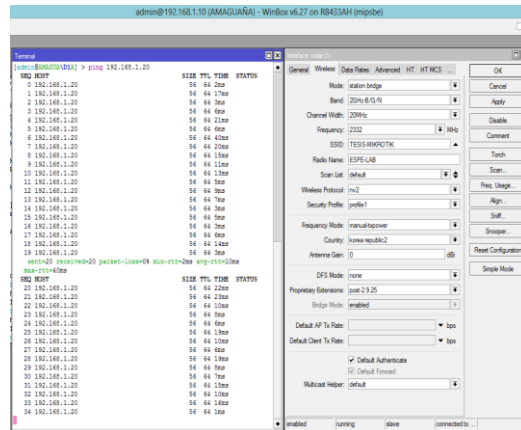


Figura 153. Ping desde ESPE hasta AMAGUAÑA a 2.4GHz con Nv2

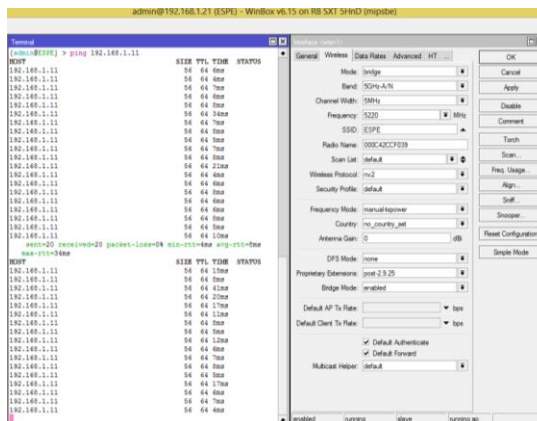
En la figura 154 se puede apreciar que efectivamente existe conectividad en el enlace a 2.4GHz con el protocolo Nv2 entre el dispositivo AMAGUAÑA con direccionamiento IP 192.168.1.10 y el dispositivo ESPE con dirección IP 192.168.1.20



**Figura 154. Ping desde AMAGUAÑA hasta ESPE a 2.4GHz con Nv2**

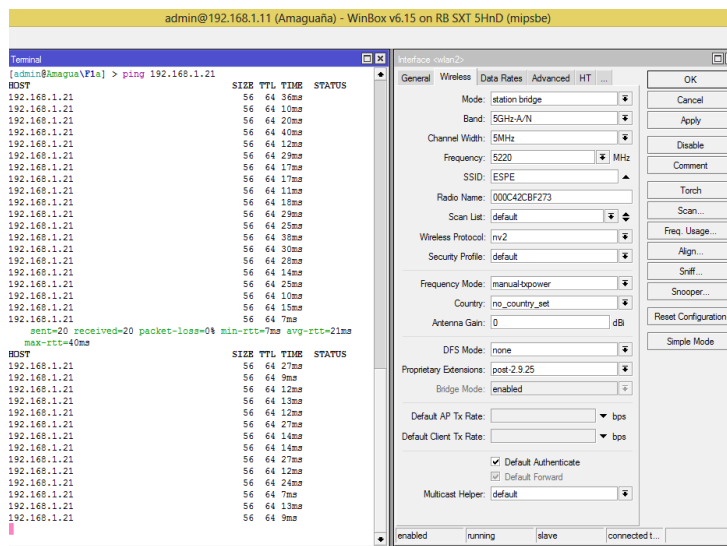
#### 4.7.4 Prueba de conectividad por medio del comando ping en la frecuencia de 5.8GHz con el protocolo Nv2

Con el comando ping hacia el equipo AMAGUAÑA con dirección IP 192.168.1.11, desde el dispositivo ESPE con dirección IP 192.168.1.21 se comprueba la conectividad y funcionamiento del enlace inalámbrico a 5.8GHz con el protocolo Nv2.



**Figura 155. Ping desde ESPE hasta AMAGUAÑA A 5.8GHz con Nv2**

En la figura 156 se puede observar el ping realizado entre el dispositivo AMAGUAÑA con dirección IP 192.168.1.11 hacia el dispositivo Mikrotik SXT5HnD ubicado en la estación ESPE con dirección IP 192.168.1.21, con lo que se verifica que el enlace en la banda de 5.8GHZ y con el protocolo Nv2 está en pleno funcionamiento.

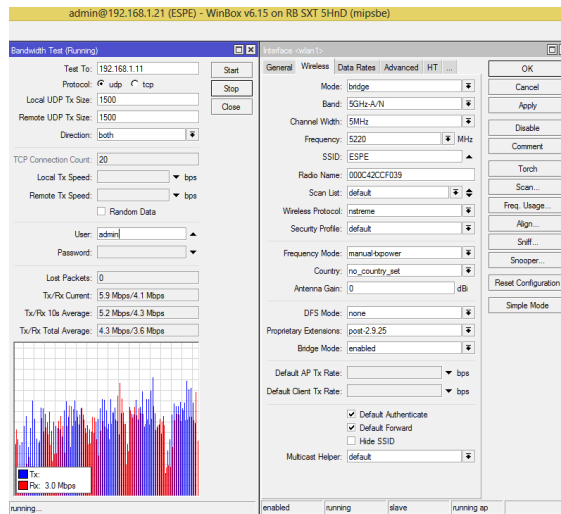


**Figura 156. Ping desde AMAGUAÑA hasta ESPE A 5.8GHz con Nv2**

#### **4.7.5 Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 2.4GHz con el protocolo Nstreme**

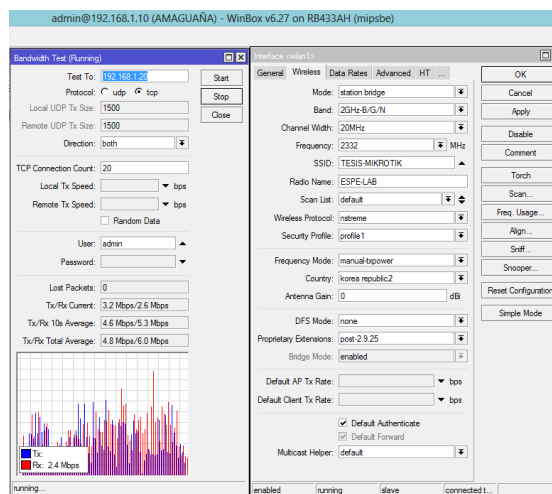
Bandwidth Test o Btest es una herramienta embebida en el sistema operativo RouterOS de Mikrotik, la cual permite realizar pruebas de ancho de banda de transmisión, recepción o en ambos sentidos, en enlaces inalámbricos punto a punto. Btest inunda con paquetes TCP o UDP el enlace inalámbrico hasta su mayor capacidad mostrando de esta manera valores de ancho de banda promedio durante un determinado tiempo; además genera un gráfico que muestra los anchos de banda obtenidos en el tiempo.

En la figura 157 se puede apreciar la prueba de ancho de banda realizada con Btest en el enlace a 2.4GHz utilizando el protocolo Nstreme desde el equipo 192.168.1.20 ubicado en la estación ESPE hacia el dispositivo 192.168.1.10 en el sector de AMAGUAÑA.



**Figura 157. Prueba con Btest desde ESPE hasta AMAGUAÑA a 2.4GHz con Nstreme**

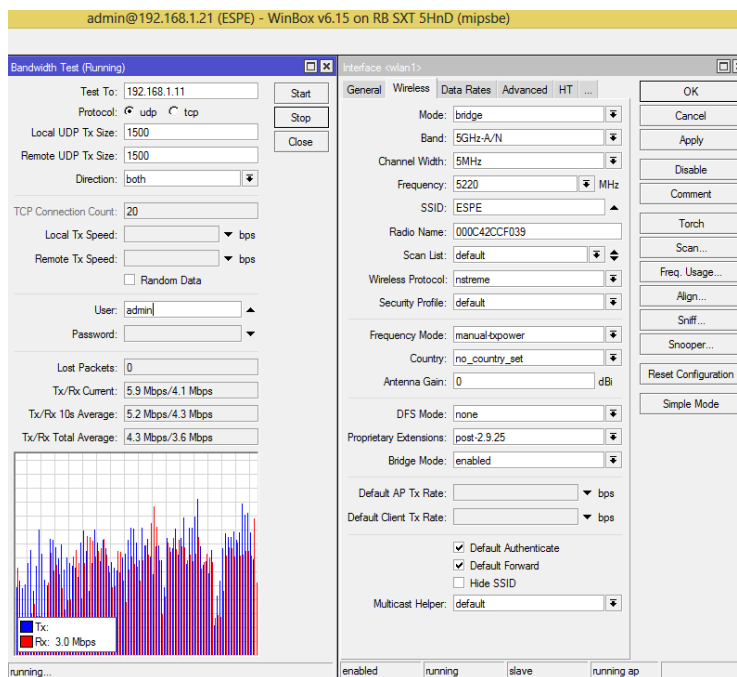
Por medio de una prueba de Bandwidth Test hacia el dispositivo ubicado en la Universidad de las Fuerzas Armadas “ESPE” con dirección IP 192.168.1.20 desde la estación AMAGUAÑA con IP 192.168.1.10, se puede observar que existe conectividad inalámbrica entre los dos puntos por medio del enlace Nstreme a 2.4GHz; la prueba fue hecha en ambas direcciones, transmisión y recepción.



**Figura 158. Prueba con Btest desde AMAGUAÑA hasta ESPE a 2.4GHz con Nstreme**

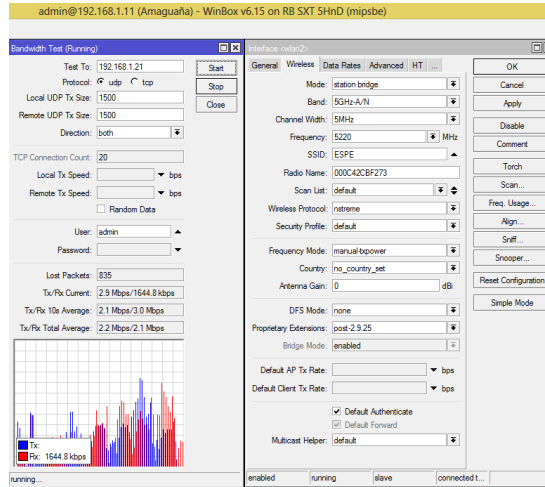
#### 4.7.6 Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 5.8GHz con el protocolo Nstreme

Con la herramienta Btest de Mikrotik se realizó pruebas de ancho de banda en el enlace a 5.8GHz con el protocolo Nstreme entre el equipo identificado con la dirección IP 192.168.1.21 que se encuentra en la estación ESPE, hacia el router Mikrotik 192.168.1.11 de la estación AMAGUAÑA.



**Figura 159. Prueba con Btest desde ESPE hasta AMAGUAÑA a 5.8GHz con Nstreme**

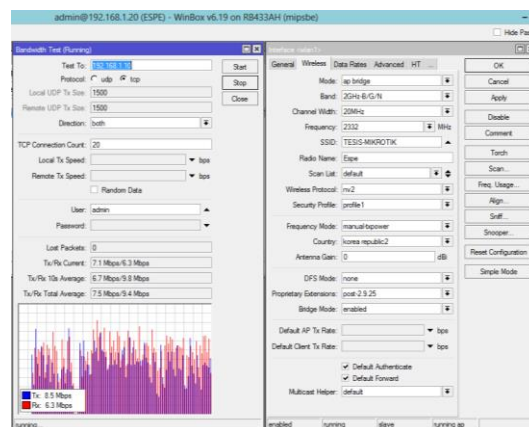
Observando la figura 160 se puede apreciar la prueba de ancho de banda por medio de Bandwidth Test realizada en el enlace Nstreme a 5.8GHz desde el router inalámbrico con dirección IP 192.168.1.11 ubicado en la estación AMAGUAÑA hacia el ubicado en el repetidor ESPE, el cual posee la dirección IP 192.168.1.21



**Figura 160. Prueba con Btest desde AMAGUAÑA hasta ESPE a 5.8GHz con Nstreme**

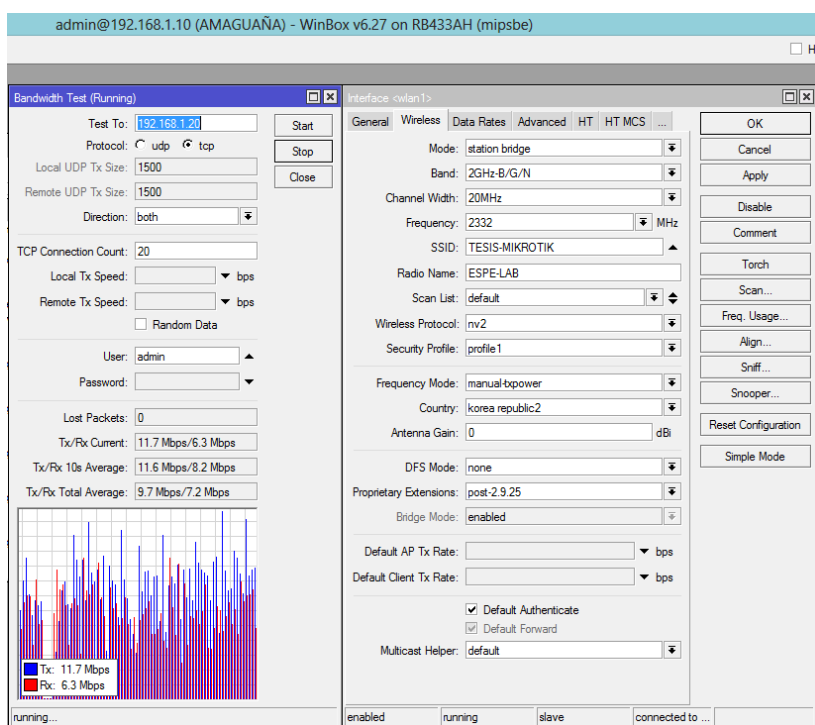
#### 4.7.7 Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 2.4GHz con el protocolo Nv2

En la figura 161 se aprecia la prueba de ancho de banda realizada en el enlace Nv2 a 2.4GHz entre el equipo que se encuentra en la estación ESPE, el cual tiene la dirección IP 192.168.1.10 hacia el dispositivo con IP 192.168.1.20 del sector AMAGUAÑA. Se puede apreciar que para esta prueba se utiliza paquetes TCP.



**Figura 161. Prueba con Btest desde ESPE hasta AMAGUAÑA a 2.4GHz con Nv2**

A través de la prueba de ancho de banda con la herramienta Btest se puede obtener valores de la capacidad de recepción y transmisión que tiene el enlace inalámbrico a 2.4GHz utilizando el protocolo Nv2. Esta prueba se realizó desde el router Mikrotik RB433AH ubicado en AMAGUAÑA con dirección IP 192.168.1.10 hasta el que se encuentra en la estación ESPE, el cual posee la dirección IP 192.168.1.20. Se puede observar valores promedios de ancho de banda, total o cada 10 segundos; estos valores varían dependiendo de factores externos como lluvia, viento, etc.



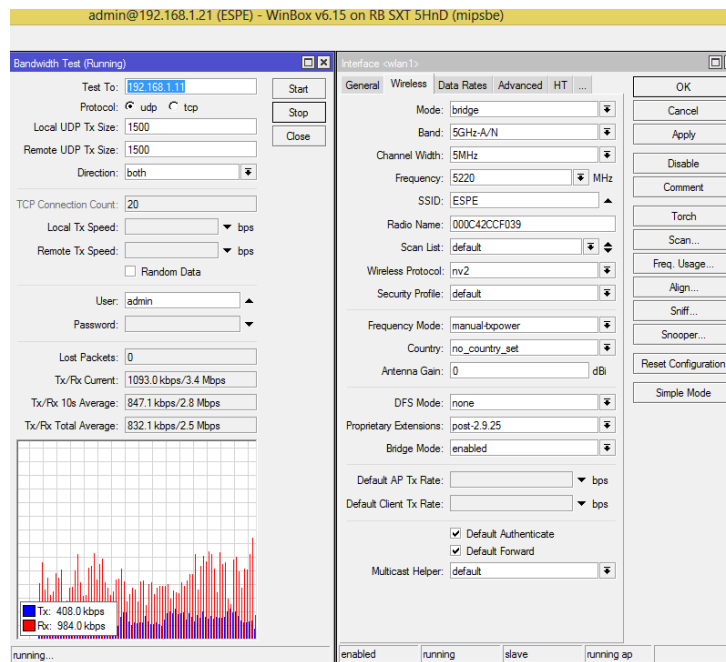
**Figura 162. Prueba con Btest desde AMAGUAÑA hasta ESPE a 2.4GHz con Nv2**

#### **4.7.8 Pruebas de comunicación y de ancho de banda utilizando la herramienta propietaria de Mikrotik Btest a 5.8GHz con el protocolo Nv2.**

Por medio de Btest se realizó una prueba de ancho de banda en el enlace inalámbrico a 5.8GHz, el cual utiliza el protocolo Nv2, entre el router inalámbrico SXT 5HnD que se encuentra instalado en la estación ESPE con dirección IP 192.168.1.21 hacia un dispositivo de las mismas características ubicado en la estación AMAGUAÑA

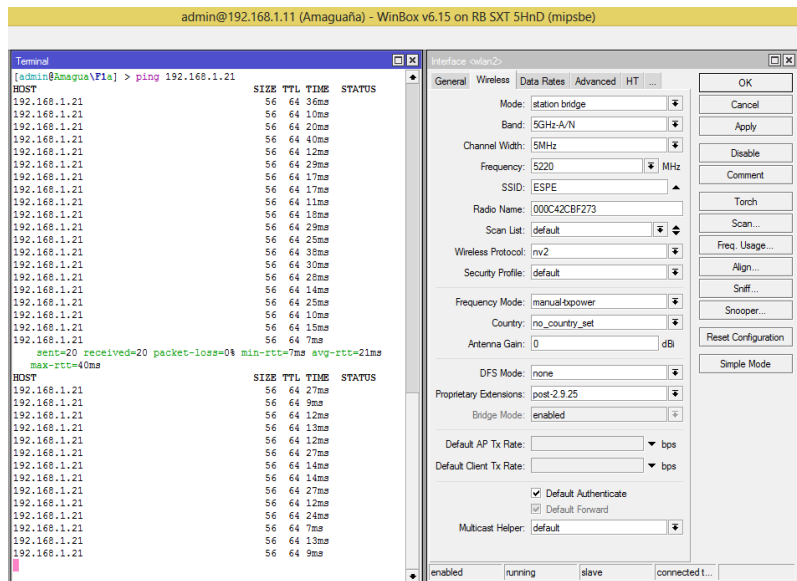


identificado con la dirección IP 192.168.1.11. Se debe tomar en cuenta que para hacer una prueba con Btest es necesario configurar el nombre del usuario del dispositivo con el que se desea conectarse.



**Figura 163. Prueba con Btest desde ESPE hasta AMAGUAÑA a 5.8GHz con Nv2**

Bandwidth Test es la herramienta de Mikrotik con la que se realizó las pruebas de conectividad y ancho de banda entre el dispositivo con IP 192.168.1.11 hacia el dispositivo 192.168.1.21. Estos dispositivos están ubicados en las estaciones AMAGUAÑA y ESPE, respectivamente; y se encuentran trabando en la banda de 5.8GHz con el protocolo Nv2. Btest reproduce un gráfico en tiempo real de la cantidad de paquetes que circulan en el enlace; los datos de color azul identifican la tasa de transmisión, mientras que los de color rojo a la de recepción.



**Figura 164. Prueba con Btest desde AMAGUAÑA hasta ESPE a 5.8GHz con Nv2**

#### 4.7.9 Obtención de datos por medio de la tabla *Registration*

A través de la tabla *Registration* (registro) se pudo obtener algunos parámetros para el estudio comparativo entre los protocolos Nstreme y Nv2. Estos parámetros son los siguientes:

- Tx/Rx Signal Strength: Este parámetro se refiere a la potencia promedio que recibe el cliente desde el AP. Este parámetro se lo mide en dBm (decibelio-milivatio)
- Signal to Noise: Se refiere a la señal de ruido existente en el enlace. Se lo mide en db (decibelio)
- Tx/Rx CCQ: El CCQ se refiere a la calidad de conexión del enlace. CCQ es el promedio de los valores de  $T_{min}/T_{real}$ , que se calcula para cada trama de transmisión, donde  $T_{min}$  es el tiempo que se tardaría en transmitir la trama con la tasa (rate) más alta sin reintentos y  $T_{real}$  es el tiempo que se tardó en transmitir la trama en la realidad.
- Tx/Rx Rate: Es la tasa de transferencia y recepción teórica del enlace inalámbrico. Se lo mide en Mbps (megabits por segundo)

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Signal To Noise (...)	Tx/Rx CCQ (%)	Tx/Rx Rate
000C42CBF273	00:0C:42:CB:F2:73	wlan1	00:15:38	no	no	0.000	-62/-75	37	67/72	14.6Mbps/16.2Mbps

**Figura 165. Tabla Registration**

#### 4.7.10 Elección de las frecuencias menos saturadas a través de la herramienta *Frequency Usage*

La herramienta *Frequency Usage* (uso de frecuencia) realiza un escaneo de todas las frecuencias que se encuentran disponibles. A través de esta herramienta se puede observar las frecuencias menos saturadas, las cuales fueron escogidas para la realización de este proyecto.

Frequency (MHz)	Usage	Noise F.
2362	0.0	-116
2367	0.0	-116
2372	0.0	-97
2412	12.1	-112
2417	5.4	-114
2422	11.0	-112
2427	7.8	-113
2432	3.0	-113
2437	4.0	-114
2442	4.8	-108
2447	4.6	-112
2452	11.0	-111
2457	1.9	-110
2462	5.3	-108
2467	2.1	-111
2472	0.0	-97

Frequency (MHz)	Usage	Noise F.
4920	14.6	-122
4940	38.3	-122
4960	12.4	-121
4980	17.6	-121
5040	30.5	-120
5060	7.5	-119
5080	5.0	-118
5170	0.3	-117
5190	0.0	-117
5210	0.0	-117
5230	0.1	-116

**Figura 166. Frequency Usage para los enlaces a 2.4GHz y 5.8GHz**

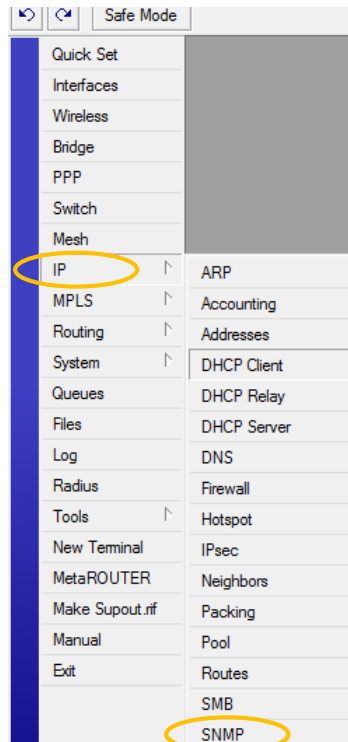
## 4.8 Activación del protocolo SNMP en equipos Mikrotik, Windows y Centos 7

SNMP (Simple Network Management Protocol) es un protocolo de la capa de aplicación del modelo de referencia OSI que permite el intercambio de información de administración entre dispositivos que se encuentren conectados a la red. Generalmente los

dispositivos que soportan SNMP son routers, switches, servidores, impresoras, estaciones de trabajo, etc.

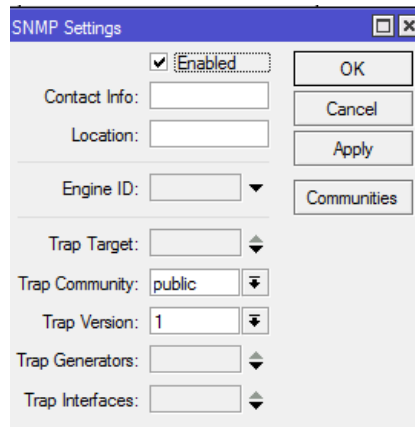
SNMP permite a los administradores de red detectar y resolver problemas dentro de la red. El dispositivo que contrala y administra la red por medio de SNMP se lo conoce como Gerente, mientras que los equipos que envían información al gerente a través de SNMP se los conoce como agentes.

Para activar el protocolo SNMP en un equipo Mikrotik se lo hace por medio de Winbox, en el menú principal, se debe seleccionar la opción *IP* y a continuación *SNMP*.



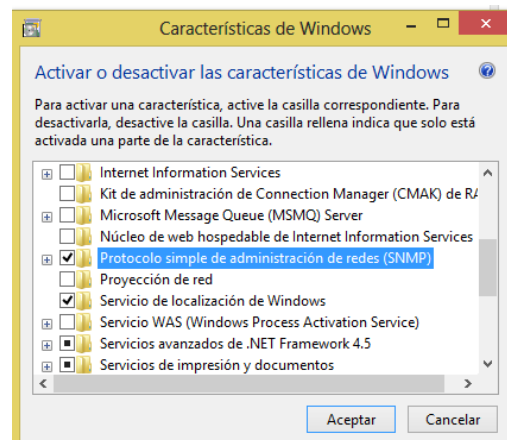
**Figura 167. Menú Principal**

Dentro de la ventana *SNMP Settings* se procede a habilitar la opción *enable*, el nombre de la comunidad va a ser *public*, y la versión del protocolo va a ser la primera. Se utiliza una comunidad pública porque la gestión se lo realizará solo dentro de la LAN.



**Figura 168. Habilitación SNMP en RouterOS**

Para activar el protocolo SNMP en equipos con sistema operativo Windows se debe dirigirse hacia el *Panel de Control* y escoger la opción *Programas*, a continuación el apartado *Activar o desactivar las características de Windows* y una vez allí se activa el *Protocolo simple de administración de redes (SNMP)*.



**Figura 169. Habilitación SNMP en Windows**

Para activar en dispositivo con sistema operativo Centos 7 el protocolo SNMP se debe ingresar como súper usuario al terminal e instalar los paquetes *net-snmp* y *net-snmp-utils*.

```
[tesis@localhost ~]$ su root
Contraseña:
[root@localhost tesis]# yum install -y net-snmp net-snmp-utils
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: centos.brisanet.com.br
* extras: centos.brisanet.com.br
* updates: centos.brisanet.com.br
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete net-snmp.x86_64 1:5.7.2-20.el7_1.1 debe ser instalado
--> Procesando dependencias: net-snmp-libs = 1:5.7.2-20.el7_1.1 para el paquete:
1:net-snmp-5.7.2-20.el7_1.1.x86_64
--> Procesando dependencias: net-snmp-agent-libs = 1:5.7.2-20.el7_1.1 para el pa
quete: 1:net-snmp-5.7.2-20.el7_1.1.x86_64
--> Procesando dependencias: perl(Data::Dumper) para el paquete: 1:net-snmp-5.7.
2-20.el7_1.1.x86_64
--> Procesando dependencias: libnetsnmptrapd.so.31()(64bit) para el paquete: 1:n
et-snmp-5.7.2-20.el7_1.1.x86_64
--> Procesando dependencias: libnetsnmpmibs.so.31()(64bit) para el paquete: 1:ne
t-snmp-5.7.2-20.el7_1.1.x86_64
--> Procesando dependencias: libnetsnmpagent.so.31()(64bit) para el paquete: 1:n
et-snmp-5.7.2-20.el7_1.1.x86_64
--> Paquete net-snmp-utils.x86_64 1:5.7.2-20.el7_1.1 debe ser instalado
--> Ejecutando prueba de transacción
--> Paquete net-snmp-agent-libs.x86_64 1:5.7.2-20.el7_1.1 debe ser instalado
--> Paquete net-snmp-libs.x86_64 1:5.7.2-20.el7 debe ser actualizado
--> Paquete net-snmp-libs.x86_64 1:5.7.2-20.el7_1.1 debe ser una actualización
```

**Figura 170. Habilitación SNMP en Centos 7**

Después de que se han instalado los paquetes necesarios para el correcto funcionamiento del protocolo SNMP se procede a arrancar el servicio.

```
[root@localhost tesis]# systemctl start snmpd
```

#### 4.9 Gestión de la red por medio de la herramienta The Dude

The Dude es una herramienta de monitoreo y gestión desarrollada por Mikrotik; permite escanear automáticamente todos los dispositivos especificados en una subred, dibuja y etiqueta el mapa de red, supervisa los servicios que corren sobre la red y alerta en caso de que exista algún tipo de problema. Las características The Dude son:

- El sistema de monitoreo The Dude es gratuito
- Descubre cualquier dispositivo independientemente de la marca
- Soporta SNMP, ICMP, DNS y TCP
- Se ejecuta en entornos Linux, MacOS y Windows
- Acceso directo a herramientas de control remoto para la gestión de dispositivos

Para descubrir los dispositivos de la red de manera automática en el menú principal

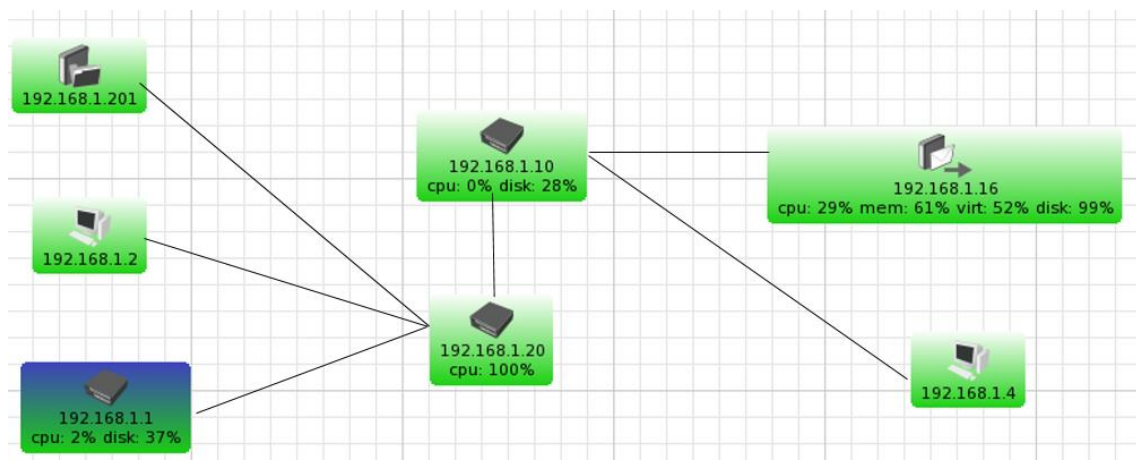
de The Dude se escoge la opción *Discovery*; aparecerá una ventana en donde se escribe la dirección de red a escanear; opcionalmente se puede configurar los protocolos por los cuales va a escanear como DNS, SNMP, IP y NETBIOS.



**Figura 171. Descubrimiento de dispositivos con The Dude**

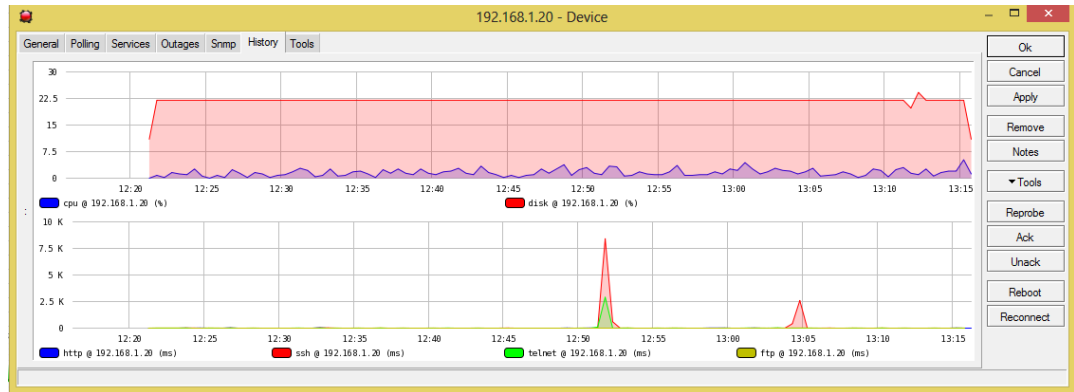
#### 4.9.1 Gestión en el enlace de 2.4GHZ con The Dude

En la figura 172 se puede apreciar la topología completa del enlace de 2.4GHz, en donde se puede verificar el funcionamiento de los dos routers Mikrotik RB433AH que se están utilizando para realizar el enlace inalámbrico a 2.4GHz; estos están identificados con las direcciones IP 192.168.1.10 y 192.168.1.20, respectivamente.

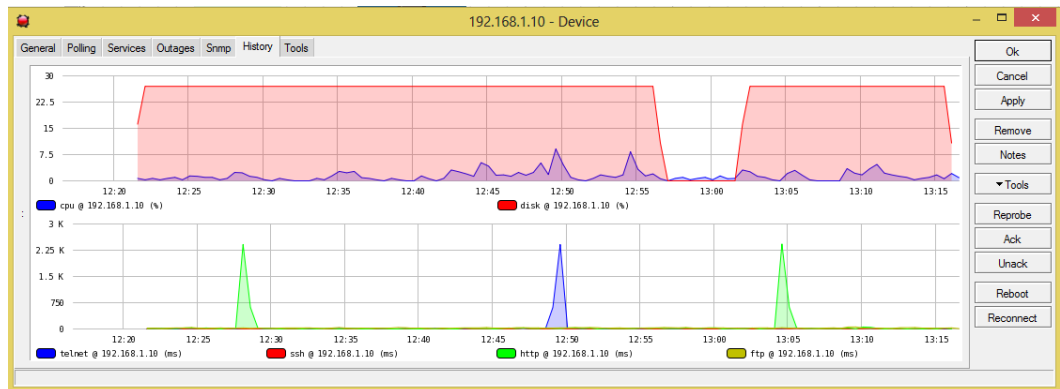


**Figura 172. Topología del enlace a 2.4GHz con The Dude**

The Dude genera graficas del comportamiento de cada uno de los dispositivos que se encuentran en la red, estas graficas permiten observar los servicios que están consumiendo recursos de la red. En las figuras 173 y 174 se muestra el comportamiento los router RB433AH que se utilizaron en el enlace de 2.4GHz en un periodo de una hora diaria durante 5 días consecutivos.



**Figura 173. Comportamiento del router ESPE**



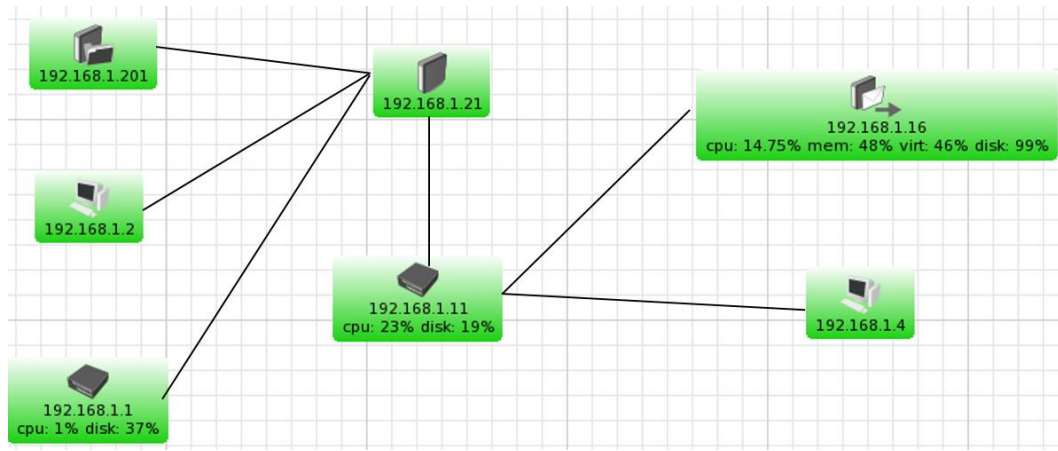
**Figura 174. Comportamiento del router AMAGUAÑA**

#### 4.9.2 Gestión en el enlace de 5.8GHZ con The Dude

En la figura 175 se observa el mapa de red del enlace inalámbrico a 5.8GHz obtenido por descubriendo automático con la herramienta The Dude, se puede apreciar que se encuentran conectados todos los servidores al router inalámbrico con dirección IP

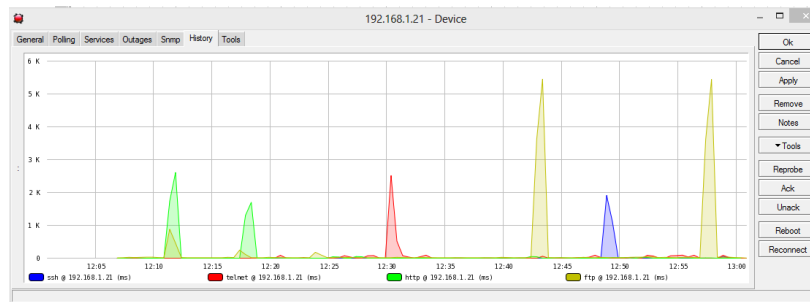


192.168.1.21, y que los clientes están en el lado del equipo 192.168.1.11

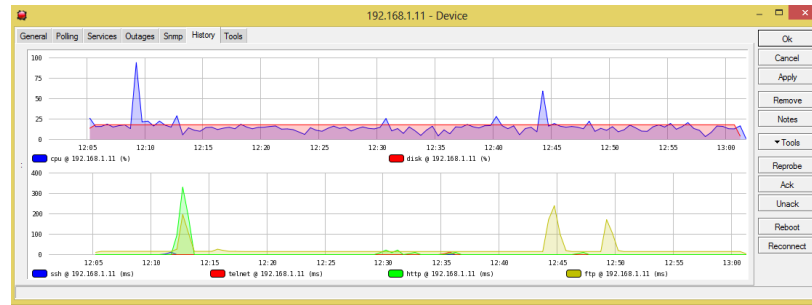


**Figura 175. Topología de red del enlace a 5.8GHz con The Dude**

En las siguientes dos figuras se puede apreciar la prueba de comportamiento realizada durante una hora diaria durante 5 días consecutivos de los dispositivos inalámbrico SXT 5HnD los cuales fueron utilizados para la implementación del enlace de 5.8GHz



**Figura 176. Comportamiento del router ESPE A 5.8GHz**




**Figura 177. Comportamiento del router AMAGUAÑA A 5.8GHz**

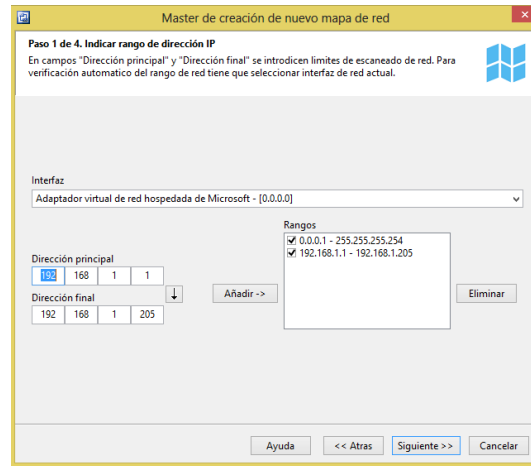
#### 4.10 Gestión de la red por medio de la herramienta LANState PRO

LANState es un software para el monitoreo y administración de redes desarrollado por 10-Strike Software, esta herramienta posee dos versiones: LANState Standard y LANState PRO.

LANState Standard permite un monitoreo básico y administración de dispositivos de manera remota, es recomendado para redes TCP/IP con equipos Windows, soporta un máximo de 50 hosts de manera simultánea.

La versión LANState PRO es la versión más avanzada, permite el acceso remoto por medio de un servidor Web, provee funcionalidades avanzadas de SNMP, soporte para Syslog, posee una licencia para el monitoreo de 100 hosts simultáneamente por lo que se recomienda el uso para red corporativas.

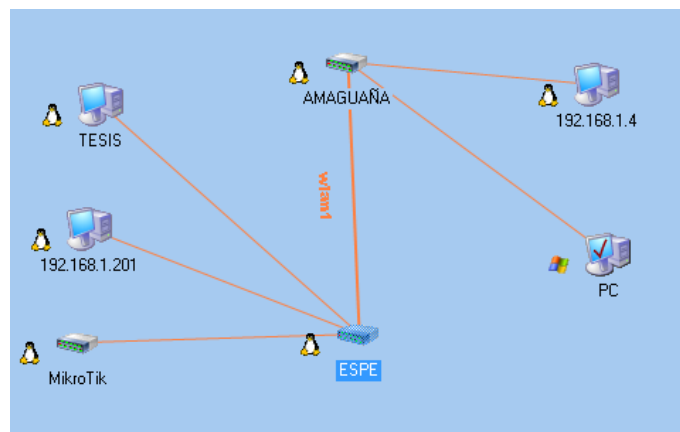
Para realizar el monitoreo de una red con LANState PRO se escoge la opción *Master de creación del mapa de página* la cual está identificada con el símbolo  , a continuación se ingresa el rango de direcciones IP que se desea monitorear y automáticamente comenzaran a aparecer los elementos descubiertos.



**Figura 178. Descubrimiento de dispositivos con LANState PRO**

#### 4.10.1 Gestión en el enlace de 2.4GHZ con LANState PRO

La figura 179 permite apreciar los dispositivos descubiertos del enlace a 2.4GHz en donde se destaca los routers RB433AH que se encuentran denominados como ESPE y AMAGUAÑA. LANState permite además apreciar que sistema operativo está corriendo en cada uno de los equipos.



**Figura 179. Topología de red a 2.4GHz con LANState PRO**

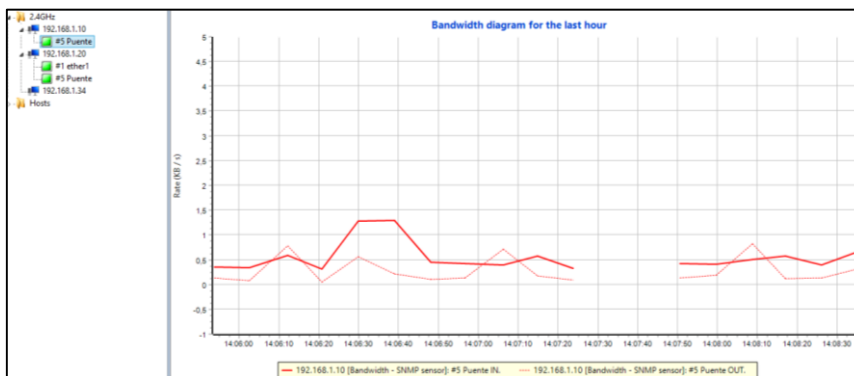
LANState genera una lista de todos los dispositivos, en ella se muestra las direcciones IP de cada uno de los equipos de la red, su nombre y el estado de conexión;

en la figura 180 se puede apreciar que todos los dispositivos se encuentran funcionando y conectados correctamente.

Nombre y direcció...	Nombre en m...	Nombre de m...	Tipo de verificación	Estado	Estatus	Tie...	Val...	Ultimo mensaje	Tiempo de u...	Tier
192.168.1.1	MikroTik	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.2	TESIS	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.4	192.168.1.4	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.10	AMAGUAÑA	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	3 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.16	PC	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.20	ESPE	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/
192.168.1.201	192.168.1.201	Untitled1.lsm	ICMP-ping	Encendido	Se termino...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 2...	23/

**Figura 180. Lista de dispositivos a 2.4GHz**

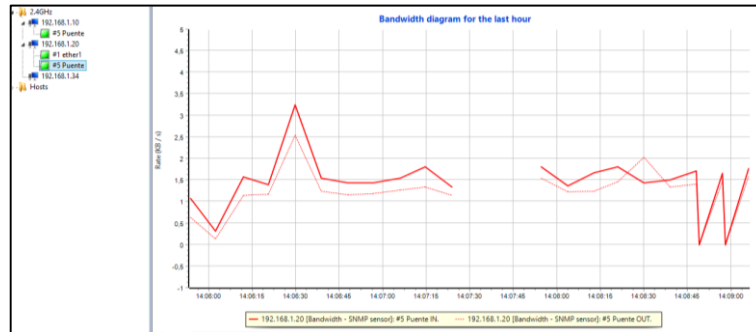
La herramienta 10-Strike Bandwidth Monitor, permite realizar el monitoreo de la tasa de transferencia en las interfaces de los dispositivos durante una hora, a continuación se muestra la grafica que fue generada por el dispositivo 192.168.1.10 que se encuentra ubicado en la estacion AMAGUAÑA, este monitoreo fue hecho en la interface Puente, la cual es un bridge entre la interface wlan1 y la ether1. Esta prueba fue realizada durante un periodo de 5 dias.



**Figura 181. Ancho de banda del router AMAGUAÑA a 2.4GHz**

La figura 182 permite observar el monitoreo de la tasa de transferencia realizado en la interface puente (bridge) del dispositivo ESPE que posee la dirección IP

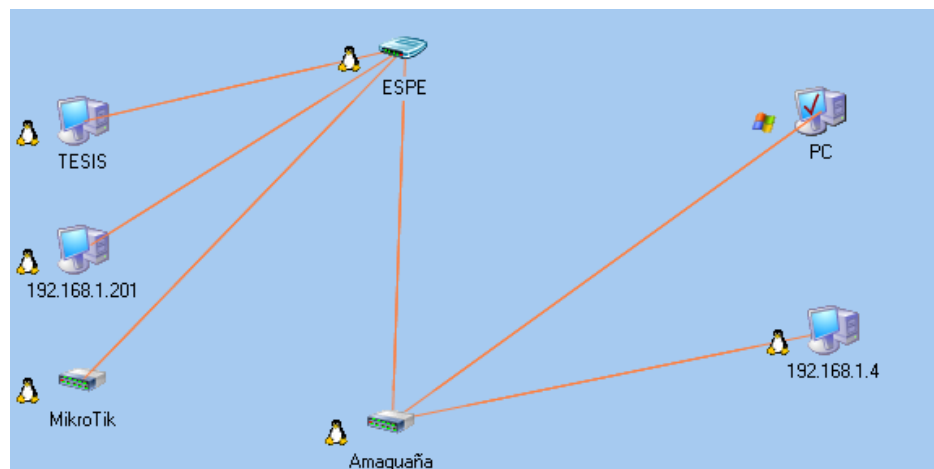
192.168.1.20; esta grafica permite apreciar la tasa de transferencia que ha estado circulando en el enlace inalámbrico. La prueba fue realizada durante una hora diaria en un lapso de 5 días.



**Figura 182. Ancho de banda del router ESPE a 2.4GHz**

#### 4.10.2 Gestión en el enlace de 5.8GHZ con LANState PRO

Por medio el software de administración de redes LANState PRO se puede realizar el descubrimiento de la red que utiliza el enlace inalámbrico de 5.8GHz, en donde se puede apreciar cada uno de los dispositivos utilizados. Los dispositivos inalámbricos SXT 5HnD utilizados para la implementación del enlace se encuentran identificados en la topología como ESPE y AMAGUAÑA.



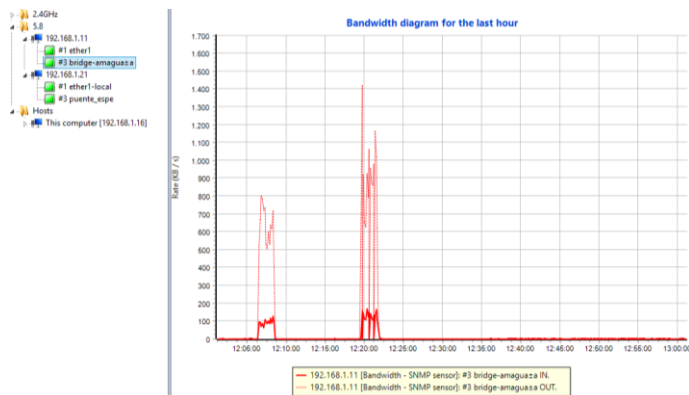
**Figura 183. Topología de red a 5.8GHz con LANState PRO**

En la figura 184 se aprecia el listado de los dispositivos descubiertos que se utilizaron para la implementación del enlace a 5.8GHz, se puede identificar a los dispositivos por medio de la dirección IP o por el nombre, y parámetros como el estado, estatus, tiempo de conexión, etc.

Nombre y direcció...	Nombre en m...	Nombre de m...	Tipo de verificación	Estado	Estatus	Tie...	Val...	Ultimo mensaje	Tiempo de u...	Tier
> 192.168.1.1	MikroTik	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.2	TESIS	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.4	192.168.1.4	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.11	Amaguaña	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.16	PC	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	0 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.21	ESPE	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/
> 192.168.1.201	192.168.1.201	Untitled1.lsm	ICMP-ping	Encendido	Se termino ...	1 ms	-	ICMP-Pingrespuesta re...	23/10/2015 1...	23/

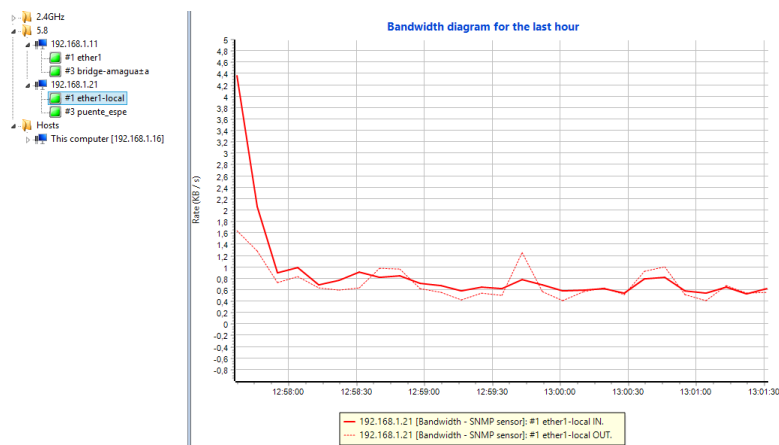
**Figura 184. Lista de dispositivos a 5.8GHz**

A través de la herramienta 10-Strike Bandwidth Monitor se puede obtener mediciones del ancho de banda circulante en el enlace inalámbrico. En la figura 185 se aprecia el monitoreo, en la interface puente (bridge), de la tasa de transferencia que el dispositivo 192.168.1.21 ha estado transmitiendo durante la última hora.



**Figura 185. Ancho de banda del router AMAGUAÑA a 5.8GHz**

En la figura 186 se puede apreciar el monitoreo realizado al enlace inalámbrico a 5.8GHZ desde la interface puente (bridge) del equipo ubicado en la estación AMAGUANA, en este gráfico se puede apreciar la cantidad de tráfico que ha estado circulando por la interface inalámbrica.



**Figura 186. Ancho de banda del router ESPE a 5.8GHz**

#### 4.11 Gestión de la red por medio de la herramienta PRTG

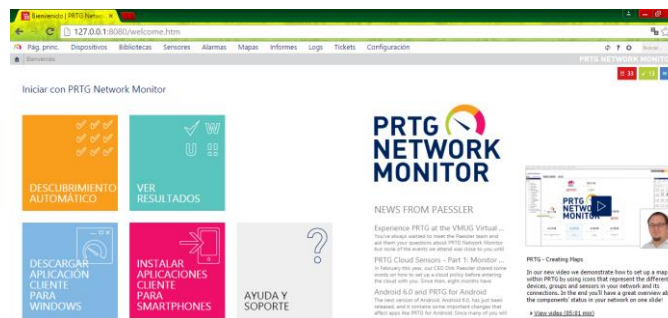
PRTG Network Monitor es un software que está disponible en inglés, Alemán, Español, Francés, Holandés, Japonés, Checo y Chino. Se puede acceder a PRTG desde una computadora de escritorio con Windows o a través de un navegador web corriendo en cualquier plataforma, colectando varias estadísticas de las maquinas, software, y equipos los cuales se ha designado. También se puede auto detectarlos, ayudándole así a mapear su red. También retiene los datos para que se pueda visualizar datos históricos. PRTG está.

PRTG viene con una interface web fácil de usar y con configuración point-and-click. Puede fácilmente compartir los datos con colegas sin conocimiento técnico y con sus clientes, incluyendo gráficas en tiempo real y reportes.

PRTG Network Monitor incluye más de 170 tipos de sensores, de cada tipo de servicio de red común incluyendo HTTP, SMTP/POP3 (email), FTP, etc. Con lo cual se podrá notificar de caídas incluso antes de que el usuario las note, incluyendo vía email, SMS.

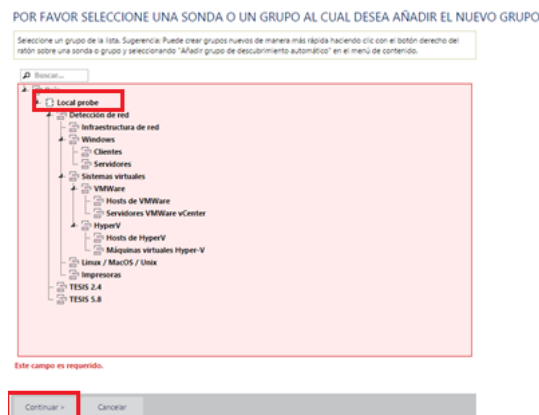
#### 4.11.1 Gestión en el enlace de 2.4GHz con PRTG Network Monitor

Una vez instalado PRTG se presenta la siguiente pantalla y donde se elige *Descubrimiento Automatico* con lo cual se va a conocer todos los dispositivos que existen en nuestra red.



**Figura 187. Inicio PRTG.**

En esta parte se selecciona el grupo *Local probe* el cual permitira detectar todos los dispositivos conectados a la red ya sean PCs, servidores, maquinas virtuales, etc. Y despues se hace clic en *Continuar*.

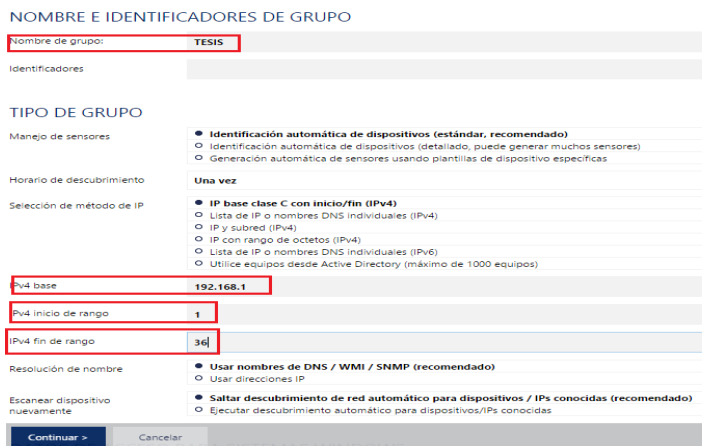


**Figura 188. Selección de Grupo**



Ahora se procede a escribir un nombre al grupo antes creado, en la sección **TIPO DE GRUPO** no se modifica nada ya que se quiere descubrir todos los dispositivos conectados y que estén configurados con IPv4.

En **IPv4 base** se ingresa la red además en **IPv4 inicio de rango** y **IPv4 fin de rango** se ingresa desde que ip hasta que ip se desea descubrir.



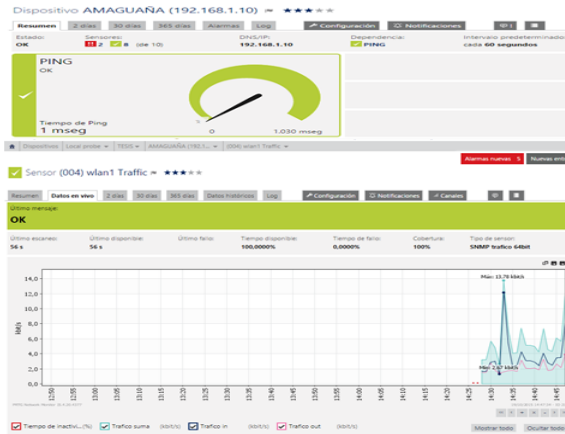
**Figura 189. Nombre e Identificadores de Grupo**

Una vez que ha concluido el escaneo de la red se puede observar todos los dispositivos descubiertos en el enlace con sus respectivas IPs. Además se puede observar que los dispositivos están activos y funcionando correctamente.



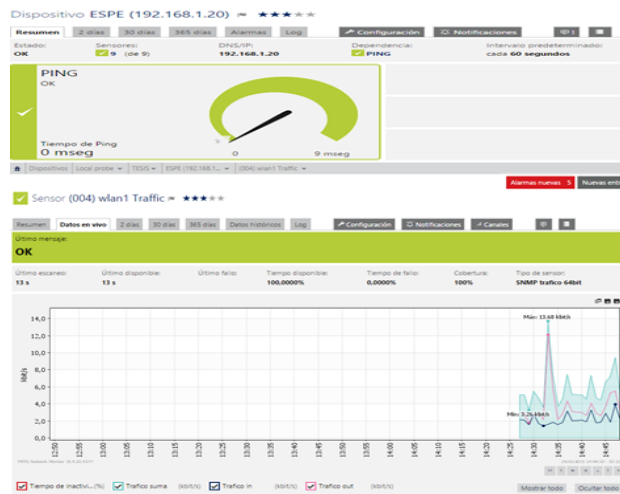
**Figura 190. Sensores Enlace 2.4GHz**

En esta imagen se puede observar el tráfico en kbit/s tanto de entrada como de salida que está circulando por la interfaz wlan1 de la estación Amaguaña con su respectiva IP 192.168.1.10. Además este gestor permite observar el tráfico que se genera en una hora, 2 días, 30 días y 365 días, en este caso se realizó pruebas durante una hora por 5 días consecutivos.



**Figura 191. Trafico Wlan1 Amaguaña en 2.4GHz**

Aquí se puede observar el tráfico en kbit/s tanto de entrada como de salida que está pasando por la interfaz wlan1 de la estación ESPE con su respectiva IP 192.168.1.20.



**Figura 192. Trafico Wlan1 ESPE en 2.4GHz**

### 4.11.2 Gestión en el enlace de 5.8 GHz con PRTG Network Monitor

El mismo procedimiento realizado anteriormente para escanear los dispositivos se lo realiza de la igual manera para el enlace de 5.8GHz, una vez que haya concluido el escaneo de la red se puede observar que los dispositivos descubiertos en el enlace con sus respectivas IPs. También se puede observar que los dispositivos están activos y funcionando correctamente.



**Figura 193. Sensores Enlace 5.8GHz**

Ahora en el enlace de 5.8Ghz se elige el sensor ping para observar el tiempo de respuesta de nuestro dispositivo y además el tráfico tanto de entrada como de salida que está circulando en la estación Amaguaña con su respectiva IP 192.168.1.11.



**Figura 194. Sensor Ping Amaguaña en 5.8GHz**

Lo mismo se realiza en la estación ESPE donde también podemos observar el tiempo de respuesta de nuestro dispositivo y además el tráfico tanto de entrada como de salida que está circulando.



**Figura 195. Sensor Ping ESPE en 5.8GHz**

## CAPITULO V

### ANALISIS DE RESULTADOS

#### 5.1 Análisis de resultados para el enlace inalámbrico a 2.4GHz

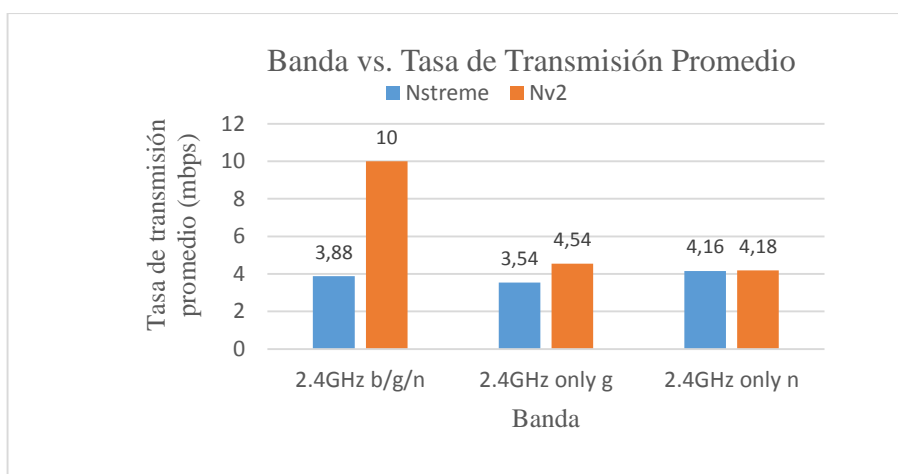
##### 5.1.1 Análisis de resultados para el enlace a inalámbrico 2.4GHz variando la banda

La figura 196 permite apreciar que el protocolo Nv2 ofrece una tasa de transmisión promedio mayor que el protocolo Nstreme en todas las bandas. La mayor tasa de transmisión promedio (10 mbps) se obtuvo en la banda 2.4GHz b/g/n con Nv2 y la menor (3.54 mbps) con Nstreme en la banda 2.4GHz only g.

**Tabla 11.**

**Banda vs. Tasa de transmisión promedio a 2.4GHz**

Banda	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
2.4GHz b/g/n	3,88	10
2.4GHz only g	3,54	4,54
2.4GHz only n	4,16	4,18



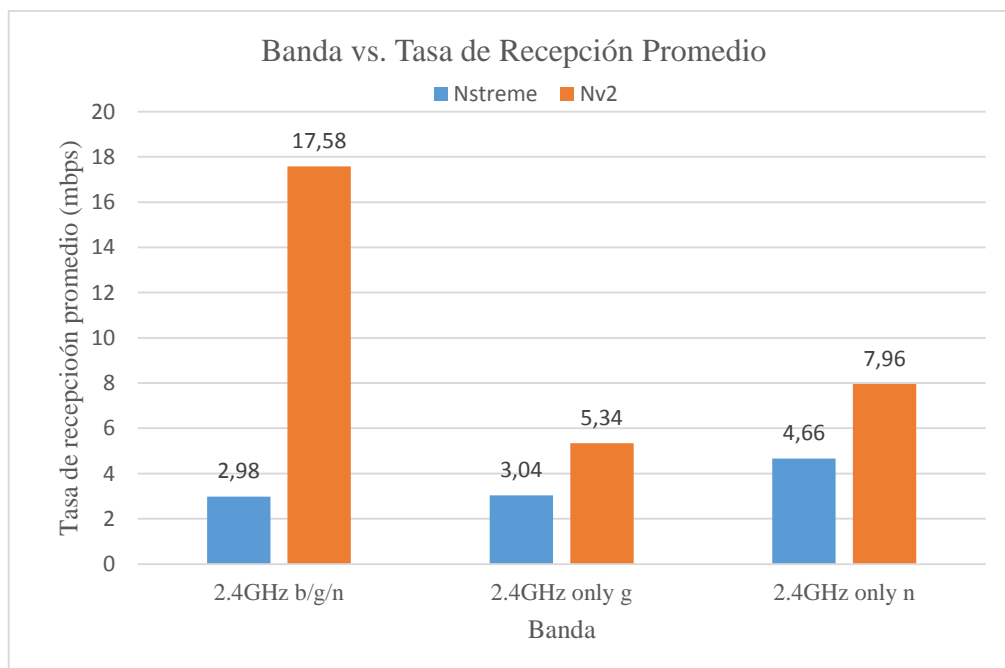
**Figura 196. Banda vs. Tasa de transmisión promedio a 2.4GHz**

La figura 197 permite apreciar que la tasa de recepción promedio es mayor utilizando el protocolo Nv2 en todas las bandas en las que se realizó las pruebas. La mayor tasa de recepción promedio (17.48 mbps) se obtuvo en la banda 2.4GHz b/g/n con el protocolo Nv2; mientras que la menor tasa (2.98 mbps) se obtuvo en la banda 2.4GHz b/g/n con el protocolo Nstreme

**Tabla 12.**

**Banda vs. Tasa de Recepción Promedio a 2.4GHz**

Banda	Tasa de Recepción Promedio Nstreme (mbps)	Tasa de Recepción Promedio Nv2 (mbps)
2.4GHz b/g/n	2,98	17,58
2.4GHz only g	3,04	5,34
2.4GHz only n	4,66	7,96



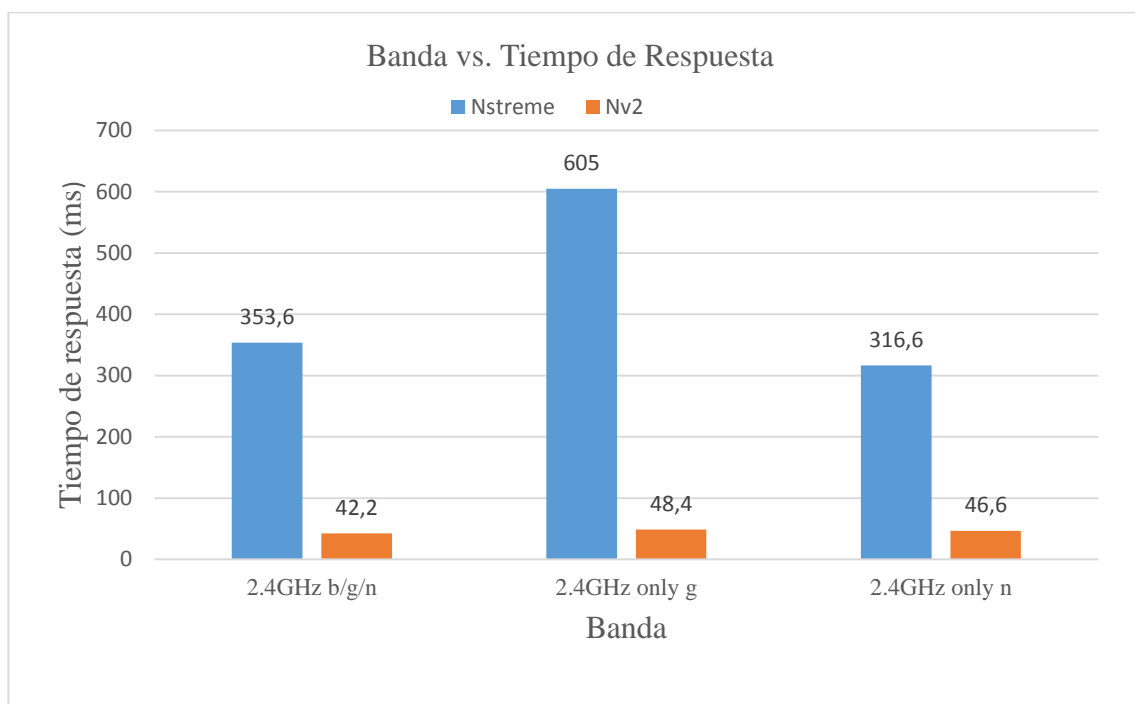
**Figura 197. Banda vs. Tasa de Recepción Promedio a 2.4GHz**

En la figura 198 se puede observar que el tiempo de respuesta con el protocolo Nv2 es mucho menor que con el protocolo Nstreme para cada una de las bandas. El menor tiempo de respuesta (42.2 ms) se obtuvo con Nv2 en la banda 2.4GHz b/g/n; mientras que el mayor tiempo (605 ms) se obtuvo con Nstreme a 2.4GHz only g.

**Tabla 13.**

**Banda vs. Tiempo de respuesta a 2.4GHz**

Banda	Tiempo de respuesta Nstreme (ms)	Tiempo de repuesta Nv2 (ms)
2.4GHz b/g/n	353,6	42,2
2.4GHz only g	605	48,4
2.4GHz only n	316,6	46,6



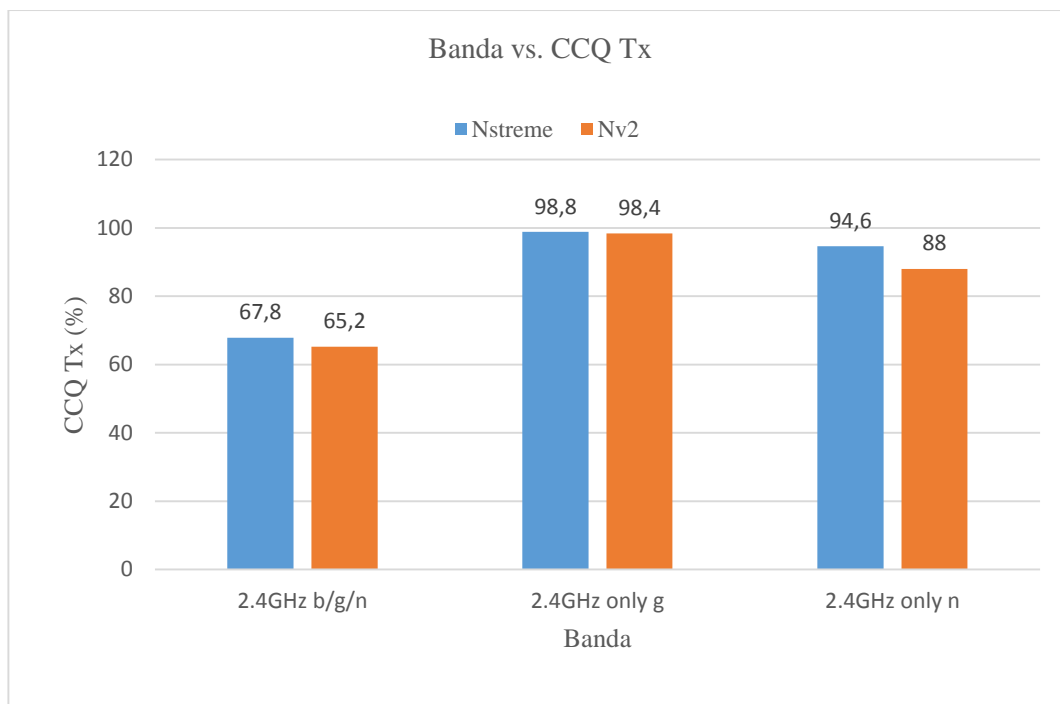
**Figura 198. Banda vs. Tiempo de respuesta a 2.4GHz**

En la figura 199 se observa que la calidad del enlace en transmisión (CCQ Tx) es similar en todas las bandas utilizando los protocolos Nstreme y Nv2. El mayor CCQ Tx (98.8%) obtenido en el enlace es con el protocolo Nstreme en la banda 2.4GHz only g, mientras que el menor (65.2%) se lo obtuvo con la banda 2.4GHz b/g/n con Nv2

**Tabla 14.**

**Banda vs. CCQ Tx a 2.4GHz**

Banda	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
2.4GHz b/g/n	67,8	65,2
2.4GHz only g	98,8	98,4
2.4GHz only n	94,6	88



**Figura 199. Banda vs. CCQ Tx a 2.4GHz**

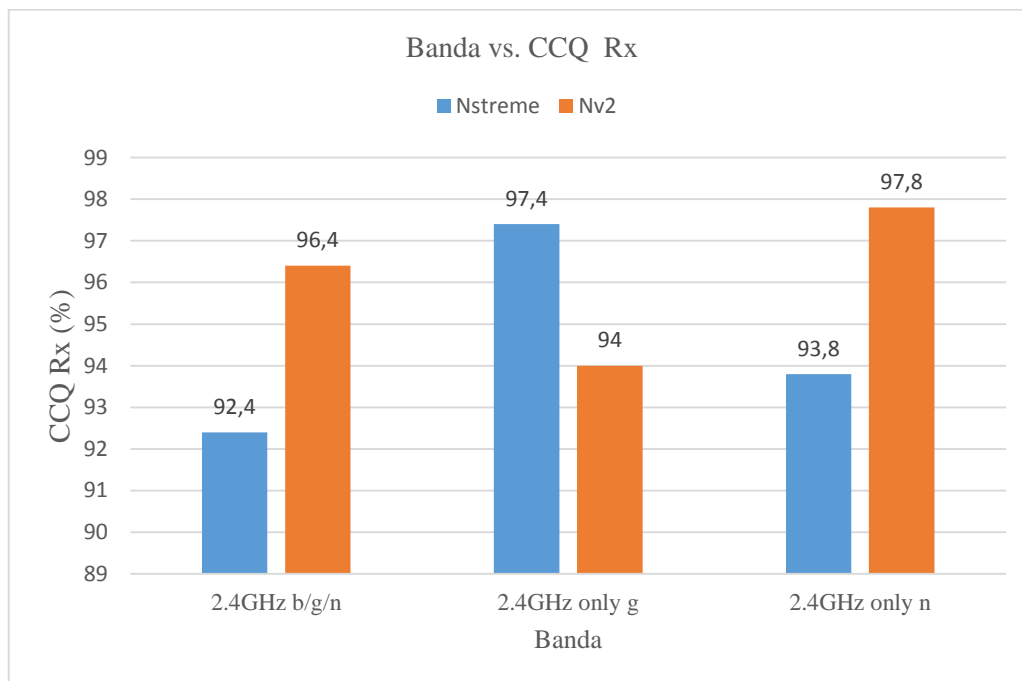


En la figura 200 se puede apreciar que en las bandas 2.4Ghz b/g/n y 2.4GHz only n se obtuvo un CCQ de recepción mayor con el protocolo Nv2; pero en la banda 2.4GHz only g el CCQ Rx es menor. El mayor CCQ de recepción (97.8%) se obtuvo con el protocolo Nv2 con la banda 2.4GHz only n; mientras que la menor calidad de enlace (92.4%) se midió en el protocolo Nstreme en banda 2.4GHz b/g/n.

**Tabla 15.**

**Banda vs. CCQ Rx a 2.4GHz**

Banda	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
2.4GHz b/g/n	92,4	96,4
2.4GHz only g	97,4	94
2.4GHz only n	93,8	97,8



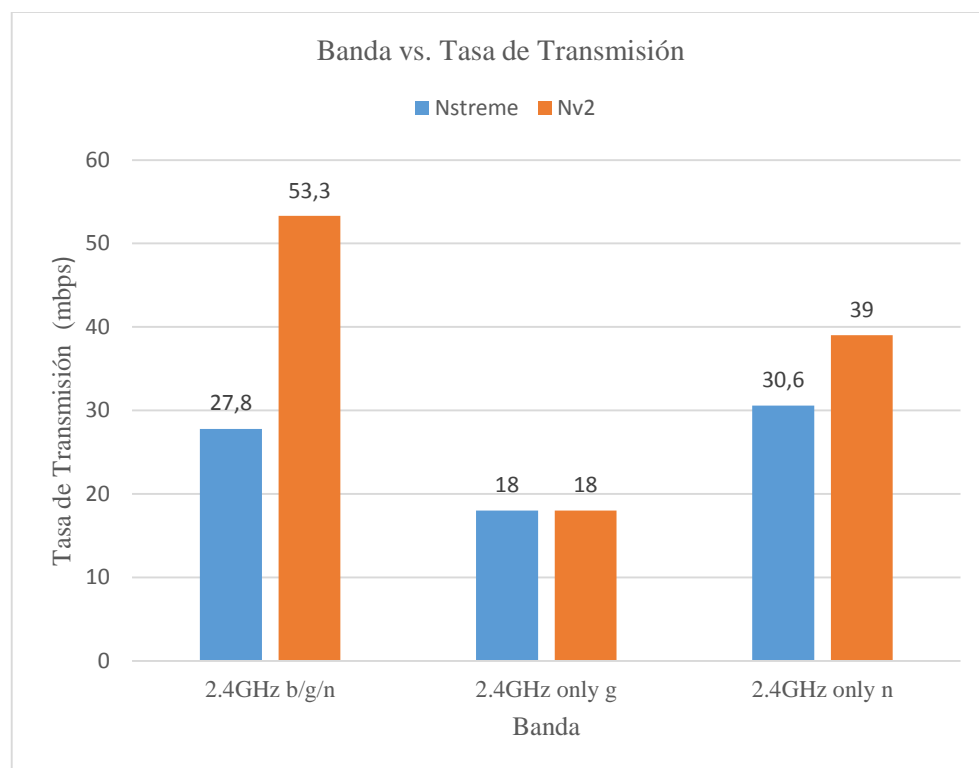
**Figura 200. Banda vs. CCQ Rx a 2.4GHz**

En la figura 201 se puede verificar que la tasa de transmisión con el protocolo Nv2 es mayor para las bandas 2.4GHz b/g/n y 2.4GHz only n; pero igual (18 mbps) con la banda 2.4GHz only g. La mayor tasa de transmisión (53.3 mbps) se registra con Nv2 a 2.4GHz b/g/n.

**Tabla 16.**

**Banda vs. Tasa de transmisión a 2.4GHz**

Banda	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
2.4GHz b/g/n	27,8	53,3
2.4GHz only g	18	18
2.4GHz only n	30,6	39



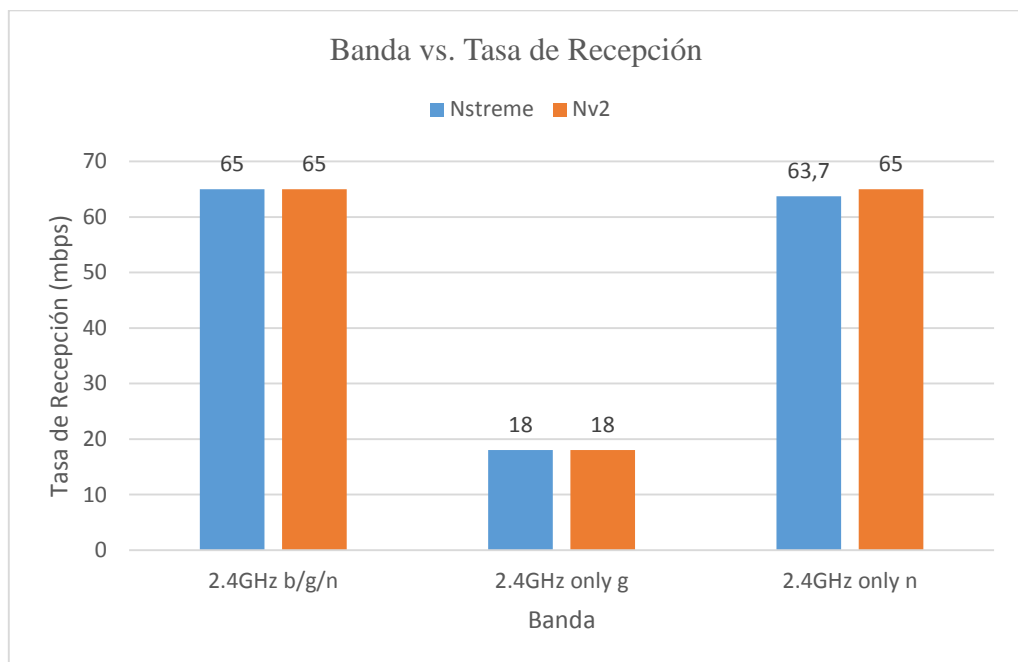
**Figura 201. Banda vs. Tasa de transmisión a 2.4GHz**

En la figura 202 se observa que las tasas de recepción en las bandas 2.4GHz b/g/n y 2.4GHz only g son iguales utilizando los protocolos Nstreme y Nv2; mientras que en la banda 2.4GHz only n es ligeramente inferior con el protocolo Nstreme.

**Tabla 17.**

**Banda vs. Tasa de Recepción a 2.4GHz**

Banda	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
2.4GHz b/g/n	65	65
2.4GHz only g	18	18
2.4GHz only n	63,7	65



**Figura 202. Banda vs. Tasa de Recepción a 2.4GHz**

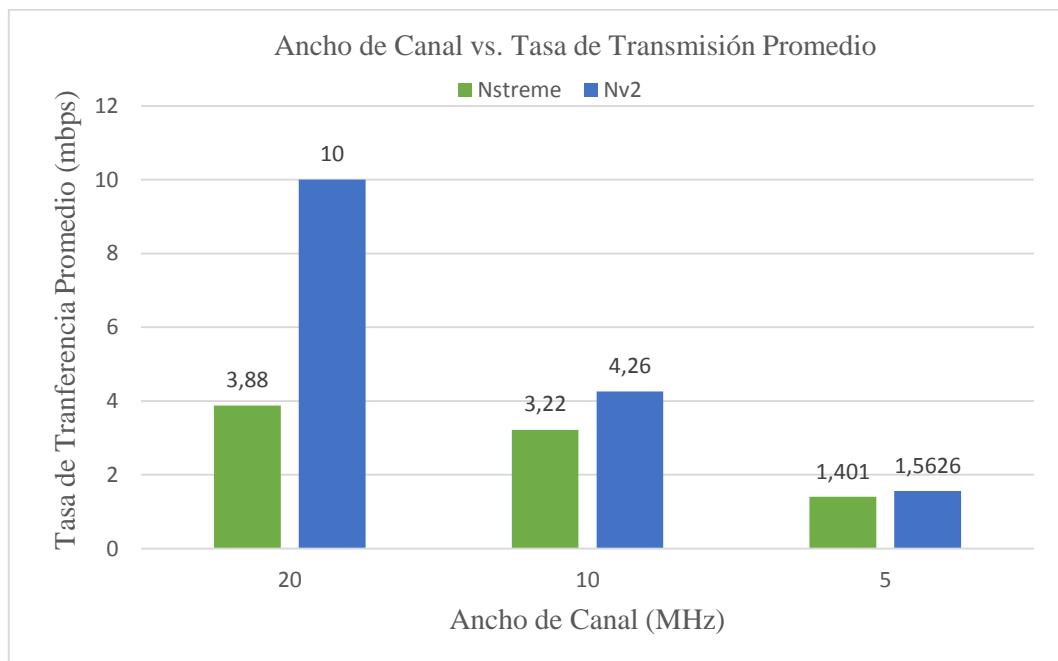
### 5.1.2 Análisis de resultados para el enlace inalámbrico a 2.4GHz variando el ancho de canal

En la figura 203 se aprecia que la tasa de transmisión promedio con el protocolo Nv2 es superior en relación a la tasa de transmisión promedio con el protocolo Nstreme en cada uno de los anchos de canal estudiados. La mayor tasa de transmisión (10 Mbps) se la obtuvo con Nv2 a 20MHz de ancho de canal, mientras que la menor (1.401 Mbps) se la obtuvo con el protocolo Nstreme a 5MHz.

**Tabla 18.**

#### Ancho de Canal vs. Tasa de Transmisión Promedio a 2.4GHz

Ancho de canal	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
20	3,88	10
10	3,22	4,26
5	1,401	1,5626



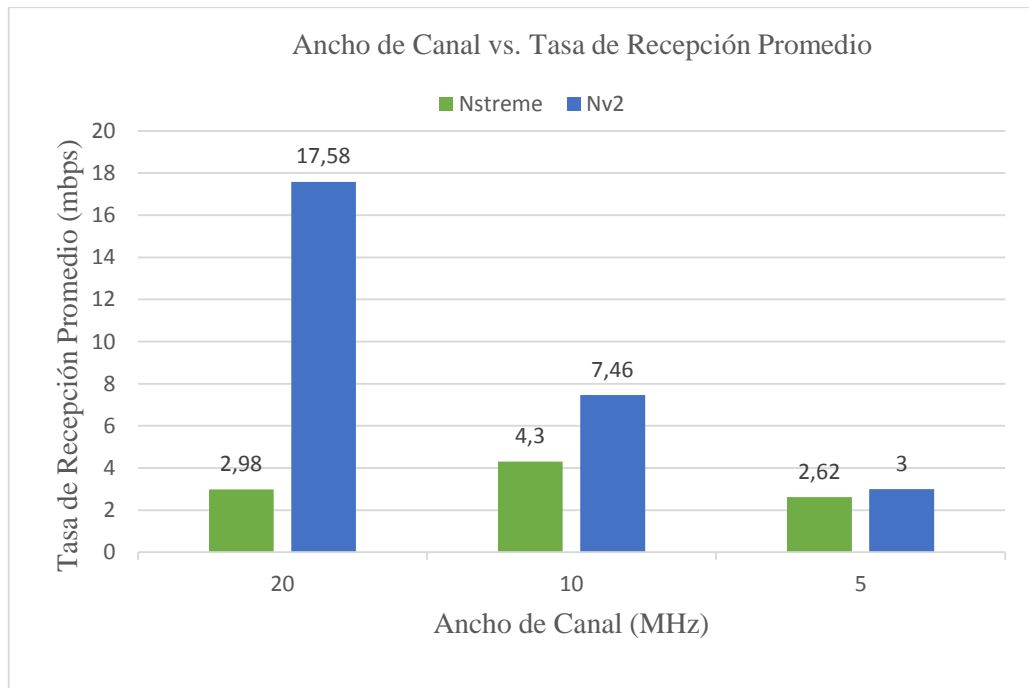
**Figura 203. Ancho de Canal vs. Tasa de Transmisión Promedio a 2.4GHz**

En la figura 204 se muestra que la tasa de recepción promedio con el protocolo Nv2 es superior con respecto a la tasa de recepción promedio con el protocolo Nstreme. La mayor tasa de recepción (17.58 mbps) se obtuvo a un ancho de canal de 20Mhz con el protocolo Nv2, y por el contrario la menor tasa de recepción (2.62 mbps) fue dada a 5MHz de ancho de canal con Nstreme

**Tabla 19.**

**Ancho de canal vs. Tasa de recepción promedio a 2.4GHz**

Ancho de canal	Tasa de Recepción Promedio Nstreme (mbps)	Tasa de Recepción Promedio Nv2 (mbps)
20	2,98	17,58
10	4,3	7,46
5	2,62	3



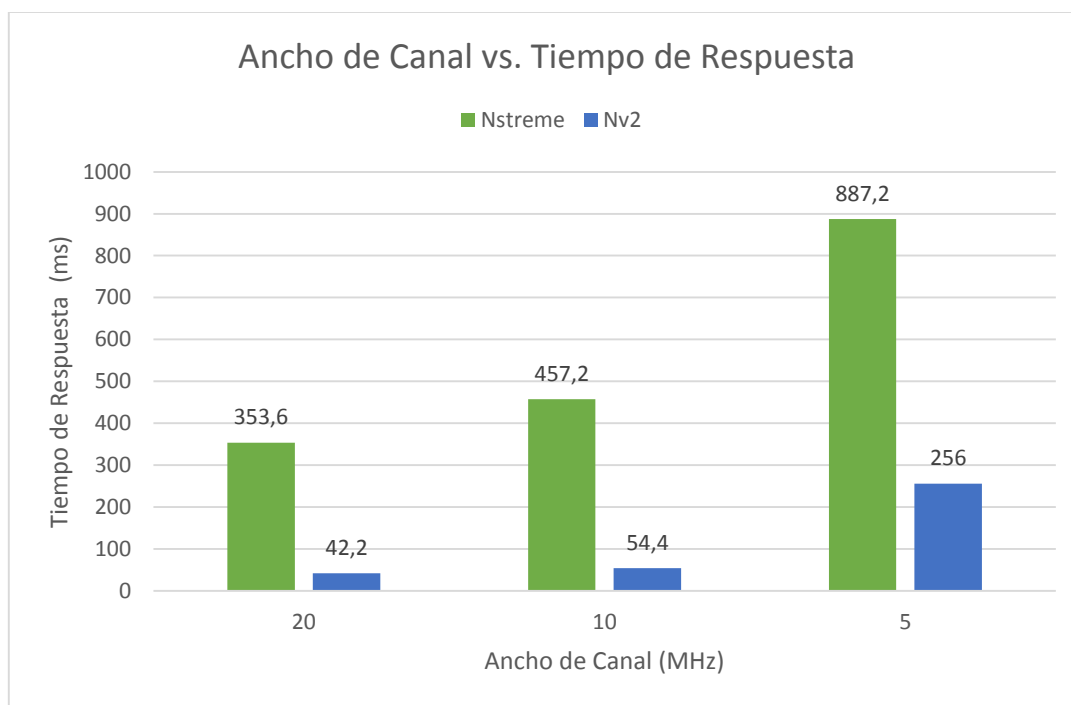
**Figura 204. Ancho de canal vs. Tasa de recepción promedio a 2.4GHz**

En la figura 205 se puede apreciar que el tiempo de respuesta es significativamente menor con el protocolo Nv2 que con Nstreme. El mayor tiempo de respuesta (887.2 ms) se lo obtuvo con el protocolo Nstreme a 5MHz de ancho de canal; mientras que el menor tiempo de respuesta (42.2 ms) se lo obtuvo con el protocolo Nv2 a 20MHz.

**Tabla 20.**

**Ancho de Canal vs. Tiempo de Respuesta a 2.4GHz**

Ancho de canal	Tiempo de Respuesta Nstreme (ms)	Tiempo de Respuesta Nv2 (ms)
20	353,6	42,2
10	457,2	54,4
5	887,2	256



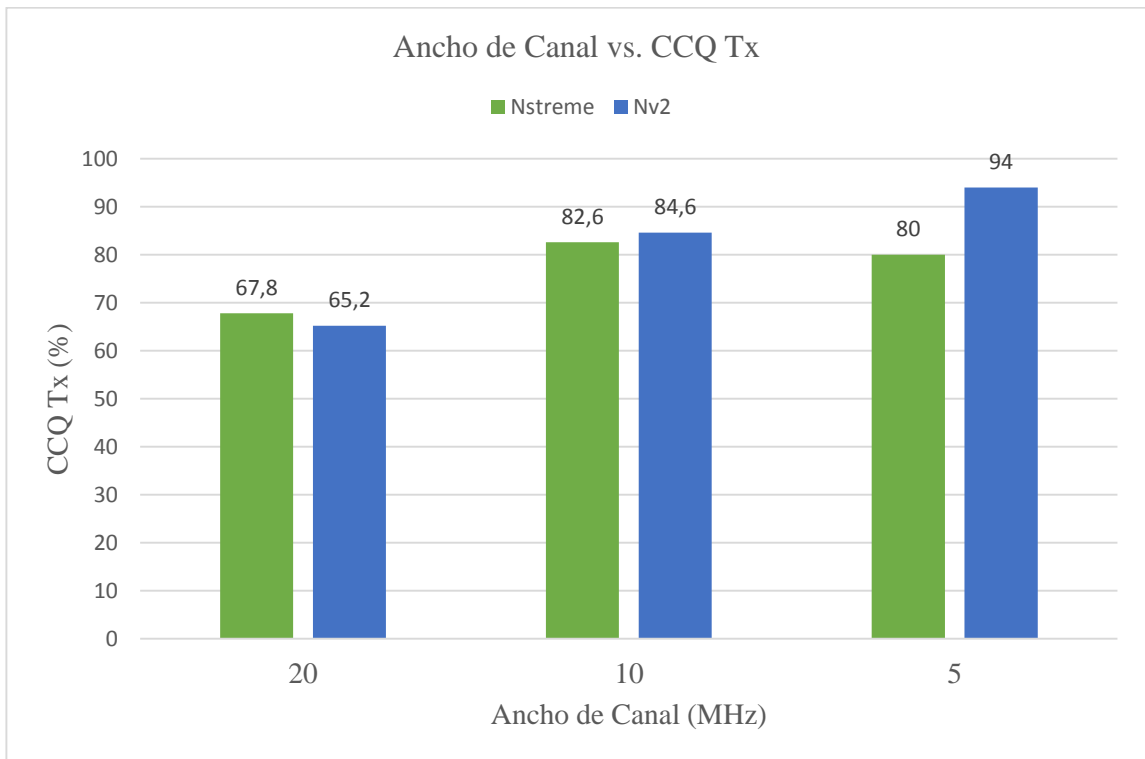
**Figura 205. Ancho de Canal vs. Tiempo de Respuesta a 2.4GHz**

En las figura 206 se aprecia que el CCQ de transmisión con el protocolo Nstreme es superior al obtenido con Nv2 para un ancho de canal de 20MHz; mientras que con Nv2 se tiene un CCQ Tx mayor en los anchos de canal a 10MHz y 5MHz. El mayor CCQ Tx (94 %) se lo obtuvo con Nv2 a 5MHz mientras que el menor CCQ (65.2%) fue medido con Nv2 a 20MHz

**Tabla 21.**

**Ancho de Canal vs. CCQ Tx a 2.4GHz**

Ancho de canal	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
20	67,8	65,2
10	82,6	84,6
5	80	94



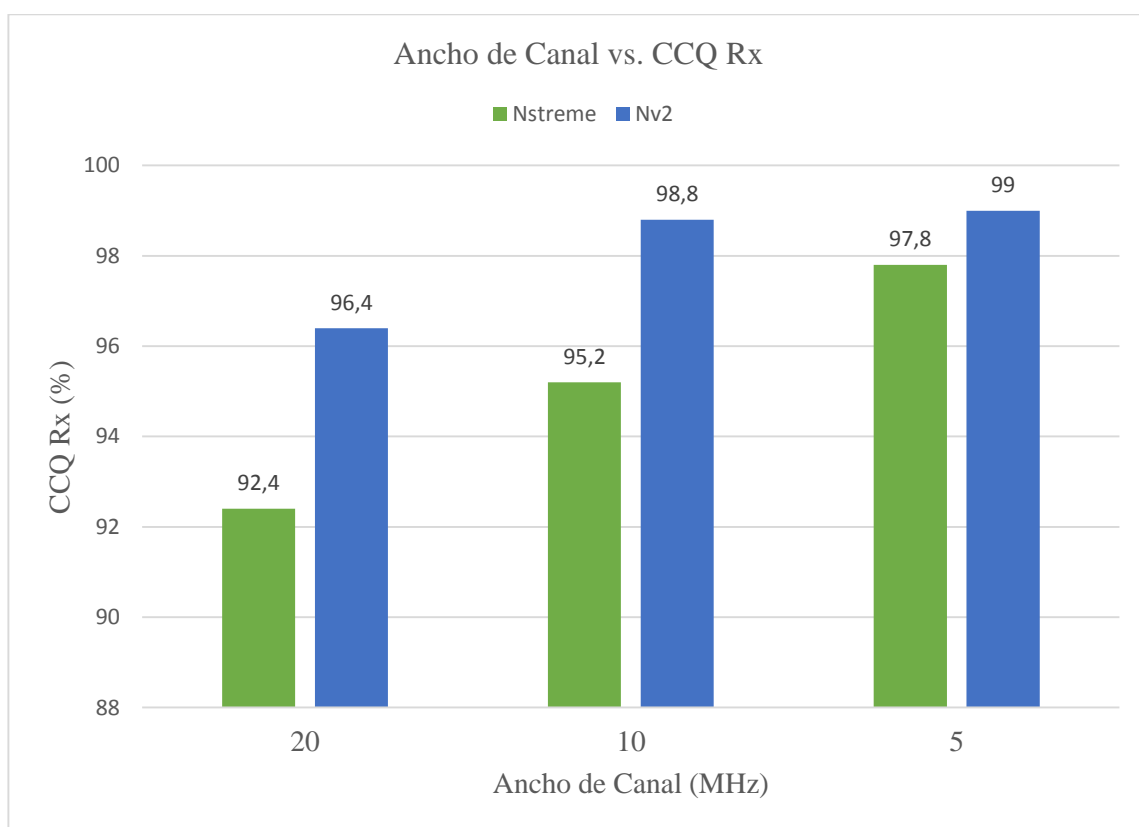
**Figura 206. Ancho de Canal vs. CCQ Tx a 2.4GHz**

En la figura 207 se puede mirar que con el protocolo Nv2 se obtiene un CCQ de recepción mayor que el obtenido con Nstreme en todos los anchos de canal. El mayor CCQ Rx (99%) se tiene con Nv2 en un ancho de canal de 5MHz y el menor valor (92.4%) esta con el protocolo Nstreme con 20MHz de ancho de canal.

**Tabla 22.**

**Ancho de Canal vs. CCQ Rx a 2.4GHz**

Ancho de canal	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
20	92,4	96,4
10	95,2	98,8
5	97,8	99



**Figura 207. Ancho de Canal vs. CCQ Rx a 2.4GHz**

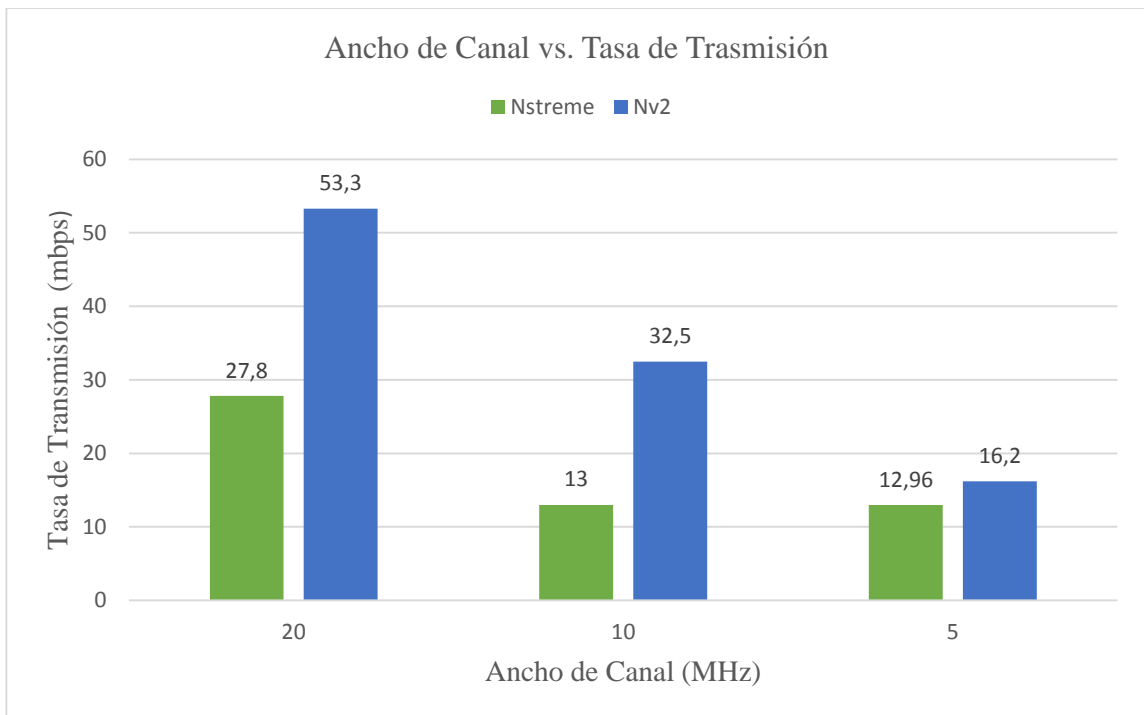


En la figura 208 se puede apreciar que con Nv2 se obtiene una mejor tasa de transmisión en comparación con los datos obtenidos con el protocolo Nstreme. La mayor tasa de transmisión (53.3 mbps) se obtuvo con Nv2 con 20MHz de ancho de canal; mientras que la menor tasa (12.96 mbps) se encuentra en los 5MHz de ancho de canal con Nstreme

**Tabla 23.**

**Ancho de Canal vs. Tasa de Transmisión a 2.4GHz**

Ancho de canal	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
20	27,8	53,3
10	13	32,5
5	12,96	16,2



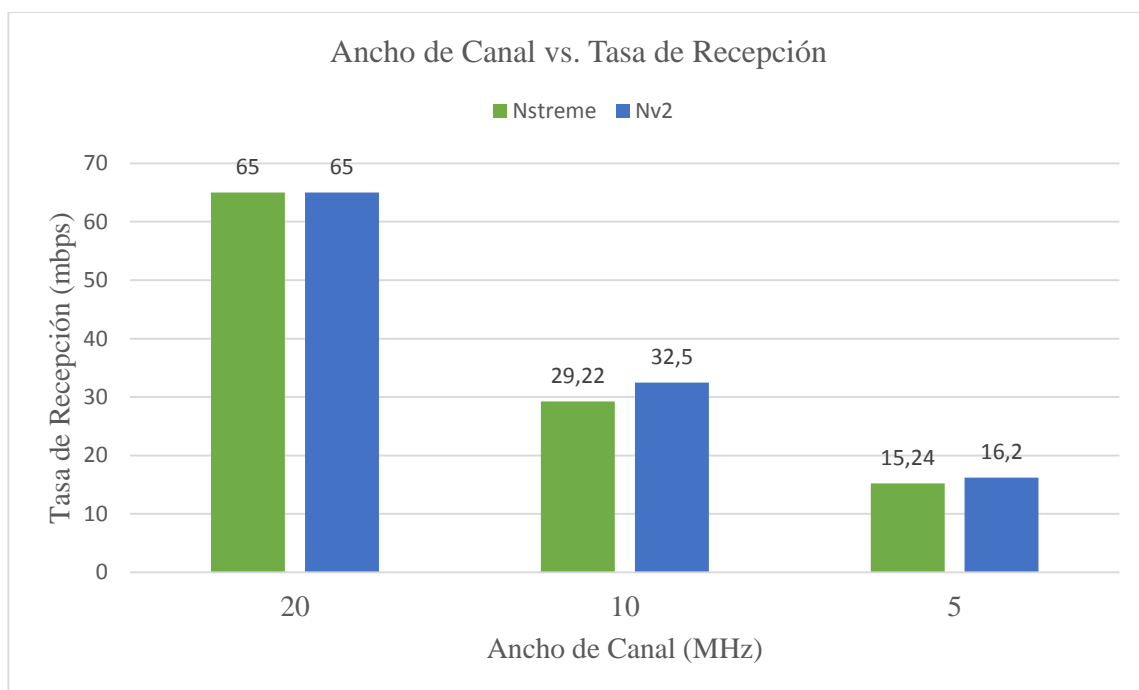
**Figura 208. Ancho de Canal vs. Tasa de Transmisión a 2.4GHz**

La figura 209 permite apreciar una igualdad en la tasa de recepción utilizando los protocolos Nstreme y Nv2 con un ancho de canal de 20MHz; mientras que con 5MHz y 10MHz se identifica una tasa de recepción superior con Nv2. La mayor tasa de recepción (65 mbps) se encuentra en el ancho de canal de 20MHz; por el contrario, la menor tasa está a 5MHz con Nstreme

**Tabla 24.**

**Ancho de Canal vs. Tasa de Recepción a 2.4GHz**

Ancho de canal	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2(mbps)
20	65	65
10	29,22	32,5
5	15,24	16,2



**Figura 209. Ancho de Canal vs. Tasa de Recepción a 2.4GHz**

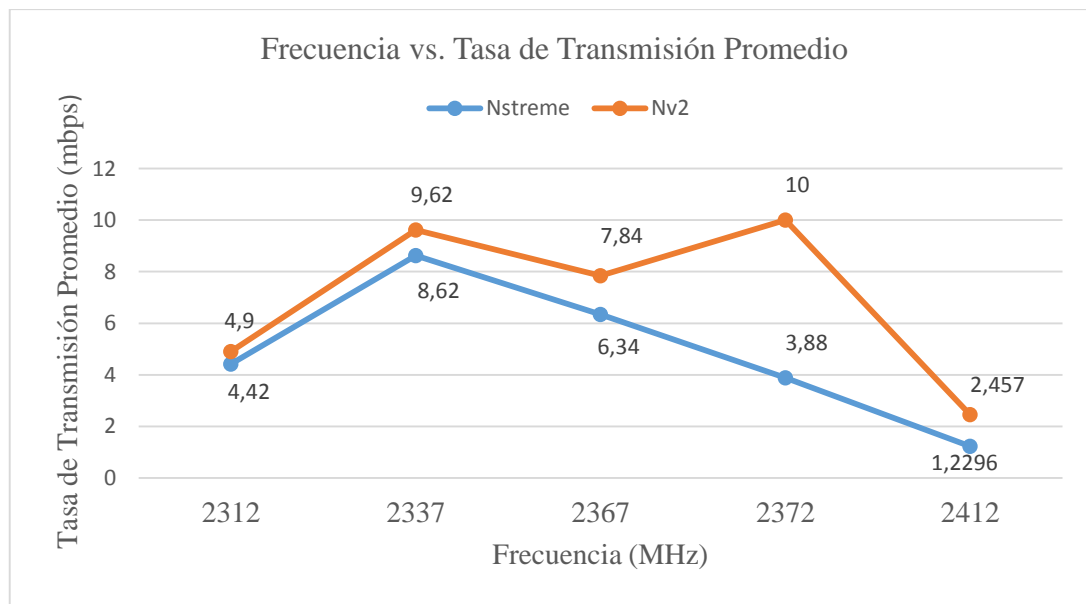
### 5.1.3 Análisis de resultados para el enlace inalámbrico a 2.4GHz variando la frecuencia

La figura 210 permite apreciar una mayor tasa de transmisión utilizando el protocolo Nv2 con relación al protocolo Nstreme en todas las frecuencias en las que se realizó las mediciones. La mayor tasa de transmisión promedio (10 mbps) se obtuvo en la frecuencia 2372 MHz con Nv2; mientras que la menor (1.2296 mbps) se encuentra en 2412 MHz con Nstreme.

**Tabla 25.**

#### Frecuencia vs. Tasa de Transmisión Promedio a 2.4GHz

Frecuencia	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
2312	4,42	4,9
2337	8,62	9,62
2367	6,34	7,84
2372	3,88	10
2412	1,2296	2,457



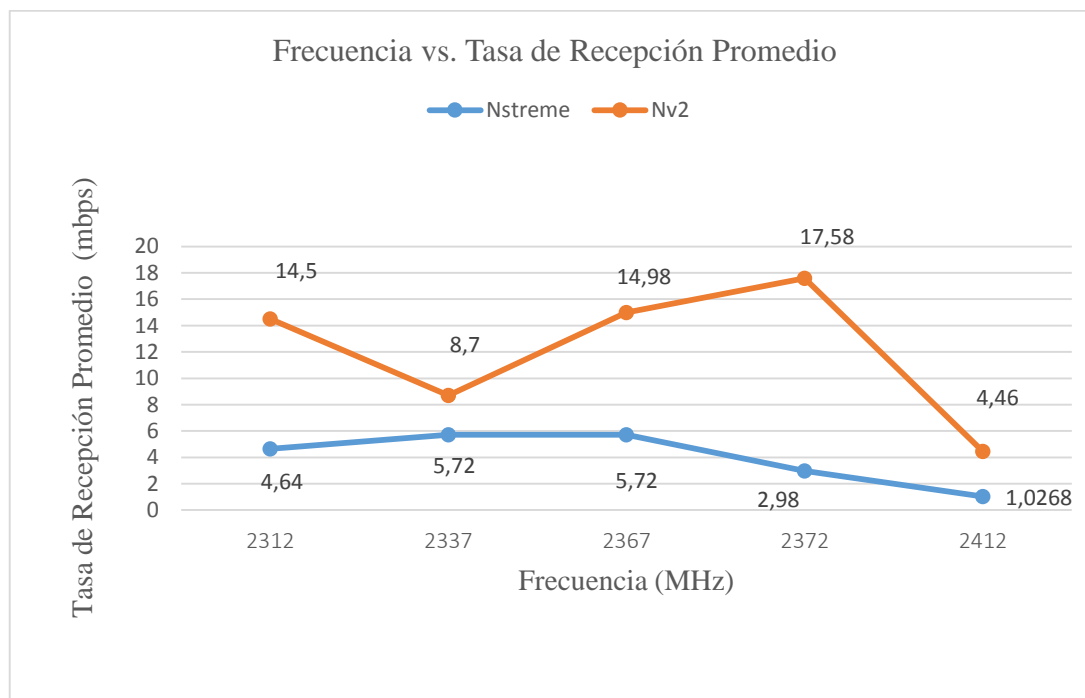
**Figura 210. Frecuencia vs. Tasa de Transmisión Promedio a 2.4GHz**

La figura 211 permite verificar que la tasa de recepción promedio es superior utilizando el protocolo Nv2 con relación a Nstreme en cada una de las frecuencias. La mayor tasa de recepción promedio (17.58 mbps) se obtuvo con Nv2 a una frecuencia de 2372 MHz; mientras que la menor tasa (1.0268 mbps) se lo tiene en la frecuencia de 2412 MHz con Nstreme.

**Tabla 26.**

**Frecuencia vs. Tasa de Recepción Promedio a 2.4GHz**

Frecuencia	Tasa de Recepción Promedio Nstreme (mbps)	Tasa de Recepción Promedio Nv2 (mbps)
2312	4,64	14,5
2337	5,72	8,7
2367	5,72	14,98
2372	2,98	17,58
2412	1,0268	4,46



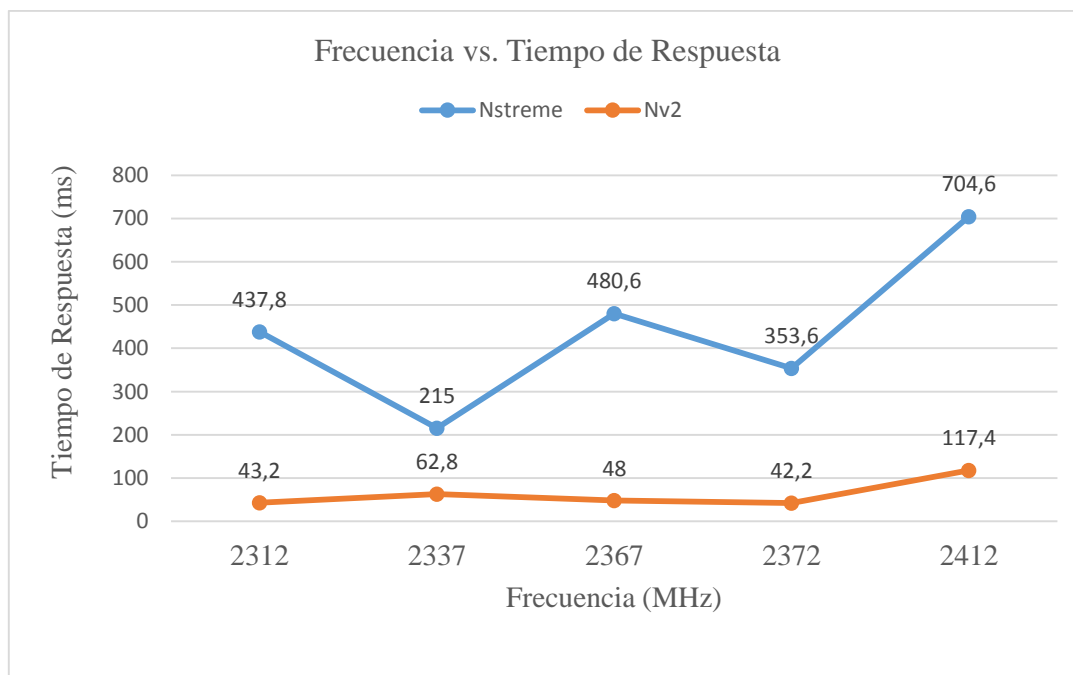
**Figura 211. Frecuencia vs. Tasa de Recepción Promedio a 2.4GHz**

Por medio de la figura 212 se puede apreciar que los tiempos de respuesta con el protocolo Nv2 son siempre menor a los del protocolo Nstreme. El mejor tiempo de respuesta (42.2 ms) se encuentra en la frecuencia 2372 MHz con Nv2 y el mayor tiempo de respuesta (704.6 ms) se obtuvo con Nstreme a una frecuencia de 2412 MHz

**Tabla 27.**

**Frecuencia vs. Tiempo de Respuesta a 2.4GHz**

Frecuencia	Tiempo de Respuesta Nstreme (ms)	Tiempo de Respuesta Nv2 (ms)
2312	437,8	43,2
2337	215	62,8
2367	480,6	48
2372	353,6	42,2
2412	704,6	117,4



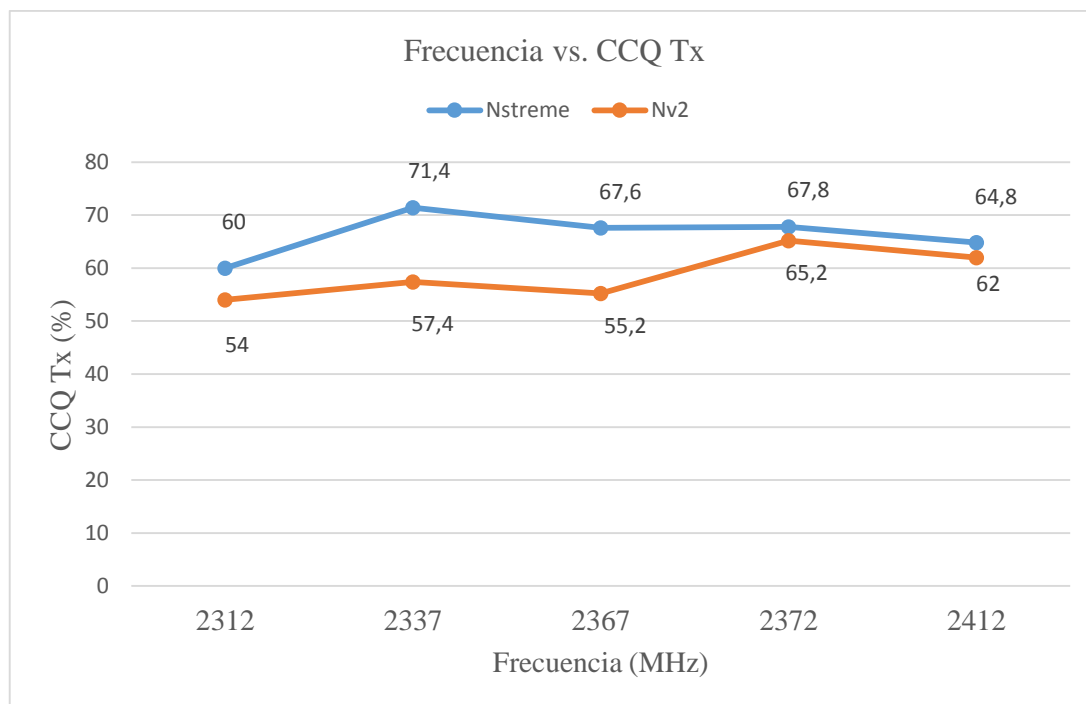
**Figura 212. Frecuencia vs. Tiempo de Respuesta a 2.4GHz**

En la figura 213 se puede observar que el CCQ de transmisión es similar utilizando los protocolos Nstreme y Nv2. Se registra una ligera superioridad con Nstreme. El mayor CCQ Tx (71.4%) se registra en la frecuencia 2337 MHz con Nstreme; mientras que el menor (54%) se encuentra en 2312 MHz con Nv2

**Tabla 28.**

**Frecuencia vs. CCQ Tx a 2.4GHz**

Frecuencia	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
2312	60	54
2337	71,4	57,4
2367	67,6	55,2
2372	67,8	65,2
2412	64,8	62



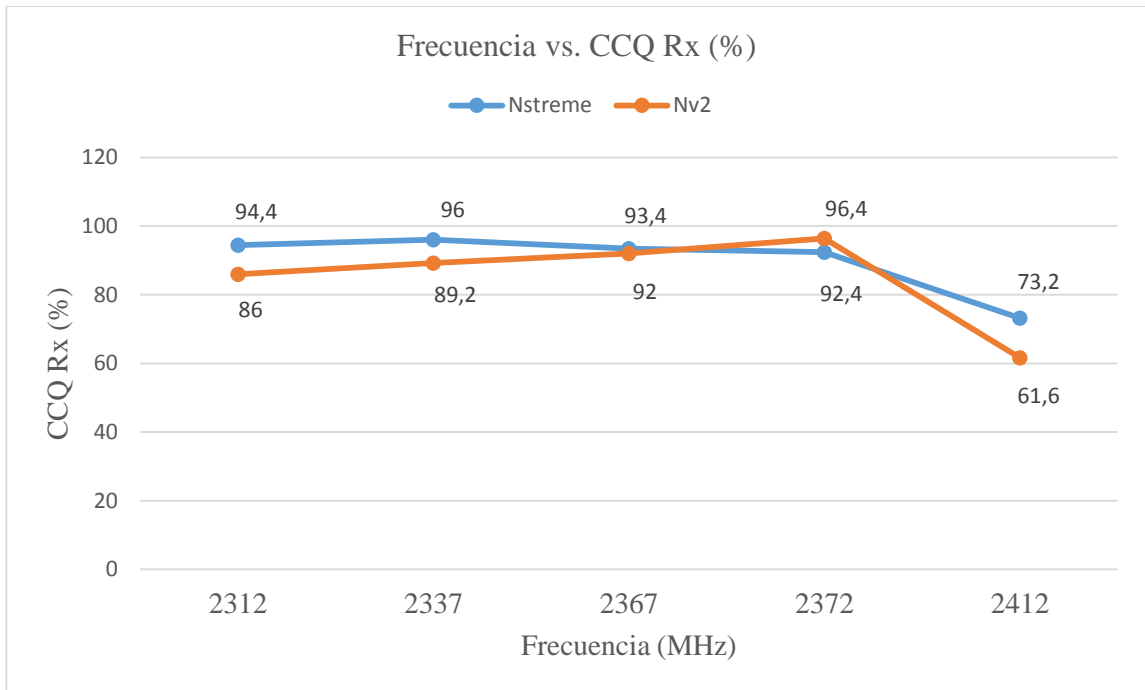
**Figura 213. Frecuencia vs. CCQ Tx a 2.4GHz**

Igual que con el CCQ de transmisión, en la figura 214 se observa una ligera superioridad de la calidad del enlace de recepción (CCQ Rx) por parte del protocolo Nstreme; a excepción de la frecuencia 2372 MHz en donde Nv2 es superior. El mayor CCQ Rx (96.4%) se registra con Nv2; mientras que la menor calidad de enlace está en la frecuencia 2412 MHz con Nv2.

**Tabla 29.**

**Frecuencia vs. CCQ Rx a 2.4GHz**

Frecuencia	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
2312	94,4	86
2337	96	89,2
2367	93,4	92
2372	92,4	96,4
2412	73,2	61,6



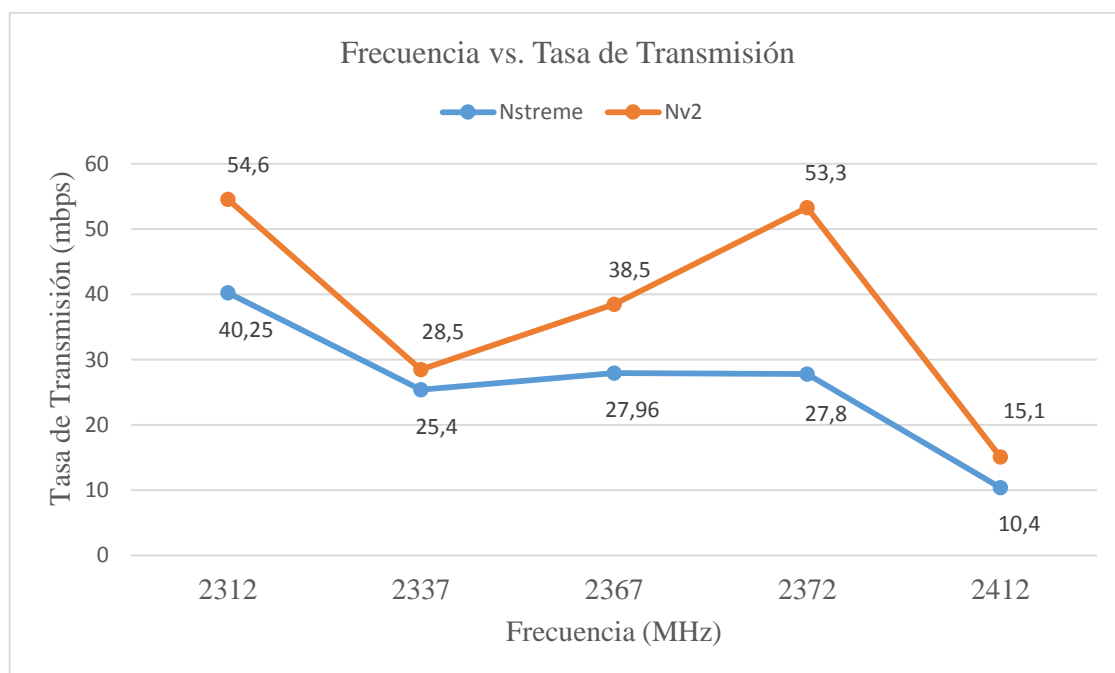
**Figura 214. Frecuencia vs. CCQ Rx a 2.4GHz**

La figura 215 permite apreciar una mayor tasa de transmisión con el protocolo Nv2 con respecto al protocolo Nstreme en todas las frecuencias en las que se realizó las pruebas. La mayor tasa de transmisión (53.3 mbps) se ubica en la frecuencia 2372 MHz; mientras que la menor tasa (25.4 mbps) se encuentra en la frecuencia 2337 MHz con Nstreme

**Tabla 30.**

**Frecuencias vs. Tasa de Transmisión a 2.4GHz**

Frecuencia	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
2312	40,25	54,6
2337	25,4	28,5
2367	27,96	38,5
2372	27,8	53,3
2412	10,4	15,1



**Figura 215. Frecuencia vs. Tasa de Transmisión a 2.4GHz**

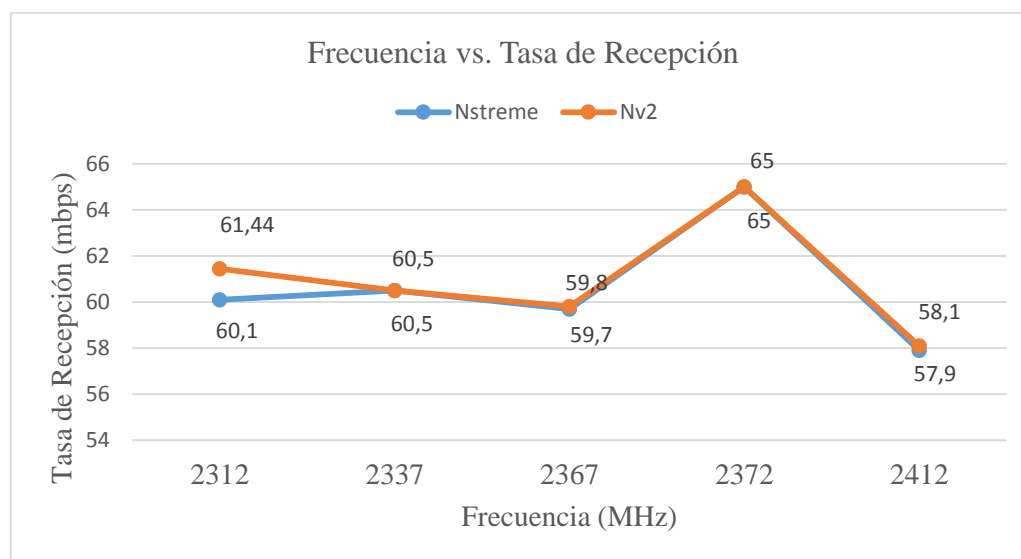


En la figura 216 se observa que existe una relativa igualdad en la tasa de recepción utilizando los protocolos Nstreme y Nv2. Existe una mínima superioridad por parte del protocolo Nv2. La mayor tasa de recepción (65 mbps) se registra en la frecuencia 2372 MHz con ambos protocolos; mientras que la menor se encuentra en la frecuencia 2412 MHz con Nstreme

**Tabla 31.**

**Frecuencia vs. Tasa de Recepción a 2.4GHz**

Frecuencia	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
2312	60,1	61,44
2337	60,5	60,5
2367	59,7	59,8
2372	65	65
2412	57,9	58,1



**Figura 216. Frecuencia vs. Tasa de Recepción a 2.4GHz**

## 5.2 Análisis de resultados para el enlace a 5.8 GHz

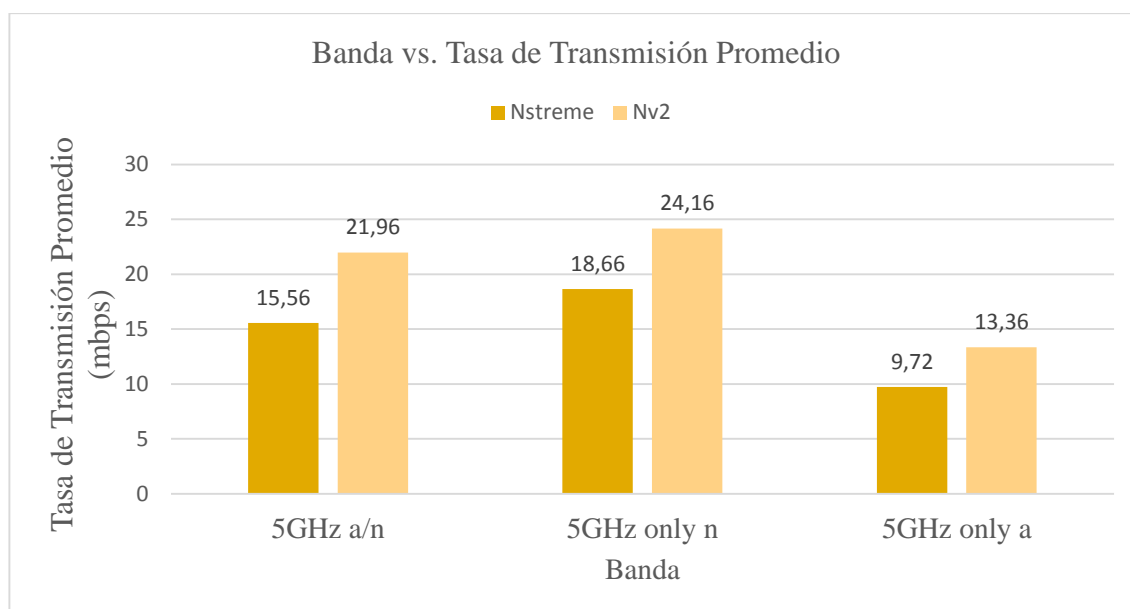
### 5.2.1 Análisis de resultados para el enlace a 5.8 GHz variando la banda

En la figura 217 la tasa de transmisión promedio es mayor utilizando el protocolo Nv2 mientras que con el protocolo Nstreme su tasa de transmisión promedio es menor en todas las bandas. La mayor tasa de transmisión promedio (24.16 mbps) se encuentra en la banda 5GHz only n; mientras que la menor tasa (9.72 mpbs) esta con el protocolo Nstreme en la banda 5GHz only a.

**Tabla 32.**

#### Banda vs. Tasa de Transmisión Promedio a 5.8GHz

Banda	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
5GHz a/n	15,56	21,96
5GHz only n	18,66	24,16
5GHz only a	9,72	13,36



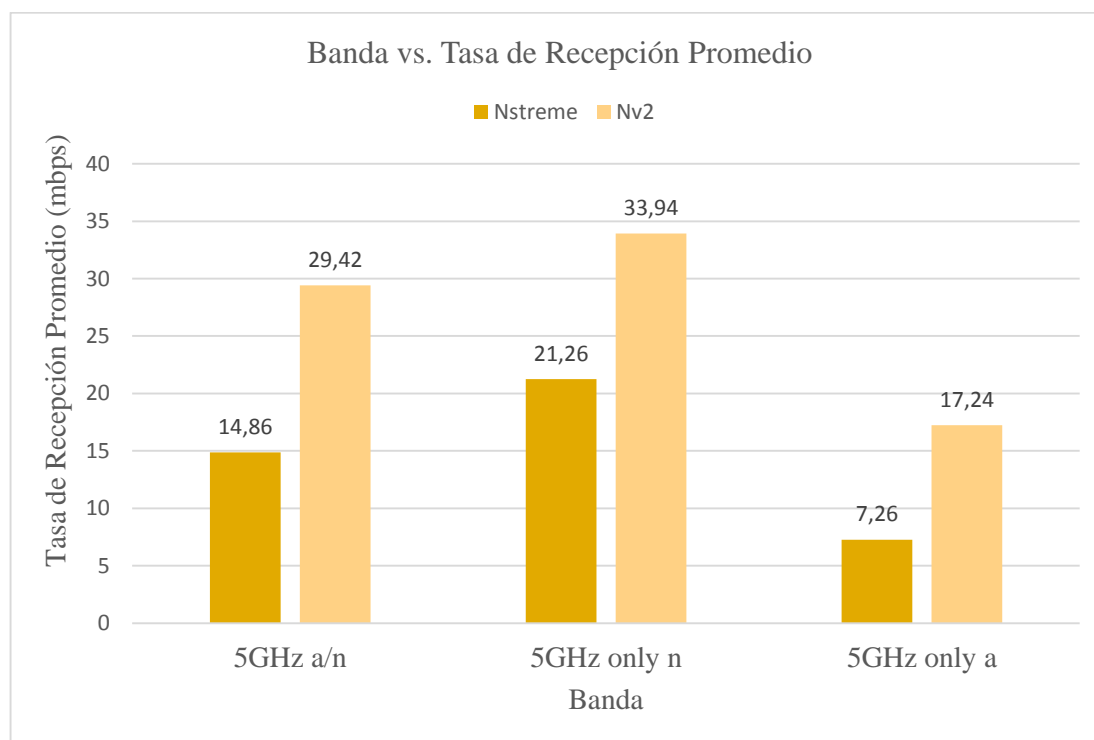
**Figura 217. Banda vs. Tasa de Transmisión Promedio a 5.8GHz**

En la figura 218 se observa que la tasa de recepción promedio con el protocolo Nv2 es mucho mayor con referencia al protocolo Nstreme. La mayor tasa de recepción promedio (33.94 mbps) se encuentra en la banda only n con el protocolo Nv2; mientras que la menor tasa de recepción (7.26 mbps) está con el protocolo Nstreme en la banda 5GHz only a.

**Tabla 33.**

**Banda vs. Tasa de Recepción Promedio a 5.8GHz**

Banda	Tasa de Recepción Promedio Nstreme(mbps)	Tasa de Recepción Promedio Nv2 (mbps)
5GHz a/n	14,86	29,42
5GHz only n	21,26	33,94
5GHz only a	7,26	17,24



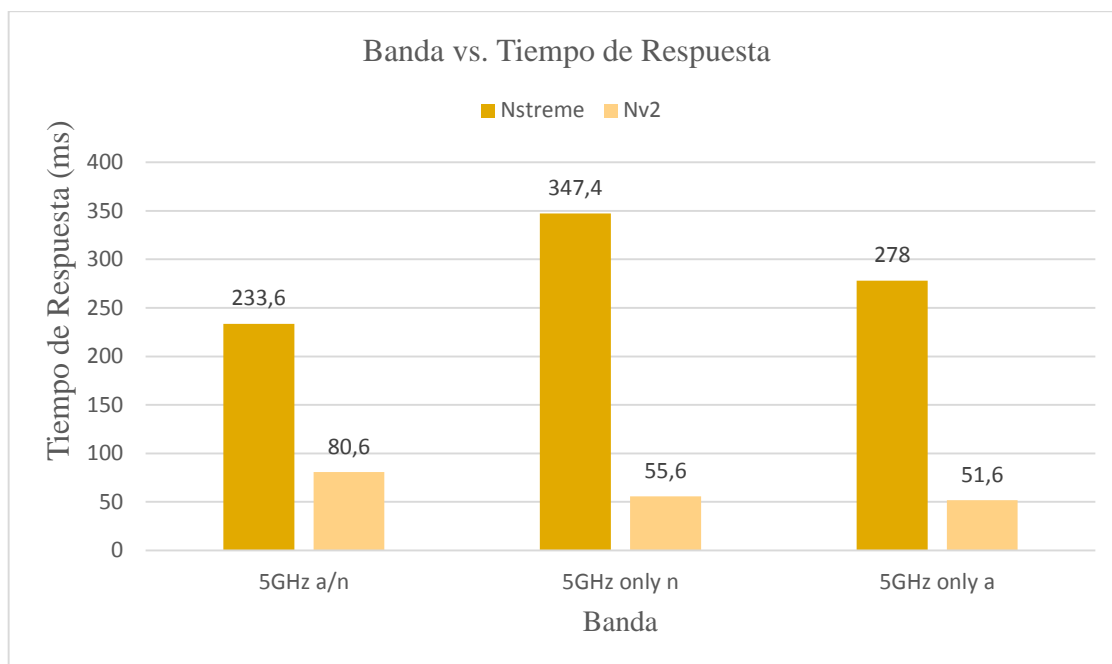
**Figura 218. Banda vs. Tasa de Recepción Promedio a 5.8GHz**

En la figura 219 se observa que el protocolo Nv2 tiene un mejor tiempo de respuesta que el protocolo Nstreme. El mejor tiempo de respuesta (51.6 ms) se obtuvo con la banda 5GHz only a con el protocolo Nv2; mientras que el mayor tiempo (347.4 ms) de respuesta se encuentra en la banda 5GHz only n con el protocolo Nstreme.

**Tabla 34.**

**Banda vs. Tiempo de Respuesta a 5.8GHz**

Banda	Tiempo de Respuesta Nstreme (ms)	Tiempo de Respuesta Nv2 (ms)
5GHz a/n	233,6	80,6
5GHz only n	347,4	55,6
5GHz only a	278	51,6



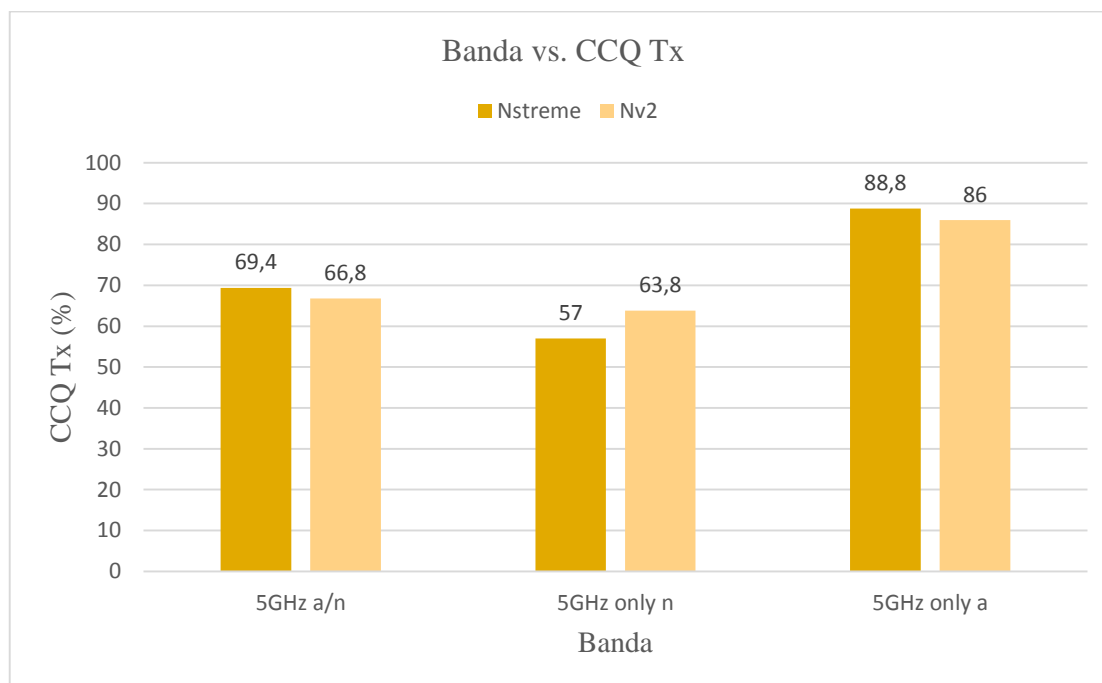
**Figura 219. Banda vs. Tiempo de Respuesta a 5.8GHz**

En la banda 5GHz a/n y 5GHz only a se muestra que el CCQ Tx es levemente mayor al utilizar el protocolo Nstreme mientras que en la banda de 5GHz only n el CCQ Tx es mayor al utilizar Nv2. La figura 220 muestra que el mayor CCQ Tx (88.8%) se ubica con el protocolo Nstreme en la banda 5GHz only a; por el contrario, el menor CCQ Tx (57%) está en la banda 5GHz only n con el protocolo Nstreme.

**Tabla 35.**

**Banda vs. CCQ Tx a 5.8GHz**

Banda	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
5GHz a/n	69,4	66,8
5GHz only n	57	63,8
5GHz only a	88,8	86



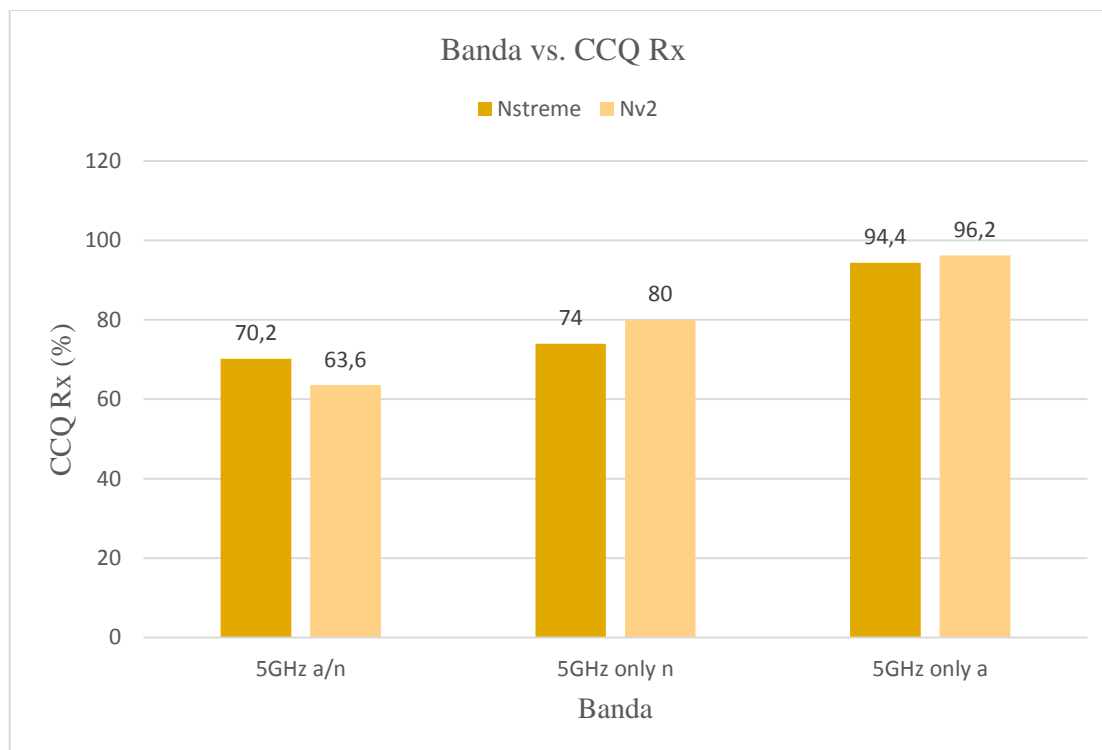
**Figura 220. Banda vs. CCQ Tx a 5.8GHz**

Con el protocolo Nv2 se observa que hay un mayor CCQ Rx en las bandas 5GHz only n y 5GHz only a mientras que en la banda de 5GHz a/n el CCQ Rx es mayor con el protocolo Nstreme. El mayor CCQ Rx (96.2%) se registra en el protocolo Nv2 en 5GHz only a; mientras que el menor se localiza en la banda 5GHz a/n con Nv2

**Tabla 36.**

**Banda vs. CCQ Rx a 5.8GHz**

Banda	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
5GHz a/n	70,2	63,6
5GHz only n	74	80
5GHz only a	94,4	96,2



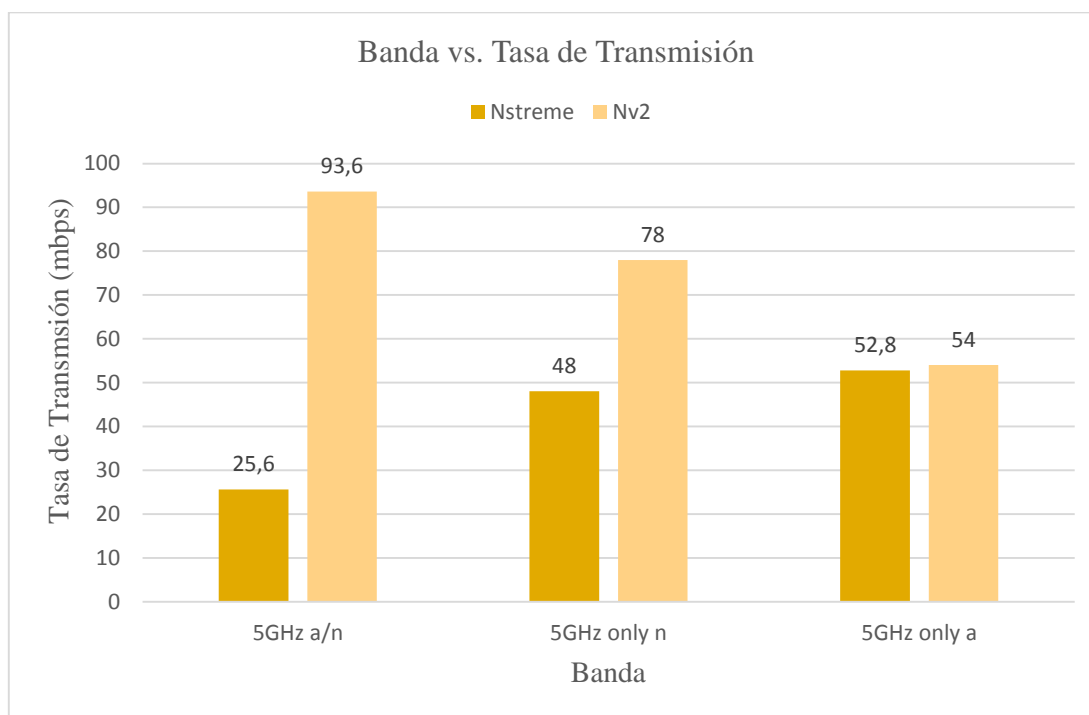
**Figura 221. Banda vs. CCQ Rx a 5.8GHz**

En la figura 222 se observa que la tasa de transmisión es superior en todas las bandas de 5GHz con Nv2 en relación con Nstreme. La mayor tasa de transmisión (93.6 mbps) se encuentra en la banda 5GHz a/n con Nv2 y la menor (25.6 mbps) se ubica en el protocolo Nstreme en la banda 5GHz a/n

**Tabla 37.**

**Banda vs. Tasa de Transmisión a 5.8GHz**

Banda	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
5GHz a/n	25,6	93,6
5GHz only n	48	78
5GHz only a	52,8	54



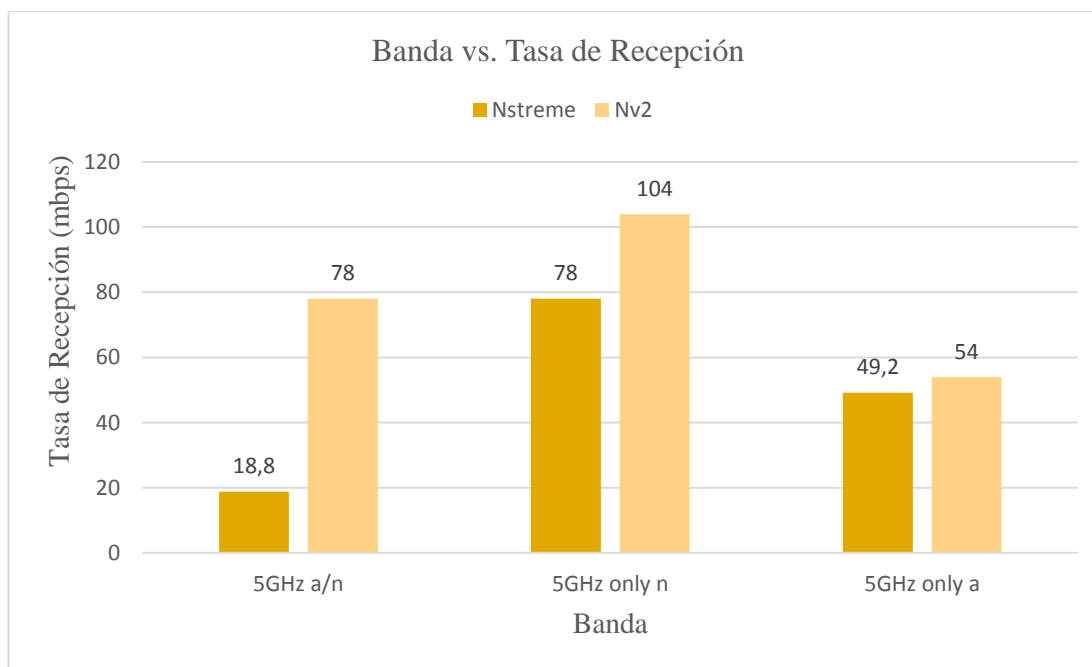
**Figura 222. Banda vs. Tasa de Transmisión a 5.8GHz**

En la figura 223 se observa que la tasa de recepción con Nv2 es mayor en relación a Nstreme. La mayor tasa de recepción (104 mbps) se encuentra en la banda 5GHz only n con el protocolo Nv2; por lo contrario la menor tasa de recepción (18.8 mbps) está en la banda 5GHz a/n con el protocolo Nstreme

**Tabla 38.**

**Banda vs. Tasa de Recepción a 5.8GHz**

Banda	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
5GHz a/n	18,8	78
5GHz only n	78	104
5GHz only a	49,2	54



**Figura 223. Banda vs. Tasa de Recepción a 5.8GHz**



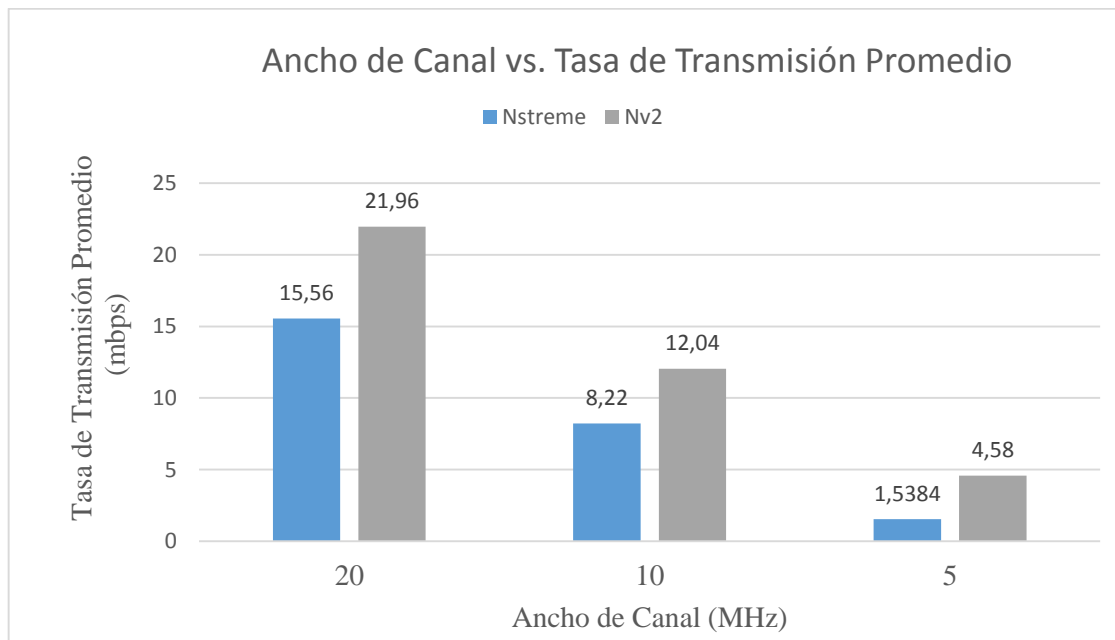
### 5.2.2 Análisis de resultados para el enlace a 5.8 GHz variando en ancho de canal

Como se puede observar en la figura 224; en el enlace de 5GHz variando el ancho de canal se obtiene una mayor tasa de transmisión promedio usando el protocolo Nv2 con respecto a Nstreme. La mayor tasa de transmisión promedio (21.96 mbps) se obtuvo con el protocolo Nv2 a un ancho de canal de 20 MHz; por el contrario; la menor tasa de transmisión se ubica en el ancho de canal de 5MHz con Nstreme.

**Tabla 39.**

**Ancho de Canal vs. Tasa de Transmisión Promedio a 5.8GHz**

Ancho de canal	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
20	15,56	21,96
10	8,22	12,04
5	1,5384	4,58



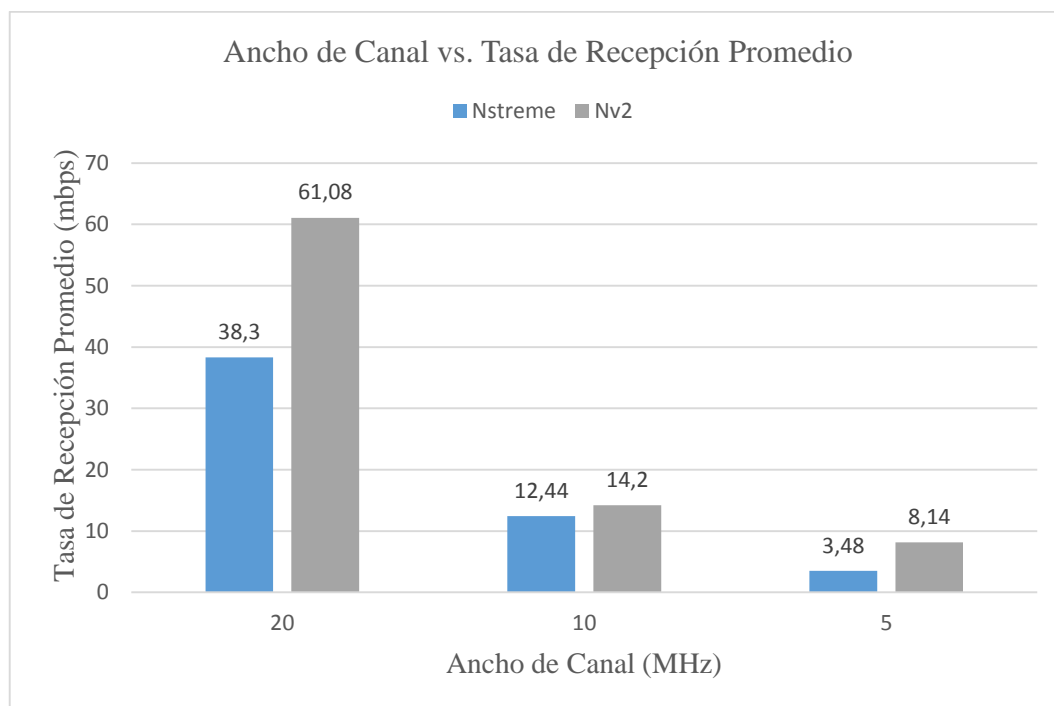
**Figura 224. Ancho de Canal vs. Tasa de Transmisión Promedio a 5.8GHz**

En la figura 225 se muestra que la tasa de recepción promedio en el ancho de canal de 20MHz con Nv2 es muy superior a Nstreme mientras que en 10 MHz y 5 MHz la tasa de recepción promedio es levemente superior con Nv2. La mayor tasa de recepción promedio (61.08 mbps) se ubica en el ancho de canal de 20Mhz con Nv2; mientras que la menor tasa (3.48 mbps) se encuentra a los 5MHz con Nstreme

**Tabla 40.**

**Ancho de Canal vs. Tasa de Recepción Promedio a 5.8GHz**

Ancho de canal	Tasa de Recepción Promedio Nstreme(mbps)	Tasa de Recepción Nv2 (mbps)
20	38,3	61,08
10	12,44	14,2
5	3,48	8,14



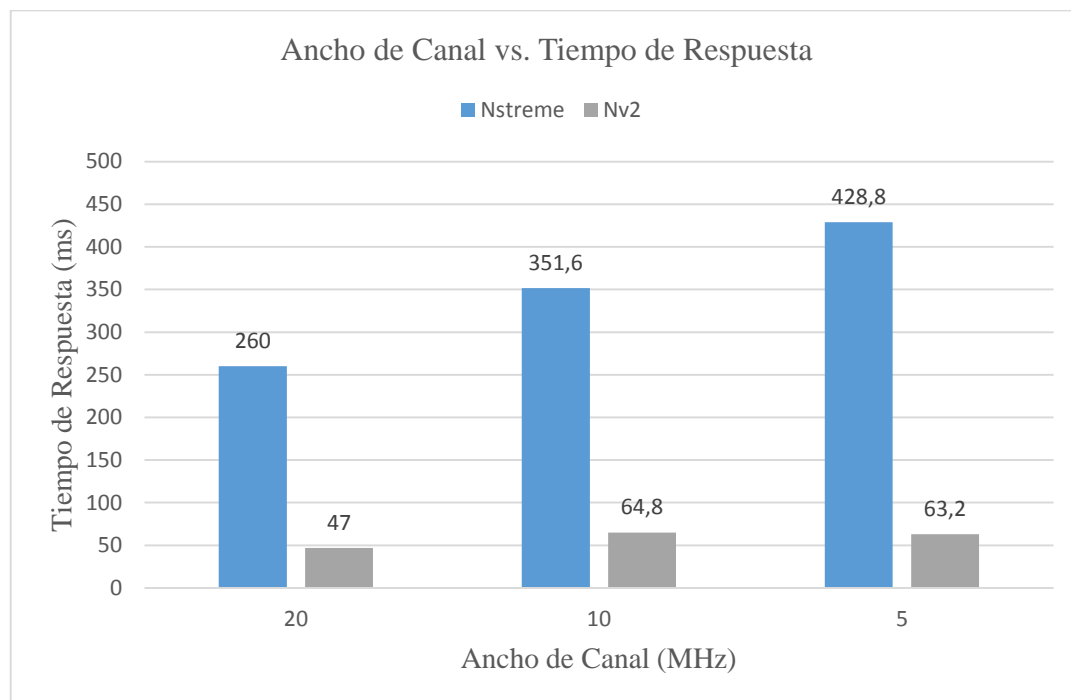
**Figura 225. Ancho de Canal vs. Tasa de Recepción Promedio a 5.8GHz**

En la figura 226 se puede observar que al utilizar el protocolo Nv2 los tiempos de respuesta bajan considerablemente en relación a los tiempos de Nstreme. El mejor tiempo de respuesta (47 ms) se obtuvo con un ancho de canal a 20MHz con Nv2 y el mayor tiempo (428.8 ms) se encuentra en los 5Mhz de ancho de canal con Nstreme.

**Tabla 41.**

**Ancho de Canal vs. Tiempo de Respuesta a 5.8GHz**

Ancho de canal	Tiempo de Respuesta Nstreme (ms)	Tiempo de Respuesta Nv2 (ms)
20	260	47
10	351,6	64,8
5	428,8	63,2



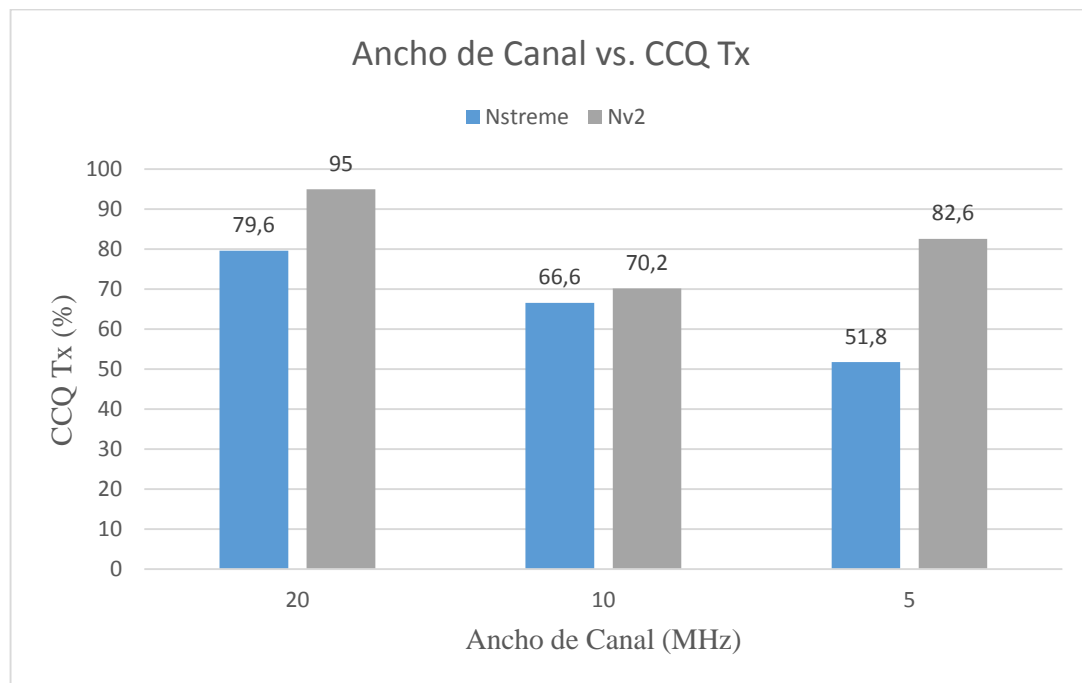
**Figura 226. Ancho de Canal vs. Tiempo de Respuesta a 5.8GHz**

En la figura 227 se observa que con un ancho de canal a 20MHz con el protocolo Nstreme tenemos un 79% de CCQ Tx mientras que con Nv2 obtenemos un mejor CCQ con un 95% de transmisión; en el ancho de canal de 10MHz se tiene un 66.6% con Nstreme y un 70.2% con Nv2 y por ultimo con 5MHz se observa un 51.8% con Nstreme y un 82.6% con Nv2.

**Tabla 42.**

**Ancho de Canal vs. CCQ Tx a 5.8GHz**

Ancho de canal	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
20	79,6	95
10	66,6	70,2
5	51,8	82,6



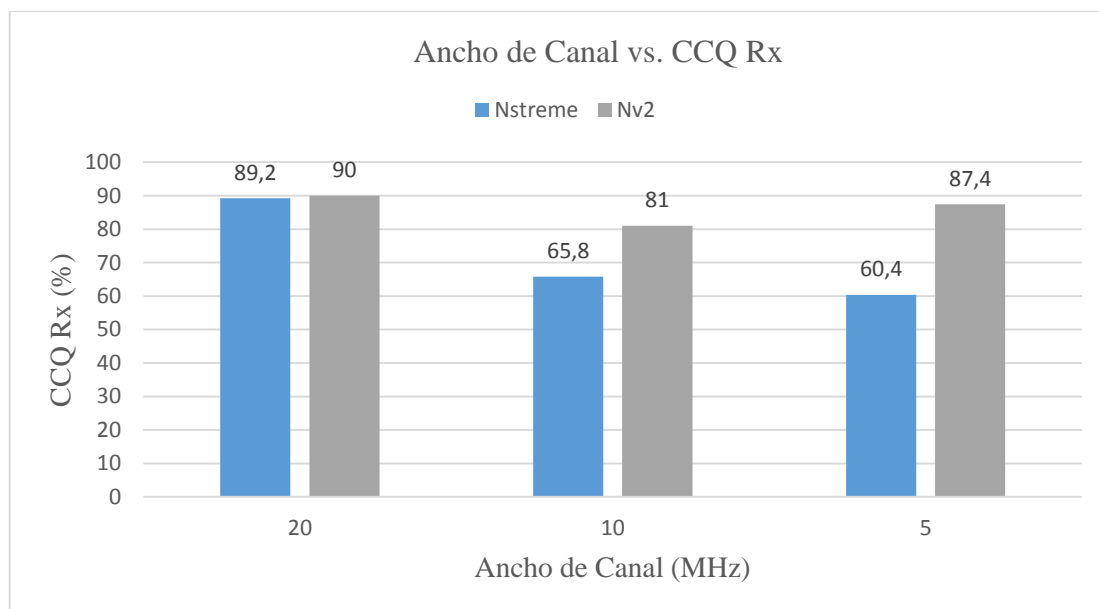
**Figura 227. Ancho de Canal vs. CCQ Tx a 5.8GHz**

En la figura 228 se observa que con un ancho de canal de 20MHz con el protocolo Nstreme se tiene un 89.2% de CCQ Rx mientras que con Nv2 se obtiene un mejor CCQ Rx con un 90% de recepción, en el ancho de canal de 10MHz hay un 65.8% con Nstreme y un 81% con Nv2 y por ultimo con 5MHz se observa un 60.4% con Nstreme y un 87.4% con Nv2.

**Tabla 43.**

**Ancho de Canal vs. CCQ Rx a 5.8GHz**

Ancho de canal	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
20	89,2	90
10	65,8	81
5	60,4	87,4



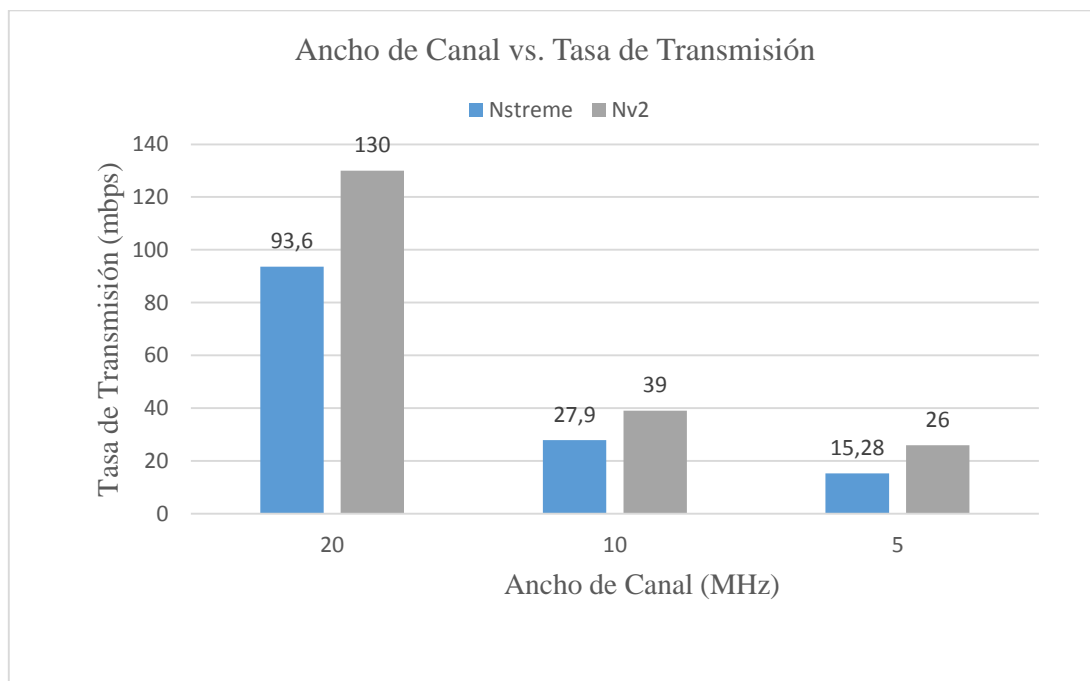
**Figura 228. Ancho de Canal vs. CCQ Rx a 5.8GHz**

En la figura 229 se observa que la tasa de transmisión es mucho mayor con Nv2 en relación a Nstreme. La mayor tasa de transmisión (130 mbps) se obtuvo con Nv2 en un ancho de canal de 20MHz; a diferencia que con el protocolo Nstreme a 5MHz se registra la menor tasa de transmisión (15.28 mbps)

**Tabla 44.**

**Ancho de Canal vs. Tasa de Transmisión a 5.8GHz**

Ancho de canal	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
20	93,6	130
10	27,9	39
5	15,28	26



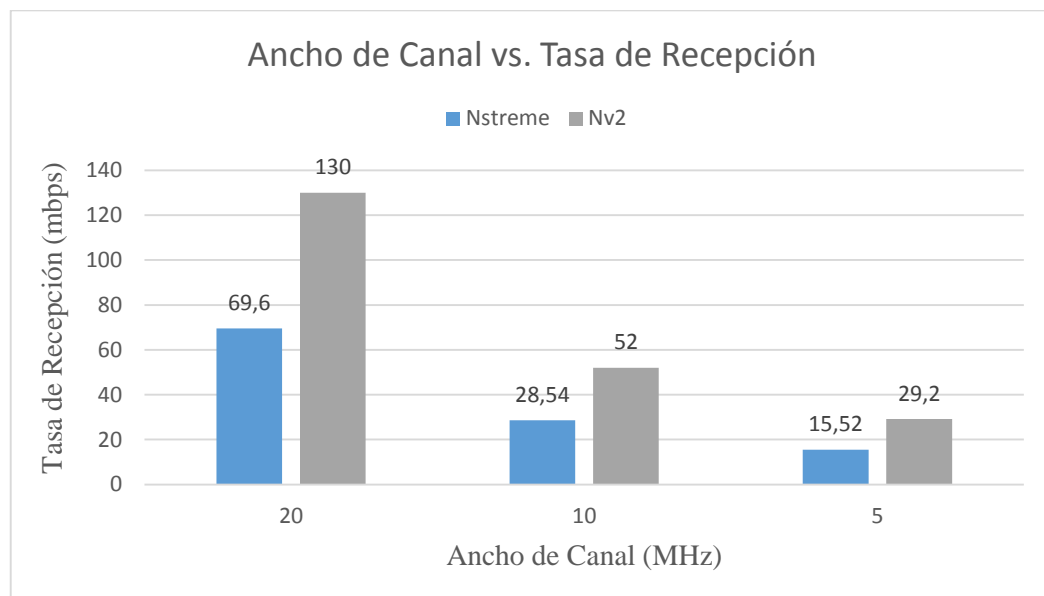
**Figura 229. Ancho de Canal vs. Tasa de Transmisión a 5.8GHz**

Al igual que con la tasa de transmisión, en la figura 230 se observa que la tasa de recepción usando el protocolo Nv2 es superior al protocolo Nstreme. La mayor tasa de recepción (130 mbps) se localiza a 20MHz con Nv2; y la menor tasa (15.52 mbps) se ubica en 5Mhz de ancho de canal con Nstreme

**Tabla 45.**

**Ancho de Canal vs. Tasa de Recepción a 5.8GHz**

Ancho de canal	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
20	69,6	130
10	28,54	52
5	15,52	29,2



**Figura 230. Ancho de Canal vs. Tasa de Recepción a 5.8GHz**

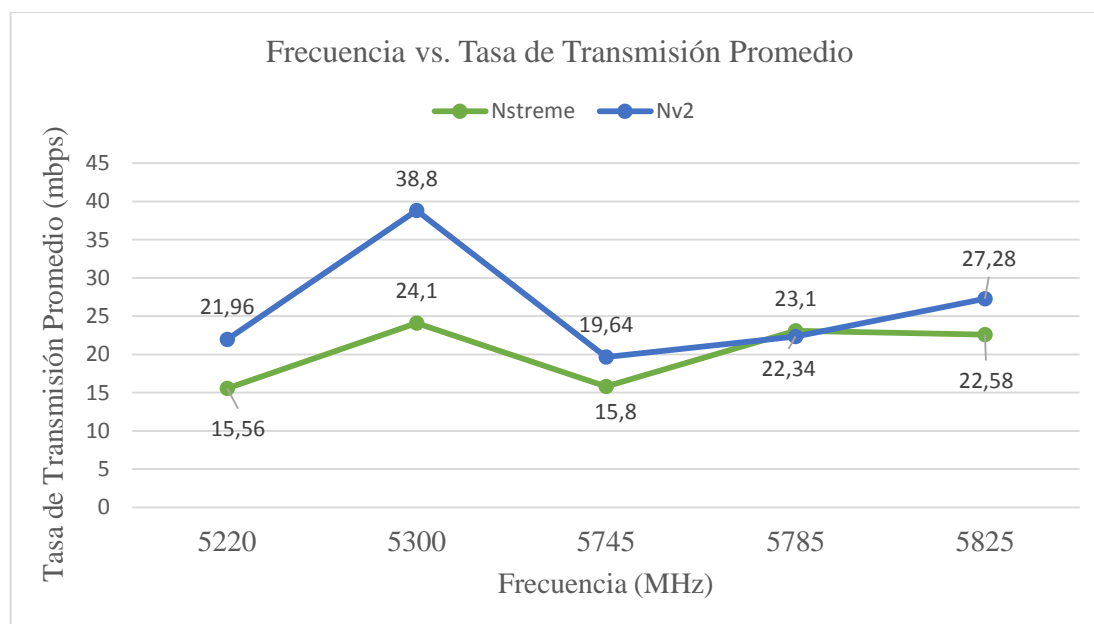
### 5.2.3 Análisis de resultados para el enlace a 5.8 GHz variando la frecuencia

En la figura 231 se puede observar que la tasa de transmisión promedio en todas las frecuencias de 5.8GHz es mayor utilizando el protocolo NV2 en relación al protocolo. La mayor tasa de transmisión (38.8 mbps) se registra en la frecuencia de 5300MHz con Nv2, mientras que la menor tasa (15.56 mbps) se ubica con el protocolo Nstreme en la frecuencia 5220MHz

**Tabla 46.**

**Frecuencia vs. Tasa de Transmisión a 5.8GHz**

Frecuencia	Tasa de Transmisión Promedio Nstreme (mbps)	Tasa de Transmisión Promedio Nv2 (mbps)
5220	15,56	21,96
5300	24,1	38,8
5745	15,8	19,64
5785	23,1	22,34
5825	22,58	27,28



**Figura 231. Frecuencia vs. Tasa de Transmisión Promedio a 5.8Ghz**

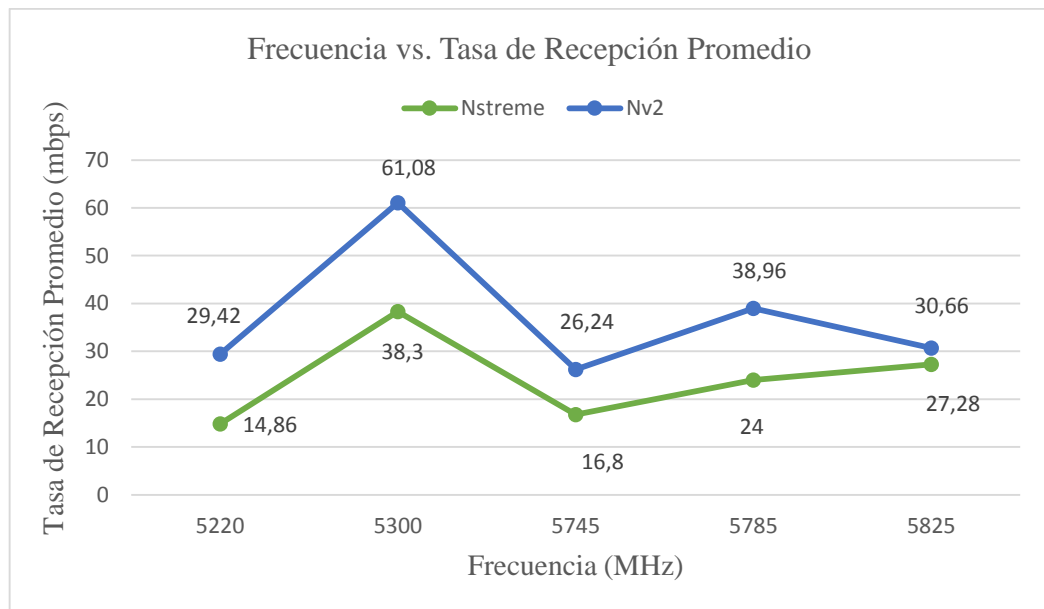


En esta figura se muestra que la tasa de recepción promedio utilizando el protocolo Nv2 es mucho mejor en todas las frecuencias a diferencia del protocolo Nstreme que su tasa de recepción no es muy buena. La mejor tasa de recepción (61.08 mbps) se obtuvo con Nv2 en la frecuencia 5300MHz, mientras que la menor (14.86 mbps) se encuentra en la frecuencia 5220MHz.

**Tabla 47.**

**Frecuencia vs. Tasa de Recepción Promedio a 5.8GHz**

Frecuencia	Tasa de Recepción Promedio Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
5220	14,86	29,42
5300	38,3	61,08
5745	16,8	26,24
5785	24	38,96
5825	27,28	30,66



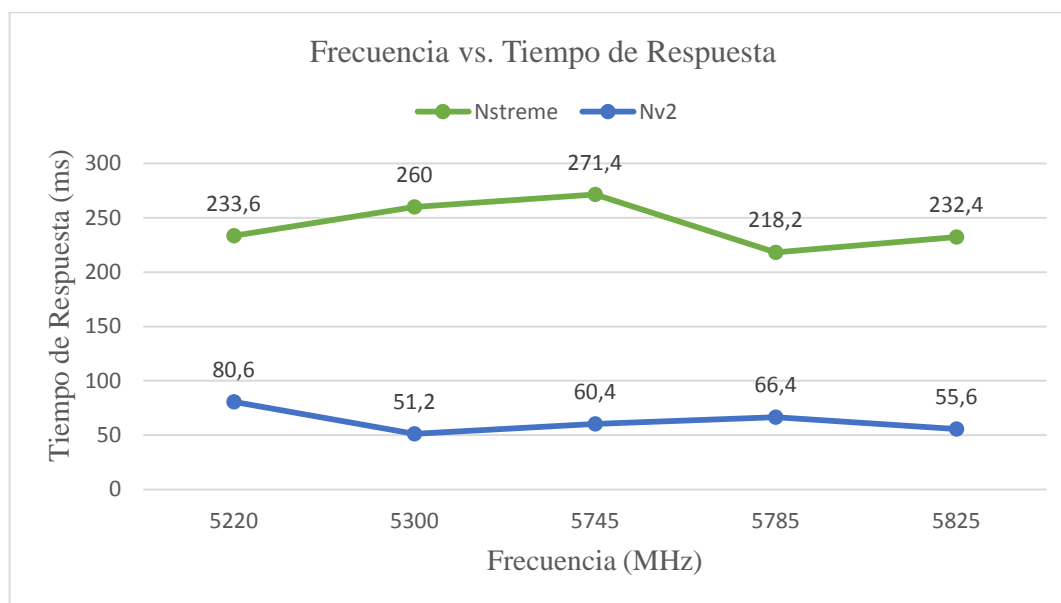
**Figura 232. Frecuencia vs. Tasa de Recepción a 5.8GHz**

En la figura 233 se puede apreciar que el tiempo de respuesta con el protocolo Nv2 en cada una de las frecuencias mencionadas es mucho mejor que con el protocolo Nstreme con el cual se obtuvo un tiempo de respuesta es muy deficiente. El mejor tiempo de respuesta (51.2 ms) se obtuvo en la frecuencia 5825 MHz con Nv2; mientras tanto que el peor tiempo (271.4 ms) obtenido se localiza en Nstreme a 5745 MHz.

**Tabla 48.**

**Frecuencia vs. Tiempo de Respuesta a 5.8GHz**

Frecuencia	Tiempo de Respuesta Nstreme (ms)	Tiempo de Respuesta Nv2 (ms)
5220	233,6	80,6
5300	260	51,2
5745	271,4	60,4
5785	218,2	66,4
5825	232,4	55,6



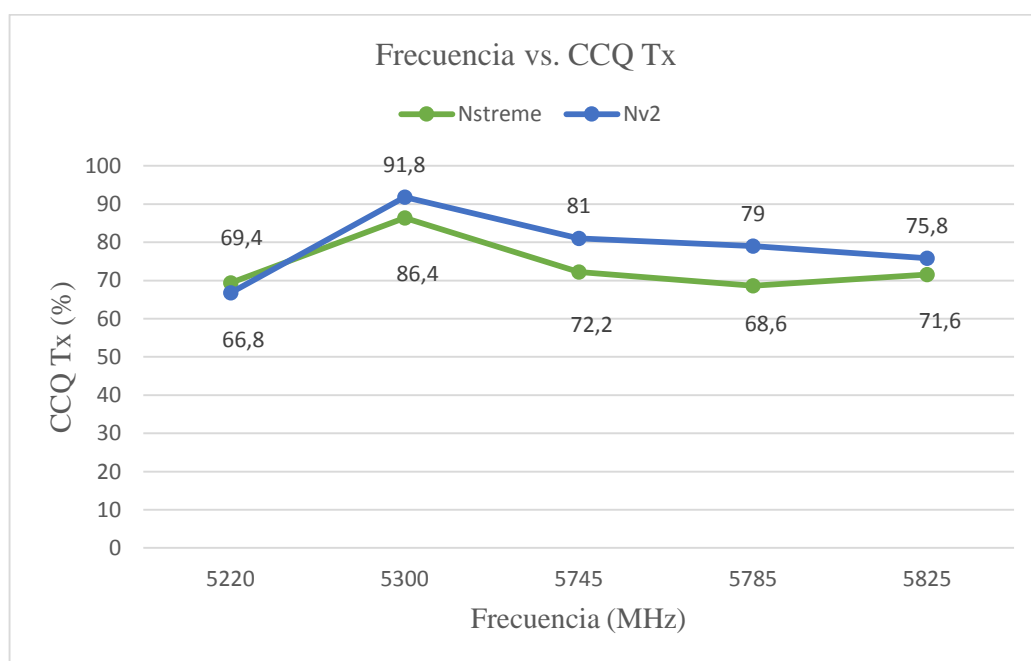
**Figura 233. Frecuencia vs. Tiempo de Respuesta a 5.8GHz**

Como se puede observar en la figura 234 en la frecuencia 5220MHz el CCQ Tx de transmisión con Nstreme es ligeramente mayor a Nv2, pero también se puede apreciar que en las demás frecuencias el CCQ de transmisión es levemente superior con Nv2. EL mayor CCQ Tx (91.8%) se encuentra con Nv2 a una frecuencia de 5300Mhz; por el contrario, le menor CCQ de transmisión (66.8%) está en la frecuencia 5220MHz con Nv2

**Tabla 49.**

**Frecuencia vs. CCQ Tx A 5.8GHz**

Frecuencia	CCQ Tx Nstreme (%)	CCQ Tx Nv2 (%)
5220	69,4	66,8
5300	86,4	91,8
5745	72,2	81
5785	68,6	79
5825	71,6	75,8



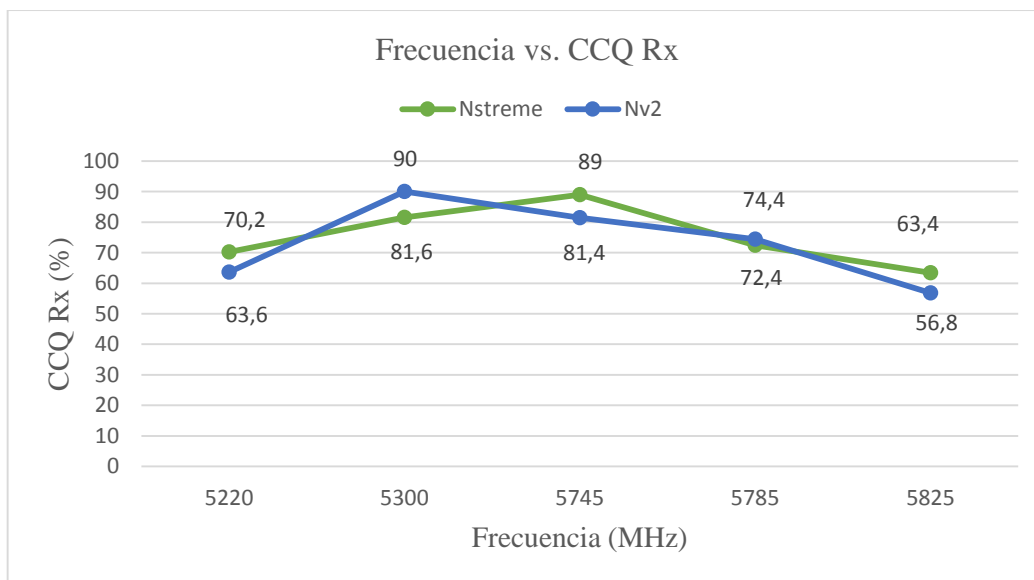
**Figura 234. Frecuencia vs. CCQ Tx a 5.8GHz**

Como se puede observar en la figura 235, en las frecuencias 5220MHz, 5745MHz y 5825MHz el CCQ de recepción es mayor utilizando el protocolo Nstreme que con el protocolo NV2. Además en las frecuencias 5300MHz y 5785MHz el CCQ de recepción es mayor con el protocolo Nv2 en relación a Nstreme. El mejor CCQ Rx (90%) se encuentra en la frecuencia 5300Mhz con Nv2, mientras que la menor calidad de enlace (56.8%) se ubica a 5825MHz con Nv2

**Tabla 50.**

**Frecuencia vs. CCQ Rx a 5.8GHz**

Frecuencia	CCQ Rx Nstreme (%)	CCQ Rx Nv2 (%)
5220	70,2	63,6
5300	81,6	90
5745	89	81,4
5785	72,4	74,4
5825	63,4	56,8



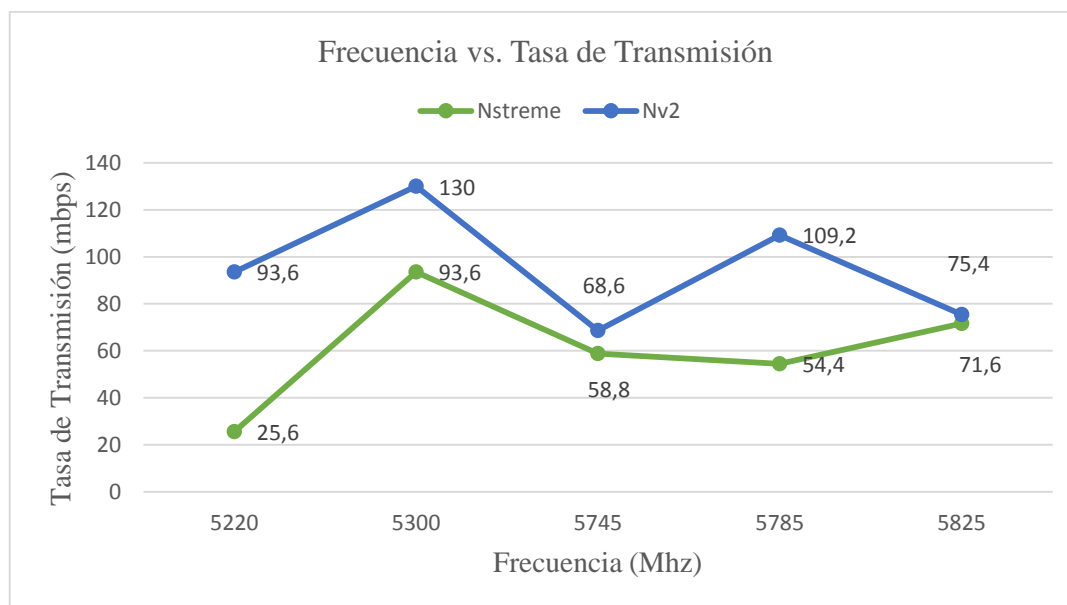
**Figura 235. Frecuencia vs. CCQ Rx a 5.8Ghz**

En la figura 236 se aprecia que la tasa de transmisión con el protocolo Nv2 es mayor para cada una de las frecuencias con relación a la tasa de transmisión con Nstreme. La mayor tasa de transmisión (130 mbps) se localiza en la frecuencia de 5300MHz con Nv2; y la menor tasa (25.6 mbps) se encuentra en el protocolo Nstreme a 5220Mhz.

**Tabla 51.**

**Frecuencia vs. Tasa de Transmisión a 5.8GHz**

Frecuencia	Tasa de Transmisión Nstreme (mbps)	Tasa de Transmisión Nv2 (mbps)
5220	25,6	93,6
5300	93,6	130
5745	58,8	68,6
5785	54,4	109,2
5825	71,6	75,4



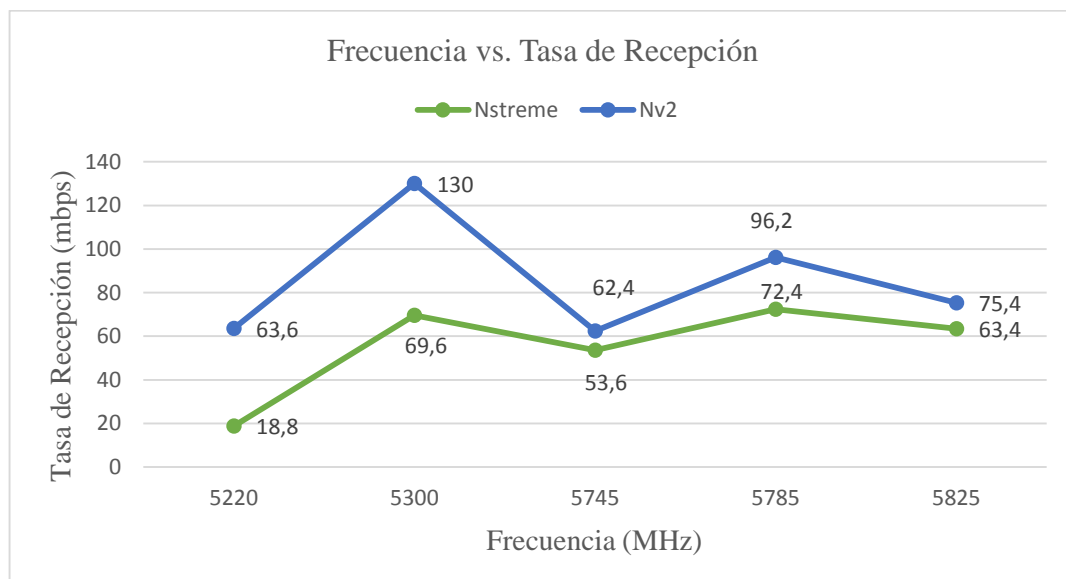
**Figura 236. Frecuencia vs. Tasa de Transmisión a 5.8GHz**

La figura se 237 muestra que al utilizar el protocolo Nv2 la tasa de recepción es mucho mayor que al utilizar el protocolo Nstreme. La mayor tasa de recepción (130 mbps) se encuentra en la frecuencia 5300Mhz con Nv2; la menor tasa (18.8 mbps) se localiza a 5220MHz con Nstreme

**Tabla 52.**

**Frecuencia vs. Tasa de Recepción a 5.8GHz**

Frecuencia	Tasa de Recepción Nstreme (mbps)	Tasa de Recepción Nv2 (mbps)
5220	18,8	63,6
5300	69,6	130
5745	53,6	62,4
5785	72,4	96,2
5825	63,4	75,4



**Figura 237. Frecuencia vs. Tasa de Recepción a 5.8GHz**

## CAPITULO VI

### CONCLUSIONES Y RECOMENDACIONES

#### 6.1 Conclusiones

A través de la implementación de un enlace inalámbrico de aproximadamente 10 kilómetros de distancia entre la estación ubicada en la Universidad de las Fuerzas Armadas-ESPE y la que se encuentra en el sector de AMAGUAÑA se pudo realizar un estudio comparativo de la tasa de transmisión y recepción, CCQ y tiempo de respuesta entre los protocolos inalámbricos Nstreme y Nv2.

Con el ancho de canal de 20MHz se obtuvo un mejor rendimiento en el enlace inalámbrico al momento de transmitir voz sobre IP, video y datos por medio de VSFTP, SMB y NFS; debido a que cuanto más ancho sea el canal, mayor tráfico de datos podrá circular.

Con el protocolo Nv2 se obtuvieron mejores tiempos de respuesta con relación a los obtenidos con Nstreme, en el enlace inalámbrico a 2.4GHz y 5.8Ghz, debido a que Nv2 posee un pequeño encabezado de trama, por lo que el tiempo de procesamiento se reduce lo que limita el tiempo de respuesta.

Se verifico con Btest que con Nv2 se obtiene una mayor tasa de transmisión debido a que este protocolo envía, por medio de broadcast, la agenda de transmisión, por lo que a diferencia del protocolo Nstreme no posee un encabezado de polling, dejando más tiempo para la transmisión de datos reales y mejorando el rendimiento.

Con los protocolos Nstreme y Nv2 se obtuvo valores de CCQ, tanto de transmisión como de recepción, similares, debido a que este parámetro indica la estabilidad del enlace inalámbrico porque realiza una comparativa entre la tasa de transmisión teórica y la real; por lo que depende en gran medida de las condiciones climáticas en las que se encuentra funcionando el enlace.

Uno de los parámetros de mayor influencia en el rendimiento de un enlace inalámbrico es la frecuencia en la que se transmite los datos. Debido a que 2.4GHz y 5.8GHz se encuentran dentro las bandas no licenciadas destinadas a la industria, medicina e investigación; estas son utilizadas indiscriminadamente dentro del campo de las telecomunicaciones, haciendo que muchas de estas frecuencias se encuentran demasiado saturadas, por lo que es necesario realizar un estudio minucioso sobre la frecuencia que se va a utilizar, porque de esto depende en gran medida el rendimiento del enlace inalámbrico.

Si bien es cierto que Nv2 y Nstreme poseen varias ventajas con relación a los protocolos que utilizan el método de acceso al medio CSMA/CA, como la eliminación del nodo oculto o el control dinámico de los slots de tiempo por parte del AP, estos protocolos al ser propietarios de Mikrotik no pueden coexistir con otros, haciendo que infraestructuras de este tipo sean poco escalables.

Con la implementación de servidores de datos, central de voz sobre IP y la transmisión de video a través de internet se puede comprobar que si es factible la implantación de una red inalámbrica convergente con estos protocolos, debido a que el ancho de banda obtenido en cada uno de los enlaces es el necesario para la implementación de estos servicios.

Gracias a las pruebas realizadas, tanto en el enlace de 2.4GHz como de 5.8GHz se puede concluir que a menor ancho de canal menor tasa de transferencia, mayor tiempo de respuesta, y mayor CCQ, esto debido a que si el ancho de canal disminuye, la cantidad de ondas portadoras de información también disminuyen haciendo que se necesite mayor cantidad de tiempo para transmisión de un determinado paquete, pero aumentando la estabilidad y disminuyendo la interferencia.

Utilizando diferentes herramientas de gestión de redes que se basan en el protocolo SNMP se puede tener visibilidad y control completo sobre toda la infraestructura de la red; esto incluyen: verificación del funcionamiento de routers, servidores, y dispositivos de usuario final; y sobretodo, monitorización del tráfico que fluyen en toda la red, en



especial en el enlace inalámbrico, con lo que se puede tener un criterio para realizar diferentes modificaciones en la configuración de los equipos con el fin de mejorar el rendimiento de la red en general.

El rendimiento de un enlace inalámbrico no solo depende de factores lógicos como el ancho de canal, banda de frecuencia, protocolo, etc; sino también de las condiciones atmosféricas y climáticas en las que esté funcionando el enlace; entre los factores que mayor perjuicio producen a un enlace inalámbrico se encuentra el viento, la lluvia y la niebla.

## **6.2 Recomendaciones**

Al momento de la implementación de un enlace inalámbrico con dispositivos Mikrotik se recomienda utilizar la opción de banda compartida (2.4Ghz a/b/n o 5GHz b/n) cuando no se conoce con exactitud el tipo de dispositivo con el que se va a conectar; caso contrario, es necesario configurar una banda en específico ya que de esta manera se ahorra capacidad de procesamiento de los equipos.

Se debe realizar una correcta instalación de los equipos que se utilizan para la implementación de enlaces inalámbricos, especialmente los que no están destinados a exteriores porque los factores climáticos no solo pueden afectar en su rendimiento sino también dañarlos definitivamente. Para esto se recomienda utilizar cajas metálicas para exteriores.

Para mejorar el rendimiento del enlace inalámbrico se debe utilizar cable FTP categoría 6a, especialmente en estaciones que tengan varias antenas trabajando en las mismas frecuencias, debido a que este tipo de cable posee un aislamiento de papel aluminio en cada uno de los pares trenzados, evitando de esta manera la interferencia que se pueda producir por las otras antenas.

Para comprobar los parámetros de diseño del enlace inalámbrico en el presente proyecto, se recomienda la utilización de PTP Link Planner u otro software que permita diseñar redes inalámbricas de cualquier tamaño y complejidad de manera sencilla, para

poder elegir con mayor facilidad las características de los equipos y no tener problemas a la hora de realizar las pruebas de rendimiento.

Es recomendable realizar una comparativa entre los datos reales y los datos teóricos sobre este tipo de enlace, para tener una referencia en base a aspectos técnicos y a la vez, si el enlace es adecuado para el estudio de los protocolos.

Para realizar la comparación entre los protocolos Nstreme y Nv2 se recomienda hacerlo en condiciones atmosféricas estables y además donde no existan muchos equipos, ya que esto produce una alta interferencia y esto hace que al momento de tomar datos estos varíen mucho, dando como resultado valores erróneos.

Para la obtención de datos al utilizar los equipos Mikrotik se debe tener en cuenta que al momento de realizar cualquier cambio en la configuración primero se lo debe hacer en el equipo que este configurado con AP bridge y después en el equipo station bridge, para evitar caídas en el enlace y se pierda la conectividad entre las dos estaciones.

Otro aspecto que hay que tener en cuenta que al momento de usar la herramienta Usage Frequency el enlace deja de funcionar mientras se la está usando, además se debe elegir las frecuencias que estén menos saturadas para poder obtener los datos de manera correcta y no tener datos erróneos.

## REFERENCIAS BIBLIOGRÁFICAS

- Acevedo, G. (14 de enero de 2012). *Fundamentos de la Informática*.
- Ahmad, A. (2005). *Wireless and Mobile Data Networks*. Canada: Wiley-Interscience.
- ALEGSA. (09 de octubre de 2009). *Diccionario de Informática y Tecnología*. Obtenido de <http://www.alegsa.com.ar/Dic/tdma.php>
- Anrrango, R. (15 de enero de 2011). *Configurar Mikrotik Wireless*. Recuperado el 11 de enero de 2015, de <http://configurarmikrotikwireless.com/blog/configurar-mikrotik-wireless-nstreme.html>
- Aquino, R. H. (9 de mayo de 2008). *Universidad de las Americas Puebla*. Obtenido de [http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/lem/hernandez\\_a\\_r/capitulo2.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/hernandez_a_r/capitulo2.pdf)
- Armijos, J. L. (marzo de 2011). *Soluciones para GNU/Linux*. Obtenido de <http://jorgearmijo-linux.blogspot.com/>
- Cardama Aznar, A., Roca, L. J., Rius Casals, J. M., Robert, J. R., Blanch, S., & Bataller, M. F. (2004). *Antenas*. Barcelona, España: Alfaomega.
- Cernevskis, U. (2010). *New Wireless Features on RouterOS v5*. Recuperado el 11 de enero de 2015, de <http://wiki.mikrotik.com/images/6/62/Uldis.pdf>
- Clep, M. (2008). *MKE Solutions*. Recuperado el 2015 de enero de 13, de <http://www.mkesolutions.net/articulos/conceptos/el-protocolo-nv2-nstreme-ver-2/>
- CyberService. (2013). *OverService*. Obtenido de [www.cyberservice.net](http://www.cyberservice.net)
- Dueñas, J. B. (2015). *Alcance Libre*. Obtenido de <http://www.alcance Libre.org/>
- Glisic, S. (2007). *Advanced Wireless Communication*. Chichester, Inglaterra: John Wiley & Sons, Ltd.

- Mikrotik. (25 de abril de 2008). *Enlaces Inalambricos con RouterOS*. Recuperado el 18 de enero de 2015, de [http://wiki.mikrotik.com/wiki/Enlaces\\_Inal%C3%A1mbricos\\_con\\_RouterOS](http://wiki.mikrotik.com/wiki/Enlaces_Inal%C3%A1mbricos_con_RouterOS)
- Mikrotik. (27 de Diciembre de 2010). *Mikrotik documentation*. Obtenido de [http://wiki.mikrotik.com/wiki/Nv2\\_spanish](http://wiki.mikrotik.com/wiki/Nv2_spanish)
- Mikrotik. (2013). *Mikrotik Routers & Wireless*. Recuperado el 09 de enero de 2015, de <http://www.mikrotik.com/aboutus>
- Mikrotik documentations. (27 de diciembre de 2010). *Nv2\_spanish*. Recuperado el 09 de 01 de 2015, de [http://wiki.mikrotik.com/wiki/Nv2\\_spanish](http://wiki.mikrotik.com/wiki/Nv2_spanish)
- Mikrotik, C. (2012). *Product Catalog Q1-Q2 2012*. Latvia.
- Molish, A. (2005). *Wireless Communications*. Chichester, Inglaterra: John Wiley & Sons, Ltd.
- Mundo Teleco. (4 de octubre de 2014). Obtenido de <http://mundotelecomunicaciones1.blogspot.com/2014/10/zona-de-fresnel.html>
- Nichols, R., & Lekkas, P. (2003). *Seguridad para comunicaciones inalambricas* (Vol. 1). Madrid, España: Mc Graw Hill.
- Niebert, N., Schieder, A., Zander, J., & Hancock, R. (2007). *Ambient Networks*. Chichester, Inglaterra: John Wiley & Sons, Ltd.
- Pahlavan, K., & Levesque, A. (2005). *Wireless Information Networks* (Vol. 2). New Jersey, Estados Unidos: Wiley-Interscience.
- Romero Kanashiro, W. R. (2013). *Redes Inalambricas y simulacion de WLAN mediante OPNET*. Recuperado el 11 de enero de 2015, de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18261/8/wromeroPFC0113memoria.pdf>
- RouterBoard. (2015). *Mikrotik*. Obtenido de <http://routerboard.com/>

- Sedin Escalona, A. (2004). *Fundamentos de los sistemas de comunicaciones móviles*. Madrid, España: Mc Graw Hill.
- Tafazolli, R. (2005). *Technologies for the Wireless Future*. Chichester, Inglaterra: John Wiley & Sons, Ltd.
- Tanenbaum, A. (2003). *Redes de Computadoras*. Amsterdam: Pearson.
- Tomasi, W. (2003). *Sistema de Comunicaciones Electronicas*. Naucalpan de Juarez: Pearson Educación.
- Universidad de Navarra. (17 de Junio de 2013). *CSMA/CA*. Obtenido de [https://www.tlm.unavarra.es/~daniel/docencia/arss/arss11\\_12/slides/34-CSMA-CA.pdf](https://www.tlm.unavarra.es/~daniel/docencia/arss/arss11_12/slides/34-CSMA-CA.pdf)
- Universidad Politecnica de Valencia. (2 de diciembre de 2010). *Historia de la Informatica*. Recuperado el 09 de Enero de 2015, de <http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/>
- Walke, B., Mangold, S., & Berlemann, L. (2006). *IEEE 802 Wireless Systems*. Chichester, England: John Wiley & Sons, Ltd.
- Waterhouse, R. (2007). *Printed Antennas for Wireless Communications*. Maryland, Estados Unidos: John Wiley & Sons, Ltd.
- Yu-Kwong, R. K., & Lau, V. (2007). *Wireless Internet and Mobile Computing*. New Jersey, Estados Unidos: Wiley-Interscience.