



REPÚBLICA DEL ECUADOR

# Escuela Politécnica Nacional

"SCIENTIA HOMINIS SALUS"

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

***Respeto hacia sí mismo y hacia los demás.***

# **ESCUELA POLITÉCNICA NACIONAL**

## **FACULTAD DE INGENIERIA ELÉCTRICA Y ELECTRÓNICA**

**IMPLEMENTACIÓN DE TÉCNICAS DE CALIDAD DE SERVICIO  
(QoS) EN UN PROTOTIPO DE RED CONVERGENTE DE DATOS,  
VIDEO Y TELEFONÍA USANDO IPv6 EN UNA EMPRESA PYME  
TIPO.**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE  
“INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN”**

**MARCOS ALFREDO VIRACUCHA PILOZO**

**marcos.viracucha@hotmail.com**

**DIRECTOR: MSc. Fabio Matías González González**

**fabio.gonzalez@epn.edu.ec**

**Quito, Junio 2019**

## **AVAL**

Certifico que el presente trabajo fue desarrollado por Marcos Alfredo Viracucha Piloza, bajo mi supervisión.

---

**MSc. Fabio Matías González González**  
**DIRECTOR DEL PROYECTO**

## **DECLARACIÓN DE AUTORÍA**

Yo, Marcos Alfredo Viracucha Pilozo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

**MARCOS ALFREDO VIRACUCHA PILOZO**

## **AGRADECIMIENTOS**

A Dios, por darme la fortaleza de seguir adelante cada día de mi vida, por darme la sabiduría para elegir siempre el camino correcto.

A mis padres Jaime y Ruth, por enseñarme a ser una persona humilde, ética y con ganas de superación, les debo todo lo que soy, gracias por todo, no me alcanzará la vida para agradecerles todo lo que han hecho por mí.

A mis profesores en especial a mi director Ing. Fabio González y el Ing. Pablo Hidalgo por apoyarme hasta las últimas circunstancias y poder obtener mi título, a mis amigos, que de una u otra manera me apoyaron para lograr culminar mi carrera.

A mi esposa que no me dejó vencer y fue un pilar fundamental para terminar mi tesis.

*Marcos*

## **DEDICATORIA**

Les dedico este trabajo de titulación a mis padres Jaime y Ruth que han sido y seguirán siendo mi apoyo incondicional, gracias a ellos por el esfuerzo y sacrificio que cada día hicieron para poder darme el estudio y obtener una carrera universitaria.

A la que ahora es mi familia, mi esposa Adriana y mi hijo Mathias que son las personas que día a día me inspiran a mejorar y seguir adelante para poder ofrecerles un futuro prometedor.

*Marcos*

# ÍNDICE GENERAL

AVAL	I
DECLARACIÓN DE AUTORÍA	II
AGRADECIMIENTOS	III
DEDICATORIA	IV
ÍNDICE GENERAL	V
ÍNDICE DE FIGURAS	IX
ÍNDICE DE TABLAS	XIII
RESUMEN	XV
ABSTRACT	XVII
CAPÍTULO 1	1
1 FUNDAMENTOS TEÓRICOS	1
1.1 OBJETIVOS	2
1.2 ALCANCE	2
1.3 MARCO TEÓRICO	4
1.3.1 REDES DE COMPUTADORAS	4
1.3.2 CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS	6
1.3.3 MEDIOS DE TRANSMISIÓN	6
1.4 SISTEMAS DE CABLEADO ESTRUCTURADO	11
1.4.1 VENTAJAS DEL CABLEADO ESTRUCTURADO	12
1.4.2 NORMAS DE CABLEADO ESTRUCTURADO	13
1.4.2.1 ANSI/TIA 568.1-D Estándar de Cableado de Telecomunicaciones para Edificios Comerciales	13
1.4.2.2 ANSI/TIA-569-D Rutas y Espacios para Telecomunicaciones	13
1.4.2.3 ANSI/TIA-606-C Estándar de Administración para Infraestructura de Telecomunicaciones	14
1.4.2.4 ANSI/TIA-607-C Uniones y Puestas a Tierra Genéricas de Telecomunicaciones para las Instalaciones del Cliente	14
1.5 IPv6	15
1.5.1 VOZ SOBRE IP (VoIP)	18
1.5.2 FUNCIONES Y COMPONENTES DE VoIP	18
1.5.3 CALIDAD DE SERVICIO (QoS)	19
1.5.4 ARQUITECTURA BÁSICA QoS	21

1.6	REDES CONVERGENTES _____	21
1.7	MODELOS DE QoS _____	22
1.8	ARQUITECTURA DE SERVICIOS INTEGRADOS (RFC1633) _____	23
1.9	ARQUITECTURA DE SERVICIOS DIFERENCIADOS (RFC 2475) _____	24
1.10	COMPARACIÓN ENTRE RFC 1633 Y RFC 2475 _____	26
CAPÍTULO 2 _____		27
2	ANÁLISIS DE REQUERIMIENTOS Y DISEÑO DE LA RED CONVERGENTE ____	27
2.1	DEFINICIÓN DE LA EMPRESA _____	27
2.1.1	SUPUESTOS DE LA EMPRESA PYME TIPO _____	28
2.1.1.1	Análisis de una PYME en Ecuador _____	28
2.1.1.2	Estructura de una PYME Tipo _____	30
2.1.2	NECESIDADES DE LA EMPRESA _____	32
2.2	DISEÑO DE LA RED DE LA EMPRESA _____	34
2.2.1	TIPO DE ADMINISTRACIÓN DE LA RED _____	34
2.2.2	TOPOLOGÍA DE LA RED _____	35
2.2.2.1	Topología Red WAN _____	37
2.2.2.2	Topología Red LAN _____	38
2.2.3	DIMENSIONAMIENTO DE LA RED _____	39
2.2.3.1	Dimensionamiento de cada Servicio _____	39
2.2.3.2	Dimensionamiento de los enlaces _____	49
2.2.3.3	VLAN y Direccionamiento IP _____	52
2.2.4	PROTOCOLO DE ENRUTAMIENTO _____	59
2.2.5	PRIORIDAD DE TRÁFICO PARA LA APLICACIÓN DE QoS _____	61
CAPÍTULO 3 _____		63
3	IMPLEMENTACIÓN DEL PROTOTIPO _____	63
3.1	CONSIDERACIONES DE DISEÑO _____	63
3.1.1	ELECCIÓN DE LA ARQUITECTURA DE QoS _____	64
3.1.2	CLASIFICACIÓN Y ASIGNACIÓN DSCP POR TRÁFICO _____	67
3.2	ARQUITECTURA _____	68
3.2.1	CONFIGURACIONES DE IPs Y PUERTOS _____	70
3.2.1.1	Direccionamiento IP _____	70
3.2.1.2	Asignación de VLAN _____	72
3.2.1.3	Asignación de puertos _____	73



3.2.2	CONFIGURACIÓN DE SERVIDORES	74
3.2.2.1	Instalación del Sistema Operativo Base	74
3.2.2.2	Servidor de DNS	79
3.2.2.3	Servidor de DHCP	88
3.2.2.4	Servidor de Video Streaming	90
3.2.2.5	Servidor de FTP	99
3.2.2.6	Servidor Web	105
3.2.2.7	Servidor de Telefonía IP	113
3.2.3	CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO Y QoS	118
3.2.3.1	Router Matriz	118
3.2.3.2	Router Sucursal 1	120
3.2.3.3	Switch Matriz	121
3.2.3.4	Creación de Listas de Control de Acceso	124
3.2.3.5	Creación de Mapas de Clase	124
3.2.3.6	Creación de Mapas de Política	125
3.2.3.7	Asignación de políticas a las interfaces	127
3.2.4	CONFIGURACIÓN DEL GENERADOR DE TRÁFICO	127
3.2.5	CONFIGURACIÓN DE IP SLA	129
3.3	ANÁLISIS DE RESULTADOS	135
3.3.1	ESTADÍSTICAS DE TRÁFICO GENERADO	135
3.3.2	ANÁLISIS DE RESULTADOS	136
CAPÍTULO 4		139
4	CONCLUSIONES Y RECOMENDACIONES	139
4.1	CONCLUSIONES	139
4.2	RECOMENDACIONES	140
CAPÍTULO 5		142
5	REFERENCIAS BIBLIOGRÁFICAS	142
CAPÍTULO 6		<b>¡Error! Marcador no definido.</b>
6	ANEXOS	<b>¡Error! Marcador no definido.</b>
6.1	ANEXO I. COMPLEMENTO DE CONFIGURACIÓN DE EQUIPOS	<b>¡Error! Marcador no definido.</b>
6.1.1	CONFIGURACIÓN DE INTERFACES Y SUBINTERFACES DE R_SUC2 Y R_SUC3.	<b>¡Error! Marcador no definido.</b>

- Router Sucursal 3 \_\_\_\_\_ ¡Error! Marcador no definido.
- 6.1.2 CONFIGURACIÓN DE SWITCHES: VLANS Y ASIGNACIÓN DE PUERTOS  
\_\_\_\_\_ ¡Error! Marcador no definido.
- Switch Sucursal 1 \_\_\_\_\_ ¡Error! Marcador no definido.
- Switch Sucursal 2 \_\_\_\_\_ ¡Error! Marcador no definido.
- Switch Sucursal 3 \_\_\_\_\_ ¡Error! Marcador no definido.
- 6.1.3 CREACION DE MAPAS DE CLASE PARA R\_SUC 2 y RSUC3. \_\_\_\_\_ ¡Error!  
**Marcador no definido.**
- 6.1.4 MAPAS DE POLITICA R\_SUC2 y R\_SUC3: ¡Error! Marcador no definido.
- 6.2 ANEXO II. Fotos del Laboratorio \_\_\_\_\_ ¡Error! Marcador no definido.
- 6.3 ANEXO III. Configuración de equipos \_\_\_\_\_ ¡Error! Marcador no definido.

## ÍNDICE DE FIGURAS

<i>Figura 1.1. Diagrama general de la red</i>	4
<i>Figura 1.2. Red de computadora básica</i>	5
<i>Figura 1.3. Par Trenzado</i>	7
<i>Figura 1.4. Cable Coaxial</i>	7
<i>Figura 1.5. Fibra óptica</i>	8
<i>Figura 1.6. Radio frecuencia</i>	9
<i>Figura 1.7. Microondas</i>	10
<i>Figura 1.8. Transmisión de datos</i>	10
<i>Figura 1.9. Subsistemas de cableado estructurado</i>	12
<i>Figura 1.10. Formato de cabecera IPv6</i>	17
<i>Figura 1.11. Componentes de VoIP</i>	19
<i>Figura 1.12. Arquitectura básica QoS</i>	21
<i>Figura 1.13. Redes Múltiples vs Redes Convergentes</i>	22
<i>Figura 1.14. Modelos de QoS</i>	23
<i>Figura 1.15. Arquitectura RFC 1633</i>	24
<i>Figura 1.16. Cabecera RFC 2475</i>	25
<i>Figura 1.17. Arquitectura RFC 2475</i>	25
<i>Figura 2.1. Tamaño de Empresas en Ecuador</i>	27
<i>Figura 2.2. Evolución del número de empresas en Ecuador</i>	28
<i>Figura 2.3. Concentración de empresas por provincia</i>	29
<i>Figura 2.4. Empresas por actividad económica en Ecuador</i>	30
<i>Figura 2.5. Estructura Organizacional de la PYME Tipo</i>	31
<i>Figura 2.6. Diferentes Topologías de Red</i>	36
<i>Figura 2.7. Posibles Topologías Físicas para la red WAN</i>	37
<i>Figura 2.8. Posibles Topologías Físicas para la red LAN</i>	38
<i>Figura 2.9. Esquema de Tasas de Transmisión de la Red</i>	50
<i>Figura 2.10. Formato de Direcciones IPv6 tipo Unicats</i>	54
<i>Figura 2.11. Ilustración de la Red con el direccionamiento IPv6 definido</i>	59
<i>Figura 3.1. Instalación Ubuntu</i>	75
<i>Figura 3.2. Configuraciones para instalación Ubuntu</i>	75
<i>Figura 3.3. Tipo de instalación para Ubuntu</i>	76
<i>Figura 3.4. Ubicación para la instalación de Ubuntu</i>	76

<i>Figura 3.5. Idioma para la instalación de Ubuntu</i>	77
<i>Figura 3.6. Configuración de credenciales en Ubuntu</i>	77
<i>Figura 3.7. Finalización de la instalación de Ubuntu</i>	78
<i>Figura 3.8. Confirmación de la instalación de Ubuntu</i>	78
<i>Figura 3.9. Inicialización de Ubuntu</i>	78
<i>Figura 3.10. Escritorio de Ubuntu</i>	79
<i>Figura 3.11. Configuraciones del servidor Bind9 (1)</i>	80
<i>Figura 3.12. Configuraciones del servidor Bind9 (2)</i>	81
<i>Figura 3.13. Configuraciones del servidor Bind9 (3)</i>	81
<i>Figura 3.14. Configuraciones del servidor Bind9 (4)</i>	82
<i>Figura 3.15. Configuraciones del servidor Bind9 (5)</i>	83
<i>Figura 3.16. Configuraciones del servidor Bind9 (6)</i>	83
<i>Figura 3.17. Configuraciones del servidor DNS (1)</i>	84
<i>Figura 3.18. Configuraciones del servidor DNS (2)</i>	84
<i>Figura 3.19. Configuraciones del servidor DNS (3)</i>	85
<i>Figura 3.20. Configuraciones del servidor DNS (4)</i>	85
<i>Figura 3.21. Configuraciones del servidor DNS (5)</i>	86
<i>Figura 3.22. Configuraciones del servidor DNS (6)</i>	86
<i>Figura 3.23. Configuraciones del servidor DNS (7)</i>	87
<i>Figura 3.24. Configuraciones del servidor DNS (8)</i>	87
<i>Figura 3.25. Configuraciones del servidor DNS (9)</i>	87
<i>Figura 3.26. Configuraciones del servidor DNS (10)</i>	88
<i>Figura 3.27. Configuraciones del servidor DHCP (1)</i>	88
<i>Figura 3.28. Configuraciones del servidor DHCP (2)</i>	88
<i>Figura 3.29. Configuraciones del servidor DHCP (3)</i>	89
<i>Figura 3.30. Configuraciones del servidor DHCP (4)</i>	89
<i>Figura 3.31. Configuraciones del servidor DHCP (5)</i>	89
<i>Figura 3.32. Configuraciones del servidor DHCP (6)</i>	90
<i>Figura 3.33. Configuraciones del servidor DHCP (7)</i>	90
<i>Figura 3.34. Configuraciones del servidor de Video Streaming (1)</i>	91
<i>Figura 3.35. Configuraciones del servidor de Video Streaming (2)</i>	91
<i>Figura 3.36. Configuraciones del servidor de Video Streaming (3)</i>	92
<i>Figura 3.37. Configuraciones del servidor de Video Streaming (4)</i>	92
<i>Figura 3.38. Configuraciones del servidor de Video Streaming (5)</i>	93
<i>Figura 3.39. Configuraciones del servidor de Video Streaming (6)</i>	93
<i>Figura 3.40. Configuraciones del servidor de Video Streaming (7)</i>	94
<i>Figura 3.41. Configuraciones del servidor de Video Streaming (8)</i>	94

<i>Figura 3.42. Configuraciones del servidor de Video Streaming (9)</i>	95
<i>Figura 3.43. Configuraciones del servidor de Video Streaming (10)</i>	95
<i>Figura 3.44. Configuraciones del servidor de Video Streaming (11)</i>	96
<i>Figura 3.45. Configuraciones del servidor de Video Streaming (12)</i>	96
<i>Figura 3.46. Configuraciones del servidor de Video Streaming (13)</i>	97
<i>Figura 3.47. Configuraciones del servidor de Video Streaming (14)</i>	97
<i>Figura 3.48. Configuraciones del servidor de Video Streaming (15)</i>	98
<i>Figura 3.49. Configuraciones del servidor de Video Streaming (16)</i>	98
<i>Figura 3.50. Configuraciones del servidor de Video Streaming (17)</i>	99
<i>Figura 3.51. Configuraciones del servidor de FTP (1)</i>	99
<i>Figura 3.52. Configuraciones del servidor de FTP (2)</i>	100
<i>Figura 3.53. Configuraciones del servidor de FTP (3)</i>	100
<i>Figura 3.54. Configuraciones del servidor de FTP (4)</i>	101
<i>Figura 3.55. Configuraciones del servidor de FTP (5)</i>	101
<i>Figura 3.56. Configuraciones del servidor de FTP (6)</i>	102
<i>Figura 3.57. Configuraciones del servidor de FTP (7)</i>	102
<i>Figura 3.58. Configuraciones del servidor de FTP (8)</i>	103
<i>Figura 3.59. Configuraciones del servidor de FTP (9)</i>	103
<i>Figura 3.60. Configuraciones del servidor de FTP (10)</i>	104
<i>Figura 3.61. Configuraciones del servidor de FTP (11)</i>	104
<i>Figura 3.62. Configuraciones del servidor Web (1)</i>	105
<i>Figura 3.63. Configuraciones del servidor Web (2)</i>	105
<i>Figura 3.64. Configuraciones del servidor Web (3)</i>	106
<i>Figura 3.65. Configuraciones del servidor Web (4)</i>	106
<i>Figura 3.66. Configuraciones del servidor Web (5)</i>	107
<i>Figura 3.67. Configuraciones del servidor Web (6)</i>	107
<i>Figura 3.68. Configuraciones del servidor Web (7)</i>	107
<i>Figura 3.69. Configuraciones del servidor Web (8)</i>	107
<i>Figura 3.70. Configuraciones del servidor Web (9)</i>	108
<i>Figura 3.71. Configuraciones del servidor Web (10)</i>	108
<i>Figura 3.72. Configuraciones del servidor Web (11)</i>	109
<i>Figura 3.73. Configuraciones del servidor Web (12)</i>	109
<i>Figura 3.74. Configuraciones del servidor Web (13)</i>	109
<i>Figura 3.75. Configuraciones del servidor Web (14)</i>	110
<i>Figura 3.76. Configuraciones del servidor Web (15)</i>	110
<i>Figura 3.77. Configuraciones del servidor Web (16)</i>	110
<i>Figura 3.78. Configuraciones del servidor Web (17)</i>	111

<i>Figura 3.79. Configuraciones del servidor Web (18)</i>	111
<i>Figura 3.80. Configuraciones del servidor Web (19)</i>	111
<i>Figura 3.81. Configuraciones del servidor Web (20)</i>	112
<i>Figura 3.82. Configuraciones del servidor Web (21)</i>	112
<i>Figura 3.83. Configuraciones del servidor Web (22)</i>	112
<i>Figura 3.84. Configuraciones del servidor Web (23)</i>	113
<i>Figura 3.85. Instalación de Elastix 2.4</i>	113
<i>Figura 3.86. Configuración del idioma en Elastix 2.4</i>	114
<i>Figura 3.87. Configuración del particionamiento en Elastix 2.4</i>	114
<i>Figura 3.88. Configuración del usuario y clave en Elastix 2.4</i>	115
<i>Figura 3.89. Instalación del paquete en Elastix 2.4</i>	115
<i>Figura 3.90. Verificación de la instalación de Elastix 2.4</i>	115
<i>Figura 3.91. Acceso web de Elastix 2.4</i>	116
<i>Figura 3.92. Consola web de Elastix 2.4</i>	116
<i>Figura 3.93. Agregar extensiones en Elastix 2.4</i>	117
<i>Figura 3.94. Configuración del archivo sip_custom.conf en Elastix 2.4</i>	117
<i>Figura 3.95. Prueba de llamadas en Elastix 2.4</i>	118
<i>Figura 3.96. Generación de tráfico (1)</i>	127
<i>Figura 3.97. Generación de tráfico (2)</i>	128
<i>Figura 3.98. Generación de tráfico (3)</i>	128
<i>Figura 3.99. Generación de tráfico (4)</i>	129
<i>Figura 3.100. Configuración del router R_matriz</i>	132
<i>Figura 3.101. Configuración del IP SLA en el router R_matriz</i>	132
<i>Figura 3.102. Estadísticas del IP SLA del router R_matriz</i>	133
<i>Figura 3.103. Configuración del IP SLA 1</i>	133
<i>Figura 3.104. Configuración del IP SLA 2</i>	134
<i>Figura 3.105. Configuración del IP SLA 3</i>	134
<i>Figura 3.106. Configuración del IP SLA 4</i>	135
<i>Figura 3.107. Niveles de calidad de acuerdo a ICPIF</i>	137
<i>Figura 3.108. Rango MOS</i>	138

## ÍNDICE DE TABLAS

<i>Tabla 1.1. Clasificación de las redes de computadora</i>	6
<i>Tabla 1.2. Características de medios de transmisión guiados</i>	8
<i>Tabla 1.3. Características de medios de transmisión no guiados</i>	10
<i>Tabla 1.4. Formato de cabecera IPv6</i>	17
<i>Tabla 1.5. Modelos de QoS</i>	23
<i>Tabla 1.6. Comparación entre RFC 1633 y RFC 2475</i>	26
<i>Tabla 2.1. Distribución propuesto para el personal de la PYME tipo</i>	31
<i>Tabla 2.2. Velocidad de navegación para el servicio de Internet</i>	41
<i>Tabla 2.3. Tasa de Transmisión para el servicio de VoIP</i>	44
<i>Tabla 2.4. Tasa de Transmisión para el servicio de Datos</i>	45
<i>Tabla 2.5. Tasa de Transmisión para el servicio de Videoconferencia</i>	46
<i>Tabla 2.6. Tasa de Transmisión para el servicio de Streaming de Video</i>	48
<i>Tabla 2.7. Tasa de Transmisión para el servicio de Correo Electrónico</i>	49
<i>Tabla 2.8. Resumen de las capacidades de transmisión de todos los enlaces</i>	49
<i>Tabla 2.9. Empleados por VLAN en cada Localidad</i>	52
<i>Tabla 2.10. Dimensionamiento del direccionamiento IPV6</i>	53
<i>Tabla 2.11. Comparativa de protocolos de enrutamiento para IPV6</i>	60
<i>Tabla 3.1. Parámetros para las Clases de Servicio</i>	64
<i>Tabla 3.2. Valores de DSCP para las clases AAA, AA y A</i>	67
<i>Tabla 3.3. Clasificación de DSCP</i>	68
<i>Tabla 3.4. Equipos a utilizarse en el prototipo</i>	68
<i>Tabla 3.5. Direccionamiento Router Matriz</i>	70
<i>Tabla 3.6. Direccionamiento Router Sucursal_1</i>	71
<i>Tabla 3.7. Direccionamiento Router Sucursal_2</i>	71
<i>Tabla 3.8. Direccionamiento Router Sucursal_3</i>	71
<i>Tabla 3.9. Nombre de VLANs</i>	72
<i>Tabla 3.10. Direccionamiento Referencial Switch_Matriz</i>	72
<i>Tabla 3.11. Direccionamiento Referencial Switch Sucursal_1</i>	72
<i>Tabla 3.12. Direccionamiento Referencial Switch Sucursal_2</i>	72
<i>Tabla 3.13. Direccionamiento Referencial Switch Sucursal_3</i>	73
<i>Tabla 3.14. Asignación de puertos Switch_Matriz</i>	73
<i>Tabla 3.15. Asignación de puertos Switch Sucursal_1</i>	73

<i>Tabla 3.16. Asignación de puertos Switch Sucursal_2</i>	73
<i>Tabla 3.17. Asignación de puertos Switch Sucursal_3</i>	74
<i>Tabla 3.18. Estadísticas IP SLA</i>	136
<i>Tabla 3.19. Estadísticas IP SLA</i>	136



## **RESUMEN**

El presente proyecto tiene como propósito la implementación de calidad de servicio en una red convergente (video, voz, datos) usando el protocolo IPv6, para una empresa PYME tipo, para cumplir con este objetivo, se implementarán dos escenarios, la red con calidad de servicio y la misma red sin calidad de servicio, en los cuales se realizará la estimación y análisis técnico de los parámetros: latencia, variación de retardo, velocidad de transmisión y pérdida de paquetes, que se generan en una transmisión de datos, video o voz en la red.

En el primer capítulo se da a conocer los conceptos básicos de: IPv6, Calidad de Servicio, arquitecturas y técnicas de calidad de servicio.

En el segundo capítulo se realiza el diseño de la red convergente a implementarse, tomando en cuenta un promedio de 200 empleados en la empresa, la cual tiene 1 oficina matriz y 3 sucursales. Se desarrolla: diseño lógico de la red, direccionamiento, cálculos de ancho de banda, tipo de administración.

En el tercer capítulo se realiza la implementación de la red diseñada, en los equipos existentes (routers, switches, pc) en el laboratorio de la Universidad, también se implementa los servidores de red (VoIP, Streaming, FTP, Web, DNS). Se configuran los equipos para tener interconectividad en la red con calidad de servicio. Se realizan dos escenarios de red, uno sin calidad de servicio y otro con calidad de servicio. Se realiza las pruebas y análisis de resultados del prototipo de red implementado, las pruebas se las realiza mediante un software de análisis, el cual permite realizar la estimación de los parámetros: latencia, variación de retardo, velocidad de transmisión y pérdida de paquetes, tomando en cuenta los dos escenarios propuestos: sin y con calidad de servicio.

En el cuarto capítulo se presenta las conclusiones y recomendaciones que se pueden obtener del desarrollo de este proyecto, y así poder tener un mejor entendimiento del mismo.

**Palabras clave:** red convergente, calidad de servicio.

## ABSTRACT

*The purpose of this project is to implement quality of service in a converged network (video, voice, data) using the IPv6 protocol, for a PYME type company, To achieve this objective, two scenarios will be implemented, the network with quality of service and the same network without quality of service, in which the estimation and technical analysis of the parameters will be carried out: latency, variation of delay, transmission speed and loss of packets, which are generated in a transmission of data, video or voice on the network.*

*In the first chapter, the basic concepts of: IPv6, Quality of Service, architectures and quality of service techniques are disclosed*

*In the second chapter the design of the convergent network to be implemented is carried out, taking into account an average of 200 employees in the company, which has 1 headquarters and 3 branches. It develops: logical design of the network, addressing, bandwidth calculations, type of administration.*

*In the third chapter the implementation of the designed network is carried out, in the existing equipment (routers, switches, pc) in the University laboratory, also the network servers are implemented (VoIP, Streaming, FTP, Web, DNS). The equipment are configured to have interconnectivity in the network with quality of service. Two network scenarios are carried out, one without quality of service and the other with quality of service.*

*The tests and results analysis of the implemented network prototype are performed, the tests are carried out by means of an analysis software, which allows us to estimate the parameters: latency, variation of delay, transmission speed and packet loss, taking into account the two proposed scenarios: without and with quality of service.*

*In the fourth chapter the conclusions and recommendations that can be obtained from the development of this project are made, and in this way to have a better understanding of it.*

*Keywords: converged network, quality of service.*

# CAPÍTULO 1

## 1 FUNDAMENTOS TEÓRICOS

En la actualidad, las PYME representan la mayor fuerza económica del país. La globalización y los rápidos cambios en la tecnología imponen enormes retos a las empresas para crecer y afrontar con éxito nuevos desafíos y asegurar su permanencia en los mercados [1]. Las PYME, buscan ser productivas, cumplir con su misión y objetivos, desarrollar su recurso humano, en definitiva lograr su efectividad, competitividad y mantener su consistencia para sobrevivir en el futuro. En la gran mayoría de empresas, la red de voz se basa en uno o varios PBX (*Private Branch Exchange*) conectados a la PSTN (*Public Switched Telephone Network*), mientras que la red de datos se basa en conmutadores y enrutadores IP (*Internet Protocol*) interconectando redes LAN (*Local Area Network*) y permitiendo el acceso a Internet. Sin embargo, cada vez es mayor la necesidad de una red única en la que tanto la voz como los datos y el video converjan naturalmente y permitan, además, reducir costos de administración, mantenimiento y manejo de la información, así como aumentar la productividad y disminuir los tiempos de atención a los clientes [2].

En redes convergentes, las nuevas aplicaciones como VoIP, *e-commerce* y videoconferencia son sensibles al desempeño de la red y hacen que la capacidad de las redes de proporcionar Calidad de Servicio sea cada vez más importante. IPv6 fue desarrollado para resolver algunos de los problemas de IPv4, tales como la QoS, la seguridad y el agotamiento de las direcciones IP. Las redes IP actuales proporcionan un envío de tráfico de mejor esfuerzo, por lo tanto, no ofrecen ningún tipo de garantías de Calidad de Servicio. Las empresas al no tener calidad de servicio tendrán aplicaciones que no van a funcionar adecuadamente, ya que van a existir problemas de retardo, pérdida de paquetes, latencia, *jitter*, paquetes fuera de orden, entre otros. Muchos piensan que brindar un mayor ancho de banda solucionará los problemas de calidad de servicio, pero éste es un enfoque errado, ya que no basta con aumentar la cantidad de Mbps, sino que se debe asegurar mediante mecanismos de QoS el tráfico hacia el cliente [3].

Las empresas deben tener en su infraestructura una red convergente con calidad de servicio, para que las nuevas aplicaciones funcionen adecuadamente, y esto solo lo pueden obtener con la migración al protocolo IPv6, además siendo imperativo migrar a

este protocolo ya que IPv4, en un futuro no muy lejano, no será utilizado debido al agotamiento de sus direcciones. A pesar de esto el índice de penetración de IPv6 en Ecuador es de apenas el 15.66%. En el país existe poca información de cómo diseñar una red convergente para empresas PYME con calidad de servicio utilizando IPv6, motivo por el cual se pretende que este estudio sirva de referencia para que las empresas ecuatorianas puedan implementar calidad de servicio en sus redes convergentes cuando migren a IPv6 [4].

## 1.1 OBJETIVOS

El objetivo general de este estudio es implementar técnicas de Calidad de Servicio (QoS) en un prototipo de red convergente de datos, video y telefonía usando IPv6 en una empresa PYME tipo.

Los objetivos específicos de este estudio son:

- Analizar las características del protocolo IPv6.
- Diseñar una red tipo de alcance nacional para el soporte de diferentes servicios.
- Implementar el prototipo de red convergente con técnicas de calidad de servicio.
- Implementar servidores de red (DHCP, WEB, DNS, FTP, Video *Streaming* y VoIP) basados en el protocolo IPv6.
- Analizar los resultados de las pruebas en el prototipo de red implementado.

## 1.2 ALCANCE

En este proyecto se va a implementar técnicas de calidad de servicio sobre el prototipo de una red convergente de una empresa PYME tipo, con el protocolo IPv6. Inicialmente se realizará el estudio de los conceptos básicos y generales, cabecera, direccionamiento de IPv6. Además, se estudiarán las características específicas del protocolo que permitan la implementación de las técnicas de calidad de servicio en la red [2].

Las redes convergentes necesitan tener calidad de servicio debido a las diferentes aplicaciones que manejan, por lo tanto, se analizará en qué consiste la calidad de servicio (QoS) y el por qué es indispensable en este tipo de redes. Existen dos arquitecturas de calidad de servicio; para determinar cuál es la mejor para que las aplicaciones del

prototipo de red funcionen adecuadamente, se realizará un análisis comparativo entre ambas.

Después de tener los conceptos de IPv6 y QoS bien definidos, se procederá a realizar el diseño del prototipo de red, tomando en cuenta para el dimensionamiento, los requerimientos de red de una empresa PYME tipo.

Para efectos de este trabajo se definirá que una PYME tipo, tiene 200 empleados en su totalidad, los cuales están distribuidos en una matriz y tres sucursales. Se realizará este diseño teniendo en cuenta una red convergente de alcance nacional, la cual debe estar preparada para poder transportar numerosos y variados servicios como: Voz sobre IP, videoconferencia, *streaming* de video, Internet y mucho más [2].

Bajo este precedente se realizará la planeación de la red tomando en cuenta el propósito organizacional, las necesidades de la organización y la ubicación geográfica de las sucursales. Luego, se procederá a realizar un diseño lógico y físico de la red. Se realizará el dimensionamiento de los enlaces troncales, enlaces LAN, direccionamiento IPv6 y VLAN, se configurarán los servidores DHCP, WEB, DNS, Video *Streaming* y VoIP, todo esto cumpliendo con los requerimientos de la empresa PYME tipo mencionada anteriormente.

Una vez que el diseño esté realizado, se procederá con la implementación del prototipo para emular físicamente la red diseñada con las técnicas de calidad de servicio que mejor se ajusten a los requerimientos de la red.

Después que la topología haya funcionado correctamente, se comprobará la calidad de servicio mediante la captura de paquetes con la ayuda de un software de monitoreo y gestión de red, el cual permitirá estimar los parámetros principales de la calidad de servicio como son: ancho de banda, *jitter*, pérdida de paquetes, retardo para cada aplicación. El diagrama general de la red se muestra en la Figura 1.1 a continuación [1].

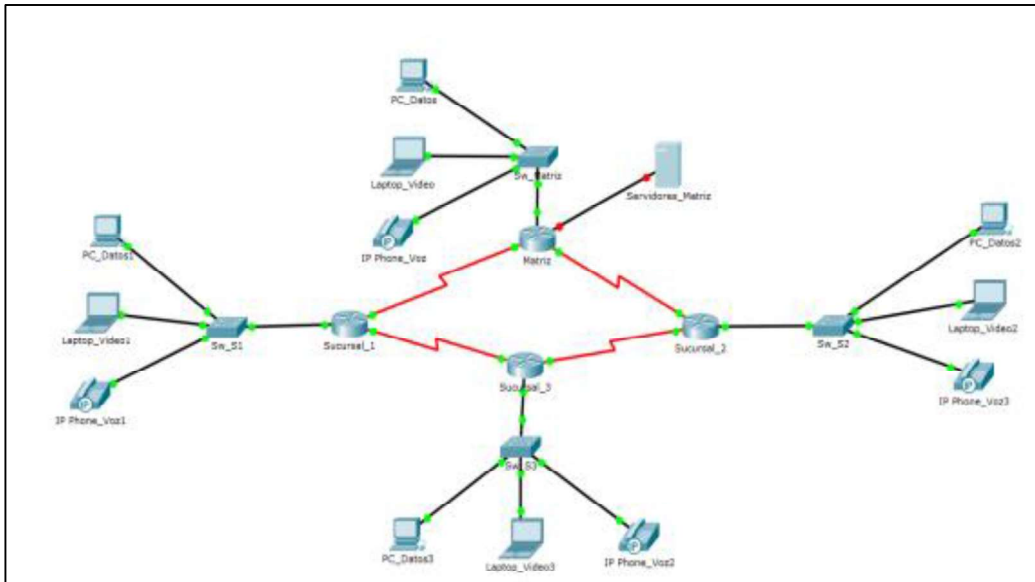


Figura 1.1. Diagrama general de la red

## 1.3 MARCO TEÓRICO

### 1.3.1 REDES DE COMPUTADORAS

En el ámbito de la tecnología de la información, una red informática, también llamada red de datos, es una serie de puntos, o nodos, interconectados por vías de comunicación con el fin de transmitir, recibir e intercambiar tráfico de datos, voz y vídeo.

Los dispositivos de red, incluidos los conmutadores y enrutadores, utilizan diversos protocolos y algoritmos para intercambiar información y transportar datos a su punto final previsto. Cada *endpoint* (a veces llamado *host*) en una red tiene un identificador único, a menudo una dirección IP o una dirección de control de acceso a medios, que se utiliza para indicar el origen o destino de la transmisión. Los *endpoints* pueden incluir servidores, ordenadores personales, teléfonos y muchos tipos de hardware de red [5].

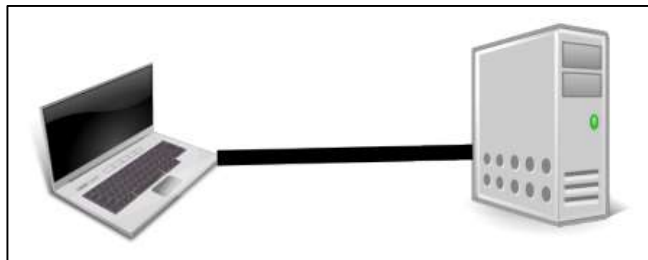
Para que dos o más *hosts* puedan intercambiar información, deben estar conectados entre sí por algún tipo de medio físico. Las redes informáticas han utilizado diversos tipos de medios físicos para intercambiar información, en particular se puede mencionar los siguientes:

- **Cables metálicos.** La información puede transmitirse a través de diferentes tipos de cables metálicos. Los más comunes son los pares trenzados (que se utilizan



en la red telefónica, pero también en las redes empresariales) y los cables coaxiales (que todavía se utilizan en las redes de televisión por cable, pero que ya no se utilizan en las redes empresariales). Algunas tecnologías de red operan sobre el cable metálico clásico [6].

- **Fibra óptica.** Las fibras ópticas se utilizan con frecuencia en redes públicas y empresariales cuando la distancia entre los dispositivos de comunicación es considerable o cuando se requiere de altas velocidades de transmisión y por ende un tendido de cobre no es suficiente. Hay dos tipos principales de fibras ópticas: multimodo y monomodo. La multimodo es mucho más barata que la fibra monomodo porque un LED se puede utilizar para enviar una señal sobre una fibra multimodo mientras que una fibra monomodo debe ser alimentada por un láser [5]. Debido a los diferentes modos de propagación de la luz, las fibras monomodo se limitan a distancias de unos pocos kilómetros, mientras que las fibras multimodo se pueden utilizar a distancias superiores a varias decenas de kilómetros. En ambos casos, los repetidores pueden ser usados para regenerar la señal óptica en un punto final de una fibra para enviarla sobre otra fibra.
- **Inalámbrico.** En este caso, se utiliza una señal de radio para codificar la información intercambiada entre los dispositivos de comunicación. Se utilizan muchos tipos de técnicas de modulación para enviar información a través de un canal inalámbrico y hay mucha innovación en este campo con nuevas técnicas que aparecen cada año. Mientras que la mayoría de las redes inalámbricas dependen de señales de radio, algunas utilizan un láser que envía pulsos de luz a un detector remoto [2].

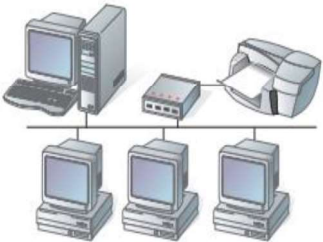
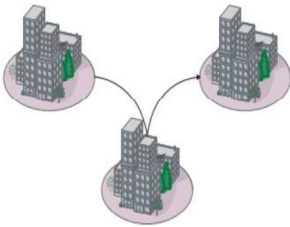
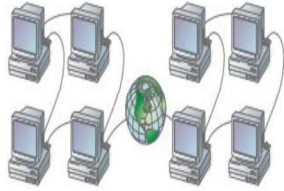


**Figura 1.2.** Red de computadora básica

### 1.3.2 CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS

Las redes de computadoras según el área geográfica en la cual se implementan se dividen:

**Tabla 1.1.** Clasificación de las redes de computadora [7]

Redes de Área Local (LAN)	Redes de Área Metropolitana (MAN)	Redes de Área Extendida (WAN)
<p>Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo. Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.</p>	<p>Corresponde a una versión más grande de una LAN en cuanto a topología, protocolos y medios de transmisión. En general, cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros puede ser considerada una MAN.</p>	<p>Son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (<i>hosts</i>). Estos están conectados por la red que lleva los mensajes de un <i>host</i> a otro. Estas LAN de <i>host</i> acceden a la subred de la WAN por un <i>router</i>. Suelen ser por tanto redes punto a punto [6].</p>
		

### 1.3.3 MEDIOS DE TRANSMISIÓN [8]

Constituye el canal que permite la transmisión de información entre dos terminales en un sistema de transmisión. Las transmisiones se realizan habitualmente empleando ondas electromagnéticas que se propagan a través del canal. A veces el canal es un medio físico y otras veces no, ya que las ondas electromagnéticas son susceptibles de ser transmitidas por el vacío [7].

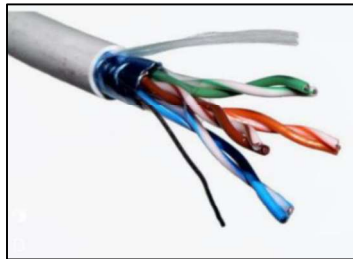
La comunicación es la transmisión de datos de un punto a otro, para que esta se dé, es imprescindible de un equipo emisor, un mensaje, el canal por el cual se envían los datos y el equipo receptor. Estos sistemas de telecomunicaciones ocupan un medio físico por el

cual viajan las señales ópticas, eléctricas o electromagnéticas, durante la transmisión de datos. Existen dos grandes grupos de medios de transmisión:

- Medios guiados
- Medios no guiados

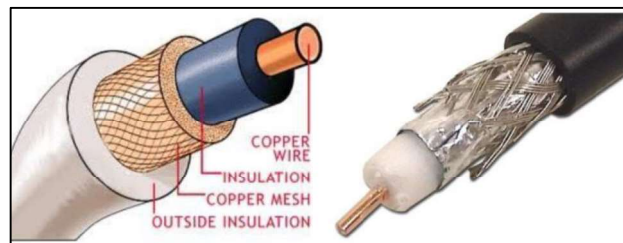
Entre los medios guiados se encuentra el par trenzado, cable coaxial, fibra óptica, entre otros.

**Par trenzado:** Consiste en un par de hilos de cobre cruzados entre sí, con el objetivo de reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía [9].



**Figura 1.3.** Par Trenzado [10]

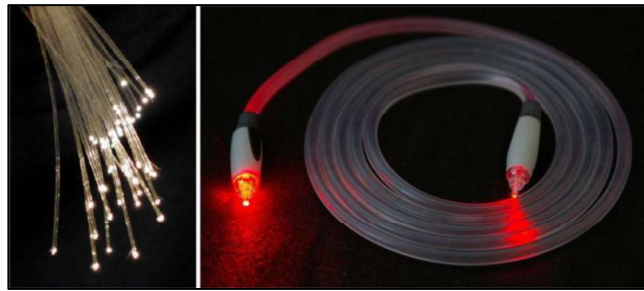
**El cable coaxial:** Es quizá el medio de transmisión más versátil, por lo que está siendo cada vez más utilizado en una gran variedad de aplicaciones. Se usa para transmitir tanto señales analógicas como digitales. El cable coaxial tiene una respuesta en frecuencia superior a la del par trenzado, permitiendo por tanto mayores frecuencias y velocidades de transmisión. Por construcción el cable coaxial es mucho menos susceptible que el par trenzado tanto a interferencias como a diafonía [7].



**Figura 1.4.** Cable Coaxial [11]

**Fibra óptica:** Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían

pulsos de luz que representan los datos a transmitir. Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión [12].



**Figura 1.5.** Fibra óptica [13]

**Tabla 1.2.** Características de medios de transmisión guiados

	PAR TRENZADO	COAXIAL	FIBRA ÓPTICA
Tipo de Señal	Corriente Eléctrica	Corriente eléctrica	Luz (onda electromagnética)
Atenuación	Considerable	Intermedia	Muy escasa
Interferencia	Considerable	Escasa	Muy escasa
Ancho de Banda	Bajo/Intermedio	Alto	Muy alto
Coste	Bajo	Medio	Medio
Uso	Corta distancia	Media/larga distancia	Larga/muy larga distancia

Entre los medios no guiados se encuentran las ondas de radio, microondas, enlaces satelitales, enlaces infrarrojos, entre otros.

**Radio:** Son omnidireccionales

- Un emisor y uno o varios receptores.
- Bandas de frecuencias LF, MF, HF y VHF.

Propiedades:

- Fáciles de generar.
- Largas distancias.
- Atraviesan paredes de edificios.
- Las señales de radio sobre los 10 GHz son absorbidas por la lluvia.
- Sujetas a interferencias por equipos eléctricos.

Sus propiedades dependen de la frecuencia:

- A baja frecuencia cruzan los obstáculos.
- A altas frecuencias tienden a viajar en línea recta y rebotan en los obstáculos.
- Tienen cinco formas de propagarse según la frecuencia: superficial, troposférica, ionosférica, en línea de visión y espacial.

Su alcance depende de:

- Potencia de emisión.
- Sensibilidad del receptor.
- Condiciones atmosféricas.
- Relieve del terreno.

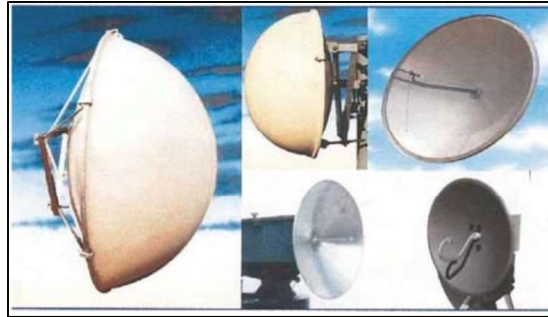


**Figura 1.6.** Radio frecuencia

**Infrarrojo:** Mediante este tipo de transmisión, el propósito es el de dar al equipo la posibilidad de realizar un comunicación punto a punto utilizando un enlace óptico al aire libre como medio de transmisión, con una longitud determinada, estando ésta dentro del infrarrojo [7].

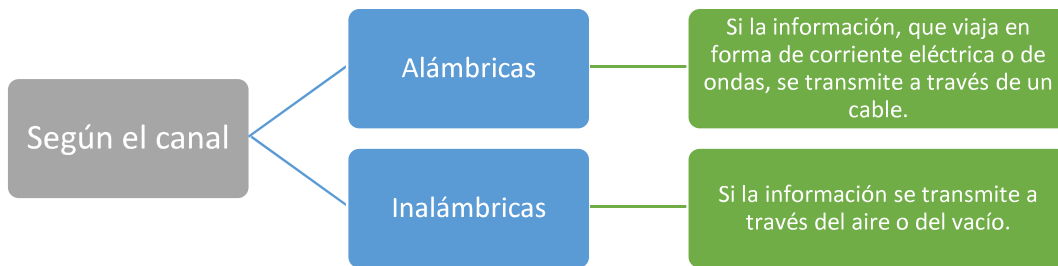
### **Microondas**

- Frecuencias muy altas de 3 GHz a 100 GHz.
- Longitud de onda muy pequeña.
- Antenas parabólicas.
- Receptor y transmisor en línea visual.
- A 100 m de altura se alcanzan unos 80 Km sin repetidores.
- Rebotan en los metales (radar).



**Figura 1.7.** Microondas

Según la naturaleza del canal por el que se transmiten la electricidad o las ondas, las comunicaciones pueden ser alámbricas o inalámbricas.



**Figura 1.8.** Transmisión de datos [14]

**Tabla 1.3.** Características de medios de transmisión no guiados

Medios No Guiados	Características	Alcance	Cubrimiento	Categorías	Ventajas	Desventajas
Radio	Ondas de longitud más larga que la luz infrarroja	Distancia larga	Cientos de kilómetros	VLF, VF, MF, HF, VHF	Cruzan obstáculos	Interferencias
Microondas	Onda unidireccional en línea recta	Distancia corta	80 km entre antenas	Telefonía celular y larga distancia	Baratas, no requieren derecho de paso	No cruzan obstáculos
Satélite	Comunicación entre estaciones terrestres	Sumamente larga	Alto cubrimiento geográfico	Televisión GPS Inteligencia militar	<ul style="list-style-type: none"> <li>Área de cobertura</li> <li>Mayor ancho de banda</li> </ul>	<ul style="list-style-type: none"> <li>Costo elevado</li> <li>Mantenimiento</li> <li>Posicionamiento</li> </ul>

## 1.4 SISTEMAS DE CABLEADO ESTRUCTURADO

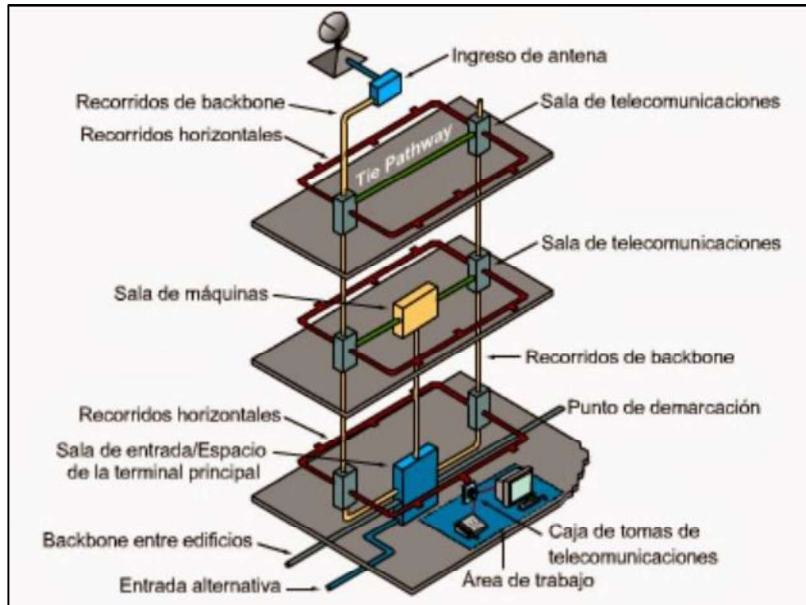
El cableado estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, administradores de red y cualquier otro técnico que trabaje con cables. Hay tres reglas que ayudan a garantizar la efectividad y la eficiencia en los proyectos de diseño de cableado estructurado.

La primera regla es buscar una solución completa de conectividad, una solución óptima que permita interconectar todo el equipamiento de red, de seguridad, servidores, dispositivos finales y demás plataformas de servicios. La implementación basada en estándares está diseñada para admitir tecnologías actuales y futuras. El cumplimiento de los estándares servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo [14].

La segunda regla es planificar el crecimiento a futuro, la cantidad de cables instalados debe satisfacer necesidades futuras. Se deben tener en cuenta las soluciones de categoría 5, 5e, 6, 6a, 7, 7a u 8 y de fibra óptica para garantizar que se satisfagan futuras necesidades. La instalación de la capa física debe poder funcionar durante diez años o más.

La regla final es conservar la libertad de elección de proveedores. Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones [15].

Existen varios subsistemas relacionados con sistemas de cableado estructurado como se ve en la Figura 1.9. Cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables:



**Figura 1.9.** Subsistemas de cableado estructurado [16]

El cableado estructurado está compuesto de varios subsistemas:

- Sistema de cableado vertical.
- Sistema de cableado horizontal.
- Sala de área de trabajo.
- Cuarto o espacio de telecomunicaciones.
- Cuarto o espacio de equipos.
- Cuarto o espacio de entrada de servicios.
- Administración, etiquetado y pruebas.
- Sistema de puesta a tierra para telecomunicaciones.

#### **1.4.1 VENTAJAS DEL CABLEADO ESTRUCTURADO [2]**

- Un sistema de cableado estructurado se define por oposición a los problemas del cableado no estructurado, no estándar o cerrado o propietario de un determinado fabricante.
- Un “sistema de cableado abierto” por otro lado, es un sistema de cableado estructurado que está diseñado para ser independiente del proveedor y de la aplicación a la vez.
- Las características claves de un sistema de cableado abierto son que todas las salidas para conexión del área de trabajo son idénticamente conectadas en estrella a algún punto de distribución central, usando una combinación de medio y



hardware que puede aceptar cualquier necesidad de aplicación que pueda ocurrir a lo largo de la vida del cableado (10 años). Estas características del sistema de cableado abierto ofrecen tres ventajas principales al dueño o usuario:

- Debido a que el sistema de cableado es independiente de la aplicación y del proveedor, los cambios en la red y en el equipamiento pueden realizarse por los mismos cables existentes.
- Debido a que las salidas están cableadas de igual forma, los movimientos de personal pueden hacerse sin modificar la base de cableado.
- La localización de los *hubs* y concentradores de la red en un punto central de distribución, en general un closet de telecomunicaciones, permite que los problemas de cableado o de red sean detectados y aislados fácilmente sin tener que parar el resto de la red [5].

#### **1.4.2 NORMAS DE CABLEADO ESTRUCTURADO**

Para la implementación de un cableado estructurado se debe tomar en cuenta algunas normas. Entre las más sobresalientes tenemos:

##### **1.4.2.1 ANSI/TIA 568.1-D Estándar de Cableado de Telecomunicaciones para Edificios Comerciales**

Que especifica requerimientos para el cableado de establecimientos comerciales. Dentro de esta norma se tiene recomendaciones para:

- Topología
- Distancia máxima entre cables
- Rendimiento de los componentes
- Tomas y conectores de telecomunicaciones

##### **1.4.2.2 ANSI/TIA-569-D Rutas y Espacios para Telecomunicaciones**

En esta norma se toma en cuenta recomendaciones para:

- Canalizaciones horizontales
- Recorridos para backbone
- Áreas de trabajo
- Armarios de telecomunicaciones
- Sala de equipos
- Instalaciones de entrada de servicios

#### **1.4.2.3 ANSI/TIA-606-C Estándar de Administración para Infraestructura de Telecomunicaciones**

Esta norma se refiere a la administración de sistemas de cableado de telecomunicaciones.

Está orientado a los siguientes puntos:

- Espacios de telecomunicaciones
- Ductos y bandejas
- Sistemas de puesta a tierra
- Cables y sistemas de terminación.

La administración adecuada de una infraestructura de telecomunicaciones requiere que la documentación e identificación incluya:

- Etiquetas, Registros y reportes
- Planos
- Ordenes de trabajo

#### **1.4.2.4 ANSI/TIA-607-C Uniones y Puestas a Tierra Genéricas de Telecomunicaciones para las Instalaciones del Cliente**

Estas recomendaciones se orientan a crear un ambiente adecuado y con capacidad de dirigir las corrientes eléctricas y voltajes pasajeros a tierra.

Estos sistemas de puesta a tierra deben garantizar la seguridad de los seres vivos, permitir que los equipos de protección reacciones rápidamente a las fallas, conducir y disipar las corrientes ajenas al sistema sea electrostática o por rayo, realizar una conexión de baja resistencia para la tierra y para los puntos de referencia de los equipos.

La norma se orienta principalmente:

- Backbone de unión de telecomunicaciones (TBB)
- Conductor de interconexión de los TBB (TBBIBC)
- Barra de puesta a tierra de telecomunicaciones (TGB)
- Barra de puesta a tierra principal de telecomunicaciones (TMGB)

## 1.5 IPv6 [17]

El esquema de direccionamiento IPv6 ha sido desarrollado para ser compatible con el actual esquema de direccionamiento IPv4, lo cual, permite a las actuales redes IPv6 coexistir con las redes IPv4. El esquema de direccionamiento IPv6 incrementa el tamaño de direcciones al pasar de 32 bits a 128 bits [2].

IPv6 ofrece las siguientes características significativas:

- Un espacio de direcciones más amplio, que se dice que es suficiente para al menos los próximos 30 años.

En comparación con los 32 bits de longitud que presenta IPv4, IPv6 utiliza 128 bits de longitud. Con un número de direcciones de  $10^{28}$ , es decir, 79 228 162 514 264 337 593 543 950 336 veces mayor que IPv4.

- Direccionamiento único y jerárquico a nivel mundial, basado en prefijos en lugar de direcciones.

Con la agregación de direcciones la red IPv6 se vuelve jerárquica en su totalidad, una dirección IPv6 tiene 3 niveles jerárquicos:

Public Topology: 48 bits.

Site Topology: 16 bits.

Interface Identifier: 64 bits.

- Clases, para mantener las tablas de enrutamiento pequeñas y el enrutamiento de la red troncal eficiente.

Las direcciones de IPv6 que son parte de internet crear una estructura jerárquica lo que da paso a múltiples niveles de ISPs, por lo que la red de internet de IPv6 tienen tablas de enrutamiento más pequeñas.

- Un mecanismo para la autoconfiguración de las interfaces de red.

Esta autoconfiguración es automática, no necesita de un router, servidor de direcciones o alguna configuración. El proceso se inicia cuando el dispositivo de red espera que se le asigne una dirección pero al no obtener respuesta entonces la dirección de enlace local se obtiene por un algoritmo. Estas direcciones siempre empiezan por FE80::.

- Una clase de servicio que distingue tipos de datos.

El campo de la cabecera IPv6, Prioridad, distingue de qué tipo de datagrama se trata según el servicio.

- Mejora de la compatibilidad con el enrutamiento multidifusión (en lugar de la radiodifusión).

- Autenticación y cifrado integrados.  
Una de las características de IPv6 es mayor seguridad, es por eso que trae IPsec integrado de forma automática para autenticar y cifrar los paquetes de datos
- Métodos de transición para migrar de IPv4.

El **IETF** diseño algunos mecanismos y estrategias para que se pueda realizar la transición de IPv4 a IPv6.

Entre las estrategias se tiene:

- Pila Dual.
- Túneles.
- Traducción de Protocolo.

Además los mecanismos más sobresalientes:

- Encapsulación 4 en 6
- Encapsulación 6 en 4
- Mecanismo 6 a 4
- ISATAP
- Teredo

- Métodos de compatibilidad para coexistir y comunicarse con IPv4.

Para que puedan coexistir ambos protocolos hasta llegar a una completa migración se incluyeron algunos mecanismos:

- Nodos de doble pila sobre redes IPv4.
- Islas de nodos de solo ipv6 sobre redes IPv4.
- Nodos de IPv4 que puedan comunicarse con redes IPv6.
- Nodos de IPv6 que puedan comunicarse con redes IPv4.

El formato de la cabecera de paquete IPv6 se simplifica con respecto a su contraparte en IPv4. La longitud de la cabecera IPv6 aumenta a 40 bytes (de 20 bytes) y contiene dos direcciones de 16 bytes (origen y destino), precedidas de 8 bytes de información de control, como se muestra en la Figura 1.10.



**Figura 1.10.** Formato de cabecera IPv6 [18]

En la figura se aprecia los siguientes elementos.

**Tabla 1.4.** Formato de cabecera IPv6 [19]

Campo	Descripción
Versión	(4 bits), para indicar la versión de IP, es decir 6.
Clase de tráfico	(8 bits), el valor de este campo especifica la clase de tráfico. Los valores de 0 a 7 están definidos para tráfico de datos con control de congestión y de 8 a 15 para tráfico de vídeo y audio sin control de la congestión.
Etiqueta de flujo	(20 bits), el estándar IPv6 define un flujo como una serie de paquetes enviados desde un origen hacia un destino determinados. Un flujo se identifica por la combinación de la dirección fuente y la etiqueta. De esta forma, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo.
Longitud del paquete	(16 bits), especifica el tamaño total del paquete, incluyendo la cabecera y los datos.
Siguiente cabecera	(8 bits), indica el tipo de cabecera que sigue a la cabecera de IPv6; por ejemplo, una cabecera TCP, UDP, ICMPv6, etc.
Límite de saltos	(8 bits), es el número máximo de saltos que le quedan al paquete. El límite de saltos es establecido por el origen en un valor máximo y este se decrementa en 1, cada vez que un nodo reenvía el paquete. Si el límite de saltos llega a 0, el paquete es descartado.
Dirección de origen	(128 bits), es la dirección del origen del paquete.
Dirección de destino	(128 bits), es la dirección del destino del paquete.

### **1.5.1 VOZ SOBRE IP (VoIP)**

La comunicación de voz utilizando el Protocolo de Internet (IP) para el transporte se conoce como Voz sobre IP (VoIP). Las redes telefónicas tradicionales, conocidas como redes telefónicas públicas conmutadas (PSTN) utilizaban conmutación de circuitos [20]. Los recursos se reservaban a lo largo de todo el canal de comunicación durante la duración de la llamada. Por el contrario, el Protocolo de Internet (IP) utiliza la conmutación de paquetes. En *PacketSwitching*, los paquetes conocen su destino, y pueden llegar allí por diferentes caminos [2].

La implementación de VoIP requiere una amplia gama de protocolos, desde los necesarios para realizar la señalización de llamadas, para el establecimiento de llamadas y más, hasta el transporte de voz en tiempo real a través de la red, para realizar enrutamiento consciente de la calidad del servicio, reserva de recursos, gestión de red y facturación sensibles a la calidad de servicio. Más adelante en este capítulo, se examinará la evolución de cada uno de estos protocolos para entender cómo encajan en las arquitecturas populares actuales.

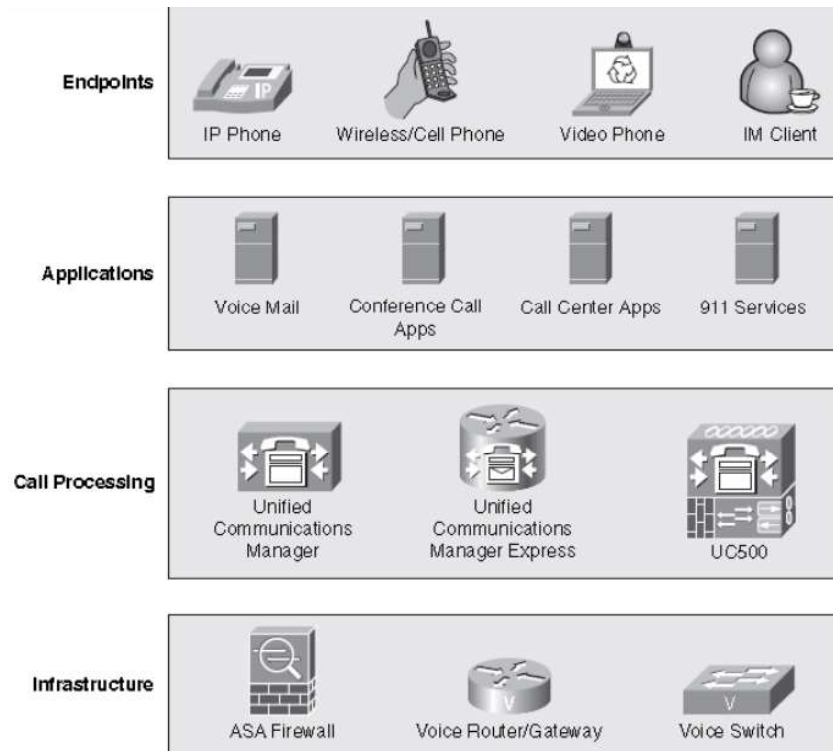
VoIP requiere un medio para que los posibles socios de comunicaciones se encuentren entre sí y para señalar a la otra parte su deseo de comunicarse. Esta funcionalidad se denomina señalización de llamada. La necesidad de funcionalidad de señalización distingue a la telefonía por Internet de otros servicios multimedios de Internet, como los servicios de radiodifusión y los servicios de medios a la carta [17].

### **1.5.2 FUNCIONES Y COMPONENTES DE VoIP**

Muchas empresas tienen cientos –o tal vez miles- de teléfonos en sus compañías. Si cada compañía contratara una línea telefónica para cada uno de esos teléfonos el costo sería demasiado alto. En su lugar, la mayoría de las organizaciones eligen utilizar un conmutador telefónico (PBX – *Private Branch Exchange*) para administrar esas líneas telefónicas internas. Con estos sistemas se permite realizar llamadas telefónicas a los usuarios internos sin utilizar recursos extras de la PSTN.

El modelo de referencia OSI fue diseñado para crear métodos de conexión y comunicación estándares a través de las redes de datos. En el mundo de las transmisiones de voz, existen modelos de conexión similares que describen este tipo de

comunicaciones. Cisco ha desarrollado un modelo que describe el sistema de comunicaciones unificadas, mostrado en la Figura 1.11.



**Figura 1.11.** Componentes de VoIP [20]

### 1.5.3 CALIDAD DE SERVICIO (QoS)

La QoS se refiere a la capacidad de una red para proporcionar un servicio mejorado al tráfico de red seleccionado a través de diversas tecnologías subyacentes, entre las que se incluyen redes de retransmisión de tramas, ATM, Ethernet y 802.1, SONET y redes con enrutamiento IP. En particular, las características de QoS proporcionan un servicio de red mejorado y más predecible proporcionando los siguientes servicios [3]:

- Mejora de las características de pérdida
- Evitar y gestionar la congestión de la red
- Configuración del tráfico de red
- Establecimiento de prioridades de tráfico en toda la red

Todas las redes pueden aprovechar los aspectos de la QoS para lograr una eficiencia óptima, ya sea que se trate de una pequeña empresa, una empresa o un proveedor de

servicios de Internet (ISP). Las diferentes categorías de usuarios de redes, como las grandes empresas, los proveedores de servicios de red y los usuarios de redes de pequeñas y medianas empresas, tienen sus propios requisitos de calidad de servicio; sin embargo, en muchas áreas estos requisitos se solapan [4].

Las redes empresariales, por ejemplo, deben proporcionar soluciones de QoS de extremo a extremo a través de las diversas plataformas que componen la red; proporcionar soluciones para plataformas heterogéneas a menudo requiere que se adopte un enfoque de configuración de QoS diferente para cada tecnología. A medida que las redes empresariales transportan aplicaciones más complejas y de misión crítica, y experimentan un aumento en el tráfico de las aplicaciones Web multimedia, QoS sirve para priorizar este tráfico y asegurar que cada aplicación obtenga el servicio que necesita [15].

Además, la QoS permite que las redes complejas controlen y presten servicio de forma predecible a una variedad de aplicaciones de red y tipos de tráfico. Casi cualquier red puede aprovechar la calidad de servicio para lograr una eficiencia óptima, ya sea una pequeña red corporativa, un proveedor de servicios de Internet o una red empresarial.

Esto proporciona algunos beneficios:

- **Control sobre los recursos:** Se tiene el control sobre qué recursos (ancho de banda, equipos, instalaciones de área amplia, etc.) se están utilizando. Por ejemplo, puede limitar el ancho de banda consumido en un enlace de red troncal mediante transferencias FTP o dar prioridad a un acceso importante a una base de datos [3].
- **Uso más eficiente de los recursos de la red:** Utilizando las herramientas de contabilidad y gestión de análisis de red, sabrá para qué se está utilizando su red y que está atendiendo el tráfico más importante para su negocio.
- **Servicios a medida:** El control y la visibilidad proporcionados por QoS permiten a los proveedores de servicios de Internet ofrecer a sus clientes grados de diferenciación de servicio cuidadosamente adaptados.



- **Coexistencia de aplicaciones de misión crítica:** las tecnologías de QoS aseguran que la WAN sea utilizada eficientemente por las aplicaciones de misión crítica más importantes para su negocio; que el ancho de banda y los retrasos mínimos requeridos por las aplicaciones multimedia y de voz sensibles al tiempo estén disponibles; y que otras aplicaciones que utilizan el enlace obtengan un servicio justo sin interferir con el tráfico de misión crítica [9].

#### 1.5.4 ARQUITECTURA BÁSICA QoS [21]

La arquitectura básica presenta tres etapas fundamentales para la implementación de la QoS (véase la Figura 1.12):

- QoS dentro de un único elemento de red (por ejemplo, herramientas de formación de colas, programación y tráfico)
- Técnicas de señalización de QoS para coordinar la QoS de extremo a extremo entre elementos de red.
- Funciones de política, gestión y contabilidad de la calidad de servicio (QoS) para controlar y administrar el tráfico de extremo a extremo a través de una red.

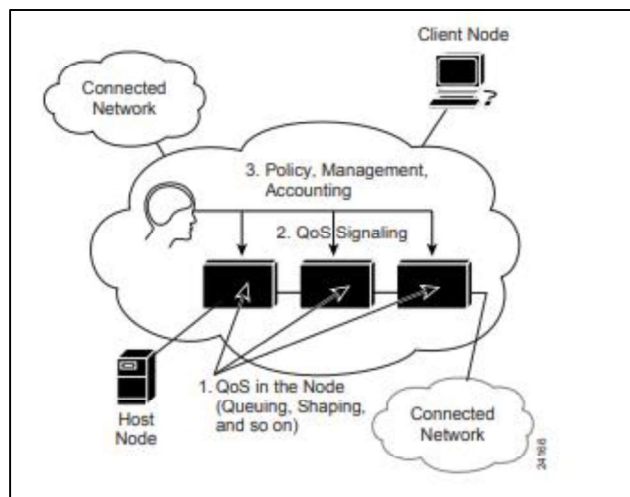


Figura 1.12. Arquitectura básica QoS [22]

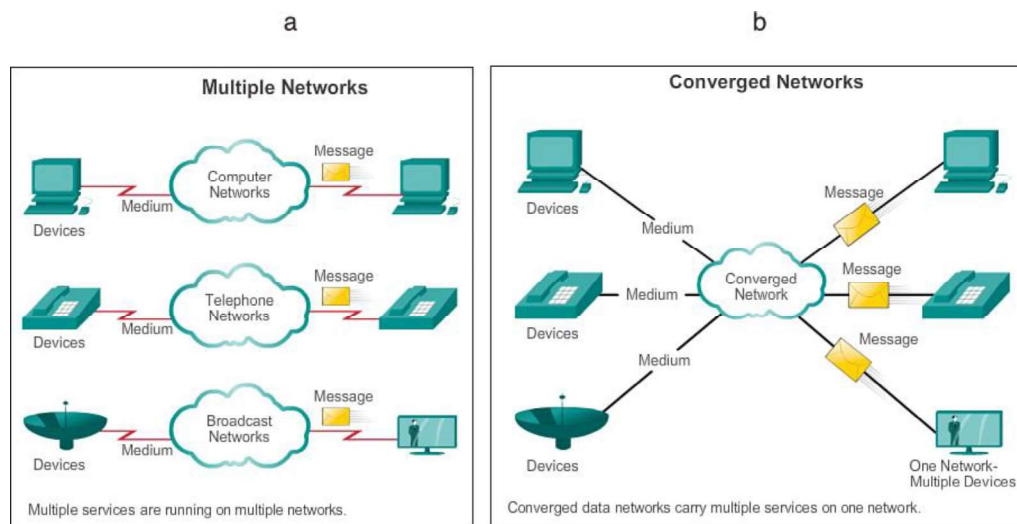
## 1.6 REDES CONVERGENTES

La convergencia de red es la coexistencia eficiente de la comunicación telefónica, de vídeo y de datos dentro de una sola red. El uso de múltiples modos de comunicación en

una sola red ofrece una comodidad y flexibilidad que no son posibles con infraestructuras separadas. La convergencia de redes también se denomina convergencia de medios [6].

Los avances tecnológicos nos están permitiendo consolidar estos diferentes tipos de redes en una plataforma denominada "red convergente". A diferencia de las redes dedicadas, las redes convergentes son capaces de entregar voz, secuencias de vídeo, texto y gráficos entre muchos tipos diferentes de dispositivos a través del mismo canal de comunicación y la misma estructura de red, como se muestra en la gráfica "b" de la Figura 1.13. Formas de comunicación previamente separadas y distintas han convergido en una plataforma común. Esta plataforma proporciona acceso a una amplia gama de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente entre sí de forma casi instantánea.

En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados, como computadoras personales, teléfonos, televisores y *tablets*, pero hay una infraestructura de red común. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación [14].



**Figura 1.13.** Redes Múltiples vs Redes Convergentes [23]

## 1.7 MODELOS DE QoS

Existen 3 modelos de QoS llamados *Best-Effort*, *IntServ* y *DiffServ*, los cuales serán definidos a continuación:



**Figura 1.14.** Modelos de QoS

**Tabla 1.5.** Modelos de QoS

<p><b>Best-Effort</b></p>	<p>Este modelo es el más sencillo. Es un modelo simple de servicio, en el cual una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido y sin informar previamente a la red. Es decir, simplemente este modelo quiere decir que no se aplica calidad en el servicio al tráfico. Además, este modelo no asegura tasa de transferencia, retraso o fiabilidad [2]. Por último, utiliza el modelo de cola FIFO (<i>First In First Out</i>) para sus transmisiones.</p>
<p><b>IntServ (Integrated Services)</b></p>	<p>Este modelo se basa en la idea de reserva de recursos en la red por flujos. Un flujo es una cadena de paquetes que fluyen por la red desde una aplicación en una computadora origen hasta una aplicación en una computadora destino. Para cada flujo entrante se definen los recursos (ancho de banda, retardo, etc.) que serán necesarios para este flujo. La reserva de recursos debe establecerse previamente en cada uno de los <i>routers</i> que forman parte del camino entre el origen y el destino. Cada nodo en el camino indica si puede asegurar la reserva y mantiene una tabla con el estado de la reserva por flujo [6].</p>
<p><b>Diffserv (Differential Services)</b></p>	<p><i>Differentiated Services</i> es un protocolo de QoS propuesto en el RFC 2475 que permite distinguir diferentes clases de servicio marcando los paquetes. Consiste en un método para marcar o etiquetar paquetes, permitiendo a los <i>routers</i> modificar su comportamiento de envío. Cada tipo de etiqueta representa un determinado tipo de QoS y el tráfico con la misma etiqueta se trata de la misma forma.</p>

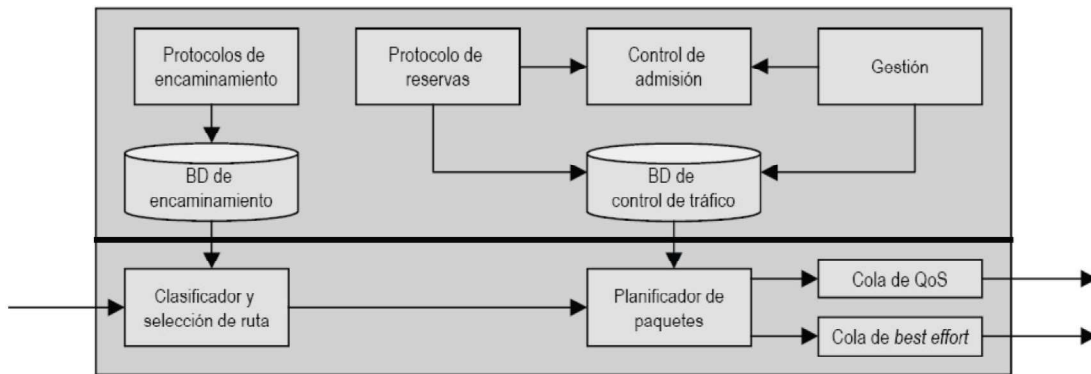
## 1.8 ARQUITECTURA DE SERVICIOS INTEGRADOS (RFC1633)

[24]

La arquitectura de Servicios Integrados tiene como objetivo ofrecer QoS a sesiones de aplicaciones individuales basándose en la reserva de recursos y control de admisión. En la arquitectura de Servicios Integrados, cada paquete IP puede asociarse a un flujo; cada flujo declara su patrón de tráfico y QoS deseada, estos dos parámetros son enviados a

cada *router* mediante un protocolo de señalización y cada *router* verifica si dispone de recursos suficientes para reservarlos, o en caso de no disponerlos, rechazará la sesión.

La arquitectura de Servicios Integrados emplea las siguientes funciones indicadas en la Figura 1.15, para gestionar la congestión y proporcionar transporte con calidad de servicio.



**Figura 1.15.** Arquitectura RFC 1633 [24]

- Protocolo de enrutamiento que mantiene la base de datos de enrutamiento (siguiente salto).
- Protocolo de reserva de recursos para nuevos flujos para una determinada QoS.
- Control de admisión que determina si hay recursos suficientes para cada nuevo flujo.
- Agente de gestión que establece las políticas de control de admisión.
- Clasificador y selección de ruta, los paquetes entrantes se clasifican en clases, una clase puede contener uno o varios flujos. Se determina el siguiente salto en función de la clase del paquete y la IP de destino.
- Gestor de la cola de salida que determina el orden en el que se transmiten los paquetes en base a la clase del paquete, el contenido de la base de datos de control de tráfico y la actividad pasada y actual del puerto de salida. Selecciona paquetes para descartarlos.

## 1.9 ARQUITECTURA DE SERVICIOS DIFERENCIADOS (RFC 2475)

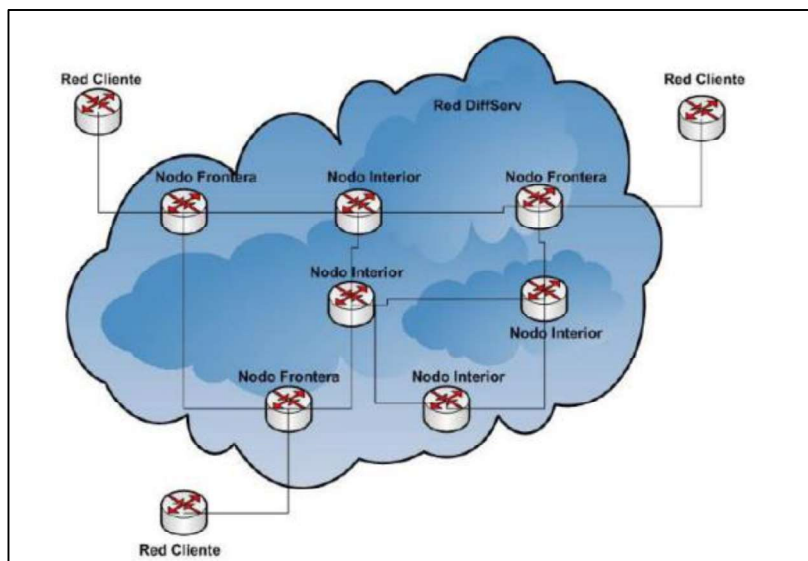
DiffServ fue desarrollada en respuesta a la necesidad de métodos toscos pero simples de proveer diferentes niveles de servicio para el tráfico de Internet y para soportar diferentes tipos de aplicaciones y negocios específicos. Para proporcionar los diferentes niveles de

servicio utiliza el campo “*Type Of Service*” (ToS) o *DiffServ Codepoint* (DSCP) de la cabecera del estándar IPv4 e IPv6. Éste es un campo de 8 bits estando los últimos 2 reservados. Con los 6 bits restantes se consiguen 64 combinaciones: 48 para el espacio global y 16 para uso local [1].



**Figura 1.16.** Cabecera RFC 2475 [25]

Para su funcionamiento, DiffServ divide el tráfico en unas pocas clases y los recursos se asignan con base a las clases, lo que hace que esta arquitectura no sufra el problema de agotamiento de recursos de la red. Para el control del tráfico DiffServ tiene dos tipos de enrutadores (*routers*): los nodos frontera y los nodos interiores. Solo los nodos frontera clasifican tráfico y marcan paquetes, mientras que los nodos interiores usan las clases codificadas en la cabecera del paquete (llamadas clases de retransmisión) para determinar el tratamiento de los paquetes [2].



**Figura 1.17.** Arquitectura RFC 2475 [26]

## 1.10 COMPARACIÓN ENTRE RFC 1633 Y RFC 2475

Tabla 1.6. Comparación entre RFC 1633 y RFC 2475

Servicios integrados RFC 1633	Servicios diferenciados RFC 2475
<ul style="list-style-type: none"><li>• Se implementa dentro de un dominio</li><li>• Limita la demanda a la capacidad de la red</li><li>• Reserva recursos dentro del dominio para ofrecer QoS.</li><li>• Complicada de implementar [3]</li></ul>	<ul style="list-style-type: none"><li>• Marca el tráfico y lo distingue, ofreciendo distinta QoS para cada tipo</li><li>• Fácil de implementar</li></ul>

## CAPÍTULO 2

### 2 ANÁLISIS DE REQUERIMIENTOS Y DISEÑO DE LA RED CONVERGENTE

En este segundo capítulo se analizarán las necesidades de una empresa PYME tipo, que requiera diferentes y variados servicios, como: VoIP, Internet, correo electrónico, conectividad de datos para aplicativos internos de la empresa, videoconferencia, e inclusive *streaming* de video; en base a este análisis, se definirán los requerimientos para la red convergente que soportará las necesidades de la empresa PYME tipo en estudio.

Una vez definidos los requerimientos de la red convergente, se realizará el diseño de la misma, para lo cual se detallará la estimación de capacidades de los enlaces LAN para servidores y enlaces WAN, considerando un crecimiento acorde a los indicadores de crecimiento de las industrias en Ecuador; también se calculará la capacidad requerida para el direccionamiento IPv6 acorde a la cantidad de trabajadores de la empresa PYME tipo y finalmente se detallará el diseño físico y lógico de la red convergente.

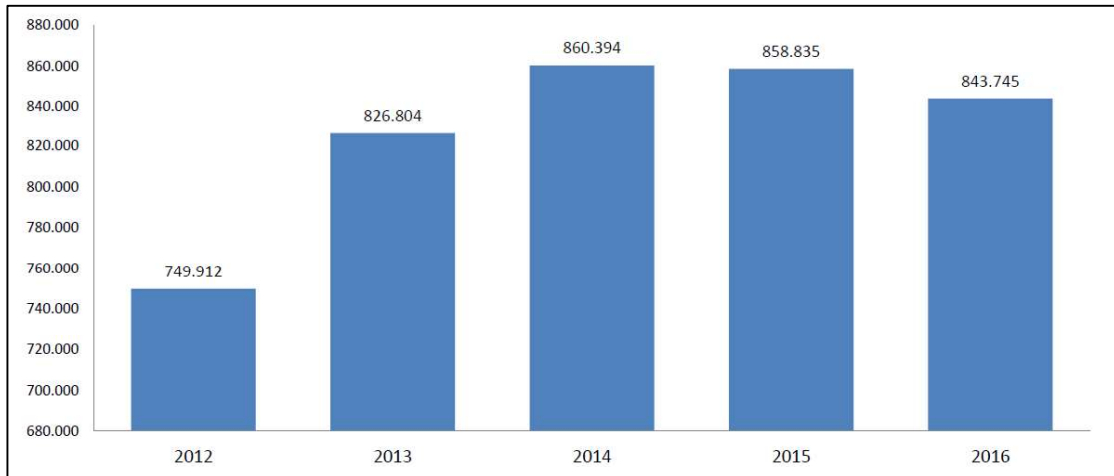
#### 2.1 DEFINICIÓN DE LA EMPRESA [27]

Una empresa es una unidad organizativa que realiza actividades económicas en uno o varios lugares, con autonomía en la toma de decisiones de mercadeo, financiamiento e inversión. En la Figura 2.1 se detalla la clasificación de las empresas en Ecuador, de acuerdo a las cifras oficiales manejadas por el INEC, el tamaño de una empresa se define de acuerdo al volumen de ventas anuales (V) y el número de personas ocupadas (P); por lo tanto, considerando la cantidad de personas o trabajadores, una pequeña empresa es aquella que cuente con 10 a 49 trabajadores y una mediana empresa es aquella que emplee de 50 a 199 trabajadores.

<b>Grande:</b> <ul style="list-style-type: none"><li>• V: \$5'000.001 en adelante. P: 200 en adelante.</li></ul>
<b>Mediana "B":</b> <ul style="list-style-type: none"><li>• V: \$2'000.001 a \$5'000.000. P: 100 a 199.</li></ul>
<b>Mediana "A":</b> <ul style="list-style-type: none"><li>• V: \$1'000.001 a \$2'000.000. P: 50 a 99.</li></ul>
<b>Pequeña:</b> <ul style="list-style-type: none"><li>• V: \$ \$100.001 a \$1'000.000. P: 10 a 49</li></ul>
<b>Microempresa:</b> <ul style="list-style-type: none"><li>• V: menor o igual a \$100.000. P: 1 a 9.</li></ul>

**Figura 2.1.** Tamaño de Empresas en Ecuador

En cuanto a la cantidad de empresas, el 90.51% son micro, el 9.03% son PYMES lo cual significa que en Ecuador existen alrededor de 75.000 empresas pequeñas y medianas; y, el 0.46% son grandes empresas. En la última entrega del manual de Directorio de Empresas y Establecimientos del 2016 elaborado por el INEC, se realiza un análisis de la evolución de nuevos emprendimientos que se convierten en empresas y de igual forma empresas que no pudieron mantenerse en el tiempo; en la Figura 2.2 se puede visualizar la evolución de las empresas en Ecuador desde el año 2012 al 2016.



**Figura 2.2.** Evolución del número de empresas en Ecuador

## **2.1.1 SUPUESTOS DE LA EMPRESA PYME TIPO**

En esta sección se hará un breve análisis de las empresas en el país, lo cual permitirá delimitar con mayor detalle a una empresa PYME tipo, con el objetivo de definir con un mejor criterio el dimensionamiento y necesidades reales de este tipo de empresas en Ecuador.

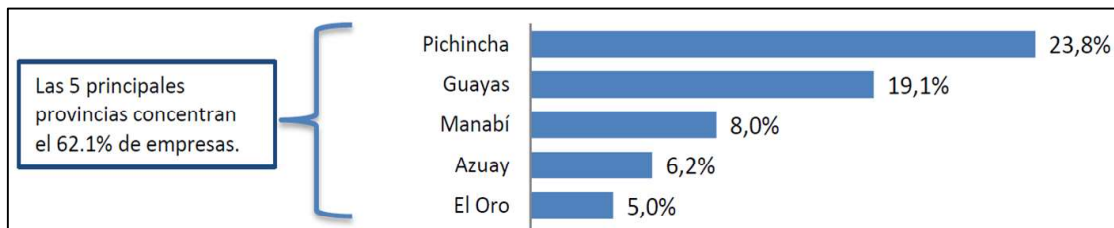
### **2.1.1.1 Análisis de una PYME en Ecuador**

Para el presente caso de estudio, se ha considerado a una empresa PYME tipo de 200 empleados, que como se indicó en apartados anteriores, es el número de empleados que se estima como máximo para que una empresa sea considerada como PYME en Ecuador; este tipo de empresa se estima que cuente con una oficina matriz y tres sucursales ubicadas en distintas ciudades del país.



Al igual que otros segmentos de la economía, las PYME tienen sus particularidades acorde con el giro de negocio y esto se ve reflejado en su distribución provincial y sectorial. Las provincias de Pichincha y Guayas concentran la mayor parte de la actividad económica, a estas provincias les siguen Manabí y Azuay.

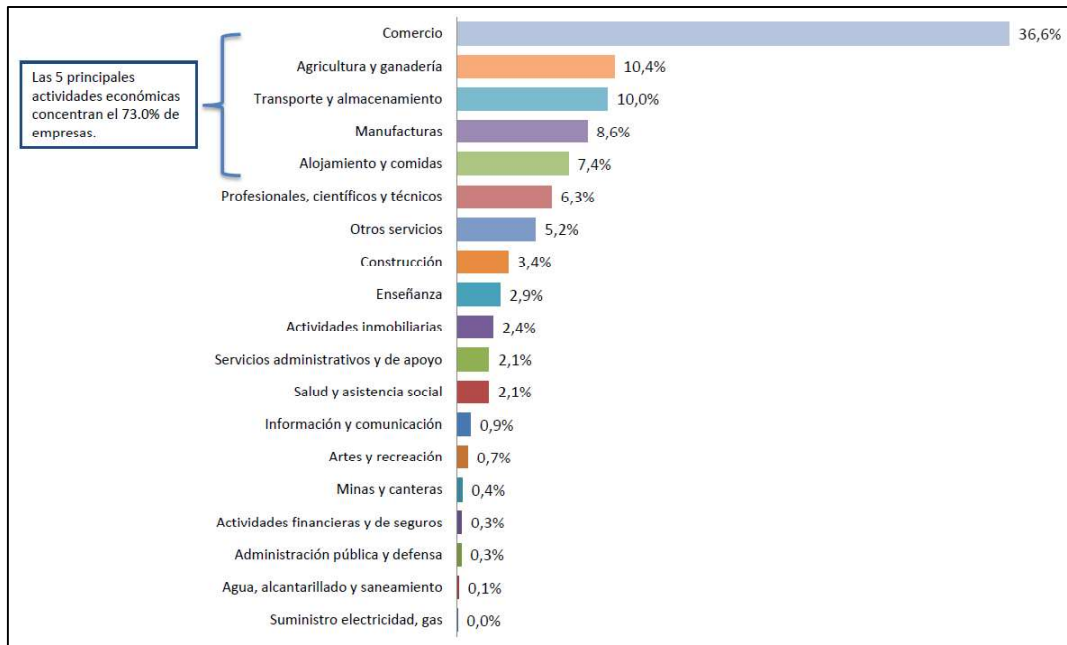
Cerca del 43% de las PYME están ubicadas en Guayas y Pichincha, concentrando en gran medida a sus clientes directamente en las zonas en las que realizan su actividad, siendo las plazas más importantes del país. En la Figura 2.3 se muestra la concentración de empresas por provincias, por lo tanto, con estas estadísticas se define que nuestra PYME tipo tendría su oficina matriz en Quito y sucursales en Guayaquil, Portoviejo y Cuenca:



**Figura 2.3.** Concentración de empresas por provincia

En cuanto a la actividad económica de las empresas en Ecuador, la mayor actividad es el comercio, las actividades comerciales son las más idóneas para el segmento PYME al constituir una alternativa más viable de negocio, frente a otras que requieren mayores inversiones.

En la Figura 2.4 se detalla la composición de empresas por actividad económica, como se puede observar en la gráfica, la principal actividad económica es el comercio, seguida de agricultura y ganadería, transporte y almacenamiento, manufactura, alojamiento y comidas; razón por la cual uno de los supuestos para el presente trabajo, es que la PYME tipo seleccionada está dentro de la actividad económica más ampliamente explotada en el país: el comercio.



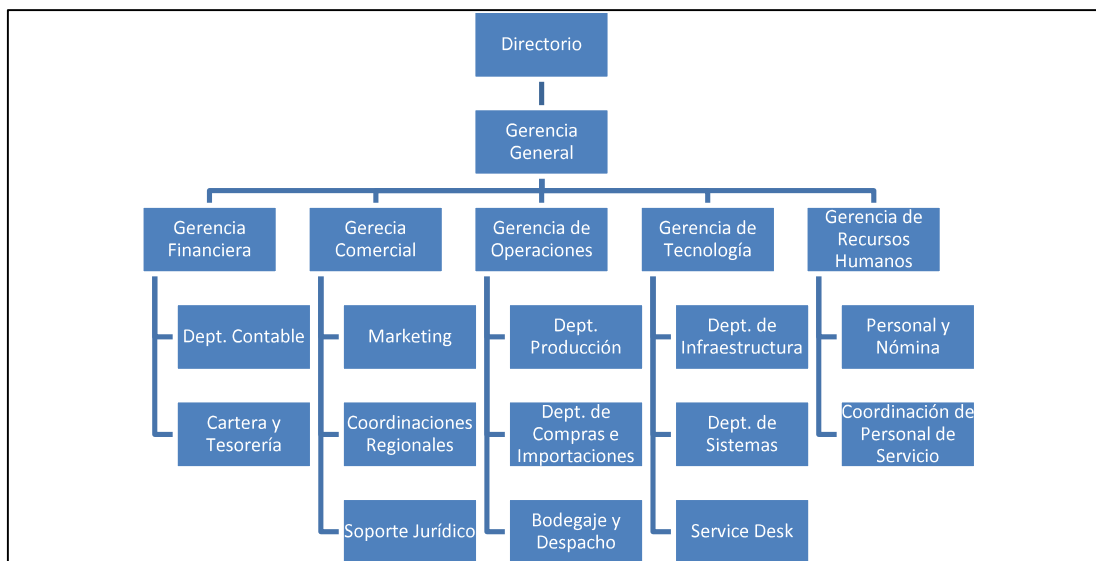
**Figura 2.4.** Empresas por actividad económica en Ecuador

De acuerdo al Fondo Monetario Internacional (FMI), el crecimiento proyectado del Producto Interno Bruto (PIB) para Ecuador con el que cerrará el 2018 es de 2.2% y para el 2019 proyectan un crecimiento del PIB del 1.7%, frente a otros países de la región como Perú que espera un crecimiento constante en el 2018 y 2019 del 4%. [28]

El crecimiento real de una empresa PYME en Ecuador dependerá de las coyunturas políticas, económicas, sociales que se desarrollen a lo largo del tiempo y también de la propia proyección realizada por la empresa, sin embargo, estos cambios podrían no ser considerados críticos dentro del dimensionamiento de una red convergente de servicios, debido al crecimiento escalable que las redes IP permiten; por lo tanto, para ilustrar el dimensionamiento de la capacidad que necesitará cada servicio y direccionamiento IP, se considerará un 10% de holgura.

### 2.1.1.2 Estructura de una PYME Tipo

La estructura de una empresa que se dedica al comercio es definida principalmente por el tamaño de la empresa, con el paso del tiempo esta estructura organizacional cambiará, sin embargo, se define que una empresa PYME tipo debería al menos tener las áreas funcionales que se muestran a continuación en la Figura 2.5:



**Figura 2.5.** Estructura Organizacional de la PYME Tipo

Otro de los supuestos que se establece previo al diseño de la red convergente, es la definición de los departamentos que formarían parte de cada una de las 5 áreas funcionales de una empresa PYME tipo, en la Figura 2.5 se detalla una estructura simple de cinco gerencias o áreas funcionales: Financiera, Comercial, Operaciones, Tecnología y Recursos Humanos; y, dentro de cada una de ellas se detallan los departamentos que formarían parte de cada gerencia.

Una vez definida la estructura organizacional, se estimó la cantidad de empleados que se requieren en cada área especificando con más detalle las actividades y por ende las funciones concretas dentro de cada departamento, en la Tabla 2.1 se detalla la distribución de los 200 empleados:

**Tabla 2.1.** Distribución propuesto para el personal de la PYME tipo

Estructura Organizacional Propuesta	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
<b>Directorio</b>	5			
<b>Gerencia General</b>	2			
<b>Gerencia Financiera</b>	2			
Departamento Contable	4			
Cartera y Tesorería	6	4	4	4
<b>Gerencia Comercial</b>	2			
Marketing	2			
Producto	6			
Soporte TI y Web	2			
BI	3			
Coordinaciones Regionales				
Coordinación Regional	2	2	2	2
Fuerza de Ventas	10	8	5	5

Estructura Organizacional Propuesta	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Contrataciones Públicas	2			
Soporte Jurídico	3	2	1	1
<b>Gerencia de Operaciones</b>	2			
Departamento de Producción	20			
Departamento de Compras e Importaciones	3			
Bodegaje y Despacho	6	4	4	4
<b>Gerencia de Tecnología</b>	2			
Departamento de Infraestructura	5			
Departamento de Sistemas	5			
Service Desk	4	2	1	1
<b>Gerencia de Recursos Humanos</b>	2			
Personal y Nómina	4			
Coordinación de Personal de Servicio	2			
Recepcionistas	1	1	1	1
Guardianía	4	3	3	3
Personal de Limpieza y Mantenimiento	3	3	2	2
Personal de Servicio	2	1	1	1
Personal de Mensajería	2	2	1	1
<b>TOTAL DE PERSONAS</b>	<b>118</b>	<b>32</b>	<b>25</b>	<b>25</b>

Esta distribución de personal será empleada para el dimensionamiento de los servicios que soportarán las necesidades de la empresa en cuanto a comunicación, navegación en Internet, consumo de aplicativos internos, correo y video.

## 2.1.2 NECESIDADES DE LA EMPRESA [29] [30]

Una empresa PYME dependiendo de su giro de negocio y actividad comercial específica, tendrá diversas necesidades informáticas y tecnológicas, sin embargo se plantean algunas de las aplicaciones más comunes y exigentes que pueden ser implementadas en una red de servicios convergentes:

- **Internet:** este servicio es una herramienta fundamental para tener al alcance casi cualquier información que se requiera, por esta razón es que muchas empresas emplean este servicio como parte de su estrategia de posicionamiento al publicar sus servicios a través de la web, ampliando sus oportunidades de negocio.
- **Correo Electrónico:** este servicio de igual forma es indispensable en una organización, debido a que facilita las relaciones comerciales al disponer de un medio digital de contacto continuo, a un bajo costo.
- **Telefonía IP:** actualmente las empresas cuentan con diversos medios de comunicación, la tecnología evoluciona y brinda nuevas formas de relacionarnos

unos con otros, sin embargo; el lenguaje humano sigue siendo necesario cuando se interactúa sobre todo con un cliente, es un medio de comunicación más personal y de respuesta rápida, al no tener que esperar por la respuesta de un correo electrónico.

- **Transmisión de Datos**: el contar con un software para la gestión empresarial como un ERP (*Enterprise Resource Planning*)<sup>1</sup> o un CRM (*Customer Relationship Management*)<sup>2</sup> es muy importante para una empresa, permite integrar los procesos de contabilidad, finanzas, producción, inventarios, ventas, etc., este *software* es instalado en un servidor centralizado y mediante enlaces de datos las localidades remotas consumen estos servicios, de ahí la importancia que una empresa cuente con enlaces que conecten sus sucursales con su matriz donde radican estos servicios de consumo interno.
- **Videoconferencia**: permite alcanzar puntos remotos ubicados a larga distancia, reduciendo costos de movilización; la videoconferencia logra aumentar la productividad de una empresa y la satisfacción de los empleados, el lenguaje audiovisual tiene algunos beneficios, entre los que están: mejora la comprensión, facilita la comunicación corporativa, agiliza la toma de decisiones, mejora la calidad de servicio al cliente y reduce viajes de trabajo, lo cual impacta positivamente en la calidad de vida de los empleados.
- **Streaming de Video**: permite ver un archivo multimedia directamente desde el servidor sin tener la necesidad de descargarlo al ordenador o dispositivo, a nivel empresarial existen algunas aplicaciones de este servicio como por ejemplo: demostración de productos y servicios, video-tutoriales para solventar dudas frecuentes de clientes, cursos de capacitación continua al personal, compartir noticias dentro de la empresa, compartir entrevistas a expertos del sector, difundir campañas de marketing digital, transmisión de eventos, entre otros.

---

<sup>1</sup> **ERP (*Enterprise Resource Planning*)**: es un sistema informático que ayuda a administrar una empresa de cualquier tipo, automatizando todos sus procesos centrales de negocio y operaciones, especialmente las que tienen que ver con la producción, la logística, el inventario, los envíos y la contabilidad.

<sup>2</sup> **CRM (*Customer Relationship Management*)**: es un software / programa / herramienta / aplicación para lograr un enfoque más comprensivo sobre la cartera de clientes y detectar cómo evoluciona cada interacción y actividad con los mismos.

Para que la red de servicios convergentes soporte todos estos requerimientos y los servicios sean altamente disponibles, es necesario tomar en cuenta las siguientes consideraciones:

- Se deberá garantizar la disponibilidad de recursos (Internet y acceso a las aplicaciones internas), mediante un correcto dimensionamiento de los servicios que van a consumir los empleados de la empresa en cada una de sus sucursales.
- Se deberá establecer la redundancia mínima requerida de enlaces para lograr continuidad de acceso a los aplicativos internos en cualquier momento, incluso en caso de fallo de enlaces; y, en concordancia con esta premisa, se deberá considerar también la robustez requerida por parte de los equipos de red que garantice alta disponibilidad de la red.
- Diseño de una arquitectura de red que permita la integración de todas las dependencias o localidades remotas, en una única red de servicios convergentes sobre la cual se integrarán los diferentes departamentos de la empresa.

## **2.2 DISEÑO DE LA RED DE LA EMPRESA**

En base a las necesidades de la empresa analizadas en apartados anteriores, en esta sección se realizará el diseño de la red de servicios convergentes, para lo cual se detallará la forma de estimar las capacidades de los enlaces en base a los servicios requeridos, definición de las VLANs y del direccionamiento con IPv6, todo esto considerando un crecimiento adecuado para la red; y, se analizarán las posibles soluciones tanto en topología como en protocolos de enrutamiento.

### **2.2.1 TIPO DE ADMINISTRACIÓN DE LA RED [31] [32]**

Dentro del tipo de administración de una red existen tres aspectos bien definidos que diferencian la centralización de la descentralización, todos ellos relacionados con el control, debido a que este es el factor clave determinante en las decisiones de centralización de servicios, frente a desplegar un ambiente distribuido; dichos factores son:

- La localización física de las instalaciones de los servidores.
- La actividad o responsabilidad dentro de la estructura de la organización.
- La toma de decisiones.

A lo largo de la historia se pasó de arquitecturas centralizadas a distribuidas y luego se empezó a hablar nuevamente de la re-centralización debido a:

- La compatibilidad de los sistemas en todas las unidades de negocio.
- La gestión de la propiedad corporativa y el intercambio de datos.
- Las economías de escala.
- Los recursos humanos compartidos.
- Los elevados costes de los centros de procesamiento de datos independientes.

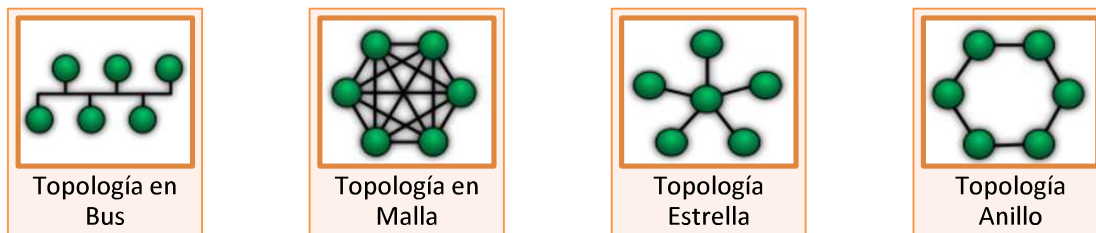
La arquitectura de servicios/servidores distribuidos aplica en el Internet, mientras que las arquitecturas centralizadas se emplean para servidores de archivos, impresoras, bases de datos, aplicaciones, correo, etc. Por lo tanto se define que el tipo de arquitectura más idónea para una empresa PYME tipo es la arquitectura centralizada de servicios.

## 2.2.2 TOPOLOGÍA DE LA RED [33]

La topología de red se refiere al diseño de una red y cómo los diferentes nodos o componentes de esa red, se conectan y comunican unos con otros. Las topologías son físicas y lógicas:

- **Topología Física**: describe la manera en la cual los componentes de la red se interconectan físicamente.
- **Topología Lógica**: describe la forma que los componentes de la red se comunican entre sí dentro de la red física.

Las topologías física y lógica son independientes una de la otra, por ejemplo la tecnología *Token Ring*, emplea una topología física en estrella, mientras que su topología lógica es en anillo para la comunicación de sus componentes. Las topologías más comunes hoy en día son: bus, estrella, anillo y malla; en la Figura 2.6 se ilustran estos cuatro tipos de topologías:



**Figura 2.6.** Diferentes Topologías de Red [34]

En una topología de bus, todos los componentes de la red se conectan a un mismo cable compartido; algunas tecnologías emplean este tipo de topologías son 10Base5 y 10Base2 Ethernet, en las cuales las computadoras se conectan mediante un conector vampiro o conector “T” a un cable coaxial, estas tecnologías físicas ya no se emplean en la actualidad, sin embargo a nivel de topología lógica la tecnología Ethernet que hoy en día se usa, emplea una topología lógica en bus.

En una topología de estrella, un dispositivo central tiene varias conexiones punto a punto con otros componentes; las topologías de estrella son usadas en despliegues en los cuales se requiere conectar varios componentes hacia un solo punto central, el principal problema con este tipo de topologías radica en que si falla el dispositivo central, los componentes no podrán comunicarse entre si; este problema se mitiga implementando una topología extendida en estrella que básicamente es múltiples topologías de estrella interconectadas, considerando las inversiones monetarias adicionales del caso.

En una topología en anillo, el dispositivo 1 se conecta con el dispositivo 2, este a su vez se conecta con un dispositivo 3 y así sucesivamente hasta el último dispositivo del anillo, el cual a su vez se conecta con el primer dispositivo; las topologías en anillo pueden implementarse con un único anillo o dos anillos, típicamente se emplean dos anillos para obtener redundancia.

Las topologías de malla son de dos tipos: malla parcial y malla completa, en una topología de malla parcial, no todos los dispositivos están conectados al resto de componentes de la red, mientras que en una topología de malla completa, todos los componentes de la red están interconectados entre sí. Las topologías en malla si bien aumentan la disponibilidad de los enlaces, son las más costosas de desplegar.

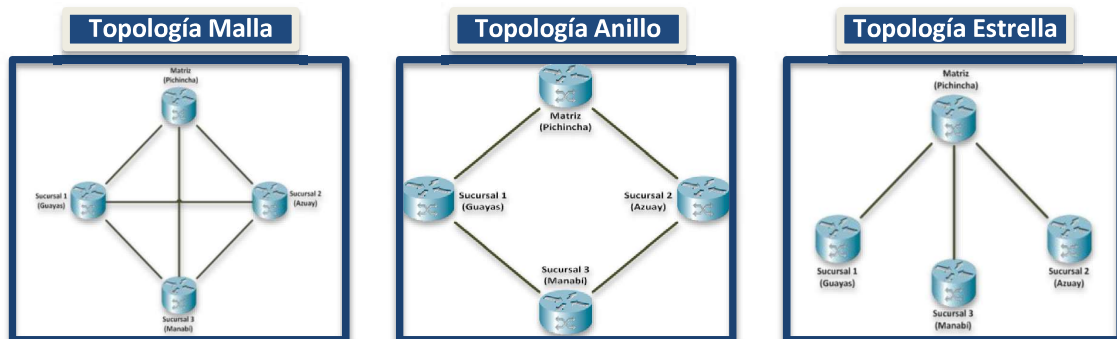


### 2.2.2.1 Topología Red WAN

#### Topología Física

Para la interconexión de las sucursales mediante una red WAN, se analizaron algunas posibles soluciones para el diseño de la topología física. En la Figura 2.7 se ilustran 3 tipos de despliegues físicos para la red WAN:

- Uno en malla en el cual se requieren 6 enlaces físicos y con el cual se logra la máxima disponibilidad por eventuales fallos de conectividad.
- Una segunda opción (la elegida para esta implementación) en la cual se plantea una conectividad en anillo, misma que requiere de 4 enlaces y considera una contingencia ante fallos (dos rutas posibles por cada sitio).
- Y una tercera opción mediante un despliegue en estrella, en el cual se requieren únicamente 3 enlaces WAN, en esta última alternativa se corre el riesgo que una sucursal quede sin servicios al fallar su enlace único enlace de conexión hacia la matriz.



**Figura 2.7.** Posibles Topologías Físicas para la red WAN [35]

Para grandes empresas que cuenten con los recursos para una implementación en alta disponibilidad, la recomendación es emplear una topología en malla, sin embargo la empresa de análisis es de tipo PYME, por lo tanto se considerará la topología en anillo por costos (Topología Malla: 6 enlaces, Topología Anillo: 4 enlaces) y debido a que se reduce el riesgo que una localidad quede aislada al fallar un enlace, gracias a que cada sitio se interconecta con otros dos sitios mediante dos enlaces diferentes.

En cuanto al equipamiento de borde en cada localidad, lo ideal es que se implemente redundancia de equipos, esto implica mayores costos para una empresa y considerando

que la empresa tipo de análisis es una PYME, lo mínimo recomendable es que los equipos de borde a emplear deban cumplir con ciertas características técnicas que minimicen el riesgo de caída del equipo, lo cual dejaría completamente aislada una localidad; estas características técnicas son por ejemplo: equipos con redundancia de fuente y procesadora.

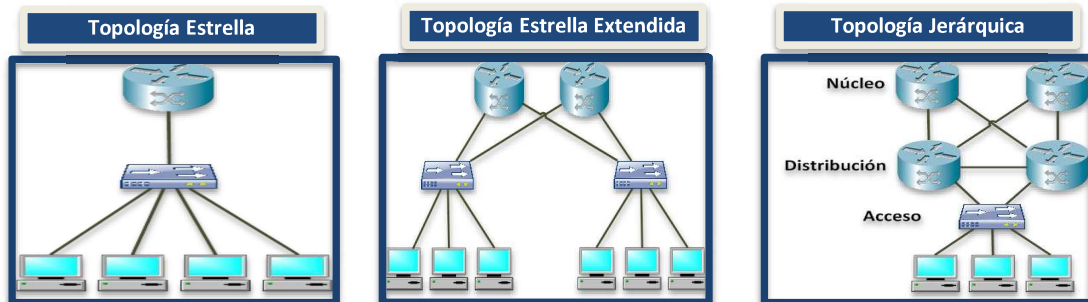
### **Topología Lógica**

La topología lógica está definida por la manera en que los componentes de la red, en este caso los *routers* se comunican entre sí, el flujo de datos a través de la Red WAN físicamente diseñada en anillo, tendría un comportamiento lógico de malla parcial debido a que todas sus sucursales están interconectadas mediante uno o dos saltos, por lo tanto los paquetes serán enviados por una u otra ruta física, acorde las métricas que se empleen o sean configuradas a nivel del Protocolo de Enrutamiento.

### **2.2.2.2 Topología Red LAN**

#### **Topología Física**

Para la interconexión de los equipos terminales en la red LAN se analizaron dos posibles alternativas, en la Figura 2.8 se ilustran estas posibles opciones: para lograr alta disponibilidad en la red, se recomendaría la implementación de un esquema redundante tanto en enlaces como en equipamiento mediante una topología de estrella extendida o mediante una topología jerárquica, sin embargo considerando que la empresa de análisis es de tipo PYME, se establece como topología física un diseño en estrella simple debido a los costos de despliegue, tomando en cuenta ciertas consideraciones.



**Figura 2.8.** Posibles Topologías Físicas para la red LAN [35]

Las consideraciones para la implementación de una LAN con topología física en estrella son:

- Equipo de borde (*router*) y concentrador (*switch*) deben tener implementada alta disponibilidad tanto a nivel de fuente como de procesadora.
- Cableado estructurado debidamente certificado al interior de cada sitio.
- Políticas de mantenimiento preventivo de toda la infraestructura.
- Monitoreo periódico del rendimiento de los equipos.

### **Topología Lógica**

Considerando que la topología lógica define la forma que los componentes de la red se comunican entre sí dentro de la red física, el flujo de datos a través de la Red LAN está definido por la tecnología Ethernet que es la que se emplea normalmente en redes LAN, esta tecnología se despliega físicamente mediante una topología física en estrella, en la cual los dispositivos terminales (computadoras) se conectan a un punto central (*switch*); y; a nivel lógico, tecnología Ethernet emplea una topología lógica en bus, en la cual el *switch* crea un dominio de colisión por cada uno de sus puertos para separar los dispositivos de usuario en múltiples segmentos físicos.

## **2.2.3 DIMENSIONAMIENTO DE LA RED**

Para el dimensionamiento de la red se debe estimar el consumo en Ancho de Banda que requerirán soportar los enlaces acorde los servicios que necesita la empresa, adicionalmente otra parte del dimensionamiento es la definición del direccionamiento IP y máscaras a emplear considerando un porcentaje adecuado de crecimiento. En esta sección se detalla la forma de cálculo de ambas premisas y se estiman las capacidades de los enlaces y direccionamiento IP para esta empresa PYME tipo.

### **2.2.3.1 Dimensionamiento de cada Servicio**

Para el cálculo del dimensionamiento de cada servicio, es necesario definir el personal por localidad que tendrá acceso y hará uso de cada servicio, a continuación se presenta una estimación de la cantidad de empleados en cada localidad por área, que tendrían acceso a cada servicio dentro de la empresa PYME tipo de análisis.

## **Servicio de Internet**

El servicio de Internet técnicamente puede ser implementado tanto de forma centralizada como de forma distribuida:

- De forma distribuida, la contratación del servicio de Internet se realizaría para cada localidad, por lo tanto en esta modalidad sería necesaria la contratación de 4 servicios de Internet para cubrir esta necesidad para todos los trabajadores de la empresa.

Si bien esta modalidad reduce la posibilidad que toda la empresa se quede sin acceso a Internet en caso de falla de uno de los enlaces hacia el ISP o por eventuales problemas del ISP en sí, se pierde el control y la posibilidad de aplicar políticas de acceso para controlar el acceso a Internet por parte de los empleados, adicionalmente sería necesaria la adquisición de equipamiento de seguridad adicional para proteger todos los puntos que tengan acceso hacia Internet, de posibles ataques y contaminación de *malware*.

- Con la contratación del servicio de Internet de forma centralizada, se logra tener control desde la Matriz, adicionalmente, el contratar una mayor capacidad en un solo punto es más económico que varios servicios de menor capacidad en algunos sitios.

Para la estimación de la Velocidad de Navegación a Internet requerida para toda la empresa, se suman las tasas de transmisión demandadas por cada localidad, para este cálculo se estima que los empleados naveguen en promedio a 750 Kbps, otro supuesto también es la simultaneidad de navegación de todos los trabajadores dentro de la empresa, este parámetro se estima en un 50% considerando que no todos los empleados estarán navegando en Internet al mismo tiempo.

El parámetro de simultaneidad dependerán del giro específico del negocio de la empresa, sin embargo para ejemplificar el dimensionamiento de este servicio para la empresa PYME tipo, se ha establecido estos parámetros considerando una empresa que requiera un uso entre medio y alto de Internet, sin llegar a requerir un servicio de Internet para uso intensivo.

Con estas consideraciones, la fórmula para el cálculo de la Velocidad de Navegación a Internet requerida por cada localidad es la siguiente:

$$\text{Velocidad de Navegación} = \frac{\text{Cantidad de Usuarios}}{\text{Usuario}} \times \frac{\text{Velocidad por Usuario}}{\text{Usuario}} \times \text{Simultaneidad}$$

A manera de ejemplo, se realiza el cálculo para la Velocidad de Navegación a Internet requerida por el personal de la Matriz:

$$\text{Velocidad de Navegación Matriz} = 87 \text{ Usuarios} \times \frac{0.75 \text{ Mbps}}{\text{Usuario}} \times 50\%$$

$$\text{Velocidad de Navegación Matriz} = 33 \text{ Mbps}$$

De la misma forma se realizan los cálculos para el resto de localidades de la empresa y la suma de todas las tasas de transmisión requeridas por todas las localidades, corresponde a la Velocidad de Internet que se deberá contratar desde la Matriz, considerando la recomendación de tener un único punto de acceso a Internet para toda la organización.

En la Tabla 2.2 se indica la Velocidad de navegación a Internet requerida por cada localidad y considerando que este servicio sería contratado desde un solo punto (Matriz), se requeriría alrededor de 44 Mbps para toda la empresa:

**Tabla 2.2.** Velocidad de navegación para el servicio de Internet

Internet				
Áreas	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Gerencia General	2			
Gerencia Financiera	6			
Gerencia Comercial	32	12	8	8
Gerencia de Operaciones	25			
Gerencia de Tecnología	16	2	1	1
Gerencia de Recursos Humanos	6			
<b>Cantidad de Usuarios Totales</b>	<b>87</b>	<b>14</b>	<b>9</b>	<b>9</b>
<b>Velocidad requerida para Navegación</b>	<b>33 Mbps</b>	<b>5 Mbps</b>	<b>3 Mbps</b>	<b>3 Mbps</b>
<b>Capacidad para Internet</b>	<b>44 Mbps</b>			

## Servicio de VoIP

La tasa de transmisión para el servicio de VoIP dependerá del códec empleado y otros factores como la cantidad de usuarios en la red y la simultaneidad esperada de llamadas, por ejemplo, la velocidad de transmisión mínima para realizar llamadas empleando un códec G.711 es de alrededor de 30 Kbps, sin embargo se recomienda dimensionar 100 Kbps para una comunicación *full duplex*, para asegurar la máxima calidad en las llamadas VoIP. [36]

Para calcular la tasa de transmisión que se requerirá para el servicio de VoIP, primero se define la cantidad de trabajadores que tendrán acceso a este servicio por localidad, también se estima el comportamiento de los usuarios en cuanto a llamadas internas y externas; y, se definen los perfiles acorde el uso que se le dará a este servicio; a cada perfil se asigna un parámetro de simultaneidad, este dependerá del uso del servicio de VoIP que cada empresa requiera, para ejemplificar este cálculo se han definido los siguientes perfiles para la empresa PYME tipo:

- **Perfil Heavy Users:** aquellos usuarios que harán uso constante del servicio, para este análisis se ha considerado al personal de Ventas, Service Desk y Recepcionistas; y, se ha estimado un factor de simultaneidad del 50% para este grupo, es decir que la mitad del personal estará al teléfono en todo momento.
- **Perfil Regular Users:** son aquellos usuarios que no harán uso constante del servicio, se ha estimado un factor de simultaneidad para este grupo del 25%, es decir que de un grupo de 4 personas una de ellas estará al teléfono en cada momento.

Con estas consideraciones, las fórmulas para el cálculo de la tasa de transmisión requerida para el servicio de VoIP por cada localidad, tanto para el tráfico de llamadas internas como externas, son las siguientes:

$$\begin{aligned} & \text{Tasa de transmisión} \\ & \text{llamadas internas} \\ & = \left[ \frac{\text{Cantidad de Heavy Users}}{\text{Cantidad de Heavy Users}} \times \% \text{ llamadas internas} \times \text{Simultaneidad} + \frac{\text{Cantidad de Regular Users}}{\text{Cantidad de Regular Users}} \times \% \text{ llamadas internas} \right. \\ & \left. \times \text{Simultaneidad} \right] \times 100 \text{ Kbps} \end{aligned}$$

*Tasa de transmisión  
llamadas externas*

$$= \left[ \frac{\text{Cantidad de Heavy Users} \times \% \text{ llamadas externas}}{\text{Heavy Users}} \times \text{Simultaneidad} + \frac{\text{Cantidad de Regular Users} \times \% \text{ llamadas externas}}{\text{Regular Users}} \times \text{Simultaneidad} \right] \times 100 \text{ Kbps}$$

A manera de ejemplo, se realiza el cálculo para la tasa de transmisión requerida por el personal de la Matriz para llamadas internas:

*Tasa de Transmisión  
llamadas internas Matriz*

$$= \left[ \sum \text{Heavy Users} \times \% \text{ llamadas internas} \times 50\% + \sum \text{Regular Users} \times \% \text{ llamadas internas} \times 25\% \right] \times \frac{100 \text{ Kbps}}{\text{Usuario}}$$

$$\text{Tasa de Transmisión llamadas internas Matriz} = 1.478 \text{ Mbps}$$

De la misma manera, se realizan los cálculos para el resto de localidades de la empresa y la cantidad de llamadas simultáneas para la contratación del servicio de Troncal Telefónica IP para toda la empresa, se calcula de la siguiente manera, considerando que el servidor de VoIP se encontrará localizado en la granja de servidores de la Matriz:

*Cantidad de Llamadas  
simultáneas*

$$= \sum \left( \frac{\# \text{ Total de Heavy Users} \times \% \text{ llamadas externas}}{\text{Heavy Users}} \right) \times \text{simultaneidad} + \sum \left( \frac{\# \text{ Total de Regular Users} \times \% \text{ llamadas externas}}{\text{Regular Users}} \right) \times \text{simultaneidad}$$

$$\text{Cantidad de Llamadas simultáneas} = 24 \times 50\% + 52.9 \times 25\%$$

$$\text{Cantidad de Llamadas simultáneas} = 25$$

En la Tabla 2.3 se indica la tasa de transmisión requerida por cada localidad para el servicio de VoIP y considerando que este servicio sería contratado desde un solo punto (Matriz), se requeriría de una Troncal Telefónica IP con capacidad de alrededor de 25 llamadas simultáneas para toda la empresa:

**Tabla 2.3.** Tasa de Transmisión para el servicio de VoIP

Telefonía IP				
Cantidad de Usuarios que usan el servicio de VoIP				
Áreas	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Gerencia General	2			
Gerencia Financiera	12	4	4	4
Gerencia Comercial	32	12	8	8
Gerencia de Operaciones	31	4	4	4
Gerencia de Tecnología	16	2	1	1
Gerencia de Recursos Humanos	9	1	1	1
<b>Total</b>	<b>102</b>	<b>23</b>	<b>18</b>	<b>18</b>
Heavy Users por área				
Gerencia General				
Gerencia Financiera				
Gerencia Comercial	10	8	5	5
Gerencia de Operaciones				
Gerencia de Tecnología	4	2	1	1
Gerencia de Recursos Humanos	1	1	1	1
Regular Users por área				
Gerencia General	2			
Gerencia Financiera	12	4	4	4
Gerencia Comercial	22	4	3	3
Gerencia de Operaciones	31	4	4	4
Gerencia de Tecnología	12			
Gerencia de Recursos Humanos	8			
Porcentaje estimado de llamadas internas por área				
Gerencia General	30%			
Gerencia Financiera	80%	90%	90%	90%
Gerencia Comercial	20%	20%	20%	20%
Gerencia de Operaciones	50%	70%	70%	70%
Gerencia de Tecnología	80%	90%	90%	90%
Gerencia de Recursos Humanos	90%	90%	90%	90%
Porcentaje estimado de llamadas externas por área				
Gerencia General	70%			
Gerencia Financiera	20%	10%	10%	10%
Gerencia Comercial	80%	80%	80%	80%
Gerencia de Operaciones	50%	30%	30%	30%
Gerencia de Tecnología	20%	10%	10%	10%
Gerencia de Recursos Humanos	10%	10%	10%	10%
Cálculo de tasas de transmisión requeridas				
Tasa de Transmisión requerida para tráfico de voz interno	1.478 Mbps	0.395 Mbps	0.315 Mbps	0.315 Mbps
Tasa de Transmisión requerida para tráfico de voz externo	1.448 Mbps	0.455 Mbps	0.31 Mbps	0.31 Mbps
CANTIDAD DE LLAMADAS SIMULTÁNEAS	25			

### Servicio de Transmisión de Datos

Para la estimación de la velocidad requerida por localidad para el servicio de datos para el consumo de aplicativos internos de la empresa como ERPs y CRMs, primero se define la cantidad de empleados que harán uso de estos aplicativos por localidad y se define la concurrencia con la que los empleados consumirán este tipo de aplicativos. Por lo tanto para ejemplificar esta estimación, se establece un factor de simultaneidad del 50% y se



define una tasa de transmisión de datos de 512 Kbps por usuario, estos parámetros dependerán de cada empresa:

Con estas consideraciones, la fórmula para el cálculo de la velocidad de transmisión requerida para el servicio de transmisión de datos por cada localidad es la siguiente:

$$\text{Tasa de Transmisión} = \frac{\text{Cantidad de Usuarios}}{\text{Simultaneidad}} \times 512 \text{ Kbps}$$

A manera de ejemplo, se realiza el cálculo para la tasa de transmisión requerida por el personal de la Matriz:

$$\text{Tasa de Transmisión Matriz} = 82 \text{ Usuarios} \times 50\% \times 512 \text{ Kbps}$$

$$\text{Tasa de Transmisión Matriz} = 21 \text{ Mbps}$$

En la Tabla 2.4 se indica la velocidad de transmisión requerida por cada localidad para el servicio de transmisión de datos:

**Tabla 2.4.** Tasa de Transmisión para el servicio de Datos

Datos (para CRM / ERP)				
Áreas	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Gerencia General	0			
Gerencia Financiera	10	4	4	4
Gerencia Comercial	23	10	7	7
Gerencia de Operaciones	29	4	4	4
Gerencia de Tecnología	14	2	1	1
Gerencia de Recursos Humanos	6			
<b>Cantidad de Usuarios Totales</b>	<b>82</b>	<b>20</b>	<b>16</b>	<b>16</b>
<b>Tasa de Transmisión requerida</b>	<b>21 Mbps</b>	<b>5 Mbps</b>	<b>4 Mbps</b>	<b>4 Mbps</b>

### **Servicio de Videoconferencia** [37] [38]

Para el servicio de videoconferencia se consideran principalmente los siguientes factores: códec de audio, códec de video, cantidad de imágenes por segundo, formato y resolución de video; adicionalmente se debe considerar la cantidad de sitios remotos y salas de videoconferencia participantes.

En escenarios de videoconferencia de tipo punto – multipunto, todos los sitios remotos establecen una sesión *full-duplex* hacia un concentrador, de tal forma que los sitios remotos requieren únicamente de la tasa de transmisión negociada con el concentrador; mientras que el concentrador requiere soportar una capacidad igual a la tasa de

transmisión de todos los sitios remotos. Los estándares de compresión H.264 y H.265 son los más empleados para videoconferencia y video llamada, por la baja tasa de transferencia (1 a 4 Mbps) que requiere y su aceptable o buena calidad.

Para la estimación de la velocidad de transmisión que se requiere para el servicio de videoconferencia, se define la cantidad de sitios participantes por localidad, para la empresa PYME tipo se ha definido que cada localidad cuente con una sala de videoconferencia y la velocidad de transmisión para lograr una buena calidad se establece en 3 Mbps por localidad.

Con estas consideraciones, la fórmula para el cálculo de la velocidad de transmisión requerida para el servicio de videoconferencia por cada localidad es la siguiente:

$$\text{Velocidad de Transmisión} = \text{Cantidad de Salas participantes} \times 3 \text{ Mbps}$$

A manera de ejemplo, se realiza el cálculo para la tasa de transmisión requerida por el personal de la Matriz:

$$\text{Velocidad de Transmisión Matriz} = 1 \text{ Sala de Videoconferencia} \times 3 \text{ Mbps}$$

$$\text{Velocidad de Transmisión Matriz} = 3 \text{ Mbps}$$

En la Tabla 2.5 se indica la velocidad de transmisión requerida por cada localidad para el servicio de videoconferencia y considerando que el concentrador será el encargado de centralizar este servicio en la Matriz, este deberá soportar una velocidad de 12 Mbps para una videoconferencia simultánea de todas las localidades de la empresa:

**Tabla 2.5.** Tasa de Transmisión para el servicio de Videoconferencia

Videoconferencia				
Áreas	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Salas para Videoconferencia	1	1	1	1
<b>Tasa de Transmisión requerida</b>	3 Mbps	3 Mbps	3 Mbps	3 Mbps

### Servicio de Streaming de Video [39]

Para obtener una resolución constante de video SD (*Standard Definition*), es recomendable tener una conexión de al menos 2 Mbps, mientras que para videos en HD (*High Definition*), 3D o 4K, es recomendable una conexión más alta, a continuación se resume la experiencia esperada acorde la velocidad de transmisión disponible:

- **2 Mbps:** para videos de definición estándar (480p).
- **4 Mbps:** para videos de alta definición (720p – 1080p).
- **5 Mbps:** para óptima experiencia de videos de alta definición.
- **15 Mbps:** para videos 4K, se recomienda 25 Mbps.

Para la estimación de la velocidad de transmisión que se requeriría para el servicio de *streaming* de video, se define la cantidad de trabajadores por localidad que tendrá acceso a este servicio, para la empresa PYME tipo se ha definido que únicamente el departamento de ventas tendrá acceso a *streaming* de video, por ejemplo para capacitaciones o programas de educación continua, se define el parámetro de simultaneidad con el que el personal consumirá este servicio y la velocidad de transmisión para obtener una buena experiencia se establece en 5 Mbps.

Con estas consideraciones, la fórmula para el cálculo de la velocidad de transmisión requerida para el servicio de *streaming* de video por cada localidad es la siguiente:

$$\text{Velocidad de Transmisión} = \frac{\text{Cantidad de Usuarios}}{\text{Simultaneidad}} \times 5 \text{ Mbps}$$

A manera de ejemplo, se realiza el cálculo para la tasa de transmisión requerida por el personal de la Matriz:

$$\text{Velocidad de Transmisión} = 20 \text{ Usuarios} \times 10\% \times 5 \text{ Mbps}$$

$$\text{Velocidad de Transmisión Matriz} = 10 \text{ Mbps}$$

En la Tabla 2.6 se indica la velocidad de transmisión requerida por cada localidad para el servicio de *streaming* de video y considerando que el servidor será el encargado de

centralizar este servicio en la Matriz, éste deberá soportar una velocidad de 23 Mbps para este servicio:

**Tabla 2.6.** Tasa de Transmisión para el servicio de *Streaming* de Video

Streaming de Video				
Áreas	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Gerencia Comercial	20	10	7	7
<b>Tasa de Transmisión requerida</b>	<b>10 Mbps</b>	<b>5 Mbps</b>	<b>4 Mbps</b>	<b>4 Mbps</b>

### **Servicio de Correo Electrónico**

El servicio de correo electrónico es indispensable dentro de cualquier empresa y requiere poca capacidad para su transmisión, un correo puede pesar entre unos pocos Kilo Bytes hasta decenas de Mega Bytes, para el cálculo de la tasa de transmisión requerida para este servicio por cada localidad, primero se ha definido la cantidad de usuarios que harán uso de este servicio, luego se estima una cantidad aproximada de correos diarios tanto enviados como recibidos y el peso de los mismos; y, con esta información se calcula el peso total de los correos diarios por localidad.

Con estas consideraciones, para calcular la velocidad de transmisión requerida para este servicio, se distribuyen los correos a lo largo de la jornada laboral (8 horas):

$$Tasa\ de\ Transmisión = \frac{KB\ totales\ por\ localidad}{por\ día\ laboral} \times \frac{8\ bits}{1\ Byte} \times \frac{1\ día\ laboral}{8\ horas} \times \frac{1\ hora}{60\ minutos} \times \frac{1\ minuto}{60\ segundos}$$

A manera de ejemplo, se realiza el cálculo para la tasa de transmisión requerida por el personal de la Matriz:

$$Tasa\ de\ Transmisión\ Matriz = \frac{4060\ KB}{por\ día\ laboral} \times \frac{8\ bits}{1\ Byte} \times \frac{1\ día\ laboral}{8\ horas} \times \frac{1\ hora}{60\ minutos} \times \frac{1\ minuto}{60\ segundos}$$

$$Velocidad\ de\ Transmisión\ Matriz = 1.128\ Kbps$$

En la Tabla 2.7 se indica la tasa de transmisión requerida por cada localidad para el servicio de correo electrónico, calculada en base a los supuestos de cantidad de correos diarios enviados y recibidos y peso crítico promedio de cada correo. Considerando que el servidor será el encargado de centralizar este servicio en la Matriz, este deberá soportar una tasa de transmisión de 1.854 Mbps:

**Tabla 2.7.** Tasa de Transmisión para el servicio de Correo Electrónico

Correo Electrónico						
Áreas	correos diarios	peso por correo (KB)	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
Gerencia General	100	500	2			
Gerencia Financiera	60	500	12	4	4	4
Gerencia Comercial	60	1000	32	12	8	8
Gerencia de Operaciones	60	500	31	4	4	4
Gerencia de Tecnología	60	500	16	2	1	1
Gerencia de Recursos Humanos	60	500	9	1	1	1
<b>Cantidad de Usuarios Totales</b>			<b>102</b>	<b>23</b>	<b>18</b>	<b>18</b>
KB diarios			4060	1050	780	780
<b>Tasa de Transmisión requerida</b>			<b>1.128 Kbps</b>	<b>0.292 Kbps</b>	<b>0.217 Kbps</b>	<b>0.217 Kbps</b>

### 2.2.3.2 Dimensionamiento de los enlaces

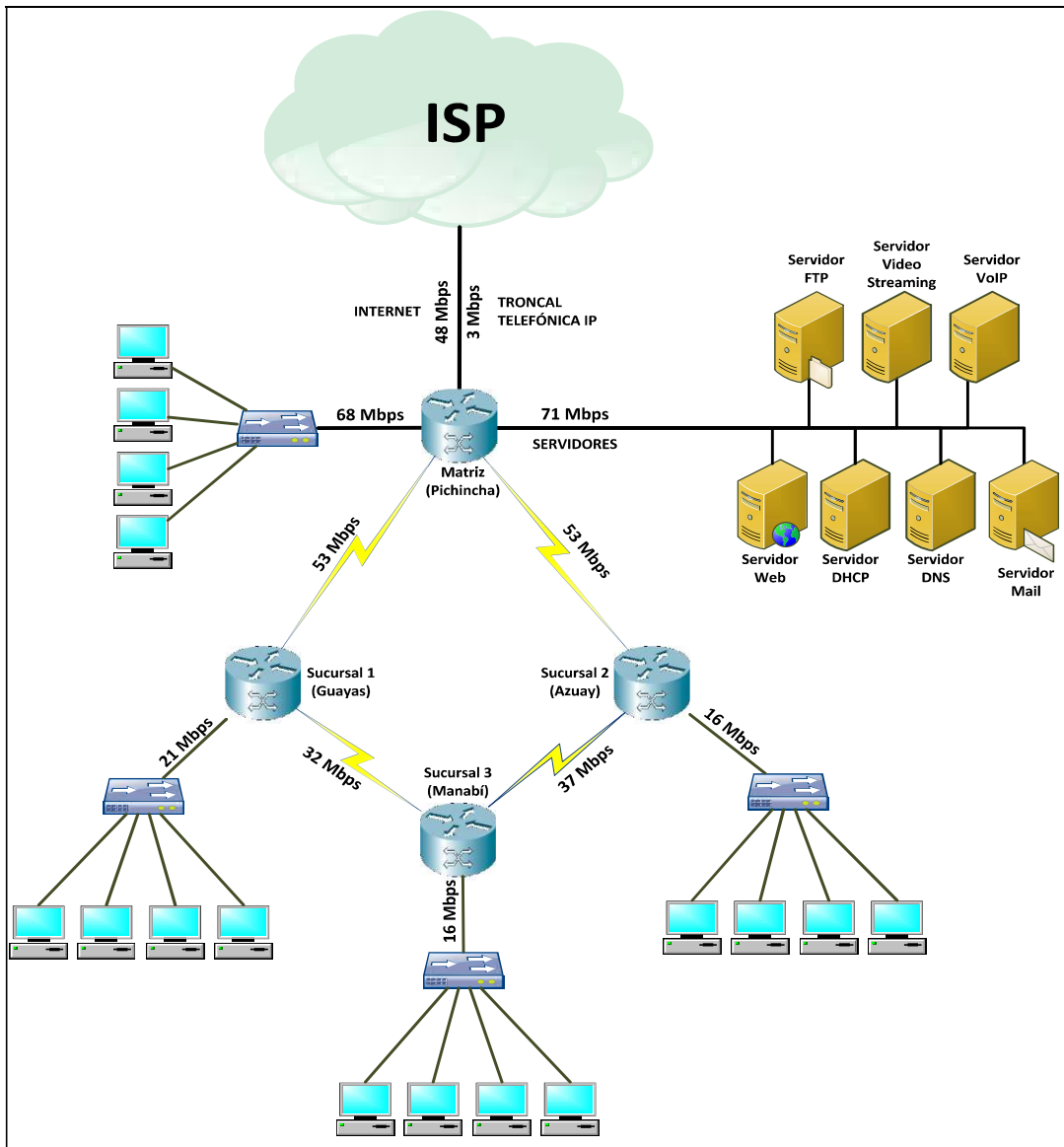
En apartados anteriores, se detallan las consideraciones para la estimación de la velocidad requerida para cada servicio y a manera de ejemplo, se indica la forma de calcular estas capacidades para una de las localidades de la empresa PYME tipo en estudio; en la Tabla 2.8 se resumen todas las velocidades requeridas por servicio y por localidad.

**Tabla 2.8.** Resumen de las capacidades de transmisión de todos los enlaces

CÁLCULO DE CAPACIDAD DE LOS ENLACES						
Tipo de servicio	Servicios	Matriz	Sucursal 1	Sucursal 2	Sucursal 3	Total + 10% crecimiento
<b>Servicio de contratación Externa</b>	Internet	33 Mbps	5 Mbps	3 Mbps	3 Mbps	48 Mbps
	Telefonía IP	1.448 Mbps	0.455 Mbps	0.31 Mbps	0.31 Mbps	3 Mbps
<b>Servidores Internos de la Empresa</b>	Telefonía IP	1.478 Mbps	0.395 Mbps	0.315 Mbps	0.315 Mbps	71 Mbps
	Datos (para CRM / ERP)	21 Mbps	5 Mbps	4 Mbps	4 Mbps	
	Videoconferencia	3 Mbps	3 Mbps	3 Mbps	3 Mbps	
	Streaming de Video	10 Mbps	5 Mbps	4 Mbps	4 Mbps	
	Correo Electrónico	1.128 Kbps	0.292 Kbps	0.217 Kbps	0.217 Kbps	
<b>Capacidad Total por sitio</b>		<b>62 Mbps</b>	<b>19 Mbps</b>	<b>15 Mbps</b>	<b>15 Mbps</b>	
<b>Crecimiento 10%</b>		<b>68 Mbps</b>	<b>21 Mbps</b>	<b>16 Mbps</b>	<b>16 Mbps</b>	

Para el cálculo de las velocidades de transmisión requeridas por cada localidad, se suman las velocidades de todos los servicios anteriormente calculados, con lo cual se determina que para la matriz se requiere una tasa de 68 Mbps, para la Sucursal 1 se estimaron 21 Mbps y para las Sucursales 2 y 3 se estimaron 16 Mbps; todas las tasas de transmisión calculadas incluyen un 10% de crecimiento.

De la sumarización de velocidades de navegación a Internet, se determina que la velocidad necesaria considerando un 10% de crecimiento es de 48 Mbps para toda la empresa, la tasa de transmisión que soportará el consumo de todos los aplicativos internos de la empresa, por parte de todos los trabajadores es de 71 Mbps y de igual forma que en el caso anterior, ésta considera un 10% de crecimiento.



**Figura 2.9.** Esquema de Tasas de Transmisión de la Red

En la Figura 2.9 se ilustran las tasas de transmisión requeridas para cada localidad, la velocidad requerida para la navegación a Internet y la tasa de transmisión para los aplicativos internos de la empresa como VoIP, correo electrónico, videoconferencia, *streaming* de video, entre otros.

En la imagen anterior también se indican las capacidades requeridas para los enlaces WAN que conectarán las diferentes localidades entre sí, estas capacidades obedecen a un diseño tanto en condiciones normales como en caso de falla de alguno de los enlaces, por lo tanto, la capacidad calculada para cada uno de los enlaces contempla una eventual contingencia ante fallos, esto es:

- En caso de falla del enlace entre las Sucursales 1 y 3, el tráfico de la sucursal 3 deberá ser dirigido a través de Azuay; por lo que el enlace entre Azuay y la Matriz deberá soportar la capacidad para el transporte de información tanto de la Sucursal 3 (16 Mbps) como de la Sucursal 2 (16 Mbps), es decir, dicho enlace deberá ser de al menos 32 Mbps.
- De igual forma que en el caso anterior, en caso de falla del enlace entre las Sucursales 2 y 3, el tráfico de la sucursal 3 deberá ser dirigido a través de Guayas; por lo que el enlace entre Guayas y la Matriz deberá soportar la capacidad para el transporte de información tanto de la Sucursal 3 (16 Mbps) como de la Sucursal 1 (21 Mbps), es decir, dicho enlace deberá ser de al menos 37 Mbps.
- En caso de falla del enlace entre la Matriz y la Sucursal 1, el tráfico de las Sucursales 1, 3 y 2 deberá ser dirigido a través de Azuay; por lo que el enlace entre Manabí y Azuay deberá soportar la capacidad para el transporte de información tanto de la Sucursal 1 (21 Mbps) como de la Sucursal 3 (16 Mbps), es decir, dicho enlace deberá ser de al menos 37 Mbps; y, el enlace entre Azuay y la Matriz deberá soportar la capacidad para el transporte de información de las Sucursales 1, 3 y 2, es decir, dicho enlace deberá ser de al menos 53 Mbps.
- Finalmente, si falla el enlace entre la Matriz y la Sucursal 2, el tráfico de las sucursales 2, 3 y 1 deberá ser dirigido a través de Guayas; por lo que el enlace entre Guayas y Manabí deberá soportar la capacidad para el transporte de información tanto de la Sucursal 2 (16 Mbps) como de la Sucursal 3 (16 Mbps), es decir, dicho enlace deberá ser de al menos 32 Mbps; y, el enlace entre Guayas y la Matriz deberá soportar la capacidad para el transporte de información de las Sucursales 1, 3 y 2, es decir, dicho enlace deberá ser de al menos 53 Mbps.

### 2.2.3.3 VLAN y Direccionamiento IP

#### Definición de las VLAN

Los equipos de capa 2 como los *switches* propagan continuamente cierto tipo de paquetes o tráfico dentro del dominio de *broadcast*, dentro de este tráfico está *broadcast*, *multicast* y tráfico con destino desconocido; este tráfico impacta a cada dispositivo dentro del dominio de *broadcast*, al ancho de banda de los enlaces de dichos dispositivos y a su capacidad de procesamiento; para hacer frente a estos inconvenientes se crean las redes LAN Virtuales (VLAN), las VLAN a más de solucionar estos problemas, proveen privacidad respecto a personas ajenas a la VLAN, reducción de latencia y facilidad para armar grupos de trabajo dentro de las empresas.

Por lo tanto para el diseño de la red de la empresa PYME tipo, se definen las VLAN acorde su estructura organizacional detallada en apartados anteriores:

- VLAN de la Gerencia General
- VLAN de la Gerencia Comercial
- VLAN de la Gerencia de Operaciones
- VLAN de la Gerencia Financiera
- VLAN de la Gerencia de Tecnología
- VLAN de la Gerencia de Recursos Humanos

La VLAN de la Gerencia General es requerida únicamente en la matriz y el resto de VLAN deberán ser implementadas tanto en la Matriz como en las Sucursales; en la Tabla 2.9 se indica la cantidad de empleados estimados por VLAN en cada una de las localidades:

**Tabla 2.9.** Empleados por VLAN en cada Localidad

VLAN	Matriz	Sucursal 1	Sucursal 2	Sucursal 3
VLAN Gerencia General	2	0	0	0
VLAN Comercial	32	12	8	8
VLAN Operaciones	31	4	4	4
VLAN Finanzas	12	4	4	4
VLAN Tecnología	16	2	1	1
VLAN Recursos Humanos	9	1	1	1



## Definición del Direcccionamiento en IPv6

De acuerdo a la cantidad de empleados estimados por área o departamento, se procede a dimensionar las subredes para cada VLAN por cada localidad, para esta estimación se ha considerado un crecimiento del 100% debido a que a diferencia del crecimiento estimado para los enlaces LAN y WAN, el crecimiento considerado para el dimensionamiento de las subredes no involucra costos adicionales; mientras que en el caso de los enlaces LAN y WAN, se estimó un crecimiento moderado a corto plazo por los costos adicionales que incurriría la empresa al contratar capacidades mayores, cuando lo aconsejable es que solicite capacidades mayores a su Proveedor de Servicios conforme vaya creciendo la empresa.

Con esta consideración, se prevén los bits requeridos para *hosts* en cada VLAN de cada una de las localidades, en la Tabla 2.10 se detalla la cantidad de usuarios estimados para una empresa PYME tipo por área o departamento, se indica también la cantidad de usuarios con un crecimiento del 100% y los bits para *hosts* en cada VLAN:

**Tabla 2.10.** Dimensionamiento del direccionamiento IPV6

VLAN	Matriz		
	Cantidad de Usuarios	Crecimiento del 100%	Bits para Hosts
Gerencia General	2	4	2
Comercial	32	64	6
Operaciones	31	62	6
Finanzas	12	24	5
Tecnología	16	32	5
Recursos Humanos	9	18	5

VLAN	Sucursal 1		
	Cantidad de Usuarios	Crecimiento del 100%	Bits para Hosts
Gerencia General			
Comercial	12	24	5
Operaciones	4	8	3
Finanzas	4	8	3
Tecnología	2	4	2
Recursos Humanos	1	2	1

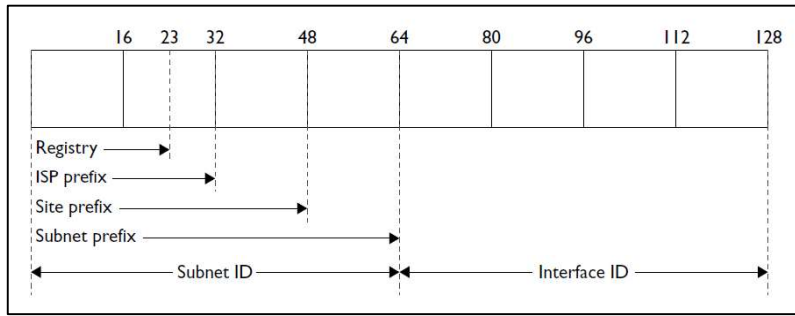
  

VLAN	Sucursal 2		
	Cantidad de Usuarios	Crecimiento del 100%	Bits para Hosts
Gerencia General			
Comercial	8	16	4
Operaciones	4	8	3
Finanzas	4	8	3
Tecnología	1	2	1
Recursos Humanos	1	2	1

VLAN	Sucursal 3		
	Cantidad de Usuarios	Crecimiento del 100%	Bits para Hosts
Gerencia General			
Comercial	8	16	4
Operaciones	4	8	3
Finanzas	4	8	3
Tecnología	1	2	1
Recursos Humanos	1	2	1

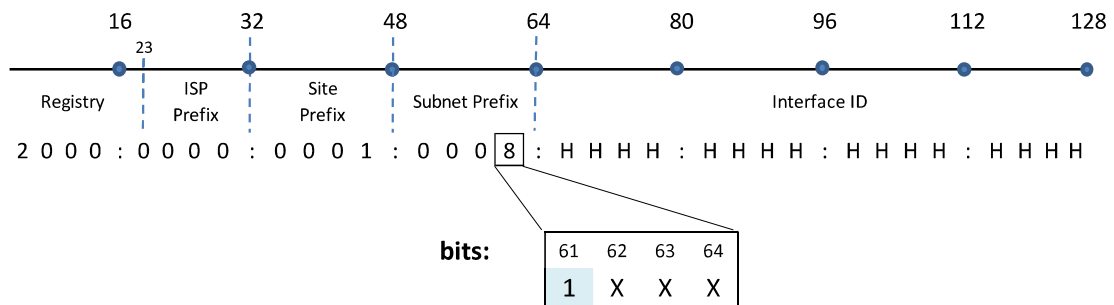
En una dirección IPv6 los primeros 23 bits son para el *Registry* que es asignado por la IANA, los siguientes 9 bits corresponden al prefijo del ISP, seguidos de 16 bits del *Site Prefix* para identificar a la empresa cliente del ISP, 16 bits para asignar subredes dentro de la empresa y los últimos 64 bits corresponden al identificador de la interfaz, en la Figura 2.10 se ilustra este formato de las direcciones IPv6:



**Figura 2.10.** Formato de Direcciones IPv6 tipo *Unicats*

Por lo tanto, el ISP es quien asigna el direccionamiento a cada cliente o empresa contratante del servicio de Internet, lo común es que se asigne una máscara entre /48 y /56 para empresas entre medianas y grandes, mientras que para PYMES se podría asignar una máscara menor; y, el direccionamiento asignado es de tipo Global.

A continuación se indica a manera de ejemplo el direccionamiento IPv6 que asignaría un ISP a una PYME: el *Registry* podría ser 2000, el prefijo del ISP es aquel que le haya sido asignado, para este ejemplo se ha seteado estos bits a ceros; el *Site Prefix* identifica a cada cliente, en este caso identifica a la PYME por lo que se ha seteado estos dígitos en 0001; finalmente, el *Subnet Prefix* mínimo que necesita la PYME tipo de análisis es de al menos 3 bits para subredes, por lo tanto la subred IPv6 mínima que se le asignaría a la PYME considerando todos los supuestos indicados sería: **2000:0:1:8::/61**.



Las subredes a habilitar con 3 bits son:

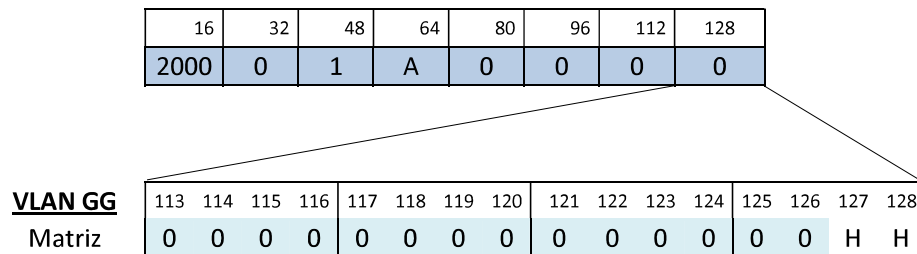
2000:0:1:8::/127      Para enlace WAN hacia el ISP

2000:0:1:9::/125	Para la granja de servidores
2000:0:1:A::/126	Para la VLAN de la Gerencia General
2000:0:1:B::/120	Para la VLAN de la Gerencia de Operaciones
2000:0:1:C::/120	Para la VLAN de la Gerencia Comercial
2000:0:1:D::/121	Para la VLAN de la Gerencia de Recursos Humanos
2000:0:1:E::/121	Para la VLAN de la Gerencia Técnica
2000:0:1:F::/121	Para la VLAN de la Gerencia Financiera

Una vez definidas las VLAN por área o departamento, se identifica la necesidad de dividir a su vez cada VLAN para asignar una subred a cada localidad dentro de la misma VLAN, con esto se logra una mejor organización lógica, simplifica la administración de la red y facilita el control del crecimiento de la misma.

**Direccionamiento VLAN Gerencia General:** esta VLAN requiere 2 bits para *hosts* y se implementa únicamente en la Matriz. Su direccionamiento es:

- VLAN GG para la Matriz: 2000:0:1:A::/126



**Direccionamiento VLAN Operaciones:** esta VLAN es requerida tanto en la Matriz como en las 3 Sucursales, para cubrir la demanda de IPs para el personal de la Matriz se requieren 6 bits de *hosts*, mientras que para las Sucursales se necesitarán 3 bits de *hosts*; su direccionamiento es:

- VLAN OPE para la Matriz: 2000:0:1:B::/122
- VLAN OPE para la Sucursal 1: 2000:0:1:B:4/125
- VLAN OPE para la Sucursal 2: 2000:0:1:B:8/125
- VLAN OPE para la Sucursal 3: 2000:0:1:B:C/125
- VLAN OPE sumariada: **2000:0:1:B::/120**

16	32	48	64	80	96	112	128
2000	0	1	B	0	0	0	0

**VLAN OPE**

	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
Matriz	0	0	0	0	0	0	0	0	0	0	H	H	H	H	H	H
Sucursal 1	0	0	0	0	0	0	0	0	0	1	0	0	0	H	H	H
Sucursal 2	0	0	0	0	0	0	0	0	1	0	0	0	0	H	H	H
Sucursal 3	0	0	0	0	0	0	0	0	1	1	0	0	0	H	H	H

**Direccionamiento VLAN Comercial:** esta VLAN también es requerida en la Matriz y en las 3 Sucursales, para la Matriz se requieren 6 bits de *hosts*, mientras que para la Sucursal 1 se necesitarán 5 bits de *hosts* y para las Sucursales 2 y 3 se necesitarán 4 bits de *hosts*; su direccionamiento es:

- VLAN OPE para la Matriz: 2000:0:1:C::/122
- VLAN OPE para la Sucursal 1: 2000:0:1:C::4/123
- VLAN OPE para la Sucursal 2: 2000:0:1:C::8/124
- VLAN OPE para la Sucursal 3: 2000:0:1:C::C/124
- VLAN OPE sumariada: **2000:0:1:C::/120**

16	32	48	64	80	96	112	128
2000	0	1	C	0	0	0	0

**VLAN COM**

	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
Matriz	0	0	0	0	0	0	0	0	0	0	H	H	H	H	H	H
Sucursal 1	0	0	0	0	0	0	0	0	0	1	0	H	H	H	H	H
Sucursal 2	0	0	0	0	0	0	0	0	1	0	0	0	H	H	H	H
Sucursal 3	0	0	0	0	0	0	0	0	1	1	0	0	H	H	H	H

**Direccionamiento VLAN Recursos Humanos:** esta VLAN también es requerida en la Matriz y en las 3 Sucursales, para la Matriz se requieren 5 bits de *hosts*, mientras que para las Sucursales se necesitará 1 bit para *hosts*; su direccionamiento es:

- VLAN OPE para la Matriz: 2000:0:1:D::/123
- VLAN OPE para la Sucursal 1: 2000:0:1:D::2/127
- VLAN OPE para la Sucursal 2: 2000:0:1:D::4/127
- VLAN OPE para la Sucursal 3: 2000:0:1:D::6/127
- VLAN OPE sumariada: **2000:0:1:D::/121**

	16	32	48	64	80	96	112	128	
	2000	0	1	D	0	0	0	0	

<b>VLAN RRHH</b>	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
Matriz	0	0	0	0	0	0	0	0	0	0	0	H	H	H	H	H
Sucursal 1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	H
Sucursal 2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	H
Sucursal 3	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	H

**Direccionamiento VLAN Técnica:** esta VLAN también es requerida en la Matriz y en las 3 Sucursales, para la Matriz se requieren 5 bits de *hosts*, mientras que para la Sucursal 1 se necesitarán 2 bits de *hosts* y para las Sucursales 2 y 3 se necesitará 1 bit para *hosts*; su direccionamiento es:

- VLAN OPE para la Matriz: 2000:0:1:E::/123
- VLAN OPE para la Sucursal 1: 2000:0:1:E::2/126
- VLAN OPE para la Sucursal 2: 2000:0:1:E::4/127
- VLAN OPE para la Sucursal 3: 2000:0:1:E::6/127
- VLAN OPE sumariada: 2000:0:1:E::/121

16	32	48	64	80	96	112	128
2000	0	1	E	0	0	0	0

<u>VLAN TEC</u>	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
Matriz	0	0	0	0	0	0	0	0	0	0	0	H	H	H	H	H
Sucursal 1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	H	H
Sucursal 2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	H
Sucursal 3	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	H

**Direccionamiento VLAN Financiera:** esta VLAN también es requerida en la Matriz y en las 3 Sucursales, para la Matriz se requieren 5 bits de *hosts*, mientras que para las Sucursales se necesitarán 3 bits de *hosts*; su direccionamiento es:

- VLAN OPE para la Matriz: 2000:0:1:F::/123
- VLAN OPE para la Sucursal 1: 2000:0:1:F::2/125
- VLAN OPE para la Sucursal 2: 2000:0:1:F::4/125
- VLAN OPE para la Sucursal 3: 2000:0:1:F::6/125
- VLAN OPE sumariada: **2000:0:1:F::/121**

16	32	48	64	80	96	112	128
2000	0	1	F	0	0	0	0

<u>VLAN FIN</u>	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
Matriz	0	0	0	0	0	0	0	0	0	0	0	H	H	H	H	H
Sucursal 1	0	0	0	0	0	0	0	0	0	0	1	0	0	H	H	H
Sucursal 2	0	0	0	0	0	0	0	0	0	1	0	0	0	H	H	H
Sucursal 3	0	0	0	0	0	0	0	0	0	1	1	0	0	H	H	H

A manera de ilustración gráfica, a continuación en la Figura 2.11 se indica el diagrama general de la red con su respectivo direccionamiento IP por VLAN en cada Localidad:

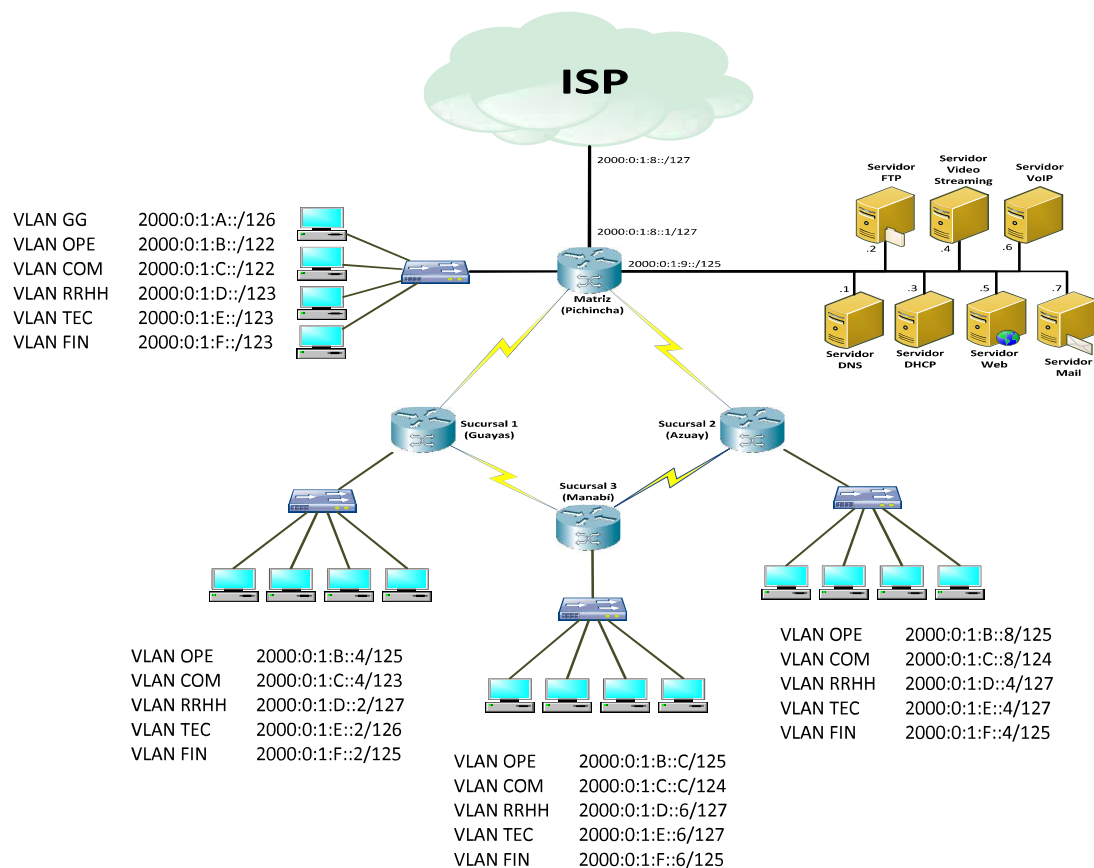


Figura 2.11. Ilustración de la Red con el direccionamiento IPv6 definido

## 2.2.4 PROTOCOLO DE ENRUTAMIENTO [33] [40] [41]

De forma similar a IPv4, los *routers* en IPv6 encuentran los mejores caminos hacia los destinos basándose en métricas y distancias administrativas, los *routers* que trabajan con IPv6 encuentran el prefijo de más amplia coincidencia en las tablas de ruteo IPv6 para enviar el paquete hacia su destino. La principal diferencia es que el router que trabaja con IPv6 revisa 128 bits para tomar las decisiones de ruteo en lugar de 32 bits.

IPv6 soporta tanto enrutamiento estático como dinámico, los protocolos soportados para el enrutamiento dinámico dentro de sistemas autónomos (enrutamiento de sistemas intrautónomos) son: RIPng, OPSFv3, IS-IS para IPv6 y EIGRP para IPv6; mientras que MP-BGP4 es empleado para el enrutamiento de sistemas interautónomos (enrutamiento entre dos o más sistemas autónomos).

Los protocolos OSPFv3 e IS-IS para IPv6 son empleados principalmente en redes de proveedores de servicio de tipo *Carriers* Nacionales o ISPs, estos protocolos de estado de enlace se emplean en topologías jerárquicas, su tiempo de convergencia es rápido y para determinar el costo de un enlace emplean diversas variables; no son muy empleados en redes empresariales por su relativa complejidad de implementación.

Por otra parte los protocolos de vector distancia: RIPng y EIGRP para IPv6, son ampliamente implementados en redes empresariales, su tiempo de convergencia es más lento y el cálculo de su métrica es más simple que el de los protocolos de estado de enlace. En la Tabla 2.11 se detallan las principales diferencias de estos protocolos de enrutamiento para sistemas intrautónomos en IPv6:

**Tabla 2.11.** Comparativa de protocolos de enrutamiento para IPv6

RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6
Estándar en la Industria.	Antes propietario, ahora estándar en la industria.	Estándar en la Industria.	Estándar en la Industria.
Protocolo de vector distancia.	Protocolo de vector distancia.	Protocolo de estado de enlace.	Protocolo de estado de enlace.
Utilizado en redes Empresariales.	Utilizado en redes Empresariales.	Utilizado en redes Empresariales, Proveedores de Servicios de Internet y Centros de Datos.	Utilizado en redes de Proveedores de Servicios de Internet.
Admite máximo 15 saltos, registra solo el mejor camino	Balancea carga sobre 16 rutas de igual costo.	Usa áreas para formar la topología jerárquica.	Usa niveles para formar topologías jerárquicas.
Tiempo de convergencia lento.	Tiempo de convergencia medio.	Tiempo de convergencia rápido.	Tiempo de convergencia rápido.
Métrica basada en número de saltos.	Métrica basada en ancho de banda y en el valor acumulado del retardo en el camino.	Costo determinado por el ancho de banda.	Costo basado en la métrica (Costo, Retraso, Costo Monetario de la utilización de los enlaces y Error).

El protocolo RIP es el protocolo de enrutamiento por vector de distancia más antiguo y a pesar que carece de la sofisticación de los protocolos de enrutamiento más avanzados, su simplicidad y compatibilidad con la mayoría de fabricantes, hace que este sea ampliamente utilizado. Por lo tanto, considerando el diagrama lógico de red de la PYME tipo, se establece como la mejor alternativa el empleo del protocolo RIPng, mientras que al tratarse de una empresa de mediana a grande se recomienda emplear EIGRP para IPv6 u OSPFv3.



## 2.2.5 PRIORIDAD DE TRÁFICO PARA LA APLICACIÓN DE QoS [33] [42]

Tal como se indicó en el capítulo anterior, una de las funcionalidades que tiene IPv6 es que la cabecera puede incluir información para Calidad de Servicio (QoS), mediante una etiqueta que identifica el tipo de tráfico, esto permite que los dispositivos intermedios de la red no tengan que examinar el contenido dentro de los paquetes, las cabeceras TCP/UDP y la información del *payload*, para poder clasificar el tráfico para una aplicación correcta de QoS.

Considerando que la red de servicios convergentes objeto del presente análisis, contempla los servicios de Internet, VoIP, datos, videoconferencia, *streaming* de video y correo electrónico, es necesario la priorización de todo este tipo de tráfico para lograr una correcta aplicación de QoS; a continuación se define en orden de criticidad las aplicaciones de la empresa PYME tipo de análisis:

1. **Aplicaciones de Tiempo Real**: son todas aquellas aplicaciones que se transmiten en tiempo real, son interactivas o bidireccionales; en esta categoría están los servicios de videoconferencia y voz sobre IP; estas aplicaciones requieren garantías mínimas para un *throughput* variable, bajos índices de pérdida de paquetes, bajo retardo y bajo *jitter*.
2. **Video Unidireccional**: el tráfico de *streaming* de video es unidireccional y generalmente no se ve afectado por el retardo, el video es muy sensible a pérdida o descarte de paquetes debido a que la información transportada por los paquetes es enviada de forma comprimida.
3. **Datos Críticos**: se refiere a aplicaciones corporativas de las cuales depende el normal desarrollo del giro de negocio de la empresa, por ejemplo los CRMs y ERPs; estas aplicaciones requieren un Ancho de Banda garantizado y bajo retardo. A pesar que este tipo de aplicaciones generalmente requieren un bajo *throughput*, deben ser priorizadas respecto a otros tipos de tráfico de datos para garantizar un buen desempeño de estos aplicativos, aún en situaciones de congestión.
4. **Datos no Críticos**: son aquellas aplicaciones de datos categorizadas por la empresa como no críticas, para las cuales el tiempo de respuesta puede tener un

rango de tolerancia mucho más amplio que el de las aplicaciones críticas; dentro de esta categoría están las aplicaciones de tipo intranet, estas son aplicaciones adaptativas (generalmente basadas en TCP), requieren un *throughput* garantizado relativamente alto y variable.

5. **Mejor Esfuerzo**: para aplicaciones poco exigentes en relación a los requisitos de red (retardo, *jitter*, *throughput*), dentro de esta categoría están las aplicaciones asociadas a la navegación en Internet y al correo electrónico, estas aplicaciones tienen una buena tolerancia a descarte de paquetes y soportan valores altos de tiempos de ida y vuelta (RTT<sup>3</sup>).

---

<sup>3</sup> **RTT (Round Trip Time)**: es el tiempo que tarda un paquete de datos enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino. Este valor es interviente de modo crucial en la eficiencia de numerosos sistemas: por ejemplo, durante la carga de una página internet utilizando el protocolo HTTP.

## CAPÍTULO 3

### 3 IMPLEMENTACIÓN DEL PROTOTIPO [43] [44] [45]

#### 3.1 CONSIDERACIONES DE DISEÑO

En las redes IP se puede proporcionar calidad de servicio a través de ciertas metodologías conocidas, tales como las estrategias de manipulación de paquetes dado el caso se presenten congestiones; o evitar que se alcance tal estado, descartando paquetes en el momento que estos ingresan a la red.

En este diseño al tratarse de 4 nodos se ha implementado políticas de modelamiento, manipulación y clasificación de tráfico, para poder administrar eficientemente los recursos de la red.

La clasificación separa paquetes según ciertas características, predefiniendo valores en el campo de ToS. El marcado se conoce como la acción en la cual el campo de ToS puede remplazarse por un valor relevante a las políticas de QoS definidas en la red.

Ahora, para poder manipular los tráficos y ofrecerles calidad de servicio, se utilizan procedimientos básicos de clasificación y asignación de prioridad, denominados Mapas de clase y Mapas de política.

- Mapas de clase: mecanismo usado para nombrar y aislar un flujo de tráfico específico, que define el criterio utilizado para comparar el tráfico y luego clasificarlo.
- Mapa de política: específica en qué clase de tráfico actuará. Las acciones que puede tomar son confiar en valores de clase de servicio, DSCP o precedencia IP de la clase de tráfico; establecer un valor específico de estos o especificar límites de ancho de banda. Antes que un mapa de política sea efectivo, debe pertenecer a una interfaz.

Los elementos parte de la red, como los nodos y los enlaces WAN entre los mismos, tienen cierto impacto sobre la calidad de servicio que perciben los usuarios. Por lo tanto se toma en cuenta la influencia que estos elementos (*throughput*, retardos, varianza de retardo, y pérdidas de paquetes.) tienen sobre los atributos de la QoS.

Para poder brindar calidad de servicio en una red, deben tomarse en consideración los acuerdos de nivel de servicio establecidos (SLA) y los requerimientos de tráfico solicitados dentro de la red. Un esquema de calidad de servicio, se diseña con el propósito de administrar los enlaces, de tal modo que se asegure el cumplimiento de ancho de banda contratado, para evitar períodos de congestión que incrementen la tasa de paquetes descartados (o perdidos), disminuyendo la eficiencia de la red.

A través de los procedimientos de administración de ancho de banda en los enlaces, se elimina el tráfico que quede por fuera del perfil contratado. No obstante, si un paquete marcado con prioridad alta queda por fuera del perfil contratado, no se descartará, sino que se encolarán durante periodos de congestión.

Para el modelamiento del esquema propuesto, se establecerán cuatro clases de servicio, conforme a parámetros como tasa de paquetes entregados, jitter y latencia. Las categorías ofrecidas serán: AAAA, AAA, AA y A. La Tabla 3.1 muestra los parámetros comprometidos para cada clase de servicio.

**Tabla 3.1.** Parámetros para las Clases de Servicio

Parámetro	CLASES DE SERVICIO			
	AAAA	AAA	AA	A
Paquetes entregados	99.90%	99,50%	99%	-
RTT	< 150 ms	< 150 ms	-	-
<i>Jitter</i>	< 30ms	-	-	-

### 3.1.1 ELECCIÓN DE LA ARQUITECTURA DE QoS

Existen dos arquitecturas de servicios según el IETF que permiten establecer QoS en equipamientos de red: servicios integrados y servicios diferenciados.

La modalidad de servicios diferenciados ofrece ciertas ventajas sobre la arquitectura de servicios integrados, tales como su buen funcionamiento, flexibilidad, escalabilidad, entre otras.

El denominado DiffServ nos garantiza QoS al modificar el campo de servicios diferenciados en el encabezado de cada paquete (en IPv4 el octeto TOS y en IPv6 al octeto Traffic Class).

Entre las ventajas de esta arquitectura se tiene:

- No es necesario reservar el canal. Suficiente con especificar en las cabeceras de cada paquete el tipo de tráfico.
- Reducir la carga de red. Como no existe reserva de canal la red se encuentra más libre para otro tipo de tráfico que lo necesite.
- Escalabilidad. Es la mayor ventaja en comparación con IntServ y se debe a que DiffServ puede aumentar el número de operaciones sin perder QoS además esta estructura pueda garantizar el crecimiento continuo sin perder calidad de servicio.
- Sencillez de señalización. Es más sencillo que RSVP de IntServ.

Por consiguiente, se selecciona la arquitectura de DiffServ como la base para el desarrollo del esquema de QoS que será implementado en la red del presente documento.

La metodología utilizada por DiffServ para ofrecer QoS, es a través de un comportamiento de envío predeterminado, o comportamiento por saltos (PHB). Con ellos se define el encolamiento y el tratamiento de retransmisión que recibirá un paquete perteneciente a un grupo de tráfico.

Se ha utilizado 3 estándares PHB con sus respectivos valores de DSCP:

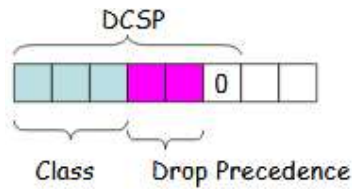
- **EXPEDITED FORWARDING (EF) PHB:** Definido en el RFC 2598, tiene un valor DSCP igual a 101110, ofreciendo un servicio de bajas pérdidas, baja latencia, bajo jitter y ancho de banda asegurado para aplicaciones en tiempo real. Este es para el servicio AAAA.
- **ASSURED FORWARDING (AF) PHB:** Proporciona cuatro clases diferentes de comportamientos de reenvío que puede especificar para el marcador. La siguiente tabla muestra las clases, las tres precedentes de descarte que se proporcionan con cada clase y los DSCP recomendados que están asociados con cada

precedencia. Cada DSCP está representado por su valor de AF, su valor en decimal y su valor en binario.

En la RFC 2597 “Assured Forwarding PHB Group” nos indica que hay 4 grupos de PHBs (*Per-Hop behaviors*) que son: AF1x, AF2x, AF3x, AF4x y cada uno de ellos tiene una reserva en cada nodo, y disponen de 3 probabilidades de descarte (drop).

Entonces se tiene

DSCP **xxx****yy**0: **xxx** es la clase, **yy** la drop. Donde una drop alta implica mayor probabilidad de descarte.



$$p_L \leq p_M \leq p_H$$

DROP	Class 1	Class 2	Class 3	Class 4	Drop Probabilidad
LOW	00 <b>10</b> 10	0 <b>100</b> 10	0 <b>110</b> 10	1 <b>000</b> 10	$P_L$
MEDIUM	00 <b>11</b> 00	0 <b>101</b> 00	0 <b>111</b> 00	1 <b>001</b> 00	$P_M$
HIGH	00 <b>11</b> 10	0 <b>101</b> 10	0 <b>111</b> 10	1 <b>001</b> 10	$P_H$

Para el caso del presente diseño se ha considerado tres clases para los servicios AAA, AA y A.

**Tabla 3.2.** Valores de DSCP para las clases AAA, AA y A

	Class 1 AAA	Class 2 AA	Class 3 A	Class 4
<b>Low-Drop Precedence</b>	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
<b>Medium-Drop Precedence</b>	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
<b>High-Drop Precedence</b>	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

- **PHB POR DEFECTO:** detallado en el RFC 2474, con un valor DSCP igual a 000000. Equivale al servicio del mejor esfuerzo tradicional. El tráfico de este PHB no recibirá ningún tipo de tratamiento especial.

En el prototipo de red se utiliza la clasificación y marcado de tráfico basado en clases, los dos campos más populares para el marcado de tráfico para QoS son el campo prioridad (Precedence) y el campo "DSCP" (Differentiated Services Code Point). El marcado de tráfico se lo realiza en el Router.

### 3.1.2 CLASIFICACIÓN Y ASIGNACIÓN DSCP POR TRÁFICO

Dependiendo del tipo de tráfico se clasificará conforme a sus requerimientos de calidad de servicio.

Así para la CoS AAAA se tiene las aplicaciones que necesitan mayor calidad de servicio como son: VoIP, video conferencia, para ellas se proveerá un ancho de banda de máximo 800 Kbps cuando exista mayor congestión.

En la CoS AAA se ubica a las aplicaciones de streaming ya que los valores de AF nos entregan datos de jitter, retardo y tasa de paquetes perdidos, para esto se tendrá un 25% del ancho de banda disponible en periodos de congestión.

En la clase AA se ubicara aplicaciones como SSL, bases de datos, HTTPS, FTP, y trabajaran con un máximo del 20% del ancho de banda.

Finalmente en la clase A entran las aplicaciones de TELNET, SSH, ICMP, se les ha asignado un 10% del ancho de banda.

En la Tabla 3.3 se han asignado los valores de PHP a cada tipo de tráfico:

**Tabla 3.3.** Clasificación de DSCP


CoS	DSCP	APLIACACIÓN	% Buffer
AAAA	EF=46	Voip, Videoconferencia	800 Kbps
AAA	AF13=14	Streaming	25%
AA	AF21=18	SSL, BD	20%
	AF23=22	HTTPS, FTP	
A	AF31=26	TELNET,SSH	10%
	AF33=30	ICMP	
<i>Best Effort</i>	BE=0	-	-

### 3.2 ARQUITECTURA

Equipos a utilizarse:

**Tabla 3.4.** Equipos a utilizarse en el prototipo

EQUIPO	MODELO	CANTIDAD
ROUTER	CISCO 1900 SERIES	4
SWITCH	CATALYST 2960 SERIES	5
INYECTOR DE TRAFICO	ALBEDO ETHER.GENIUS	1
CABLES SERIALES		4
CABLE DE CONSOLA		2
LAPTOPS	COMPAQ - TOSHIBA – Hacer	4
SERVIDOR	HP - QUAD CORE	1

ROUTER	CISCO 1900 SERIES
<b>CARACTERISTICAS</b>	
RJ-45 onboard LAN 10/100/1000 ports	2
RJ-45 onboard WAN	2



10/100/1000 ports	
EHWIC slots	2
USB console port	1
Power-supply options	POE externo
Dimensions (H x W x D)	1.75 x 13.5 x 11.5 in. (4.45 x 34.29 x 29.21 cm)
Protocolos	IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPsec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Gestión de Tráfico	<b>QoS</b> , Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

CARACTERISTICAS	CATALYST 2960 SERIES
Soporte para calidad de servicio	SI
Cantidad de puertos Ethernet RJ-45	24
Protocolos de red	IEEE 802.1ab, IEEE 802.1D, IEEE 802.1D, IEEE 802.1p, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1w, IEEE 802.1x, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3af, IEEE 802.3ah, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z

Vlans	255
Apilable	NO
Protocolos de gestión	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH-2
Tasa de transferencia (máx)	0,1 Gbit/s
Protocolo de transmisión de datos	Ethernet, Fast Ethernet
Memoria Flash	32 MB
Soporta Energía sobre Ethernet (PoE)	Si

### 3.2.1 CONFIGURACIONES DE IPs Y PUERTOS

#### 3.2.1.1 Direccionamiento IP

ROUTER MATRIZ:

**Tabla 3.5.** Direccionamiento Router Matriz

INTERFAZ	DIRECCIÓN IPV6	MASCARA
<b>S0/1/1</b>	2000:0:2:D::0	/127
<b>S0/1/0</b>	2000:0:2:A::0	/127
<b>Gi 0/1</b>	2000:0:1:9::1	/125
<b>Gi 0/0</b>	NO ASIGNADA	
<b>Gi 0/0.10</b>	2000:0:1:B::1	/122
<b>Gi 0/0.20</b>	2000:0:1:C::1	/122
<b>Gi 0/0.30</b>	2000:0:1:D::1	/123
<b>Gi 0/0.40</b>	2000:0:1:E::1	/122
<b>Gi 0/0.50</b>	2000:0:1:F::1	/122
<b>Gi 0/0.99</b>	2000:0:1:A::1	/126

**ROUTER SUCURSAL 1:**

**Tabla 3.6.** Direccionamiento Router Sucursal\_1

INTERFAZ	DIRECCIÓN IPV6	MASCARA
S0/0/0	2000:0:2:D::1	/127
S0/0/1	2000:0:2:C::0	/127
Gi 0/0	NO ASIGNADA	
Gi 0/0.10	2000:0:1:B::4:1	/125
Gi 0/0.20	2000:0:1:C::4:1	/123
Gi 0/0.30	2000:0:1:D::2:1	/127
Gi 0/0.40	2000:0:1:E::2:1	/126
Gi 0/0.50	2000:0:1:F::2:1	/125

**ROUTER SUCURSAL 2:**

**Tabla 3.7.** Direccionamiento Router Sucursal\_2

INTERFAZ	DIRECCIÓN IPV6	MASCARA
S0/0/0	2000:0:2:B::0	/127
S0/0/1	2000:0:2:A::1	/127
Gi 0/0	NO ASIGNADA	
Gi 0/0.10	2000:0:1:B::8:1	/125
Gi 0/0.20	2000:0:1:C::8:1	/124
Gi 0/0.30	2000:0:1:D::4:1	/127
Gi 0/0.40	2000:0:1:E::4:1	/127
Gi 0/0.50	2000:0:1:F::4:1	/125

**ROUTER SUCURSAL 3:**

**Tabla 3.8.** Direccionamiento Router Sucursal\_3

INTERFAZ	DIRECCIÓN IPV6	MASCARA
S0/1/1	2000:0:2:B::1	/127
S0/1/0	2000:0:2:C::1	/127
GI 0/0	NO ASIGNADA	
Gi 0/0.10	2000:0:1:B::C:1	/125
Gi 0/0.20	2000:0:1:C::C:1/124	/124
Gi 0/0.30	2000:0:1:D::6:1/127	/127
Gi 0/0.40	2000:0:1:E::6:1/127	/127
Gi 0/0.50	2000:0:1:F::6:1/125	/125

### 3.2.1.2 Asignación de VLAN

**Tabla 3.9.** Nombre de VLAN

NOMBRE	NUMERO DE VLAN
VLAN GG	99
VLAN OPE	10
VLAN COM	20
VLAN RRHH	30
VLAN TEC	40
VLAN FIN	50

#### SWITCH MATRIZ:

**Tabla 3.10.** Direccionamiento Referencial Switch\_Matriz

NOMBRE VLAN	RED	MASCARA
VLAN GG	2000:0:1:A::	/126
VLAN OPE	2000:0:1:B::	/122
VLAN COM	2000:0:1:C::	/122
VLAN RRHH	2000:0:1:D::	/123
VLAN TEC	2000:0:1:E::	/123
VLAN FIN	2000:0:1:F::	/123

#### SWITCH SUC\_1:

**Tabla 3.11.** Direccionamiento Referencial Switch Sucursal\_1

NOMBRE VLAN	RED	MASCARA
VLAN OPE	2000:0:1:B::4	/125
VLAN COM	2000:0:1:C::4	/123
VLAN RRHH	2000:0:1:D::2	/127
VLAN TEC	2000:0:1:E::2	/126
VLAN FIN	2000:0:1:F::2	/125

#### SWITCH SUC\_2:

**Tabla 3.12.** Direccionamiento Referencial Switch Sucursal\_2

NOMBRE VLAN	RED	MASCARA
VLAN OPE	2000:0:1:B::8	/125
VLAN COM	2000:0:1:C::8	/124
VLAN RRHH	2000:0:1:D::4	/127
VLAN TEC	2000:0:1:E::4	/127
VLAN FIN	2000:0:1:F::4	/125

### SWITCH SUC\_3:

**Tabla 3.13.** Direccionamiento Referencial Switch Sucursal\_3

NOMBRE VLAN	RED	MASCARA
VLAN OPE	2000:0:1:B::C	/125
VLAN COM	2000:0:1:C::C	/124
VLAN RRHH	2000:0:1:D::6	/127
VLAN TEC	2000:0:1:E::6	/127
VLAN FIN	2000:0:1:F::6	/125

### 3.2.1.3 Asignación de puertos

### SWITCH MATRIZ:

**Tabla 3.14.** Asignación de puertos Switch\_Matriz

PUERTOS	ASIGNACION	RED
Fa0/1	VLAN 99	2000:0:1:A::/126
Fa0/2 – 0/7	VLAN 10	2000:0:1:B::/122
Fa0/8 – 0/13	VLAN 20	2000:0:1:C::/122
Fa0/14 – 0/17	VLAN 30	2000:0:1:D::/123
Fa0/18 – 0/21	VLAN 40	2000:0:1:E::/123
Fa0/22– 0/24	VLAN 50	2000:0:1:F::/123

### SWITCH SUC\_1:

**Tabla 3.15.** Asignación de puertos Switch Sucursal\_1

PUERTOS	ASIGNACION	RED
Fa0/1 – 0/7	VLAN 10	2000:0:1:B::4/125
Fa0/8 – 0/13	VLAN 20	2000:0:1:C::4/123
Fa0/14 – 0/19	VLAN 30	2000:0:1:D::2/127
Fa0/20 – 0/22	VLAN 40	2000:0:1:E::2/126
Fa0/23 – 0/24	VLAN 50	2000:0:1:F::2/125

### SWITCH SUC\_2:

**Tabla 3.16.** Asignación de puertos Switch Sucursal\_2

PUERTOS	ASIGNACION	RED
Fa0/1 – 0/7	VLAN 10	2000:0:1:B::4/125
Fa0/8 – 0/13	VLAN 20	2000:0:1:C::4/123
Fa0/14 – 0/19	VLAN 30	2000:0:1:D::2/127
Fa0/20 – 0/22	VLAN 40	2000:0:1:E::2/126
Fa0/23 – 0/24	VLAN 50	2000:0:1:F::2/125

## SWITCH SUC\_3:

**Tabla 3.17.** Asignación de puertos Switch Sucursal\_3

PUERTOS	ASIGNACION	RED
Fa0/1 – 0/7	VLAN 10	2000:0:1:B::C/125
Fa0/8 – 0/13	VLAN 20	2000:0:1:C::C/124
Fa0/14 – 0/19	VLAN 30	2000:0:1:D::6/127
Fa0/20 – 0/22	VLAN 40	2000:0:1:E::6/127
Fa0/23 – 0/24	VLAN 50	2000:0:1:F::6/125

## 3.2.2 CONFIGURACIÓN DE SERVIDORES

### 3.2.2.1 Instalación del Sistema Operativo Base

Como primer paso lo que se realizará la instalación de Ubuntu 12.04 en un servidor físico donde se procederá a configurar todos los servidores

Instalación de Ubuntu

#### **Paso 1:**

Descargar la imagen del sistema operativo. La descarga se podrá realizar desde la página oficial de Ubuntu.

#### **Paso 2:**

Se quema el sistema operativo en un medio arrancable como un CD/DVD.

#### **Paso 3:**

Con el CD/DVD o medio conectado, se reinicia el servidor y se espera que nos muestre la siguiente pantalla.

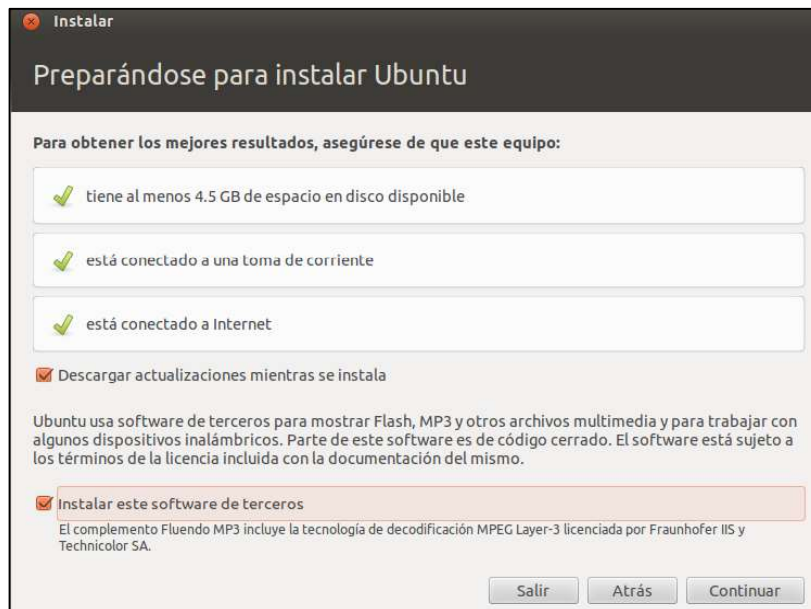


**Figura 3.1.** Instalación Ubuntu

**Paso 4:**

Se hace click en "Instalar Ubuntu". Inmediatamente se ve una imagen como la siguiente:

Se hace click en "Continuar".



**Figura 3.2.** Configuraciones para instalación Ubuntu

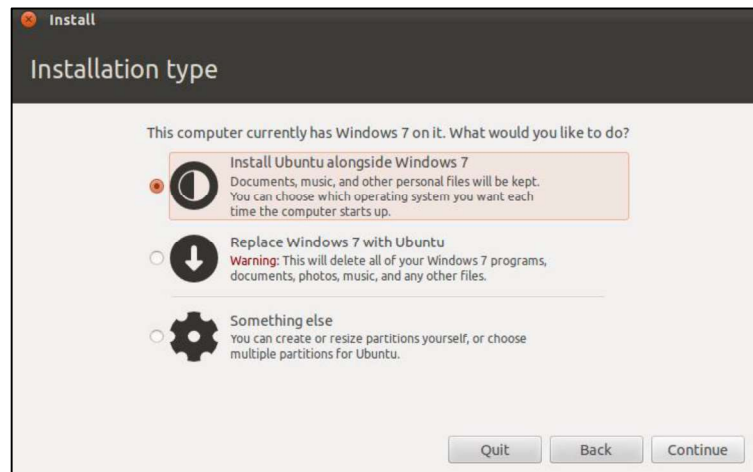
**Paso 5:**

Se instala Ubuntu sobre todo el disco asignado para este sistema operativo.

Luego de dar un clic a "Continuar" pedirá que se elija el espacio que se quiere dar a la nueva partición asignada para el sistema operativo.

**Paso 6:**

Luego de esto se asigna credenciales de usuario administrador para el ingreso al sistema una vez instalado y configurado.



**Figura 3.3.** Tipo de instalación para Ubuntu

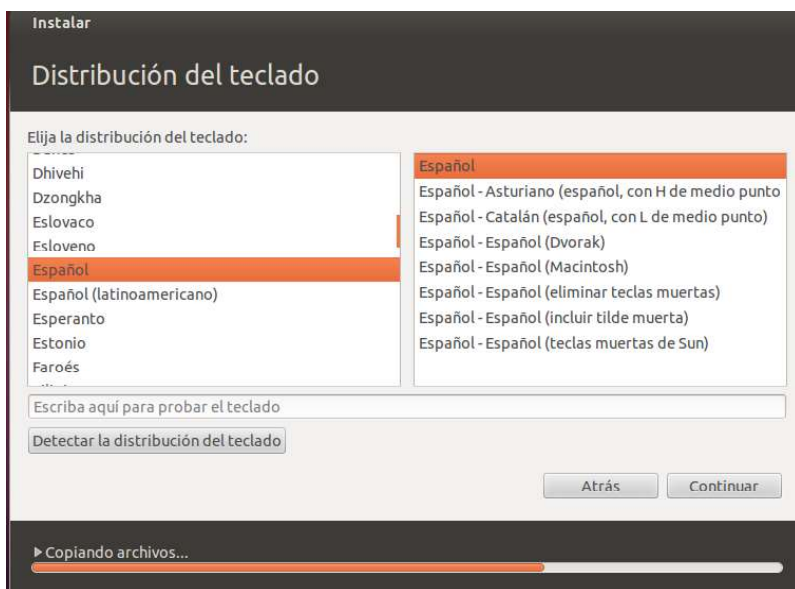
Localización: Se selecciona el lugar de origen, en nuestro caso Guayaquil.



**Figura 3.4.** Ubicación para la instalación de Ubuntu

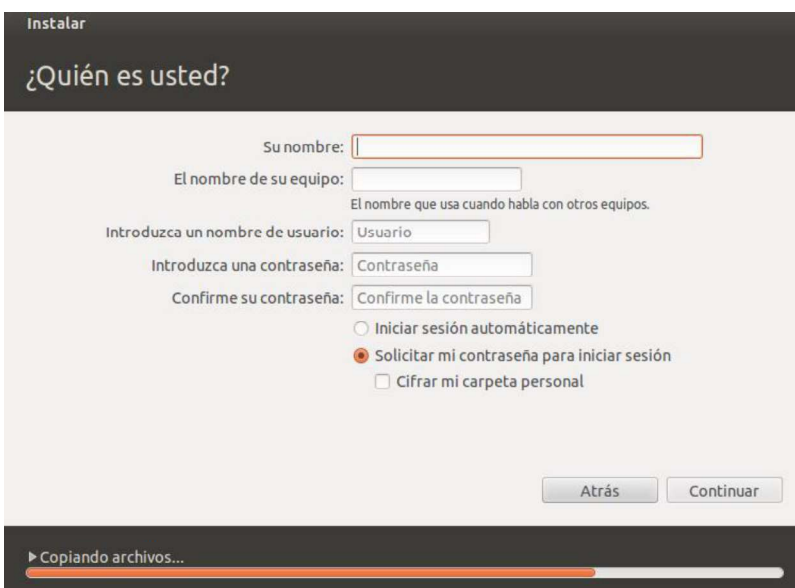


Idioma y configuración de teclado: Se selecciona el idioma “Español”.



**Figura 3.5.** Idioma para la instalación de Ubuntu

Configuración de la cuenta de usuario: Se configura el nombre de usuario y contraseña.



**Figura 3.6.** Configuración de credenciales en Ubuntu

**Paso 7:**

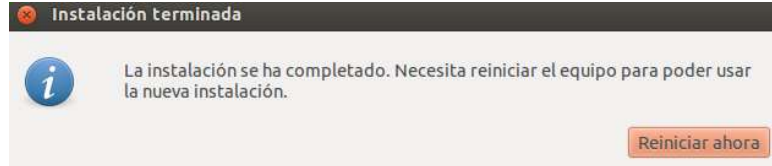
Ahora ya sólo queda esperar a que se termine la instalación:



**Figura 3.7.** Finalización de la instalación de Ubuntu

**Paso 8:**

Una vez finalizada la instalación, se reinicia el equipo:



**Figura 3.8.** Confirmación de la instalación de Ubuntu

Se quita el CD/DVD o USB antes del reinicio para que no se ejecute otra vez la instalación:

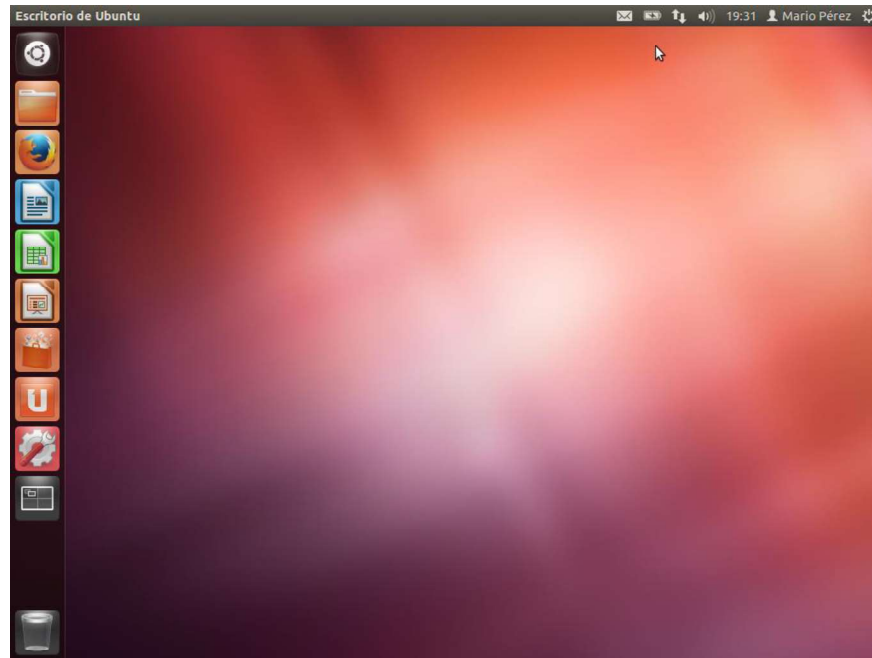
```
* All processes ended within 2 seconds... [ OK ]
modem-manager[1391]: <info> Caught signal 15, shutting down...

* Deconfiguring network interfaces... [ OK ]
* Unmounting temporary filesystems... [ OK ]
* Deactivating swap... [ OK ]
* Stopping remaining crypto disks... [ OK ]
* Stopping early crypto disks... [ OK ]
umount: /run/lock: not mounted
umount: /run/shm: not mounted
* casper is resyncing snapshots and caching reboot files...
Please remove installation media and close the tray (if any) then press ENTER:
```

**Figura 3.9.** Inicialización de Ubuntu

### **Paso 9:**

Se entra con el usuario y ya se habrá acabado:



**Figura 3.10.** Escritorio de Ubuntu

### **3.2.2.2 Servidor de DNS [46] [47]**

#### **Instalación de Bind9**

Se procedió a instalar el servicio Bind9 para poder habilitar y configurar el servidor DNS con IPV6. Es recomendable acceder a este directorio como *root* (sudo su) para no tener problemas de permisos denegados cuando se copie ficheros o se modifique los ya existentes.

Lo primero que se debe realizar para configurar un servidor DNS (bind) en Linux Ubuntu es instalarlo desde los repositorios poniendo en consola:

**sudo aptitude install bind9**

A continuación, se va al directorio del programa para editar los archivos de configuración necesarios:

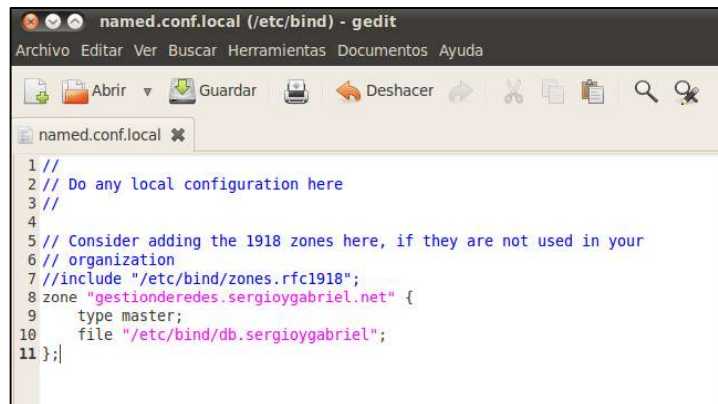
```
cd /etc/bind/
```

Una vez que se está en este directorio, basta con editar el archivo:

```
named.conf.local
```

```
gedit named.conf.local
```

Y en el archivo que se abrirá se añade lo siguiente:



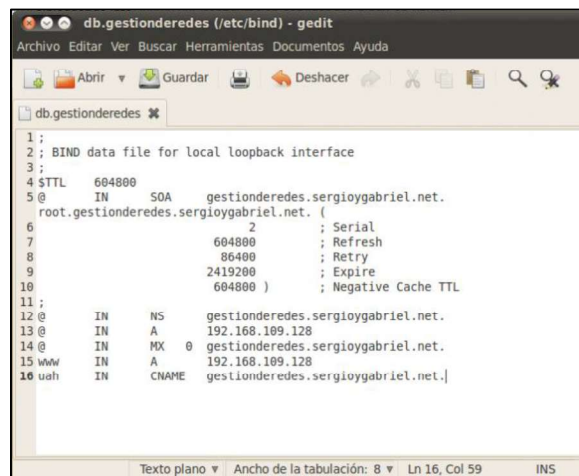
```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8 zone "gestionderedes.sergioygabriel.net" {
9     type master;
10    file "/etc/bind/db.sergioygabriel";
11};
```

Figura 3.11. Configuraciones del servidor Bind9 (1)

Se procede con la creación del fichero de configuración a partir de uno ya creado (db.local) poniendo:

```
cp db.local db.gestionderedes
```

Y a continuación se modifica los "localhost" por el nombre del dominio que se ha elegido:



```
1 ;
2 ; BIND data file for local loopback interface
3 ;
4 $TTL 604800
5 @ IN SOA gestionderedes.sergioygabriel.net.
  root.gestionderedes.sergioygabriel.net. (
6     2 ; Serial
7     604800 ; Refresh
8     86400 ; Retry
9     2419200 ; Expire
10    604800 ) ; Negative Cache TTL
11 ;
12 @ IN NS gestionderedes.sergioygabriel.net.
13 @ IN A 192.168.109.128
14 @ IN MX 0 gestionderedes.sergioygabriel.net.
15 www IN A 192.168.109.128
16 uah IN CNAME gestionderedes.sergioygabriel.net.]
```

**Figura 3.12.** Configuraciones del servidor Bind9 (2)

Una vez que se ha guardado el fichero de configuración, se reinicia el proceso bind con el siguiente comando:

```
sudo /etc/init.d/bind9 restart
```

Una vez que se inicia, se edita el fichero de configuración resolv.conf para que el computador utilice este servidor DNS que se ha configurado:

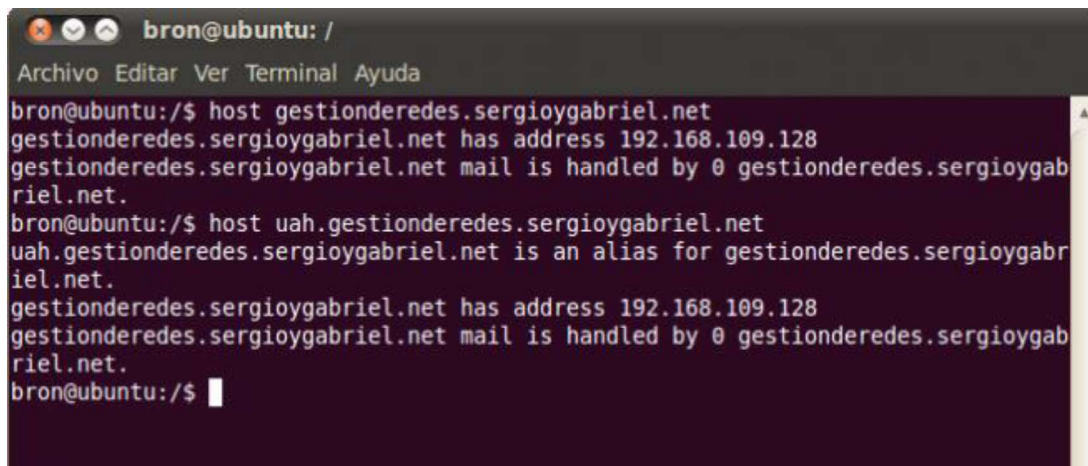
```
sudo gedit /etc/resolv.conf
```

Y únicamente se deja la siguiente línea en el fichero de texto plano:

```
nameserver 127.0.0.1
```

Si este es el servidor, se deberá hacer lo mismo con el resto de computadores de la red local, pero en lugar de poner 127.0.0.1 se tendrá que poner la IP privada del computador servidor.

Una vez que se ha hecho esto, ya se tiene todo listo para empezar la batería de pruebas y comprobar que se ha hecho todo bien. En la siguiente captura de pantalla se pueden ver las pruebas realizadas:

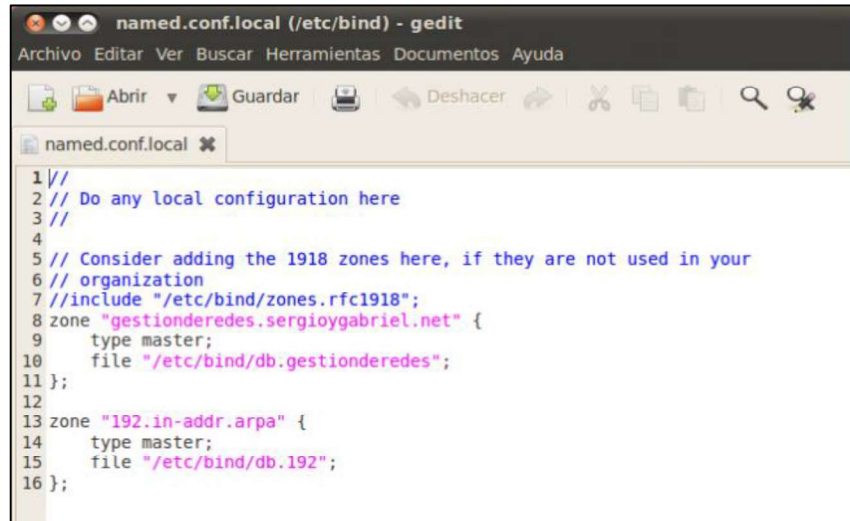


```
bron@ubuntu: /
Archivo Editar Ver Terminal Ayuda
bron@ubuntu:/$ host gestionderedes.sergioygabriel.net
gestionderedes.sergioygabriel.net has address 192.168.109.128
gestionderedes.sergioygabriel.net mail is handled by 0 gestionderedes.sergioygabriel.net.
bron@ubuntu:/$ host uah.gestionderedes.sergioygabriel.net
uah.gestionderedes.sergioygabriel.net is an alias for gestionderedes.sergioygabriel.net.
gestionderedes.sergioygabriel.net has address 192.168.109.128
gestionderedes.sergioygabriel.net mail is handled by 0 gestionderedes.sergioygabriel.net.
bron@ubuntu:/$
```

**Figura 3.13.** Configuraciones del servidor Bind9 (3)

Ahora se va a configurar el servidor DNS para que resuelva dominios a la inversa, poniendo la dirección IP y que diga a qué dominio pertenece dicha dirección IP.

Para conseguir nuestro objetivo, se deberá añadir al fichero **/etc/bind/named.conf.local** que se utilizó anteriormente:



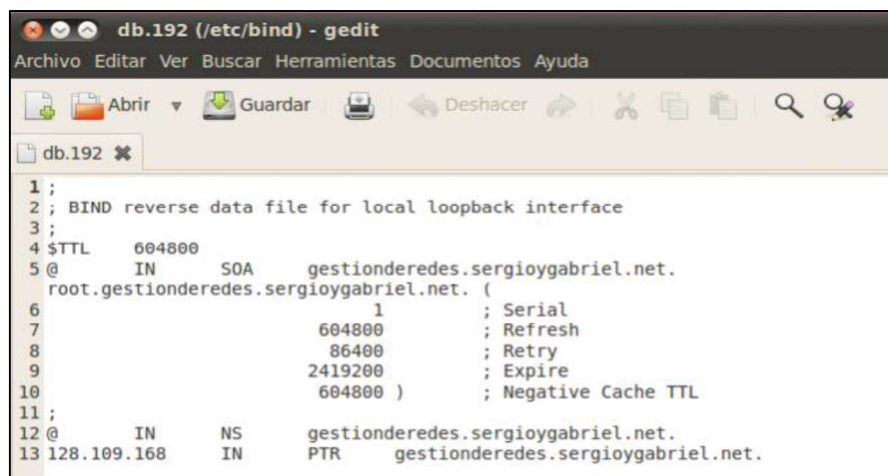
```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8 zone "gestionederedes.sergioygabriel.net" {
9     type master;
10    file "/etc/bind/db.gestionederedes";
11 };
12
13 zone "192.in-addr.arpa" {
14     type master;
15     file "/etc/bind/db.192";
16 };
```

**Figura 3.14.** Configuraciones del servidor Bind9 (4)

También se deberá copiar el archivo de configuración por defecto para editarlo. A partir del archivo db.127 se crea el db.192:

```
cp db.127 db.192
```

Una vez que se lo ha creado, basta con editarlo con la siguiente información cambiando los localhost y la última línea:



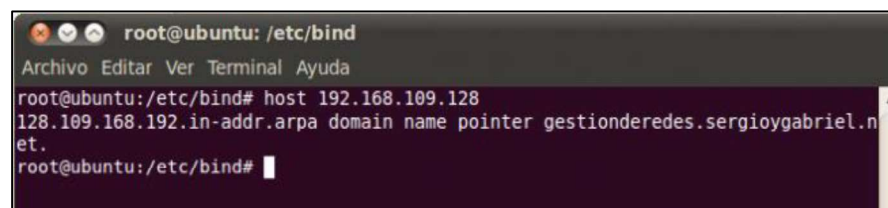
```
1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL      604800
5 @         IN      SOA      gestionderedes.sergioygabriel.net.
           root.gestionderedes.sergioygabriel.net. (
6           1             ; Serial
7           604800        ; Refresh
8           86400         ; Retry
9           2419200       ; Expire
10          604800 )      ; Negative Cache TTL
11 ;
12 @         IN      NS       gestionderedes.sergioygabriel.net.
13 128.109.168 IN     PTR     gestionderedes.sergioygabriel.net.
```

**Figura 3.15.** Configuraciones del servidor Bind9 (5)

Una vez realizado estos pasos, se reinicia de nuevo el proceso bind:

```
sudo /etc/init.d/bind9 restart
```

Y se comprueba que ha funcionado correctamente:

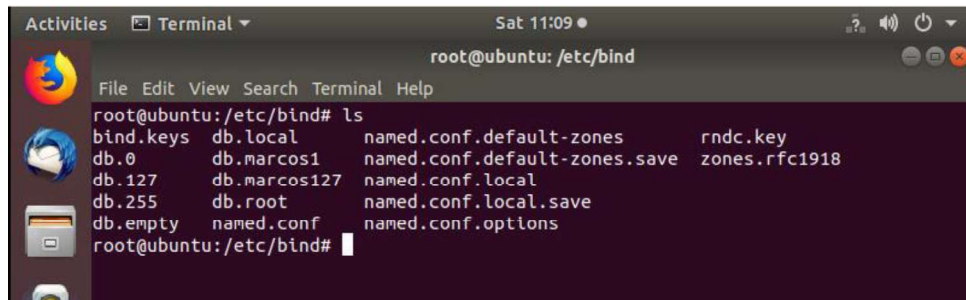


```
root@ubuntu: /etc/bind
Archivo Editar Ver Terminal Ayuda
root@ubuntu:/etc/bind# host 192.168.109.128
128.109.168.192.in-addr.arpa domain name pointer gestionderedes.sergioygabriel.net.
root@ubuntu:/etc/bind#
```

**Figura 3.16.** Configuraciones del servidor Bind9 (6)

## Instalación de DNS

Una vez instalado Bind9 se procede a modificar archivos de configuración en base a nuestro DNS, para ello se ingresa al path /etc/bind.



```
root@ubuntu: /etc/bind
File Edit View Search Terminal Help
root@ubuntu:/etc/bind# ls
bind.keys  db.local      named.conf.default-zones  rndc.key
db.0       db.marcos1    named.conf.default-zones.save  zones.rfc1918
db.127     db.marcos127  named.conf.local
db.255     db.root       named.conf.local.save
db.empty   named.conf    named.conf.options
root@ubuntu:/etc/bind#
```

**Figura 3.17.** Configuraciones del servidor DNS (1)

Se copia los archivos db.local y db.127 con el comando cp y se crea los archivos db.marcos y db.marcos127 que serán los archivos que se modificarán para crear el DNS.

Luego, se procede a editar el archivo db.marcos con el comando nano y se procede a añadir las siguientes líneas de comandos:



```
;
;
; domain name servers
;
;
@      IN      NS      marcos.org.
@      IN      AAAA    fe80::5427:489c:8500:db8f
@      IN      AAAA    fe80::20c:29ff:fe99:8c3b
www    IN      AAAA    fe80::5427:489c:8500:db8f
www2   IN      AAAA    fe80::5427:489c:8500:db8f
```

**Figura 3.18.** Configuraciones del servidor DNS (2)

Con esto se asegura que resolverá el nombre marcos.org con la dirección ipv6 asignada a este servidor.

Luego de eso, se procede a editar el archivo y se añade las siguientes líneas de comandos remarcadas en la siguiente figura:



```

root@ubuntu: /etc/bind
GNU nano 2.9.3 db.marcos127
;
; fe80::5427:489c:8500:db8f/64
;
; Zone file built with the IPv6 Reverse DNS zone builder
; http://rdns6.com/
;
; $TTL 1h ; Default TTL
@      IN      SOA      dns1.marcos.org.      admin.dns.org. (
; serial
1h     ; slave refresh interval
15m    ; slave retry interval
1w     ; slave copy expire time
1h     ; NXDOMAIN cache time
)
;
; domain name servers
;
; @      IN      NS      marcos.org.
f.8.b.d IN      PTR    marcos.org.
^G Get Help      ^O Write Out     ^W Where Is     ^K Cut Text      ^J Justify
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell

```

**Figura 3.19.** Configuraciones del servidor DNS (3)

Esto nos servirá para que la se pueda tener la zona reversa de este servidor DNS. Se edita también el archivo named.conf.local:

```

root@ubuntu:/etc/bind# ls
bind.keys  db.local      named.conf.default-zones  rndc.key
db.0       db.marcos1    named.conf.default-zones.save  zones.rfc1918
db.127     db.marcos127 named.conf.local
db.255     db.root       named.conf.local.save
db.empty   named.conf    named.conf.options
root@ubuntu:/etc/bind# nano db.marcos1
root@ubuntu:/etc/bind# nano db.marcos127
root@ubuntu:/etc/bind# nano db.marcos127
root@ubuntu:/etc/bind# nano named.conf.local
root@ubuntu:/etc/bind#

```

**Figura 3.20.** Configuraciones del servidor DNS (4)

Se procede a editar el archivo al igual que los anteriores:

```

root@ubuntu: /etc/bind
File Edit View Search Terminal Help
GNU nano 2.9.3 named.conf.local

//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "0.0.5.8.c.9.8.4.7.2.4.5.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa" {
    type master;
    file "/etc/bind/db.marcos127";
};
zone "marcos.org" {
    type master;
    file "/etc/bind/db.marcos1";
};

```

Figura 3.21. Configuraciones del servidor DNS (5)

Se procede a crear las zonas para ipv6 con la terminación .arpa y sin los primeros 4 números y añadimos la zona marcos.org.

Seguidamente, se empieza a revisar las zonas creadas, para ello se necesita ejecutar el siguiente comando named-checkzone "marcos.org":

```

root@ubuntu: /etc/bind
File Edit View Search Terminal Help
root@ubuntu:/etc/bind# ls
bind.keys  db.local      named.conf.default-zones  rndc.key
db.0       db.marcos1    named.conf.default-zones.save  zones.rfc1918
db.127     db.marcos127 named.conf.local
db.255     db.root       named.conf.local.save
db.empty   named.conf    named.conf.options
root@ubuntu:/etc/bind# nano db.marcos1
root@ubuntu:/etc/bind# nano db.marcos127
root@ubuntu:/etc/bind# nano db.marcos127
root@ubuntu:/etc/bind# nano named.conf.local
root@ubuntu:/etc/bind# nano named.conf.local
root@ubuntu:/etc/bind# named-checkzone marcos.org db.marcos1
zone marcos.org/IN: loaded serial 2018050201
OK
root@ubuntu:/etc/bind#

```

Figura 3.22. Configuraciones del servidor DNS (6)

Se comprueba la resolución satisfactoria con el OK en la pantalla.

Ya para finalizar la configuración, se procede a reiniciar la configuración DNS con el siguiente comando "/etc/init.d/bind9 restart":

```
Activities Terminal Sat 11:50
root@ubuntu: /etc/bind
File Edit View Search Terminal Help
root@ubuntu:/etc/bind# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
root@ubuntu:/etc/bind#
```

Figura 3.23. Configuraciones del servidor DNS (7)

Se prueba de igual forma, la resolución de nuestro dominio y direccionamiento IPv6.

```
Activities Terminal Sat 11:51
root@ubuntu: /etc/bind
File Edit View Search Terminal Help
root@ubuntu:/etc/bind# dig AAAA www.marcos.org
; <<>> DiG 9.11.3-1ubuntu1.1-Ubuntu <<>> AAAA www.marcos.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7351
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;www.marcos.org.                IN      AAAA
;; ANSWER SECTION:
www.marcos.org.                0      IN      AAAA   fe80::5427:489c:8500:db8f
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Dec 08 11:51:24 PST 2018
;; MSG SIZE rcvd: 71
root@ubuntu:/etc/bind#
```

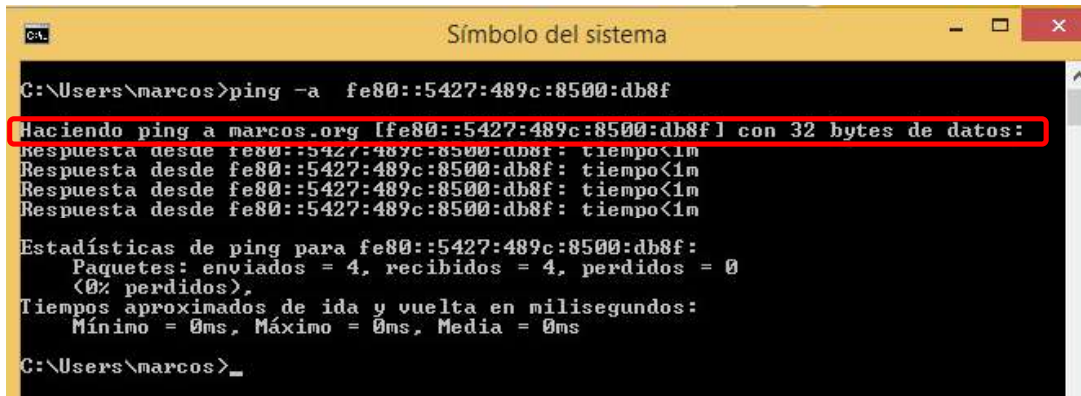
Figura 3.24. Configuraciones del servidor DNS (8)

Se mira que no existan errores en la configuración de los archivos. Se prueba la resolución inversa también de la IPv6.

```
Activities Terminal Sat 11:51
root@ubuntu: /etc/bind
File Edit View Search Terminal Help
root@ubuntu:/etc/bind# dig AAAA www.marcos.org
; <<>> DiG 9.11.3-1ubuntu1.1-Ubuntu <<>> AAAA www.marcos.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7351
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;www.marcos.org.                IN      AAAA
;; ANSWER SECTION:
www.marcos.org.                0      IN      AAAA   fe80::5427:489c:8500:db8f
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Dec 08 11:51:24 PST 2018
;; MSG SIZE rcvd: 71
root@ubuntu:/etc/bind#
```

Figura 3.25. Configuraciones del servidor DNS (9)

Al realizar un ping -a a la iv6 del servidor DNS responde lo siguiente:



```
C:\Users\marcos>ping -a fe80::5427:489c:8500:db8f
Haciendo ping a marcos.org [fe80::5427:489c:8500:db8f] con 32 bytes de datos:
Respuesta desde fe80::5427:489c:8500:db8f: tiempo<1m
Respuesta desde fe80::5427:489c:8500:db8f: tiempo<1m
Respuesta desde fe80::5427:489c:8500:db8f: tiempo<1m

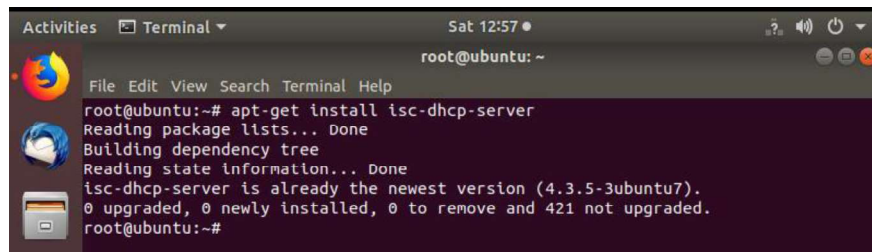
Estadísticas de ping para fe80::5427:489c:8500:db8f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\marcos>
```

Figura 3.26. Configuraciones del servidor DNS (10)

### 3.2.2.3 Servidor de DHCP

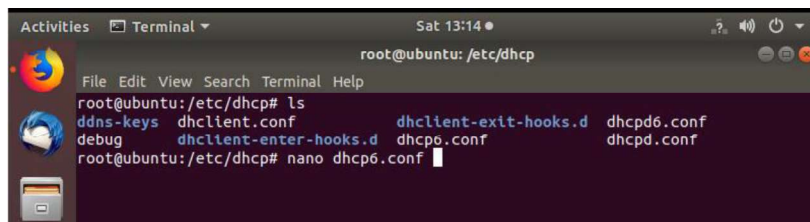
Se empieza la configuración de nuestro servidor DHCP instalando el servicio DHCP con el comando mostrado en la siguiente figura:



```
root@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu:~# apt-get install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
isc-dhcp-server is already the newest version (4.3.5-3ubuntu7).
0 upgraded, 0 newly installed, 0 to remove and 421 not upgraded.
root@ubuntu:~#
```

Figura 3.27. Configuraciones del servidor DHCP (1)

Se procede a editar el archivo dhcpd6.conf:



```
root@ubuntu: /etc/dhcp
File Edit View Search Terminal Help
root@ubuntu:/etc/dhcp# ls
ddns-keys  dhclient.conf          dhclient-exit-hooks.d  dhcpd6.conf
debug      dhclient-enter-hooks.d  dhcpd.conf              dhcpd.conf
root@ubuntu:/etc/dhcp# nano dhcp6.conf
```

Figura 3.28. Configuraciones del servidor DHCP (2)

Se procede a añadir los rangos en IPv6 para el direccionamiento dinámico y el tiempo de arrendamiento de las IPs, por defecto 12 horas.

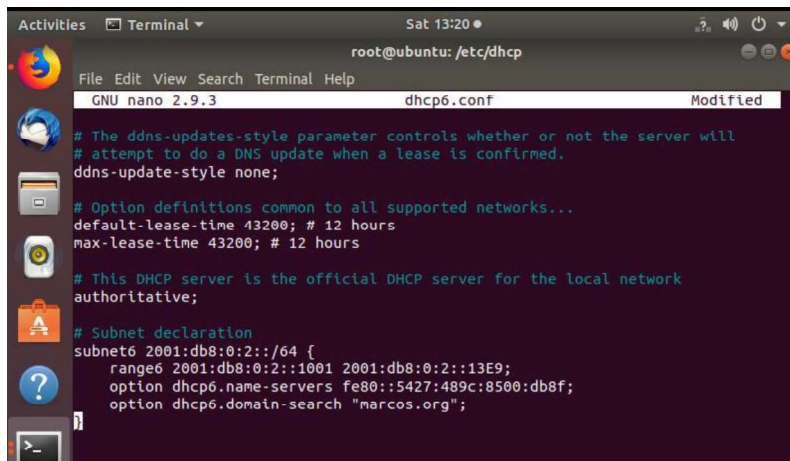


Figura 3.29. Configuraciones del servidor DHCP (3)

Se reinicia el servicio:

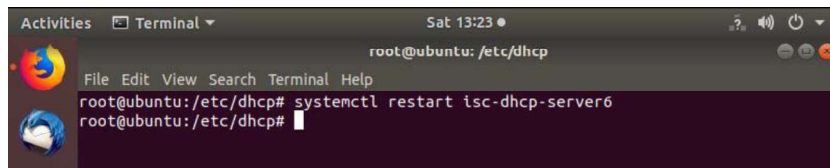


Figura 3.30. Configuraciones del servidor DHCP (4)

En el cliente se prueba el servicio DHCP configurando como automático la opción del direccionamiento IPv6:

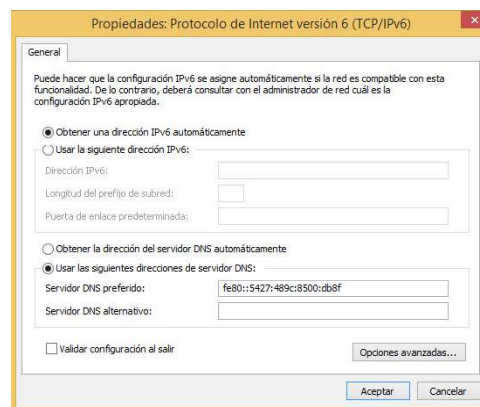
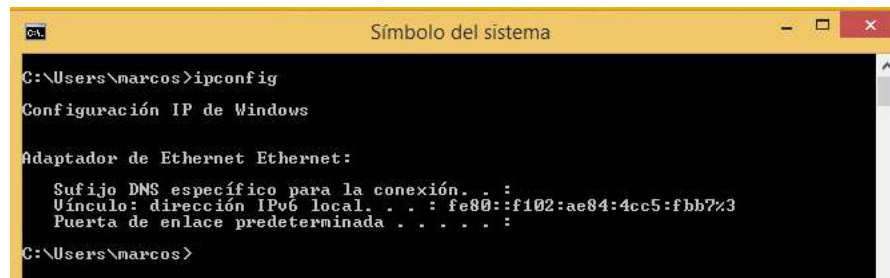


Figura 3.31. Configuraciones del servidor DHCP (5)

Al final se revisa la dirección ipv6 en el cliente y se ve la dirección IP asignada por el servidor DHCP IPv6:



```
C:\Users\marcos>ipconfig

Configuración IP de Windows

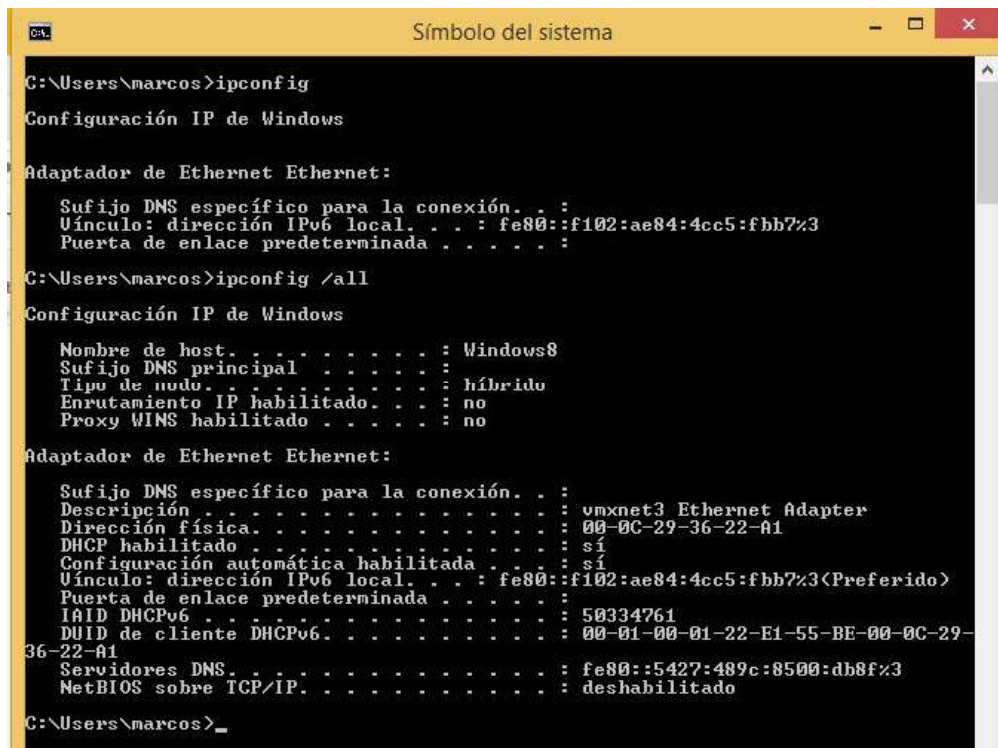
Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::f102:ae84:4cc5:bbb7%3
    Puerta de enlace predeterminada . . . . . :

C:\Users\marcos>
```

Figura 3.32. Configuraciones del servidor DHCP (6)

Se puede visualizar que la configuración automática está habilitada:



```
C:\Users\marcos>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::f102:ae84:4cc5:bbb7%3
    Puerta de enlace predeterminada . . . . . :

C:\Users\marcos>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : Windows8
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

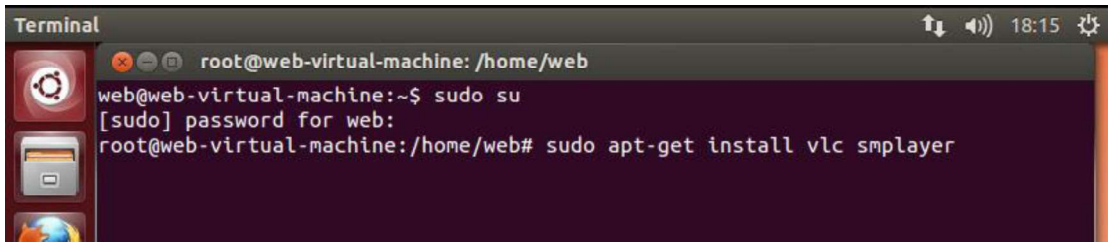
    Sufijo DNS específico para la conexión. . . :
    Descripción . . . . . : vmxnet3 Ethernet Adapter
    Dirección física. . . . . : 00-0C-29-36-22-A1
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Vínculo: dirección IPv6 local. . . . . : fe80::f102:ae84:4cc5:bbb7%3(Preferido)
    Puerta de enlace predeterminada . . . . . :
    IAID DHCPv6 . . . . . : 50334761
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-22-E1-55-BE-00-0C-29-36-22-A1
    Servidores DNS. . . . . : fe80::5427:489c:8500:db8f%3
    NetBIOS sobre TCP/IP. . . . . : deshabilitado

C:\Users\marcos>_
```

Figura 3.33. Configuraciones del servidor DHCP (7)

### 3.2.2.4 Servidor de Video Streaming

Para la implementación del servidor de *streaming* lo primero que se debe hacer es ingresar como súper usuario e instalar el paquete que se muestra en el gráfico siguiente:

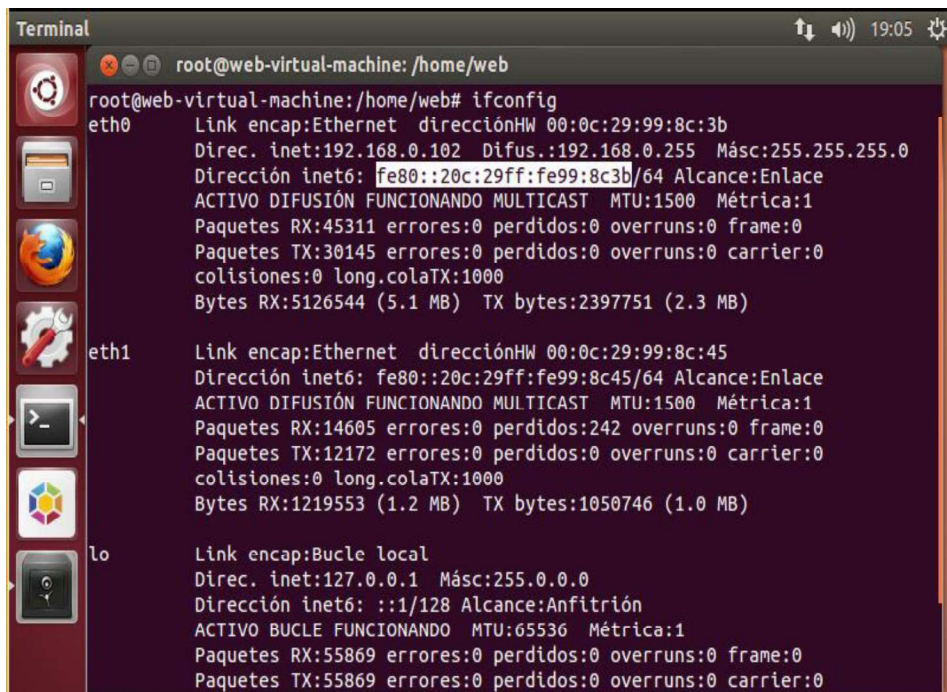


```
Terminal
root@web-virtual-machine: /home/web
web@web-virtual-machine:~$ sudo su
[sudo] password for web:
root@web-virtual-machine:/home/web# sudo apt-get install vlc smplayer
```

Figura 3.34. Configuraciones del servidor de Video Streaming (1)

Se usa VLC Media Player es un reproductor multimedia para poder generar y reproducir un video desde el servidor FTP.

Con el comando ifconfig se mira la dirección IPv6 asignada para ese servidor:



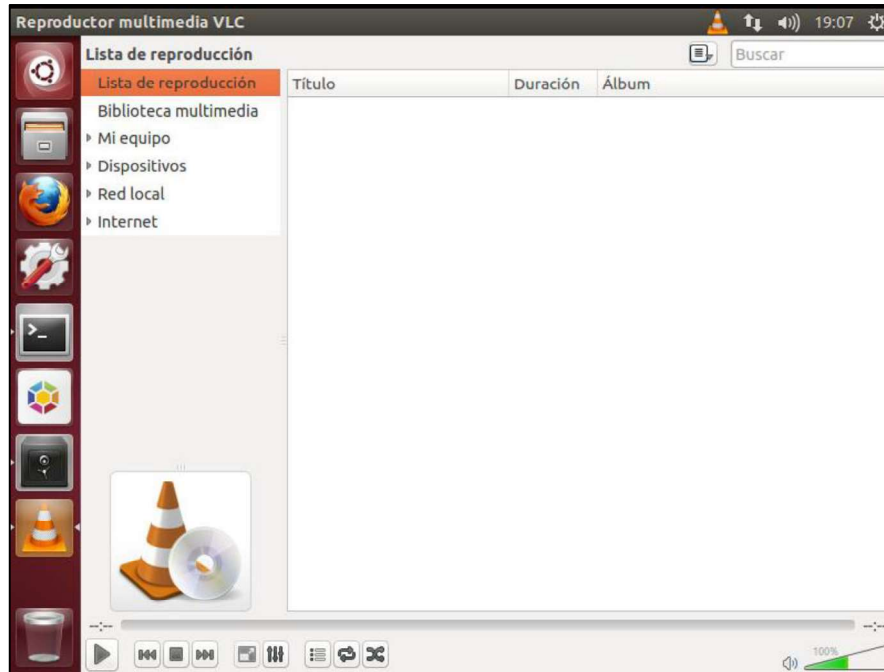
```
Terminal
root@web-virtual-machine: /home/web
root@web-virtual-machine:/home/web# ifconfig
eth0      Link encap:Ethernet direcciónHW 00:0c:29:99:8c:3b
          Direc. inet:192.168.0.102 Difus.:192.168.0.255 Másc:255.255.255.0
          Dirección inet6: fe80::20c:29ff:fe99:8c3b/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:45311 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:30145 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:5126544 (5.1 MB) TX bytes:2397751 (2.3 MB)

eth1      Link encap:Ethernet direcciónHW 00:0c:29:99:8c:45
          Dirección inet6: fe80::20c:29ff:fe99:8c45/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:14605 errores:0 perdidos:242 overruns:0 frame:0
          Paquetes TX:12172 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:1219553 (1.2 MB) TX bytes:1050746 (1.0 MB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1 Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
          Paquetes RX:55869 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:55869 errores:0 perdidos:0 overruns:0 carrier:0
```

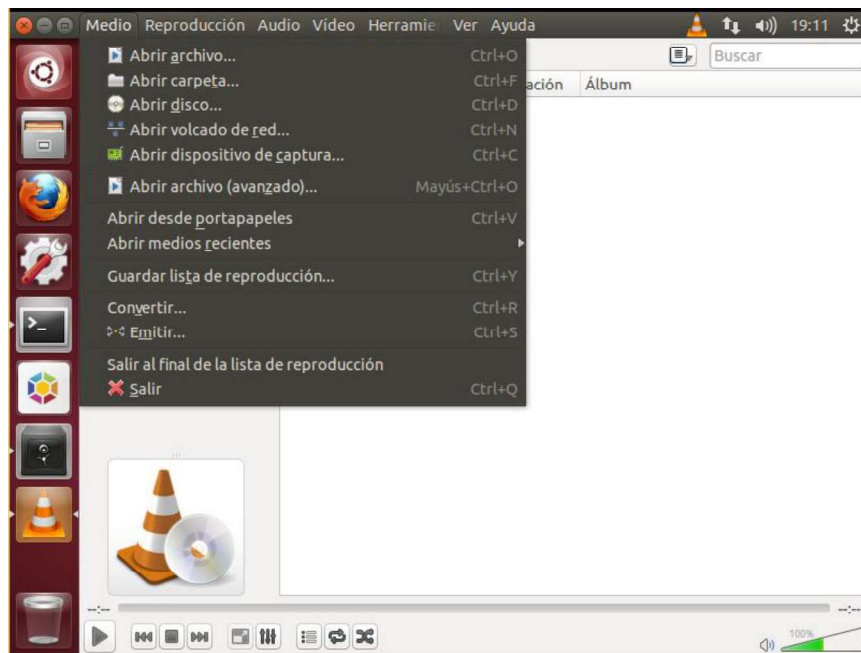
Figura 3.35. Configuraciones del servidor de Video Streaming (2)

Se abre el reproductor VLC instalado en el servidor para la transmisión por streaming.



**Figura 3.36.** Configuraciones del servidor de Video Streaming (3)

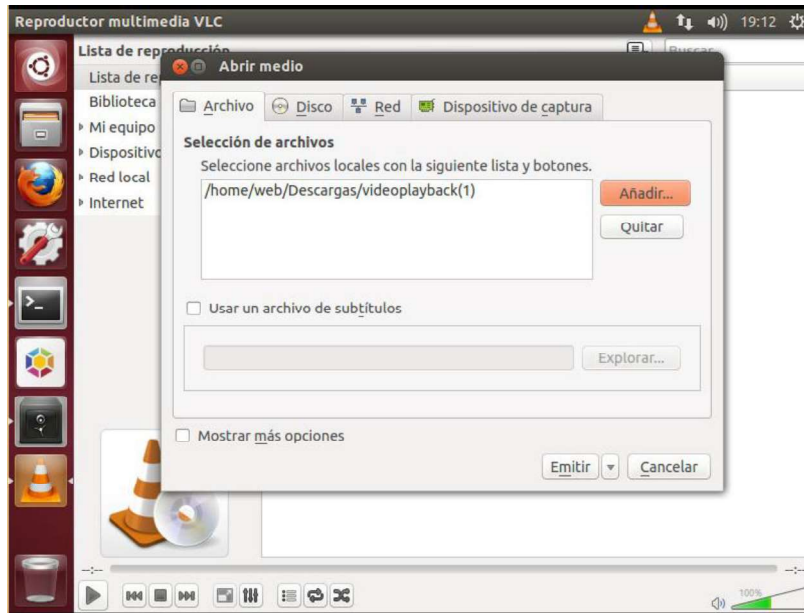
Se abre el medio para emitir y se da clic en la opción "Emitir":



**Figura 3.37.** Configuraciones del servidor de Video Streaming (4)

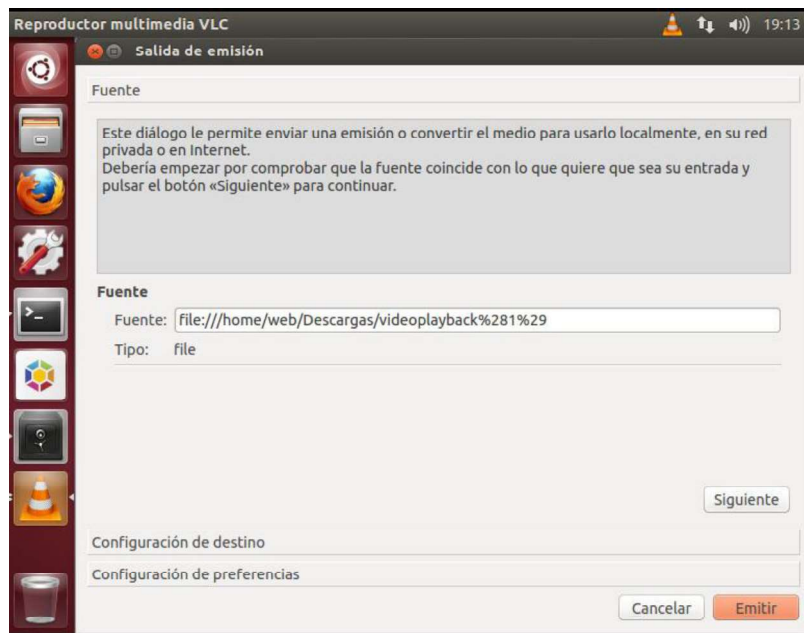
Se abre el video para la emisión.





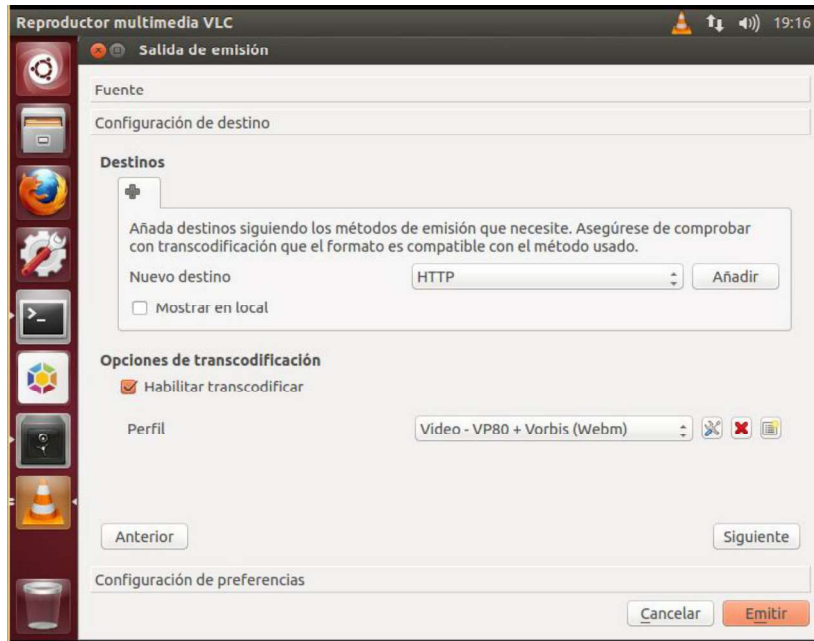
**Figura 3.38.** Configuraciones del servidor de Video Streaming (5)

Al seleccionar la opción de “Emitir” aparecerá el siguiente cuadro donde se debe dar clic en la opción “siguiente”:



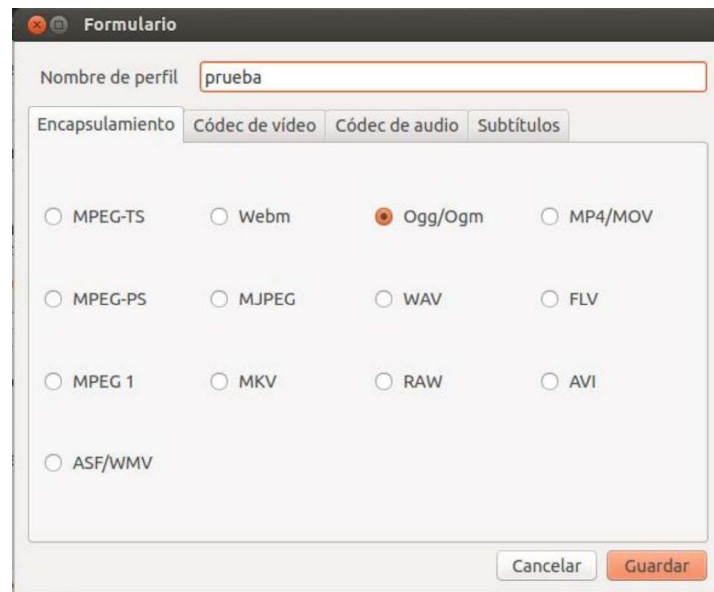
**Figura 3.39.** Configuraciones del servidor de Video Streaming (6)

Se selecciona la opción de “HTTP” en la sección Destinos y se crea el perfil prueba.



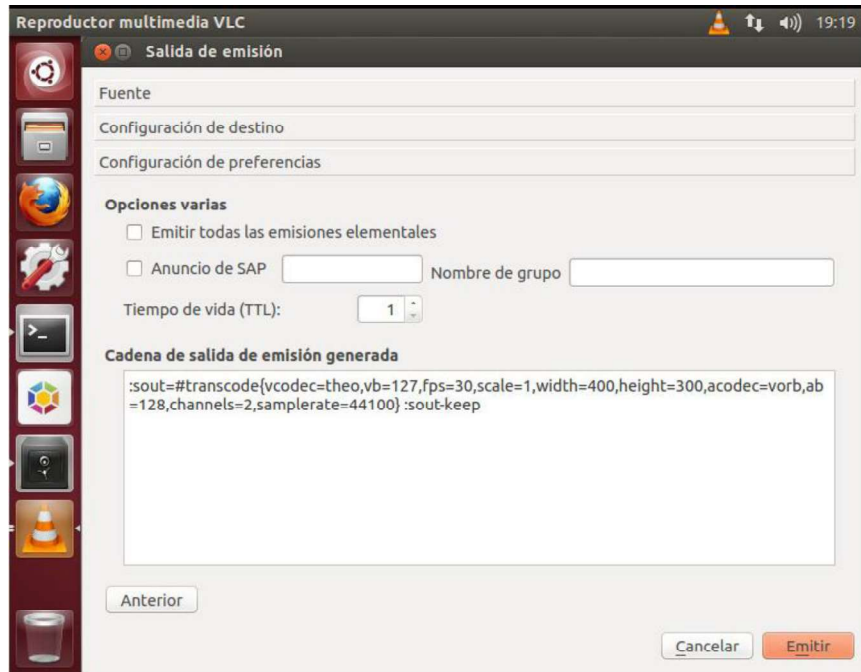
**Figura 3.40.** Configuraciones del servidor de Video Streaming (7)

El resto de las opciones se las deja por defecto, únicamente se modifica la opción del Encapsulamiento, se guarda y continúa.



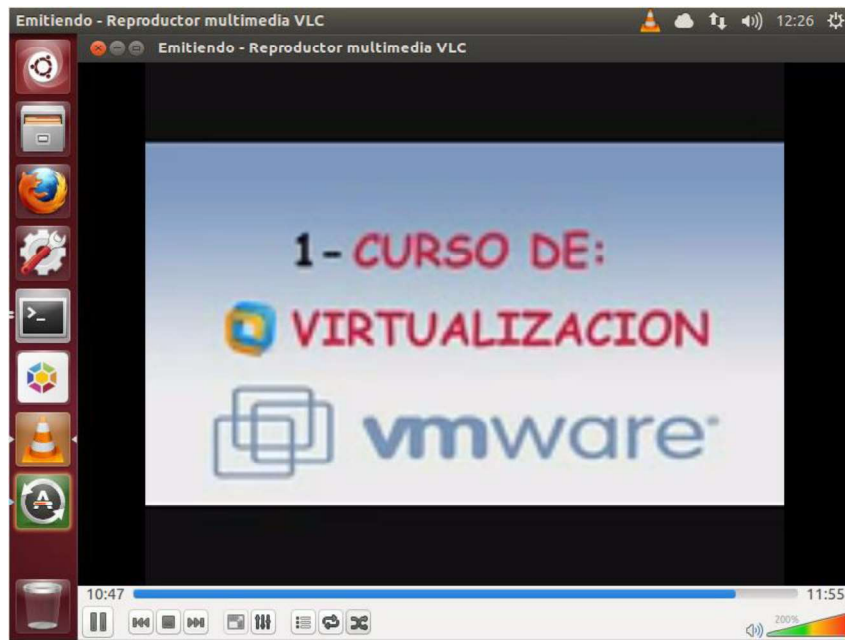
**Figura 3.41.** Configuraciones del servidor de Video Streaming (8)

En el cuadro siguiente se deja de igual manera toda la configuración por defecto.



**Figura 3.42.** Configuraciones del servidor de Video *Streaming* (9)

Se empieza la emisión del video:



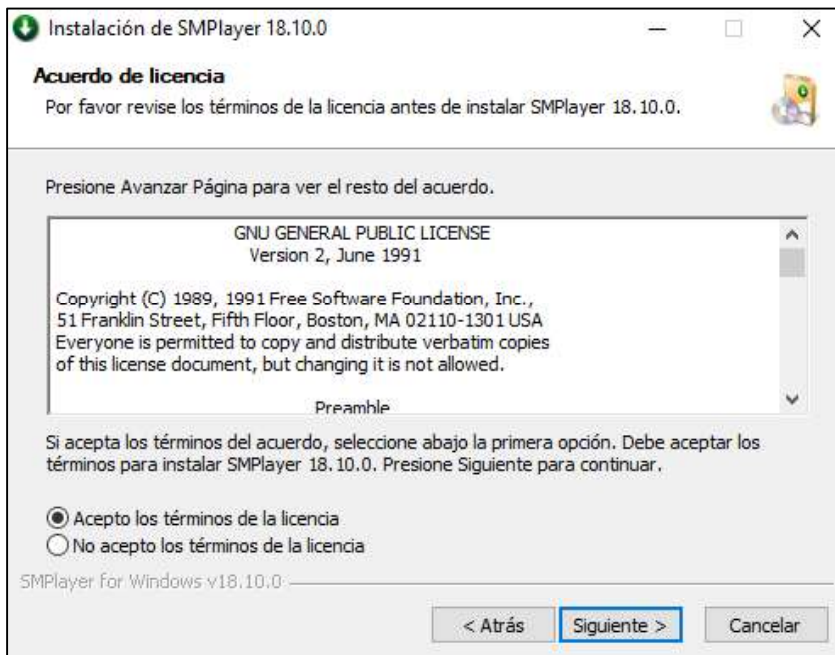
**Figura 3.43.** Configuraciones del servidor de Video *Streaming* (10)

Del lado del cliente se procede a instalar el programa SM Player para poder visualizar la transmisión:



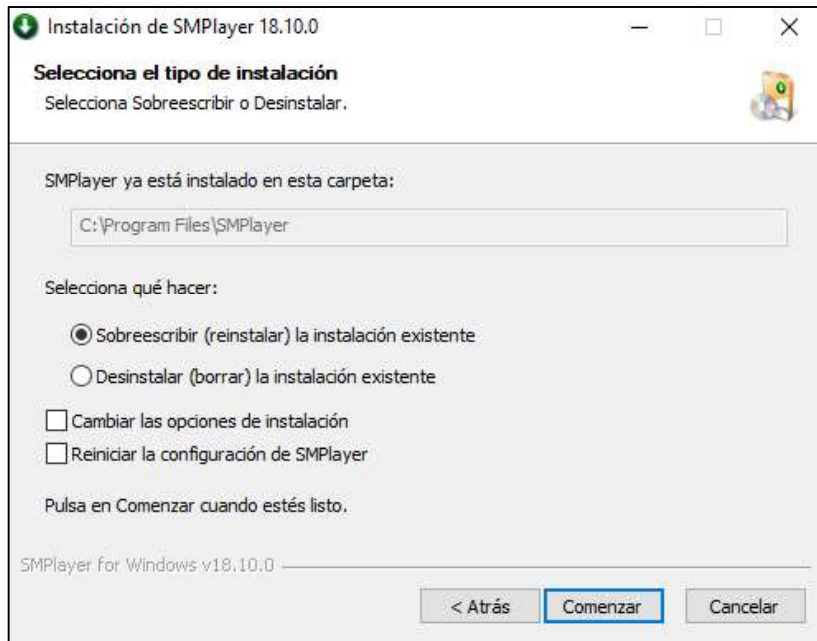
**Figura 3.44.** Configuraciones del servidor de Video *Streaming* (11)

Siguiente y se continúa la instalación:



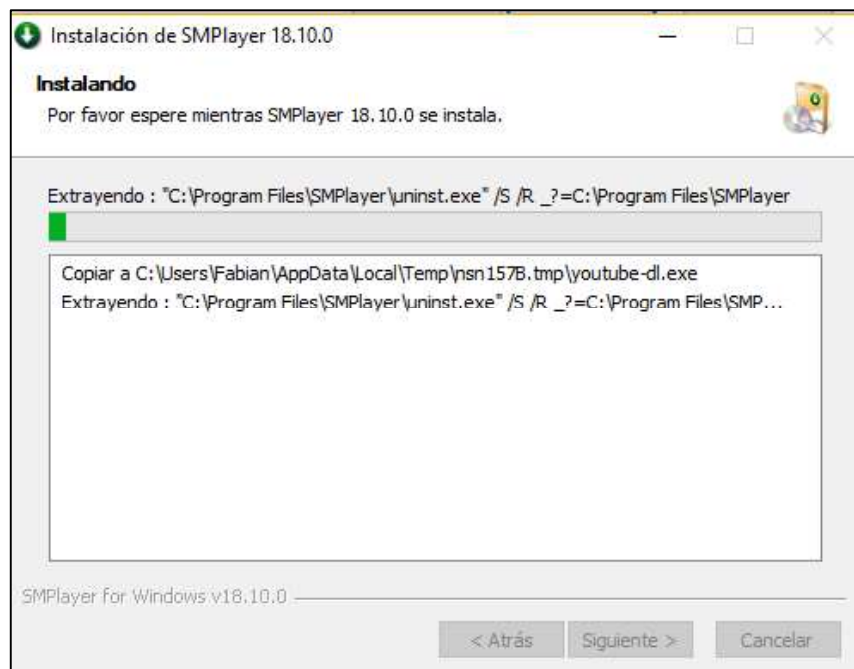
**Figura 3.45.** Configuraciones del servidor de Video *Streaming* (12)

Se instala los paquetes y el programa:



**Figura 3.46.** Configuraciones del servidor de Video *Streaming* (13)

Se espera el proceso de instalación:



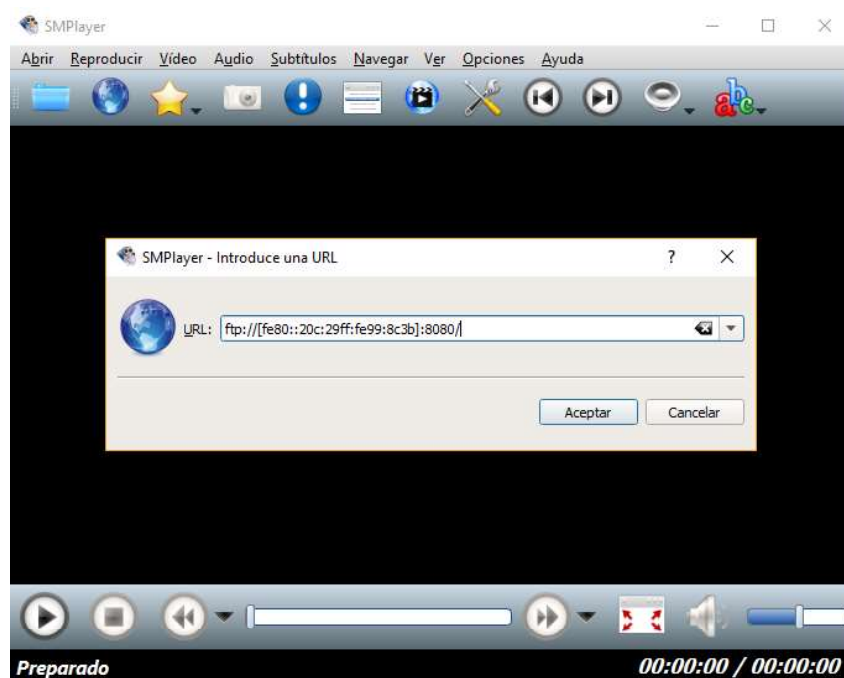
**Figura 3.47.** Configuraciones del servidor de Video *Streaming* (14)

Luego de finalizada la instalación, se procede a ejecutar el programa instalado:



**Figura 3.48.** Configuraciones del servidor de Video Streaming (15)

Se empieza a visualizar la transmisión apuntando a la URL IPv6 del servidor de streaming:



**Figura 3.49.** Configuraciones del servidor de Video Streaming (16)

Inicia la transmisión:

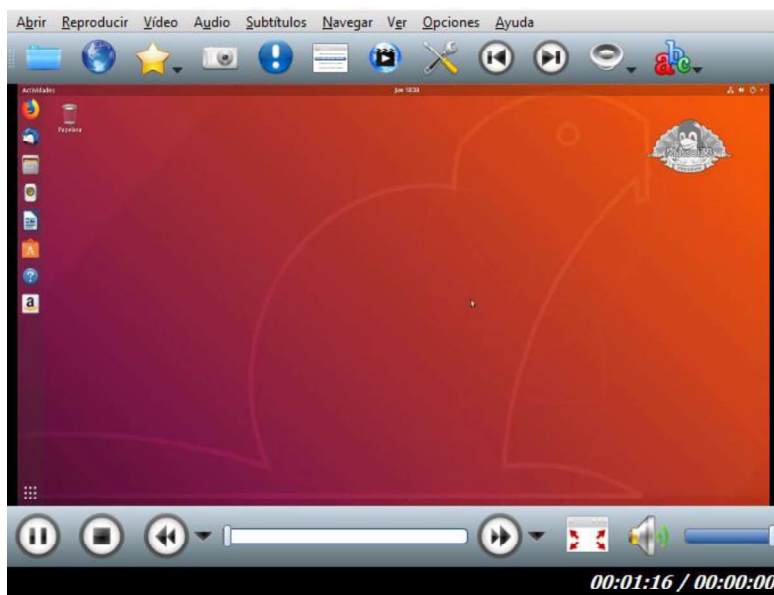


Figura 3.50. Configuraciones del servidor de Video Streaming (17)

### 3.2.2.5 Servidor de FTP

Se instala el servicio FTP con el comando `vsftpd`:

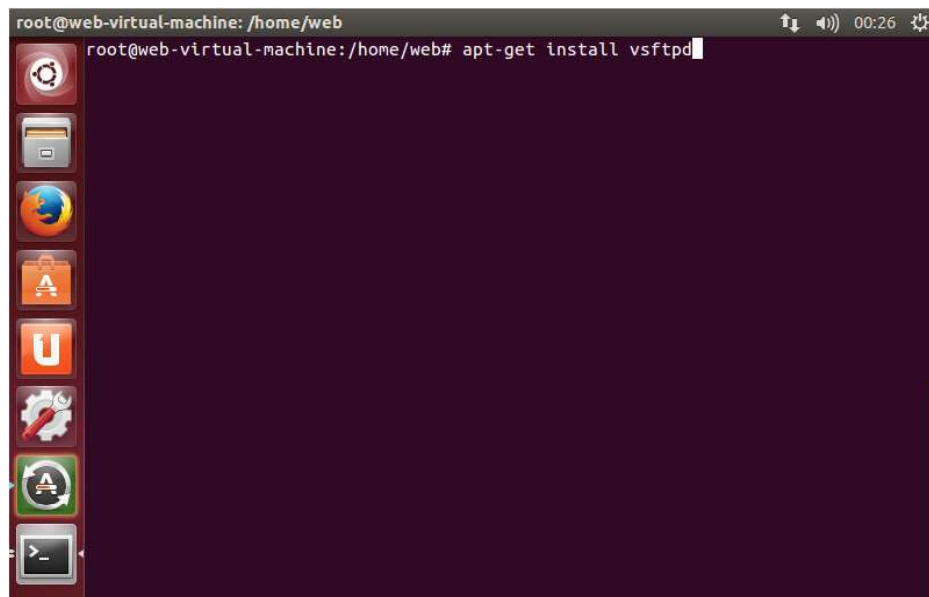
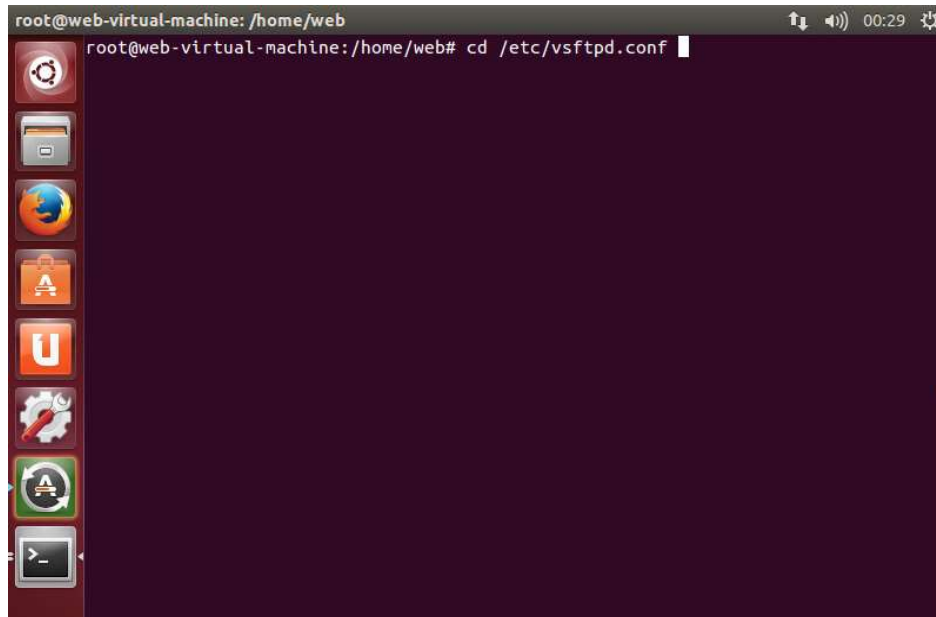


Figura 3.51. Configuraciones del servidor de FTP (1)

Debe dirigirse hacia la ubicación `/etc/vsftpd.conf`:

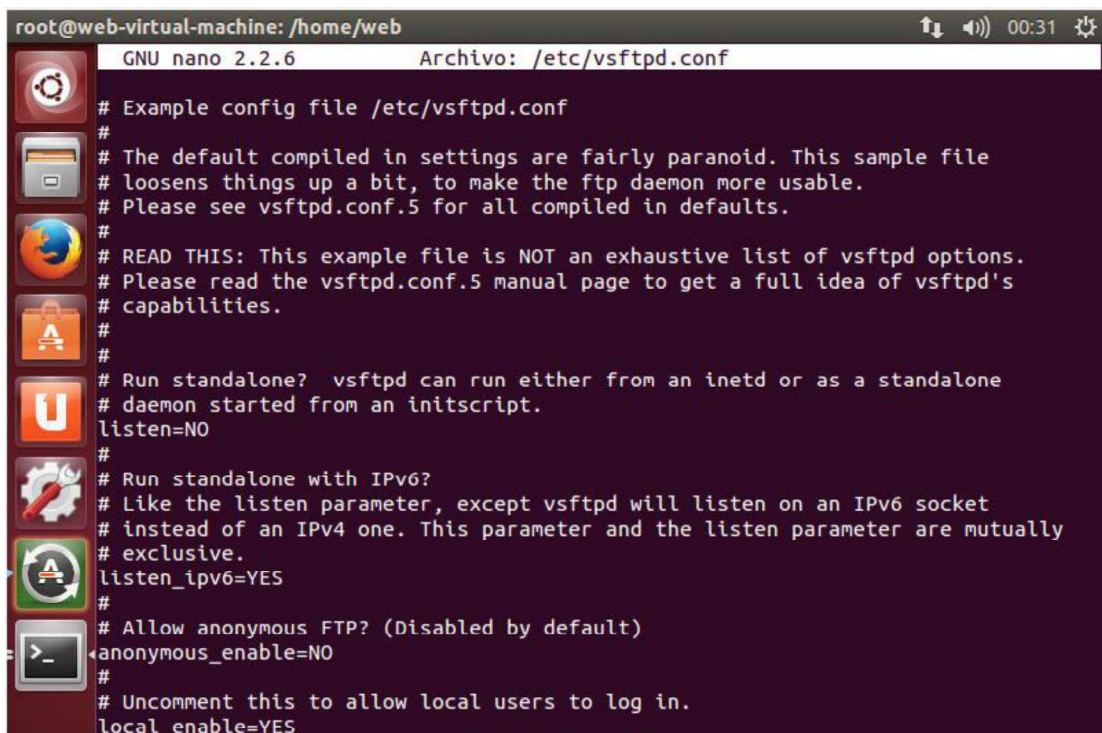


**Figura 3.52.** Configuraciones del servidor de FTP (2)

Se debe ditar el archivo y habilitar

**Listen = NO**

**listen\_ipv6 = YES**



**Figura 3.53.** Configuraciones del servidor de FTP (3)

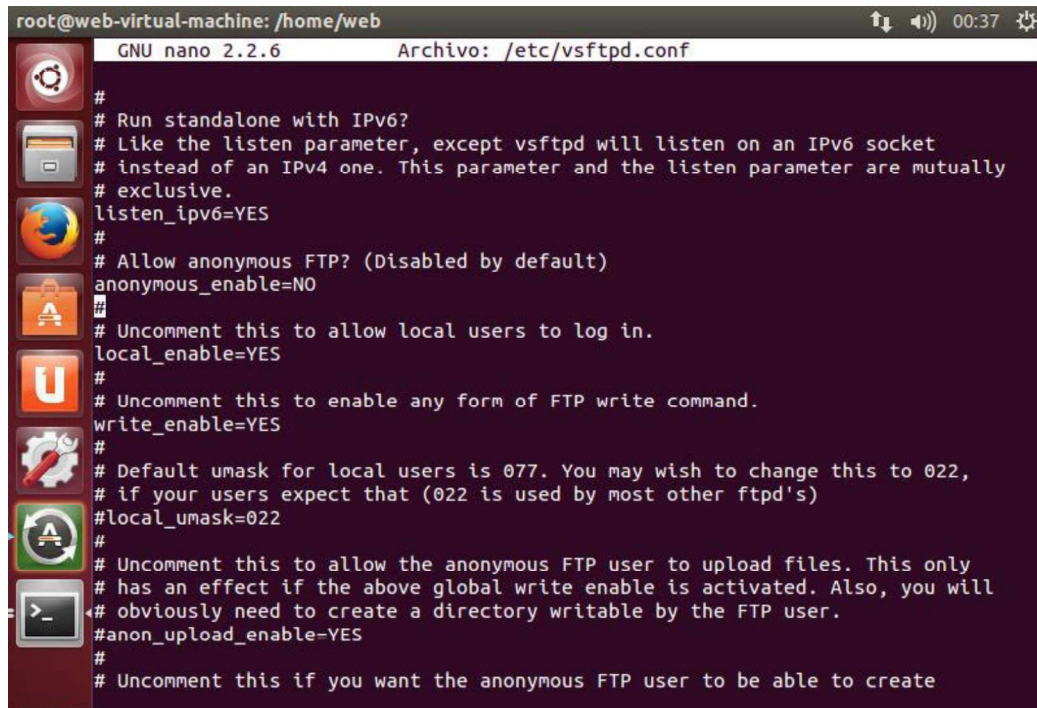
Se debe configurar.

**anonymous\_enable=NO**



local\_enable=YES

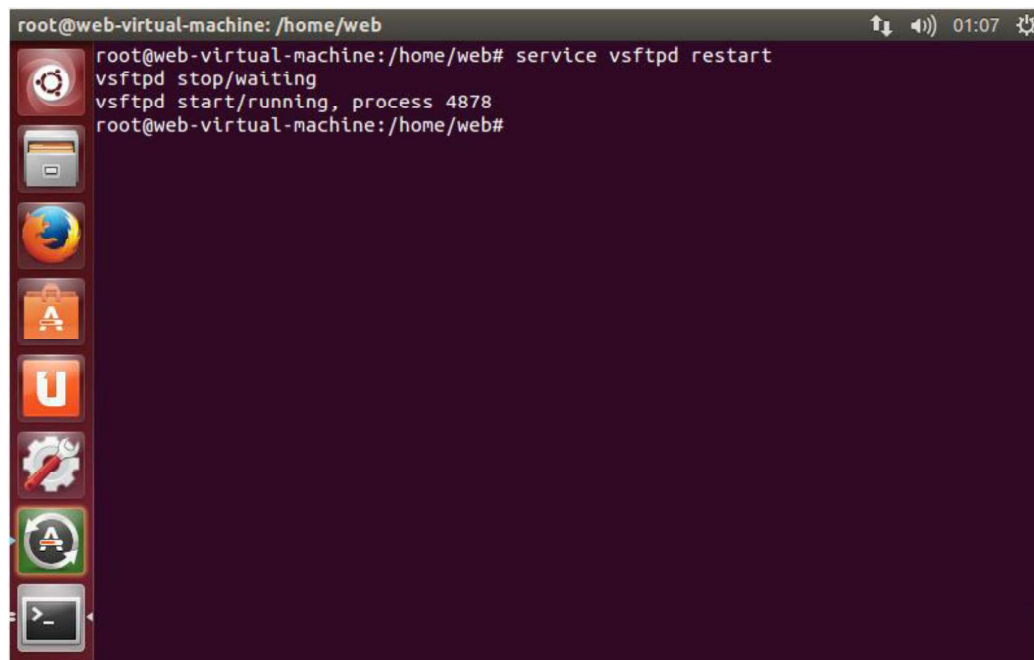
write\_enable=YES



```
root@web-virtual-machine: /home/web
GNU nano 2.2.6 Archivo: /etc/vsftpd.conf
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
```

Figura 3.54. Configuraciones del servidor de FTP (4)

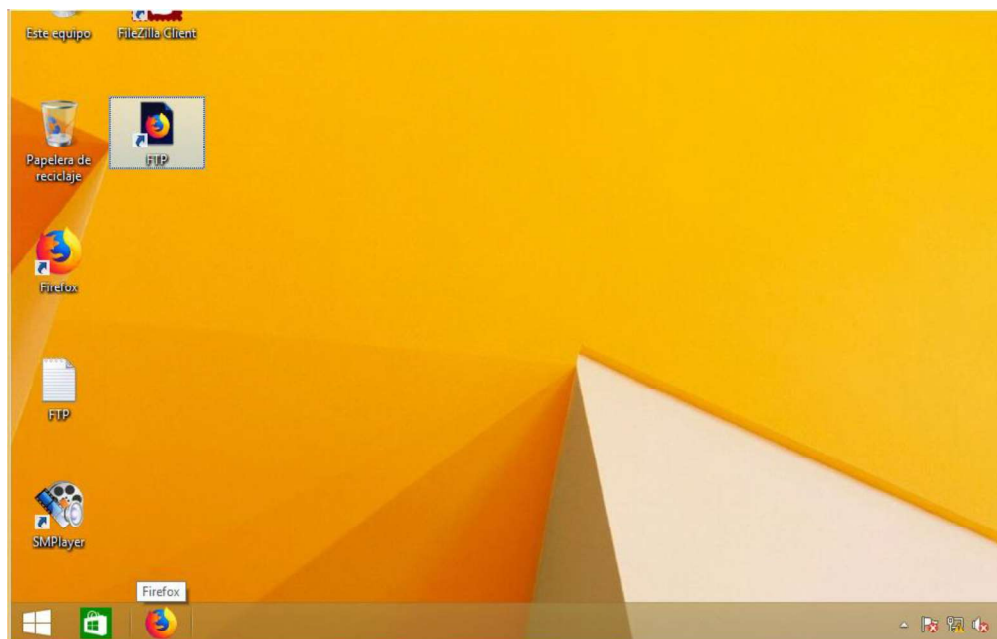
Se debe reiniciar el servicio:



```
root@web-virtual-machine: /home/web
root@web-virtual-machine:/home/web# service vsftpd restart
vsftpd stop/waiting
vsftpd start/running, process 4878
root@web-virtual-machine:/home/web#
```

Figura 3.55. Configuraciones del servidor de FTP (5)

Desde una PC con Windows 8 se crea un acceso directo al servidor FTP:

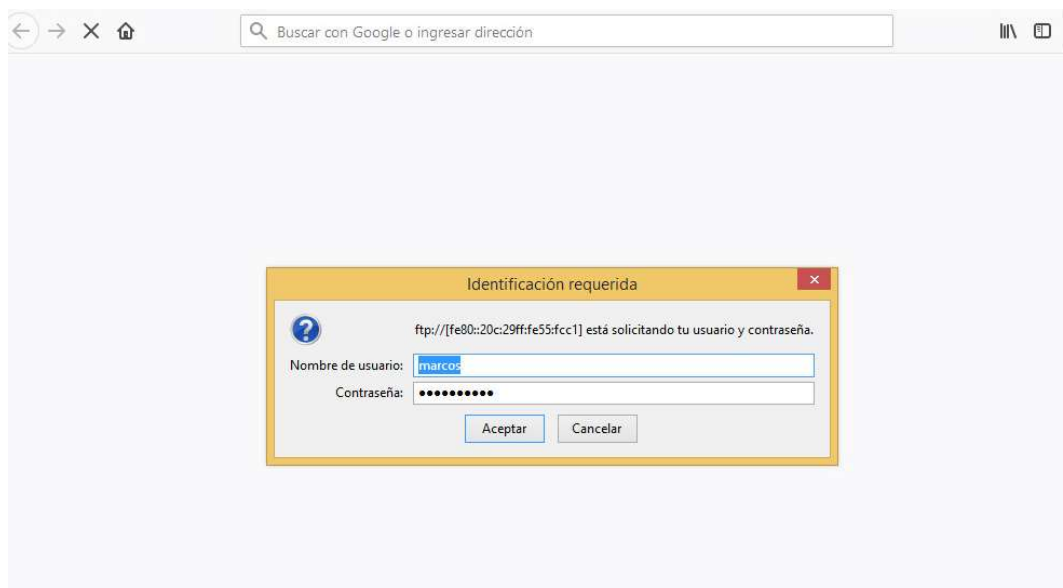


**Figura 3.56.** Configuraciones del servidor de FTP (6)

El usuario y contraseña solicitados son las credenciales del servidor FTP en Ubuntu:

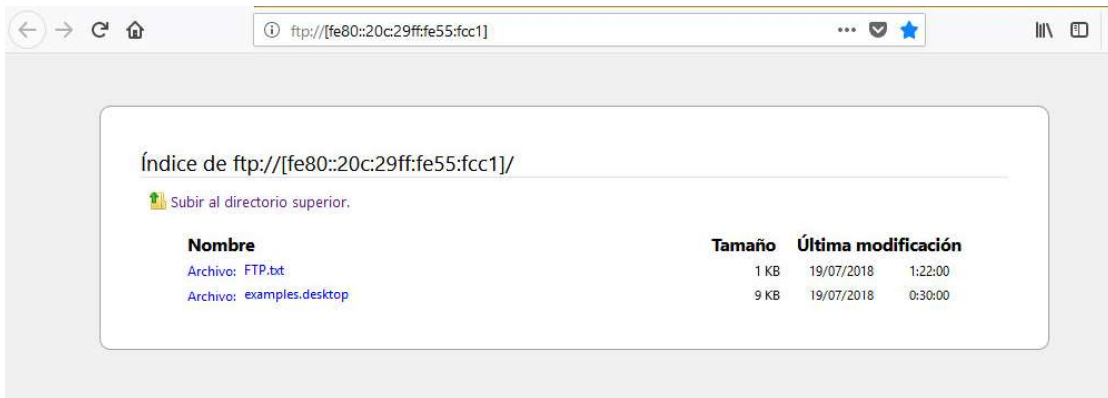
**Usuario:** marcos

**Contraseña:** ubuntu123.



**Figura 3.57.** Configuraciones del servidor de FTP (7)

Aquí se puede observar los archivos cargados al servidor:

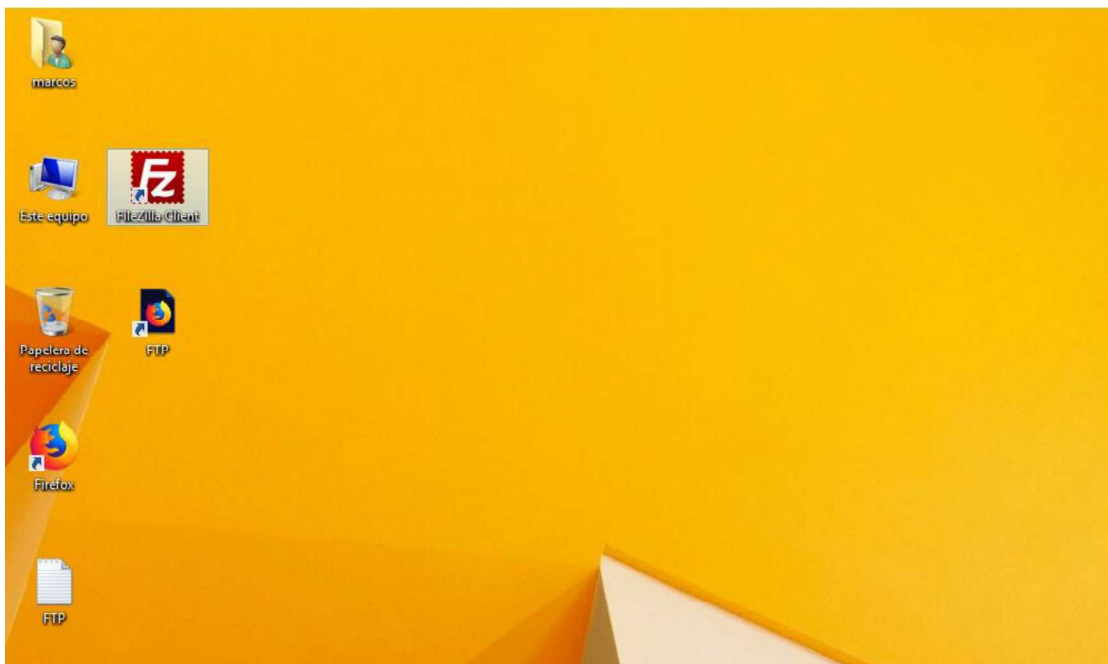


**Figura 3.58.** Configuraciones del servidor de FTP (8)

Cargar archivos al servidor FTP:

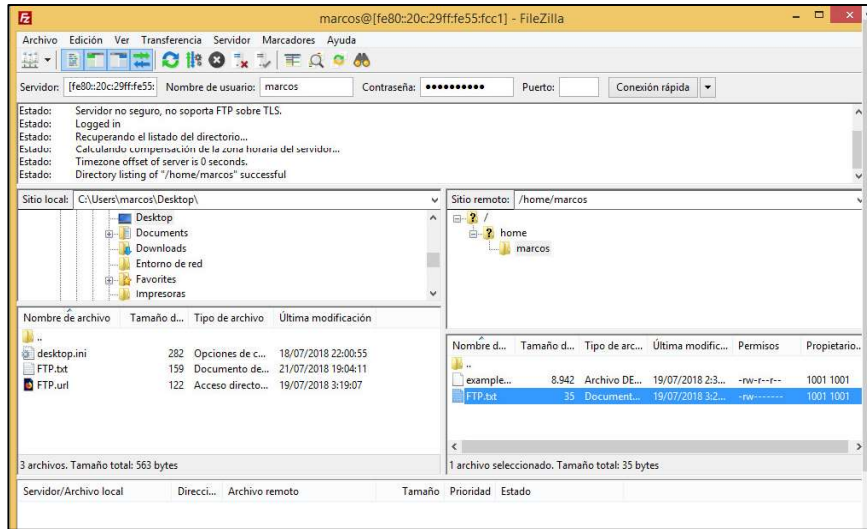
Se instala un programa en este caso Filezilla Client

Descargar de: <https://filezilla-project.org/download.php>



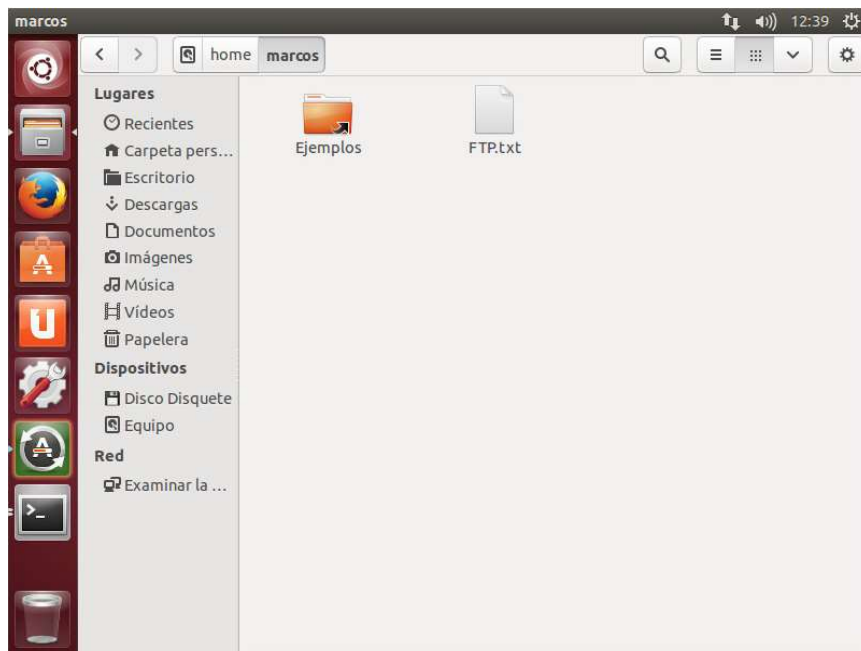
**Figura 3.59.** Configuraciones del servidor de FTP (9)

Se añade la dirección IP y las credenciales para cargar o descargar archivos del servidor FTP desde un computador como se ve a continuación:



**Figura 3.60.** Configuraciones del servidor de FTP (10)

También se aprecian los archivos cargados y el sitio para poder cargar más archivos. En la siguiente gráfica se puede verificar en el servidor FTP donde se localizan los archivos restantes.



**Figura 3.61.** Configuraciones del servidor de FTP (11)

### 3.2.2.6 Servidor Web [48]

Inicialmente con el sistema operativo base se procede a verificar los paquetes instalados para el sistema operativo.

Para ello primero se abre un terminal y se accede con las credenciales de root:

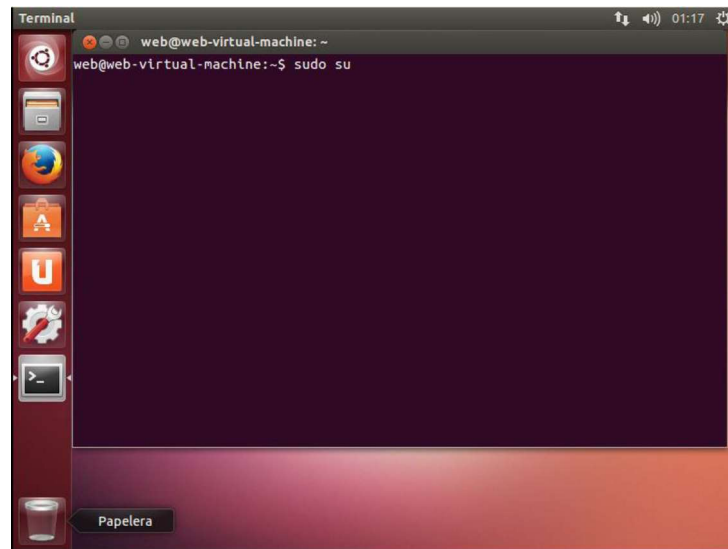


Figura 3.62. Configuraciones del servidor Web (1)

Se actualiza los paquetes:

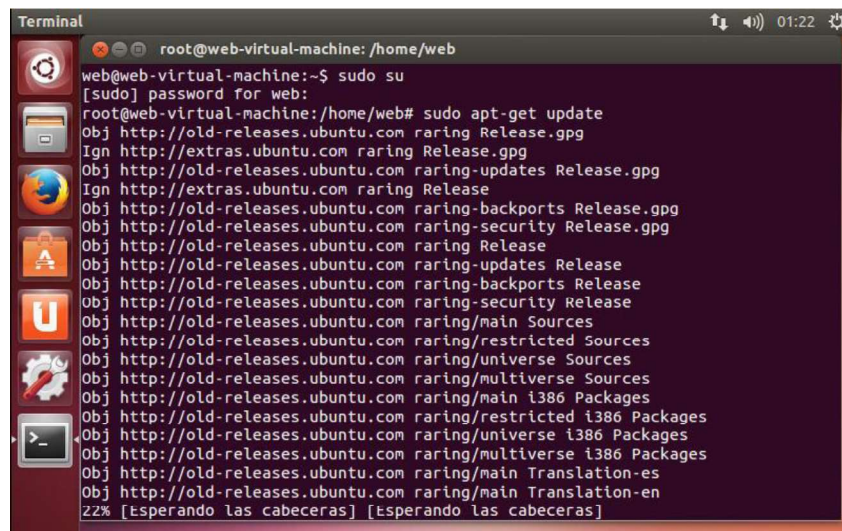
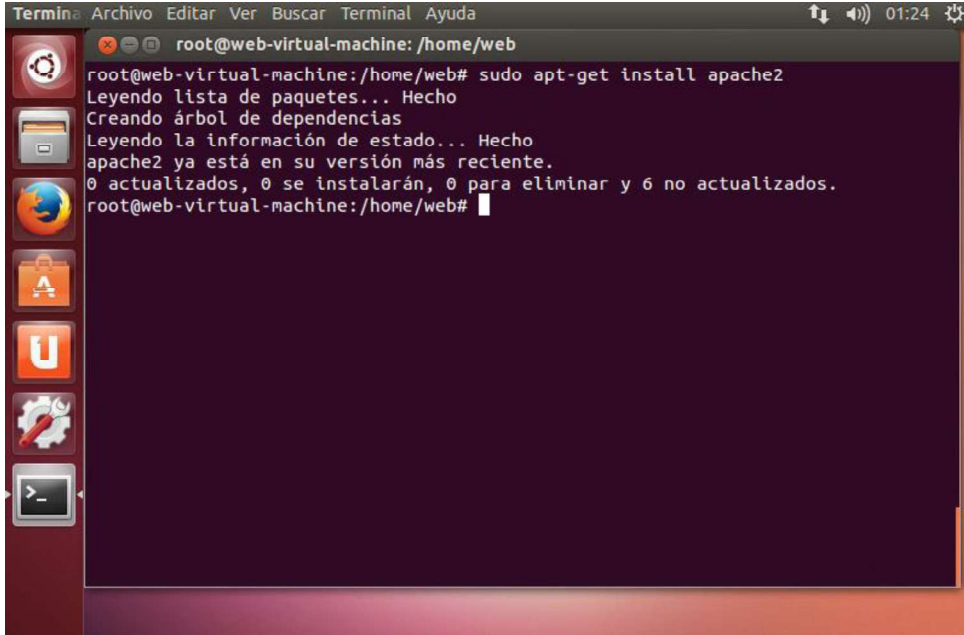


Figura 3.63. Configuraciones del servidor Web (2)

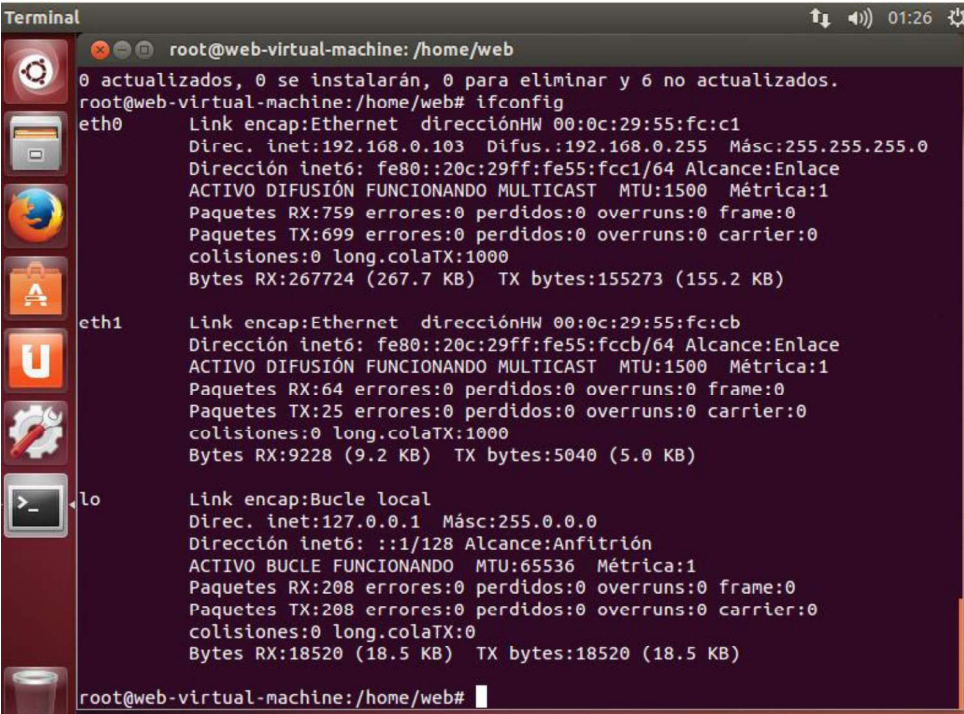
Instalamos pache2:



```
Terminar Archivo Editar Ver Buscar Terminal Ayuda
root@web-virtual-machine: /home/web
root@web-virtual-machine:/home/web# sudo apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 6 no actualizados.
root@web-virtual-machine:/home/web#
```

Figura 3.64. Configuraciones del servidor Web (3)

Verificar IPv4 y 6:



```
Terminal
root@web-virtual-machine: /home/web
0 actualizados, 0 se instalarán, 0 para eliminar y 6 no actualizados.
root@web-virtual-machine:/home/web# ifconfig
eth0      Link encap:Ethernet direcciónHW 00:0c:29:55:fc:c1
Direc. inet:192.168.0.103 Difus.:192.168.0.255 Másc:255.255.255.0
Dirección inet6: fe80::20c:29ff:fe55:fcc1/64 Alcance:Enlace
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
Paquetes RX:759 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:699 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:267724 (267.7 KB) TX bytes:155273 (155.2 KB)

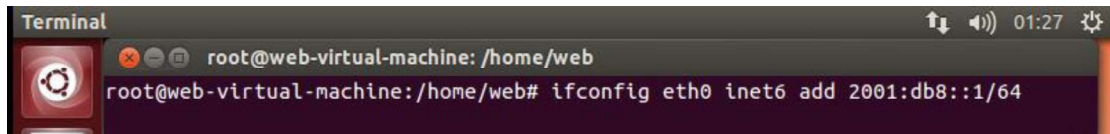
eth1      Link encap:Ethernet direcciónHW 00:0c:29:55:fc:cb
Dirección inet6: fe80::20c:29ff:fe55:fccb/64 Alcance:Enlace
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
Paquetes RX:64 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:25 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:9228 (9.2 KB) TX bytes:5040 (5.0 KB)

lo        Link encap:Bucle local
Direc. inet:127.0.0.1 Másc:255.0.0.0
Dirección inet6: ::1/128 Alcance:Anfitrión
ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
Paquetes RX:208 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:208 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:0
Bytes RX:18520 (18.5 KB) TX bytes:18520 (18.5 KB)

root@web-virtual-machine:/home/web#
```

Figura 3.65. Configuraciones del servidor Web (4)

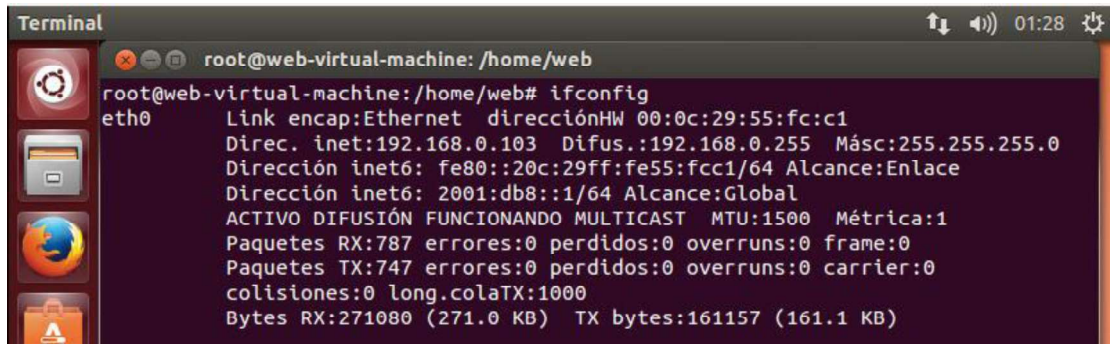
Poner IPv6:



```
Terminal
root@web-virtual-machine: /home/web
root@web-virtual-machine:/home/web# ifconfig eth0 inet6 add 2001:db8::1/64
```

Figura 3.66. Configuraciones del servidor Web (5)

Revisamos:



```
Terminal
root@web-virtual-machine: /home/web
root@web-virtual-machine:/home/web# ifconfig
eth0      Link encap:Ethernet direcciónHW 00:0c:29:55:fc:c1
          Direc. inet:192.168.0.103 Difus.:192.168.0.255 Másc:255.255.255.0
          Dirección inet6: fe80::20c:29ff:fe55:fcc1/64 Alcance:Enlace
          Dirección inet6: 2001:db8::1/64 Alcance:Global
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:787 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:747 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:271080 (271.0 KB) TX bytes:161157 (161.1 KB)
```

Figura 3.67. Configuraciones del servidor Web (6)

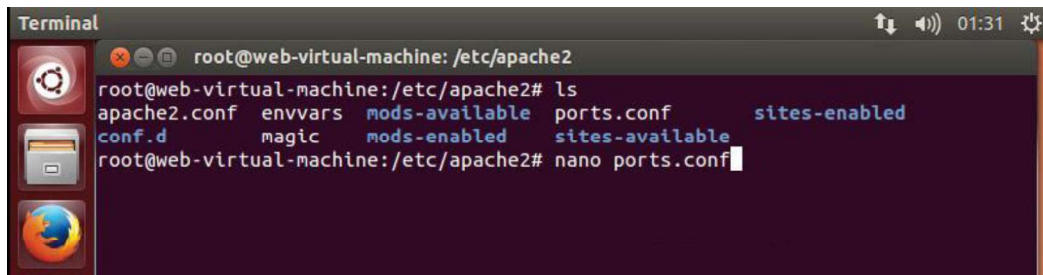
Nos dirigimos Apache 2:



```
Terminal
root@web-virtual-machine: /etc/apache2
root@web-virtual-machine:/etc/apache2# cd /etc/apache2/
```

Figura 3.68. Configuraciones del servidor Web (7)

Verificamos y procedemos a editar el archivo:



```
Terminal
root@web-virtual-machine: /etc/apache2
root@web-virtual-machine:/etc/apache2# ls
apache2.conf  envvars  mods-available  ports.conf  sites-enabled
conf.d        magic    mods-enabled    sites-available
root@web-virtual-machine:/etc/apache2# nano ports.conf
```

Figura 3.69. Configuraciones del servidor Web (8)

Verificamos interfaces de escucha y lo ponemos a escuchar por IPv6:

```

Terminal
root@web-virtual-machine: /etc/apache2
GNU nano 2.2.6 Archivo: ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz

NameVirtualHost *:80
Listen [2001:db8::1]:80
Listen 192.168.0.103:80

<IfModule mod_ssl.c>
# If you add NameVirtualHost *:443 here, you will also have to change
# the VirtualHost statement in /etc/apache2/sites-available/default-ssl
# to <VirtualHost *:443>
# Server Name Indication for SSL named virtual hosts is currently not
# supported by MSIE on Windows XP.
Listen 443
</IfModule>

<IfModule mod_gnutls.c>
Listen 443
</IfModule>

```

Figura 3.70. Configuraciones del servidor Web (9)

Verificamos puertos de escucha del servidor:

```

Terminal
root@web-virtual-machine: /etc/apache2
root@web-virtual-machine: /etc/apache2# netstat -pan | grep apach
root@web-virtual-machine: /etc/apache2# netstat -pan | grep apach
root@web-virtual-machine: /etc/apache2# /etc/init.d/apache2 restart
* Restarting web server apache2 [ OK ]
root@web-virtual-machine: /etc/apache2# netstat -pan | grep apach
tcp        0      0 192.168.0.103:80    0.0.0.0:*           ESCUCHAR
3361/apache2
tcp6       0      0 2001:db8::1:80     :::*                 ESCUCHAR
3361/apache2
unix 2      [ ACC ]   FLUJO      ESCUCHANDO    20610    3364/apache2 /
var/run/apache2/cgisock.3361
root@web-virtual-machine: /etc/apache2#

```

Figura 3.71. Configuraciones del servidor Web (10)

Telnet para probar conexión:



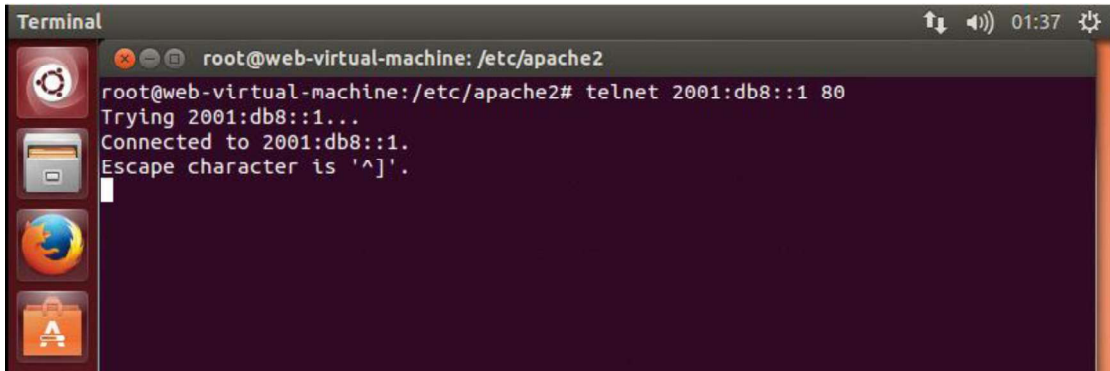


Figura 3.72. Configuraciones del servidor Web (11)

Probamos respuesta de Apache:

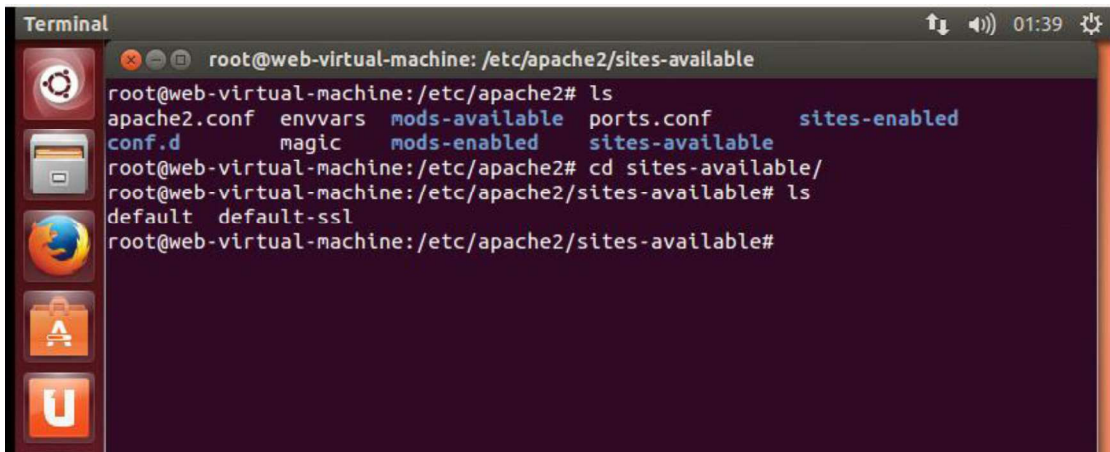


Figura 3.73. Configuraciones del servidor Web (12)

Probamos respuesta y servicio de apache levantado:

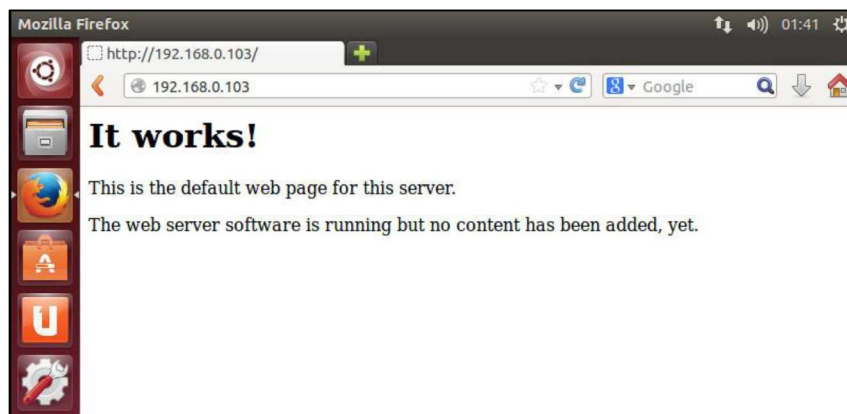
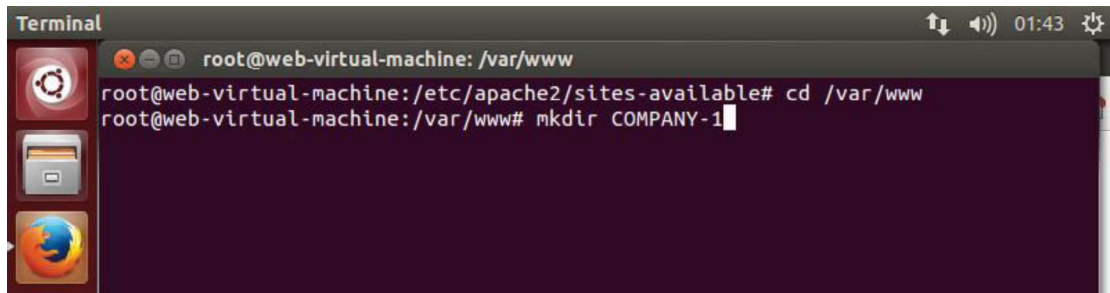


Figura 3.74. Configuraciones del servidor Web (13)

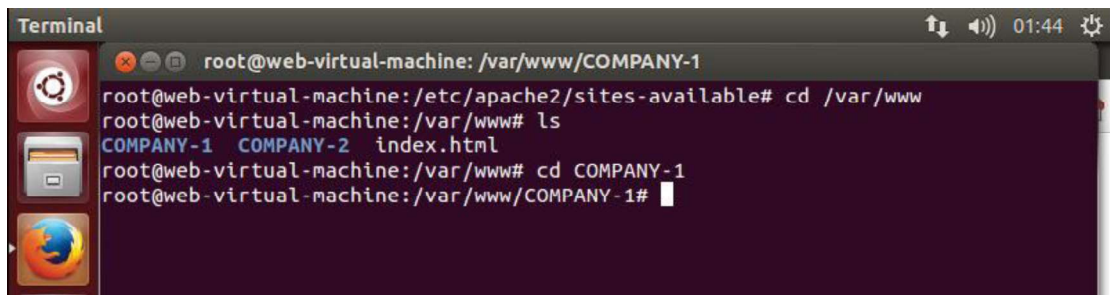
Creamos un nombre de dominio para resolver con IPv6:



```
Terminal
root@web-virtual-machine: /var/www
root@web-virtual-machine:/etc/apache2/sites-available# cd /var/www
root@web-virtual-machine:/var/www# mkdir COMPANY-1
```

**Figura 3.75.** Configuraciones del servidor Web (14)

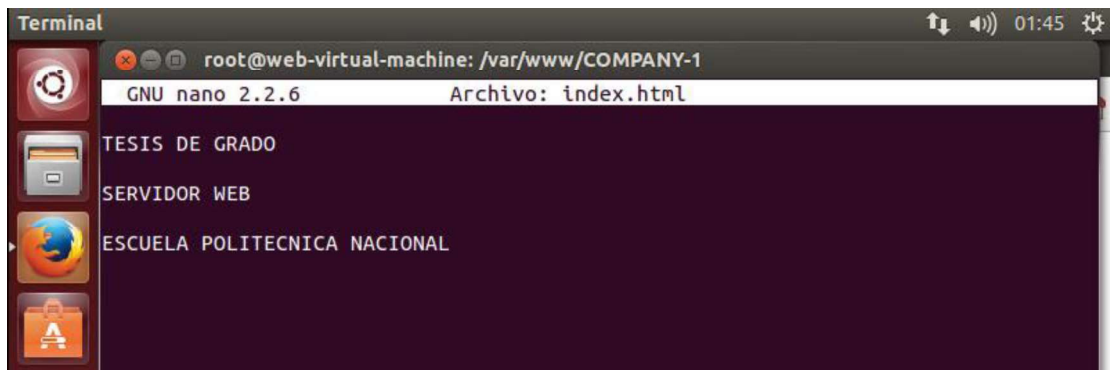
Creamos el archivo index.html:



```
Terminal
root@web-virtual-machine: /var/www/COMPANY-1
root@web-virtual-machine:/etc/apache2/sites-available# cd /var/www
root@web-virtual-machine:/var/www# ls
COMPANY-1  COMPANY-2  index.html
root@web-virtual-machine:/var/www# cd COMPANY-1
root@web-virtual-machine:/var/www/COMPANY-1#
```

**Figura 3.76.** Configuraciones del servidor Web (15)

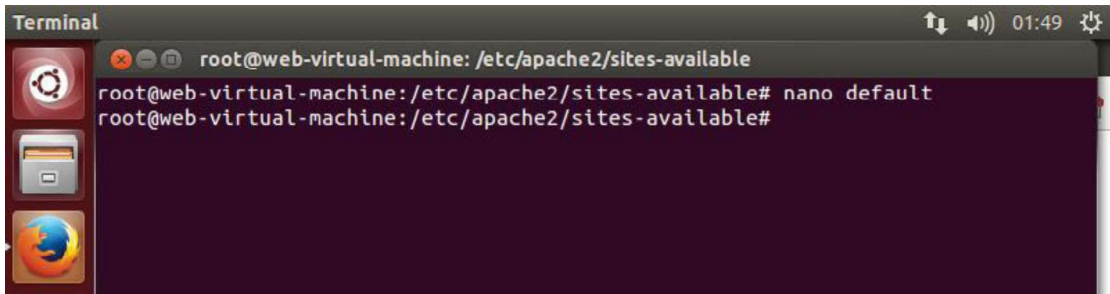
Creamos el texto para mostrar:



```
Terminal
root@web-virtual-machine: /var/www/COMPANY-1
GNU nano 2.2.6 Archivo: index.html
TESIS DE GRADO
SERVIDOR WEB
ESCUELA POLITECNICA NACIONAL
```

**Figura 3.77.** Configuraciones del servidor Web (16)

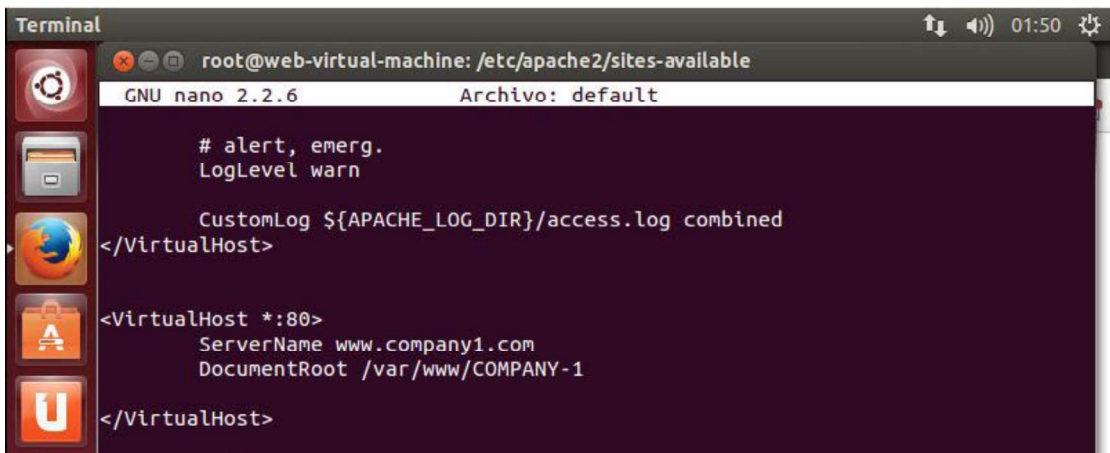
Para crear el apuntador al contenido creamos una directiva dentro del archivo default:



```
Terminal
root@web-virtual-machine: /etc/apache2/sites-available
root@web-virtual-machine:/etc/apache2/sites-available# nano default
root@web-virtual-machine:/etc/apache2/sites-available#
```

**Figura 3.78.** Configuraciones del servidor Web (17)

Editamos el archivo:



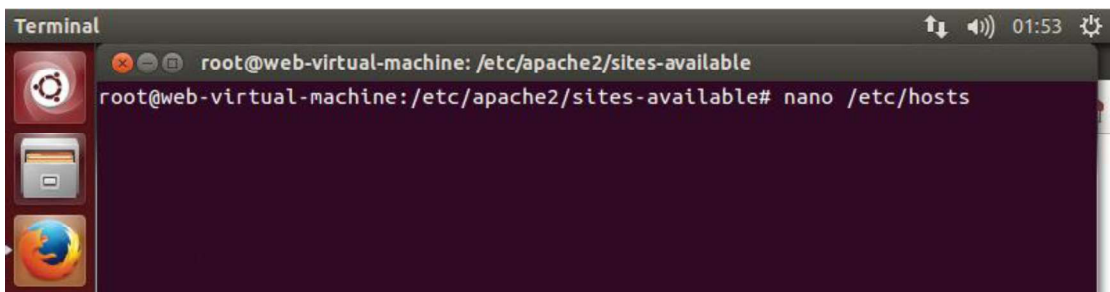
```
Terminal
GNU nano 2.2.6 Archivo: default
# alert, emerg.
LogLevel warn

CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:80>
  ServerName www.company1.com
  DocumentRoot /var/www/COMPANY-1
</VirtualHost>
```

**Figura 3.79.** Configuraciones del servidor Web (18)

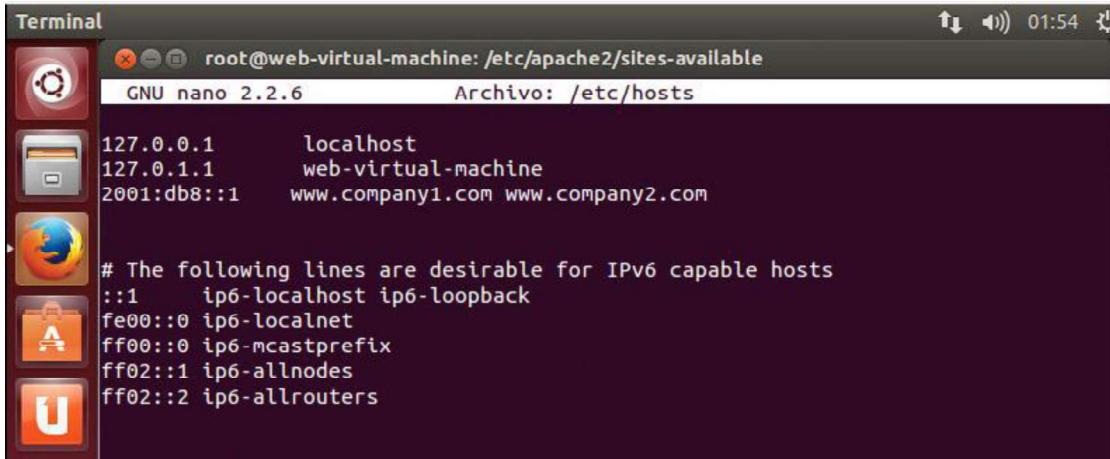
Resolución de nombre, creamos el host local:



```
Terminal
root@web-virtual-machine: /etc/apache2/sites-available
root@web-virtual-machine:/etc/apache2/sites-available# nano /etc/hosts
```

**Figura 3.80.** Configuraciones del servidor Web (19)

Añadimos el nombre para la resolución:

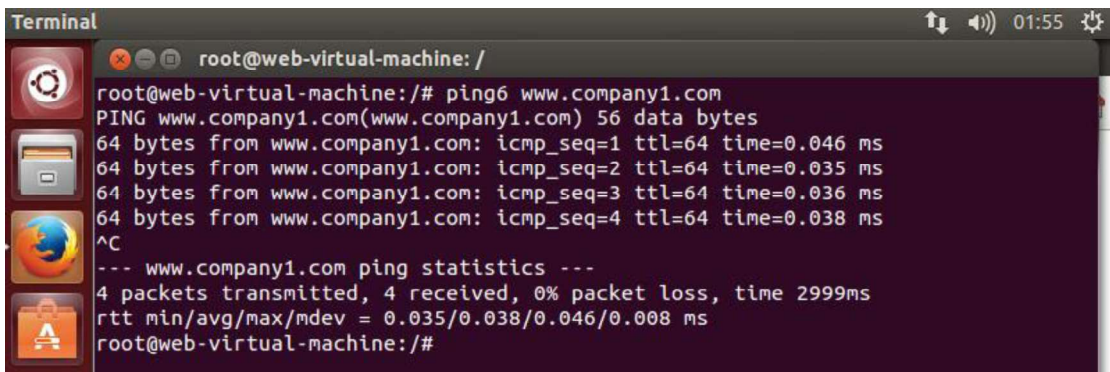


```
Terminal
root@web-virtual-machine: /etc/apache2/sites-available
GNU nano 2.2.6 Archivo: /etc/hosts
127.0.0.1 localhost
127.0.1.1 web-virtual-machine
2001:db8::1 www.company1.com www.company2.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Figura 3.81. Configuraciones del servidor Web (20)

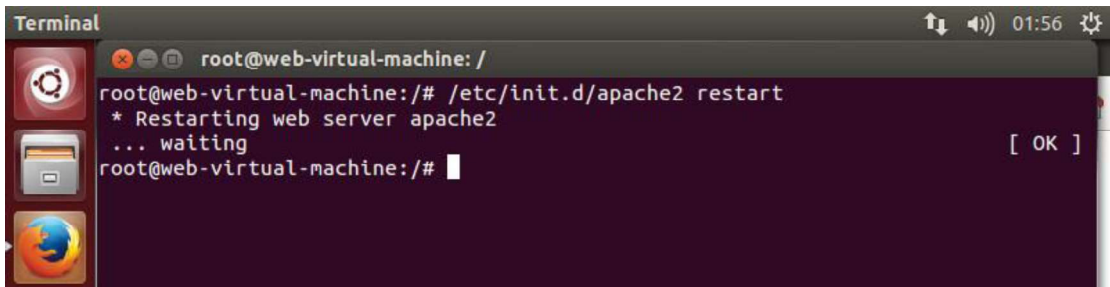
Respuesta del host creado:



```
Terminal
root@web-virtual-machine: /
root@web-virtual-machine: /# ping6 www.company1.com
PING www.company1.com(www.company1.com) 56 data bytes
64 bytes from www.company1.com: icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from www.company1.com: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from www.company1.com: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from www.company1.com: icmp_seq=4 ttl=64 time=0.038 ms
^C
--- www.company1.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.035/0.038/0.046/0.008 ms
root@web-virtual-machine: /#
```

Figura 3.82. Configuraciones del servidor Web (21)

Reiniciamos el servicio:



```
Terminal
root@web-virtual-machine: /
root@web-virtual-machine: /# /etc/init.d/apache2 restart
* Restarting web server apache2
... waiting [ OK ]
root@web-virtual-machine: /#
```

Figura 3.83. Configuraciones del servidor Web (22)

Validamos el servicio web ingresando al navegador y dirigiéndonos a la **URL** antes configurada.



**Figura 3.84.** Configuraciones del servidor Web (23)

### 3.2.2.7 Servidor de Telefonía IP

Instalación y configuración de un servidor de Telefonía IP mediante Elastix 2.4:

**Paso 1:**

Se descarga la versión de Elastix 2.4 desde la página:

<https://sourceforge.net/projects/elastix/files/>



**Figura 3.85.** Instalación de Elastix 2.4

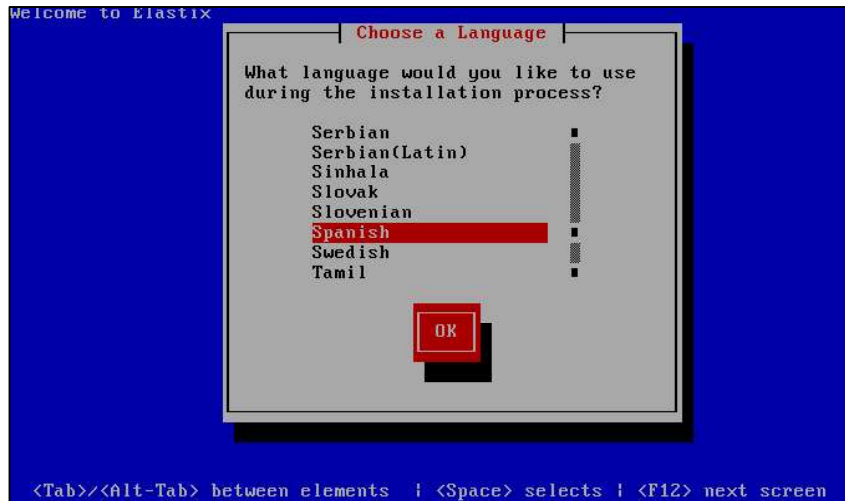


Figura 3.86. Configuración del idioma en Elastix 2.4



Figura 3.87. Configuración del particionamiento en Elastix 2.4

**Paso 2:**

En un punto de la instalación nos pide poner la dirección IPv4 o IPv6, en este caso estamos usando IPv6 y se configura la IP del servidor y Gateway:

**IP Address:** 2000:0:1:9::6

**Gateway:** 2000:0:1:9::1

**Paso 3:**

Una vez instalado el sistema ingresamos el root y contraseña:

**Usuario:** root

**Contraseña:** tesis1234



Figura 3.88. Configuración del usuario y clave en Elastix 2.4



Figura 3.89. Instalación del paquete en Elastix 2.4

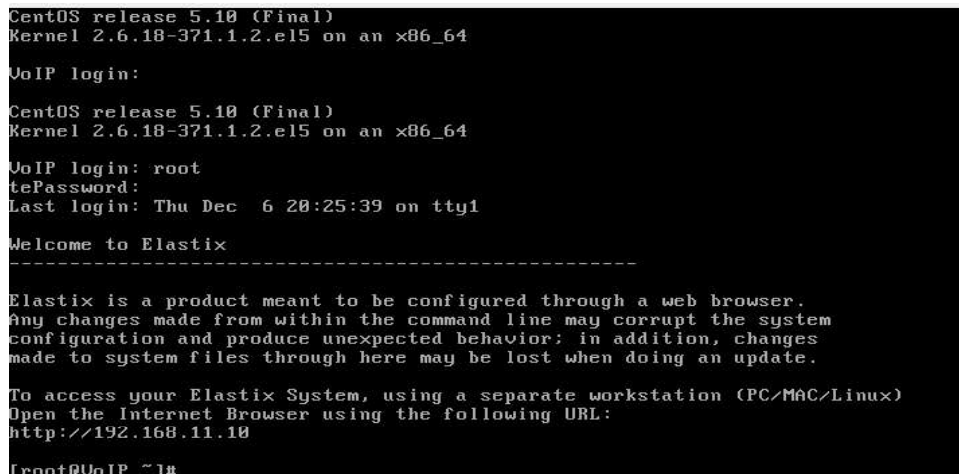
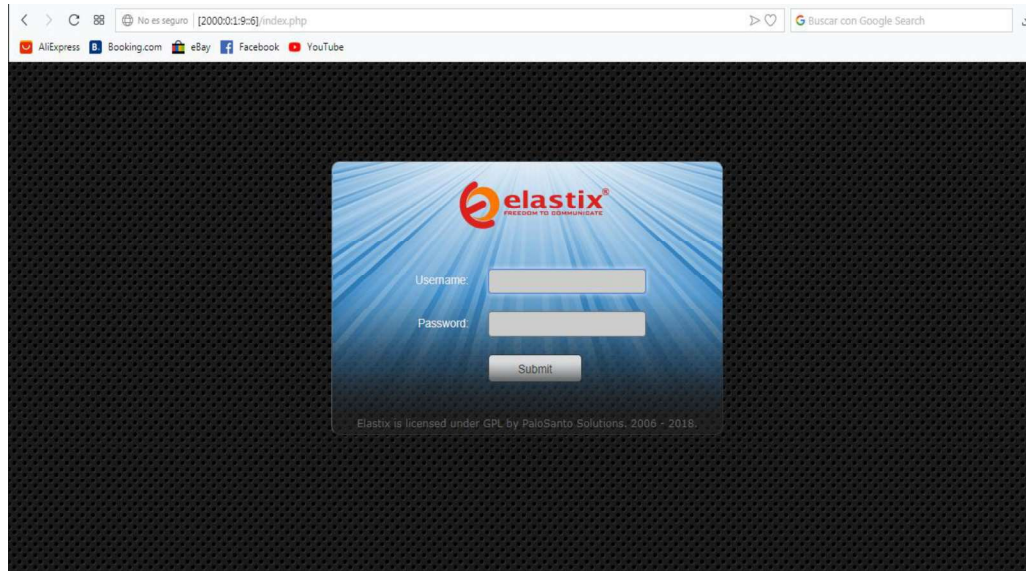


Figura 3.90. Verificación de la instalación de Elastix 2.4

#### **Paso 4:**

Ingresamos mediante página web para acceder al modo grafico de la central:

[http://\[2000:0:1:9::6\]](http://[2000:0:1:9::6])



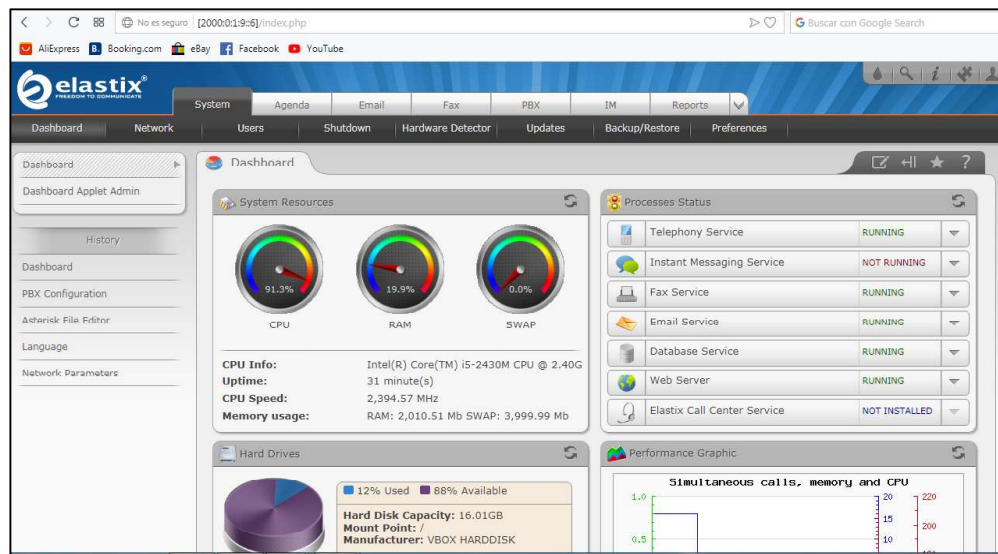
**Figura 3.91.** Acceso web de Elastix 2.4

#### **Paso 5:**

Ingresamos las credenciales configuradas:

**Username:** admin

**Password:** tesis1234

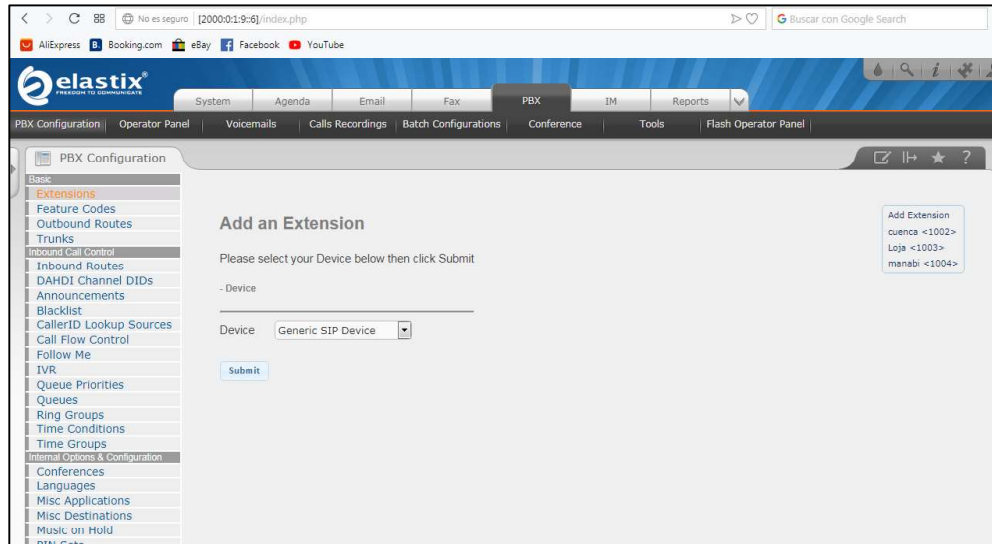


**Figura 3.92.** Consola web de Elastix 2.4



## **Paso 6:**

Agregamos extensiones:



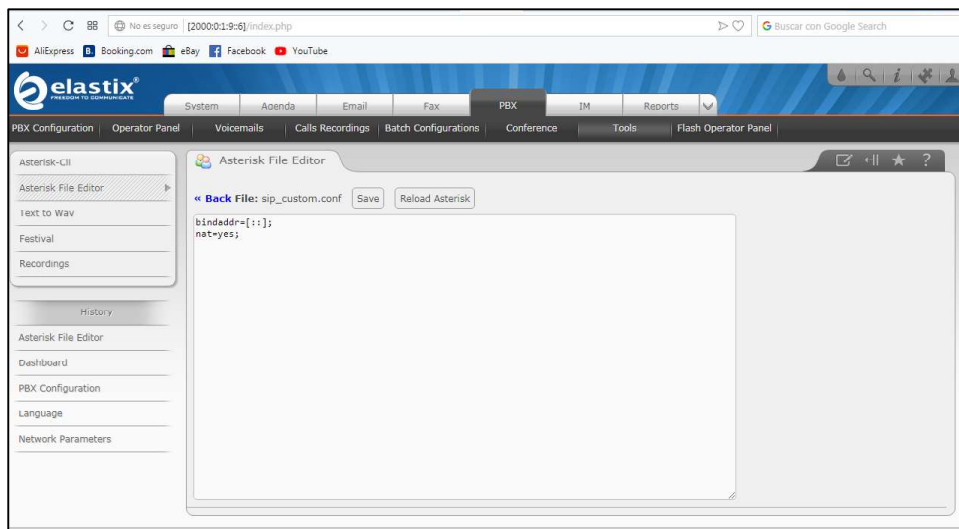
**Figura 3.93.** Agregar extensiones en Elastix 2.4

## **Paso 7:**

Se procede a modificar el archivo sip\_custom.conf (esta configuración se la realiza al configurar IPv6), se agrega los siguientes comandos:

```
bindaddr=[::];
```

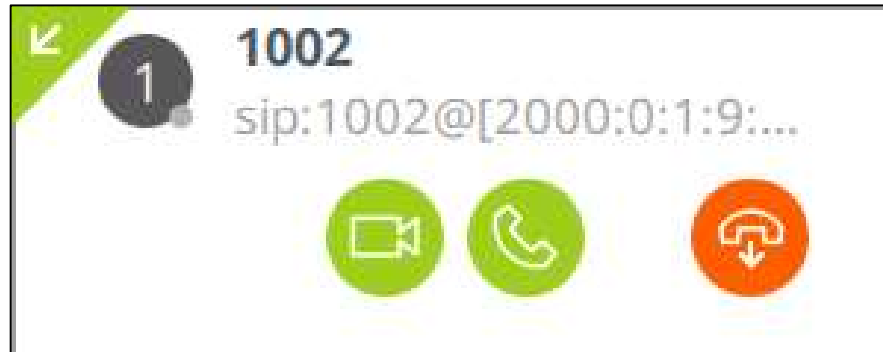
```
nat=yes;
```



**Figura 3.94.** Configuración del archivo sip\_custom.conf en Elastix 2.4

### **Paso 8:**

Prueba de llamada:



**Figura 3.95.** Prueba de llamadas en Elastix 2.4

## **3.2.3 CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO Y QoS**

Para configuración de QoS la marcación y clasificación de tráfico se realiza en el *router* de Borde R\_matriz, mientras que las políticas de manipulación para evitar el congestionamiento se realiza en los routers R\_Suc1, R\_Suc2 y R\_Suc3.

### **3.2.3.1 Router Matriz**

#### **Configuración básica:**

```
Router> enable
Router# configure terminal
Router (config)#R_matriz
```

#### **Habilitar protocolo IPv6:**

Para el enrutamiento IPv6 se usa el comando *ipv6 unicast-routing* con el que se habilita el protocolo IPv6 en las interfaces de los *routers*.

```
R_matriz (config)# ipv6 unicast-routing
```

#### **Asignación de IP a las interfaces:**

```
R_matriz(config)# interface GigabitEthernet0/1
R_matriz(config-if)#ipv6 address 2000:0:1:9::1/125
R_matriz(config-if)#no shutdown
```

```

R_matriz(config)# interface Serial0/1/0
R_matriz(config-if)#ipv6 address 2000:0:2:A::/127
R_matriz(config-if)#clock rate 64000
R_matriz(config-if)#no shutdown

R_matriz(config)# interface Serial0/1/1
R_matriz(config-if)#ipv6 address 2000:0:2:D:://127
R_matriz(config-if)#clock rate 64000
R_matriz(config-if)#no shutdown

```

## Configuración del protocolo de enrutamiento RIPng

Para configurar el protocolo RIPng utilizamos el comando **ipv6 rip IDENTIFICADOR enable** en cada una de las interfaces del router. Para este caso el identificador es TESIS.

```

R_matriz (config)# interface GigabitEthernet 0/1
R_matriz (config-if)# ipv6 rip TESIS enable
R_matriz (config-if)# exit
R_matriz (config)# interface Serial 0/1/0
R_matriz (config-if)# ipv6 rip TESIS enable
R_matriz (config-if)# exit
R_matriz (config)# interface Serial 0/1/1
R_matriz (config-if)# ipv6 rip TESIS enable
R_matriz (config-if)# exit

```

## Creación de sub interfaces para establecer la conectividad inter-VLANs.

Habilitamos la interfaz que abarcara las sub interfaces.

```

R_matriz (config)#interface GigabitEthernet0/0
R_matriz (config-subif)#ipv6 rip TESIS enable
R_matriz (config-if)#no shutdown

```

## Configuración de las subinterfaces con las IPs correspondientes y su respectiva VLAN.

```

R_matriz (config)#interface GigabitEthernet0/0.10
R_matriz (config-subif)#encapsulation dot1Q 10
R_matriz (config-subif)#ip address 2000:0:1:B::1/122
R_matriz (config-subif)#ipv6 rip TESIS enable

R_matriz (config)#interface GigabitEthernet0/0.20
R_matriz (config-subif)#encapsulation dot1Q 20
R_matriz (config-subif)#ip address 2000:0:1:C::1/12
R_matriz (config-subif)#ipv6 rip TESIS enable

R_matriz (config)#interface GigabitEthernet0/0.30
R_matriz (config-subif)#encapsulation dot1Q 30

```

```

R_matriz (config-subif)#ip address 2000:0:1:D::1/12
R_matriz (config-subif)#ipv6 rip TESIS enable

R_matriz (config)#interface GigabitEthernet0/0.40
R_matriz (config-subif)#encapsulation dot1Q 40
R_matriz (config-subif)#ip address 2000:0:1:E::1/12
R_matriz (config-subif)#ipv6 rip TESIS enable

R_matriz (config)#interface GigabitEthernet0/0.50
R_matriz (config-subif)#encapsulation dot1Q 50
R_matriz (config-subif)#ip address 2000:0:1:F::1/12
R_matriz (config-subif)#ipv6 rip TESIS enable

R_matriz (config)#interface GigabitEthernet0/0.99
R_matriz (config-subif)#encapsulation dot1Q 99
R_matriz (config-subif)#ip address 2000:0:1:A::1/12
R_matriz (config-subif)#ipv6 rip TESIS enable

```

### 3.2.3.2 Router Sucursal 1

```

Router> enable
Router# configure terminal
Router (config)#R_SUC1
R_SUC1 (config)# ipv6 unicast-routing

R_SUC1 (config)# interface Serial0/0/0
R_SUC1 (config-if)#ipv6 address 2000:0:2:D::1//127
R_SUC1 (config-if)#no shutdown

R_SUC1 (config)# interface Serial0/0/1
R_SUC1 (config-if)#ipv6 address 2000:0:2:C::1/127
R_SUC1 (config-if)#clock rate 64000
R_SUC1 (config-if)#no shutdown

R_SUC1 (config)# interface Serial 0/0/0
R_SUC1 (config-if)# ipv6 rip TESIS enable
R_SUC1 (config-if)# exit
R_SUC1 (config)# interface Serial 0/0/1
R_SUC1 (config-if)# ipv6 rip TESIS enable
R_SUC1 (config-if)# exit

R_SUC1 (config)#interface GigabitEthernet0/0
R_SUC1 (config-subif)#ipv6 rip TESIS enable
R_SUC1 (config-if)#no shutdown

R_SUC1 (config)#interface GigabitEthernet0/0.10
R_SUC1 (config-subif)#encapsulation dot1Q 10
R_SUC1 (config-subif)#ip address 2000:0:1:B::4:1/125
R_SUC1 (config-subif)#ipv6 rip TESIS enable

R_SUC1 (config)#interface GigabitEthernet0/0.20
R_SUC1 (config-subif)#encapsulation dot1Q 20
R_SUC1 (config-subif)#ip address 2000:0:1:C::4:1/123
R_SUC1 (config-subif)#ipv6 rip TESIS enable

```

```

R_SUC1 (config)#interface GigabitEthernet0/0.30
R_SUC1 (config-subif)#encapsulation dot1Q 30
R_SUC1 (config-subif)#ip address 2000:0:1:D::2:1/127
R_SUC1 (config-subif)#ipv6 rip TESIS enable

R_SUC1 (config)#interface GigabitEthernet0/0.40
R_SUC1 (config-subif)#encapsulation dot1Q 40
R_SUC1 (config-subif)#ip address 2000:0:1:E::2:1/126
R_SUC1 (config-subif)#ipv6 rip TESIS enable

R_SUC1 (config)#interface GigabitEthernet0/0.50
R_SUC1 (config-subif)#encapsulation dot1Q 50
R_SUC1 (config-subif)#ip address 2000:0:1:F::2:1/125
R_SUC1 (config-subif)#ipv6 rip TESIS enable

```

- La configuración de los routers R\_SUC2 y R\_SUC3 es similar a la configuración de R\_SUC1. (ANEXO I)

### 3.2.3.3 Switch Matriz

#### Configuración básica:

```

Switch> enable
Switch # configure terminal
Switch (config)#SW_MATRIZ

```

#### Creación de VLANs

```

SW_MATRIZ (config)#vlan 99
SW_MATRIZ (config-vlan)#name GG
SW_MATRIZ (config-vlan)#exit

SW_MATRIZ (config)#vlan 10
SW_MATRIZ (config-vlan)#name OPE
SW_MATRIZ (config-vlan)#exit

SW_MATRIZ (config)#vlan 20
SW_MATRIZ (config-vlan)#name COM
SW_MATRIZ (config-vlan)#exit

SW_MATRIZ (config)#vlan 30
SW_MATRIZ (config-vlan)#name RRHH
SW_MATRIZ (config-vlan)#exit

SW_MATRIZ (config)#vlan 40
SW_MATRIZ (config-vlan)#name TEC
SW_MATRIZ (config-vlan)#exit

SW_MATRIZ (config)#vlan 50
SW_MATRIZ (config-vlan)#name FIN
SW_MATRIZ (config-vlan)#exit

```

## Asignación de puertos a una VLAN

```
SW_MATRIZ (config)# interface FastEthernet0/1
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 99
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/2
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/3
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/4
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/5
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/6
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/7
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 10
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/8
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/9
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/10
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/11
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown
```

```

SW_MATRIZ (config)# interface FastEthernet0/12
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/13
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 20
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/14
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 30
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/15
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 30
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/16
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 30
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/17
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 30
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/18
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 40
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/19
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 40
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/20
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 40
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/21
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 40
SW_MATRIZ (config-if)#no shutdown

SW_MATRIZ (config)# interface FastEthernet0/22
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 50
SW_MATRIZ (config-if)#no shutdown

```

```
SW_MATRIZ (config)# interface FastEthernet0/23
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 50
SW_MATRIZ (config-if)#no shutdown
```

```
SW_MATRIZ (config)# interface FastEthernet0/24
SW_MATRIZ (config-if)#switchport mode access
SW_MATRIZ (config-if)#switchport access vlan 50
SW_MATRIZ (config-if)#no shutdown
```

```
SW_MATRIZ (config)# interface GigabitEthernet0/1
SW_MATRIZ (config-if)#switchport mode trunk
SW_MATRIZ (config-if)#no shutdown
```

- Se muestra como ejemplo la configuración de switch matriz, las configuraciones del SW\_SUC1, SW\_SUC2, SW\_SUC3 se describen en el ANEXO I.

### 3.2.3.4 Creación de Listas de Control de Acceso

```
R_matriz(config)# access-list 101 permit udp any any range 16384 32768
R_matriz(config)# access-list 102 permit tcp any any range 21 24
R_matriz (config)# access-list 103 permit tcp any any eq tacacs
R_matriz (config)# access-list 104 permit tcp any any eq www
R_matriz (config)# access-list 105 permit ip any any
R_matriz (config)# access-list 108 permit tcp any any eq telnet
R_matriz (config)# access-list 109 permit tcp any any eq 443
R_matriz (config)# access-list 110 permit icmp any any
```

### 3.2.3.5 Creación de Mapas de Clase

#### CONFIGURACIONES EN R\_MATRIZ:

```
R_matriz (config)# class-map match-all AAAA
R_matriz (config-cmap)# match ip dscp 46
R_matriz (config-cmap)# match access-group 101
R_matriz (config-cmap)# exit
R_matriz (config)# class-map match-all AAA
R_matriz (config-cmap)# match ip dscp 10 14
R_matriz (config-cmap)# match protocol rtsp13
R_matriz (config-cmap)# match protocol rtp14
R_matriz (config-cmap)# exit
R_matriz (config)# class-map match-all AA
R_matriz (config-cmap)# match access-group 109
R_matriz (config-cmap)# match ip dscp 18 22
R_matriz (config-cmap)# match protocol secure-http
R_matriz (config-cmap)# match protocol secure-ftp
R_matriz (config-cmap)# match protocol ipsec
R_matriz (config-cmap)# exit
R_matriz (config)# class-map match-all A
```



```

R_matriz (config-cmap)# match ip dscp 26 30
R_matriz (config-cmap)# match protocol dhcp
R_matriz (config-cmap)# match protocol icmp
R_matriz (config-cmap)# match protocol snmp
R_matriz (config-cmap)# match access-group 108
R_matriz (config-cmap)# match access-group 110
R_matriz (config-cmap)# exit
R_matriz (config)# class-map match-all B
R_matriz (config-cmap)# match access-group 105
R_matriz (config-cmap)# exit

```

### **CONFIGURACIONES EN R\_SUC1.**

```

R_SUC1 (config)# class-map match-all AAAA
R_SUC1 (config-cmap)# match ip dscp 46
R_SUC1 (config-cmap)# exit
R_SUC1 (config)# class-map match-all AAA
R_SUC1 (config-cmap)# match ip dscp 10 14
R_SUC1 (config-cmap)# exit
R_SUC1 (config)# class-map match-all AA
R_SUC1 (config-cmap)# match ip dscp 18 22
R_SUC1 (config-cmap)# exit
R_SUC1 (config)# class-map match-all A
R_SUC1 (config-cmap)# match ip dscp 26 30
R_SUC1 (config-cmap)# exit
R_SUC1 (config)# class-map match-all B
R_SUC1 (config-cmap)# match ip dscp 0
R_SUC1 (config-cmap)# exit

```

- Configuración similar se aplica a R\_SUC2 y R\_SUC3. (ANEXO I)

### **3.2.3.6 Creación de Mapas de Política**

#### **MAPAS DE POLITICA R\_MATRIZ:**

```

R_matriz (config)# ip cef
R_matriz (config)# policy-map POLITICAS-QOS
R_matriz (config-pmap)# class AAAA
R_matriz (config-pmap-c)# priority 800
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class AAA
R_matriz (config-pmap-c)# bandwidth percent 25
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class AA
R_matriz (config-pmap-c)# bandwidth percent 20
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class A
R_matriz (config-pmap-c)# bandwidth percent 10
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class B
R_matriz (config-pmap-c)# police 56000 1750 1750 conform-action
set-dscp-transmit 0 exceed-action drop violate-action drop
R_matriz (config-pmap-c)# exit

```

```

R_matriz (config)# policy-map SET-DSCP
R_matriz (config-pmap)# class AAAA
R_matriz (config-pmap-c)# set ip dscp 46
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class AAA
R_matriz (config-pmap-c)# set ip dscp 10
R_matriz (config-pmap-c)# set ip dscp 14
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class AA
R_matriz (config-pmap-c)# set ip dscp 18
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class A
R_matriz (config-pmap-c)# set ip dscp 26
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# class B
R_matriz (config-pmap-c)# set ip dscp 30
R_matriz (config-pmap-c)# exit
R_matriz (config-pmap)# exit

```

### MAPAS DE POLITICA R\_SUC1:

```

R_SUC1 (config)# policy-map POLITICA-SALIDA
R_SUC1 (config-pmap)# class AAAA
R_SUC1 (config-pmap-c)# priority 800
R_SUC1 (config-pmap-c)# exit
R_SUC1 (config-pmap)# class AAA
R_SUC1 (config-pmap-c)# bandwidth percent 25
R_SUC1 (config-pmap-c)# random-detect dscp-based
R_SUC1 (config-pmap-c)# random-detect dscp 10 20 40 10
R_SUC1 (config-pmap-c)# random-detect dscp 14 20 40 20
R_SUC1 (config-pmap-c)# exit
R_SUC1 (config-pmap)# class AA
R_SUC1 (config-pmap-c)# bandwidth percent 20
R_SUC1 (config-pmap-c)# random-detect dscp-based
R_SUC1 (config-pmap-c)# random-detect dscp 18 20 40 10
R_SUC1 (config-pmap-c)# random-detect dscp 20 20 40 10
R_SUC1 (config-pmap-c)# exit
R_SUC1 (config-pmap)# class A
R_SUC1 (config-pmap-c)# bandwidth percent 10
R_SUC1 (config-pmap-c)# random-detect dscp-based
R_SUC1 (config-pmap-c)# random-detect dscp 26 20 40 10
R_SUC1 (config-pmap-c)# random-detect dscp 30 20 40 20
R_SUC1 (config-pmap-c)# exit
R_SUC1 (config-pmap)# exit

```

- Los mapas de política de R\_SUC2 y R\_SUC3 se los configure de manera similar a R\_SUC1 (ANEXO I).

### 3.2.3.7 Asignación de políticas a las interfaces

#### R\_matriz:

```
R_matriz(config)# interface Serial 0/1/0
R_matriz (config-if)# service-policy output POLITICAS-QOS
R_matriz (config-if)# exit
R_matriz(config)# interface Serial 0/1/1
R_matriz (config-if)# service-policy output POLITICAS-QOS
R_matriz (config-if)# exit
R_matriz(config)# interface G 0//0
R_matriz (config-if)# service-policy input SET-DSCP
R_matriz (config-if)# exit
```

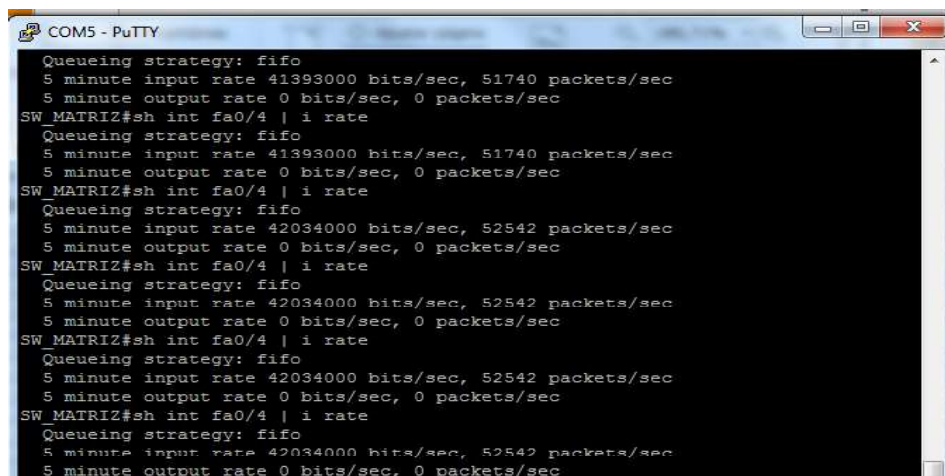
#### R\_SUC2:

```
R_SUC2 (config)# interface Serial 0/0/0
R_SUC2 (config-if)# service-policy output POLITICA-SALIDA
R_SUC2 (config-if)# exit
R_SUC2 (config)# interface Serial 0/0/1
R_SUC2 (config-if)# service-policy output POLITICA-SALIDA
R_SUC2 (config-if)# exit

R_SUC2 (config)# interface gigabitEthernet 0/0
R_SUC2 (config-if)# service-policy input POLITICA-SALIDA
R_SUC2 (config-if)# exit
```

## 3.2.4 CONFIGURACIÓN DEL GENERADOR DE TRÁFICO

Con el inyector de tráfico disponible se inyecta tráfico desde la red LAN hacia el *router* R\_suc3 con 98Mb para saturar *uplink* del *switch*. En las siguientes imágenes se muestran como el tráfico aumenta paulatinamente a través de la interfaz Fa0/4 del *switch*.



```
COM5 - PuTTY
Queueing strategy: fifo
5 minute input rate 41393000 bits/sec, 51740 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 41393000 bits/sec, 51740 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 42034000 bits/sec, 52542 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 42034000 bits/sec, 52542 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 42034000 bits/sec, 52542 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 42034000 bits/sec, 52542 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

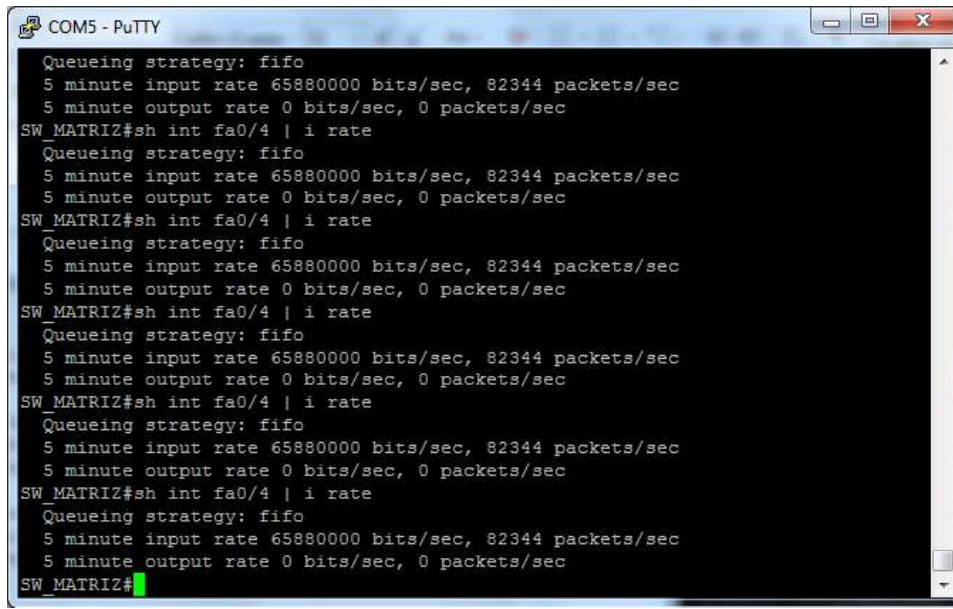
Figura 3.96. Generación de tráfico (1)

```
COM5 - PuTTY
Queueing strategy: fifo
5 minute input rate 49973000 bits/sec, 62464 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 49973000 bits/sec, 62464 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 50472000 bits/sec, 63088 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 50472000 bits/sec, 63088 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 50472000 bits/sec, 63088 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 50472000 bits/sec, 63088 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#
```

Figura 3.97. Generación de tráfico (2)

```
COM5 - PuTTY
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 56254000 bits/sec, 70314 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#
```

Figura 3.98. Generación de tráfico (3)



```
COM5 - PuTTY
Queueing strategy: fifo
5 minute input rate 65880000 bits/sec, 82344 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 65880000 bits/sec, 82344 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 65880000 bits/sec, 82344 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 65880000 bits/sec, 82344 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#sh int fa0/4 | i rate
Queueing strategy: fifo
5 minute input rate 65880000 bits/sec, 82344 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
SW_MATRIZ#
```

Figura 3.99. Generación de tráfico (4)

### 3.2.5 CONFIGURACIÓN DE IP SLA

Cisco IP SLAs es una parte del software Cisco IOS que permite a los clientes de Cisco analizar los niveles de servicio IP para IP aplicaciones y servicios mediante el monitoreo activo del tráfico (la generación de tráfico de manera continua, confiable y predecible) para medir el rendimiento de la red.

#### Creación de IP SLA

Generamos las SIGUIENTES IP SLA:

- IP SLA 1 – UDP *Jitter*
- IP SLA 2 – UDP *Jitter*, conversación con codec g711ulaw
- IP SLA 3 – UDP *Jitter*, conversación con codec g729a
- IP SLA 4 – UDP Echo
- IP SLA 5 – Conexión TCP, Telnet
- IP SLA 6 – Conexión TCP, FTP
- IP SLA 7 – Conexión TCP, HTTPS
- IP SLA 8 – Conexión TCP, SSH
- IP SLA 9 – ICMP Echo

Aplicamos las IP SLA en la VLAN OPE de la sucursal MATRIZ referente a la interfaz g0/0 del R\_matriz.

- **UDP jitter**

```
R_matriz (config)# ip sla 1
R_matriz (config-ip-sla)# udp-jitter 2000:0:1:B::4 16838
source-ip 2000:0:1:9::1
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 15
R_matriz (config-ip-sla-jitter)# traffic-class 56
R_matriz (config-ip-sla-jitter)# exit
R_matriz (config)# ip sla schedule 1 start-time now life forever
```

- **VoIP UDP jitter G.711ulaw**

```
R_matriz (config)# ip sla 2
R_matriz (config-ip-sla)# udp-jitter 2000:0:1:B::4 16834 source-
ip 2000:0:1:9::1 codec g711ulaw
R_matriz (config-ip-sla-jitter)# traffic-class 184
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 15
R_matriz (config-ip-sla-jitter)# ip sla schedule 2 life forever
start-time now
```

- **VoIP UDP jitter G.729a**

```
R_matriz (config)# ip sla 3
R_matriz (config-ip-sla)# udp-jitter 2000:0:1:B::4 16834 source-ip 2000:0:1:9::1
codec g729a
R_matriz (config-ip-sla-jitter)# traffic-class 184
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 25
R_matriz (config-ip-sla-jitter)# ip sla schedule 3 life
forever
```

- **UDP Echo**

```
R_matriz (config)# ip sla 4
R_matriz (config-ip-sla)# udp-echo 2000:0:1:B::4 16835 source-ip 2000:0:1:9::1
R_matriz (config-ip-sla-jitter)# traffic-class 184
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 10
R_matriz (config-ip-sla-jitter)# ip sla schedule 4 life
forever
```

- TCPconnect Telnet

```
R_matriz (config)# ip sla 5
R_matriz (config-ip-sla)# tcp-connect 2000:0:1:B::4 23 source-ip 2000:0:1:9::1
R_matriz (config-ip-sla-jitter)# traffic-class 104
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 20
R_matriz (config-ip-sla-jitter)# ip sla schedule 5 life
forever
```

- TCPconnect FTP

```
R_matriz (config)# ip sla 6
R_matriz (config-ip-sla)# tcp-connect 2000:0:1:B::4 21 source-ip
2000:0:1:9::1 R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 20
R_matriz (config-ip-sla-jitter)# ip sla schedule 6 life
forever
```

- TCPconnect HTTPS

```
R_matriz (config)# ip sla 7
R_matriz (config-ip-sla)# tcp-connect 2000:0:1:B::4 443 source-ip
2000:0:1:9::1
R_matriz (config-ip-sla-jitter)# traffic-class 88
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 20
R_matriz (config-ip-sla-jitter)# ip sla schedule 7 life
forever
```

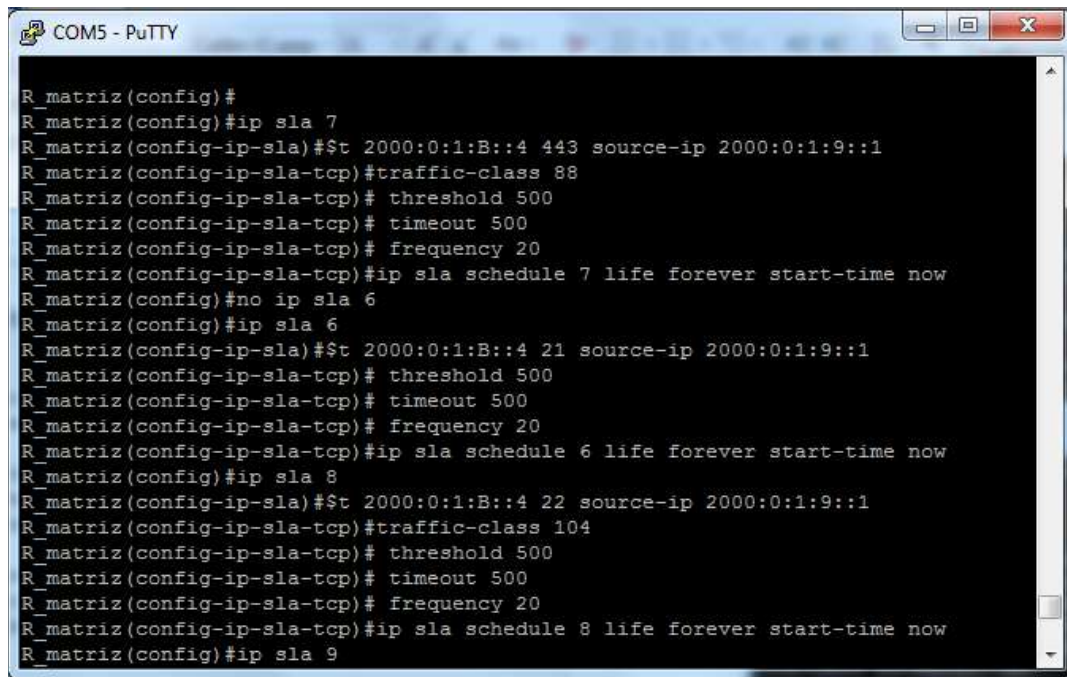
- TCPconnect SSH

```
R_matriz (config)# ip sla 8
R_matriz (config-ip-sla)# tcp-connect 2000:0:1:B::4 22 source-ip
2000:0:1:9::1
R_matriz (config-ip-sla-jitter)# traffic-class 104
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
R_matriz (config-ip-sla-jitter)# frequency 20
R_matriz (config-ip-sla-jitter)# ip sla schedule 8 life
forever
```

- ICMP Echo

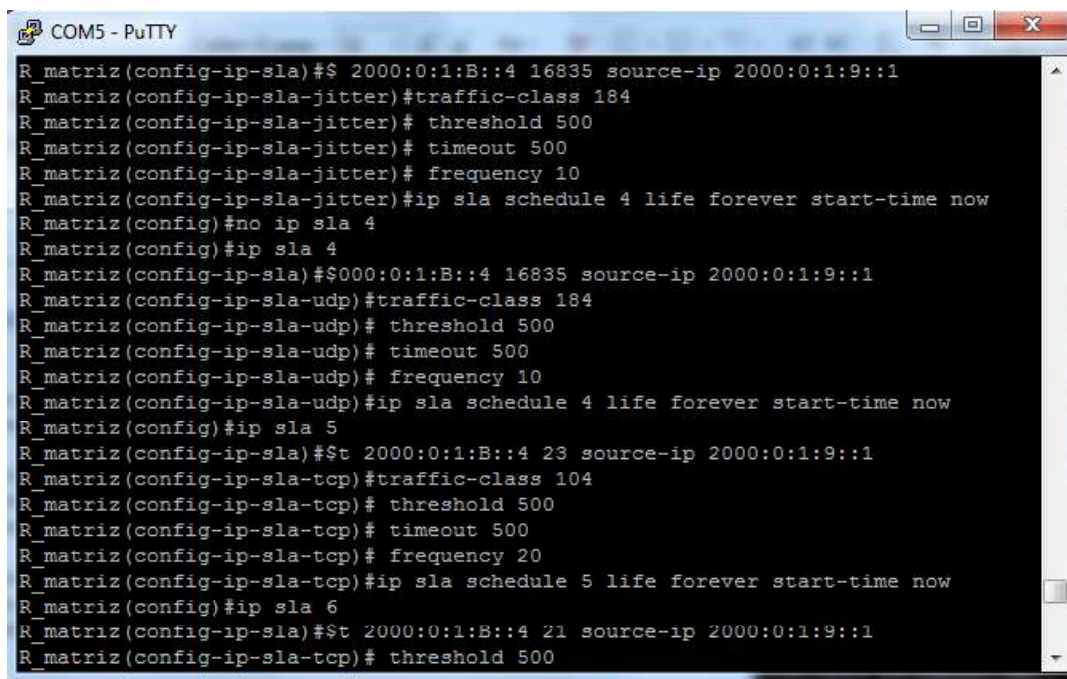
```
R_matriz (config)# ip sla 9
R_matriz (config-ip-sla)# icmp-echo 2000:0:1:B::4 22 source-interface g0/1
R_matriz (config-ip-sla-jitter)# traffic-class 120
R_matriz (config-ip-sla-jitter)# threshold 500
R_matriz (config-ip-sla-jitter)# timeout 500
```

```
R_matriz (config-ip-sla-jitter)# frequency 20
R_matriz (config-ip-sla-jitter)# ip sla schedule 9 life
forever
```



```
COM5 - PuTTY
R_matriz(config)#
R_matriz(config)#ip sla 7
R_matriz(config-ip-sla)#$t 2000:0:1:B::4 443 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-tcp)#traffic-class 88
R_matriz(config-ip-sla-tcp)# threshold 500
R_matriz(config-ip-sla-tcp)# timeout 500
R_matriz(config-ip-sla-tcp)# frequency 20
R_matriz(config-ip-sla-tcp)#ip sla schedule 7 life forever start-time now
R_matriz(config)#no ip sla 6
R_matriz(config)#ip sla 6
R_matriz(config-ip-sla)#$t 2000:0:1:B::4 21 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-tcp)# threshold 500
R_matriz(config-ip-sla-tcp)# timeout 500
R_matriz(config-ip-sla-tcp)# frequency 20
R_matriz(config-ip-sla-tcp)#ip sla schedule 6 life forever start-time now
R_matriz(config)#ip sla 8
R_matriz(config-ip-sla)#$t 2000:0:1:B::4 22 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-tcp)#traffic-class 104
R_matriz(config-ip-sla-tcp)# threshold 500
R_matriz(config-ip-sla-tcp)# timeout 500
R_matriz(config-ip-sla-tcp)# frequency 20
R_matriz(config-ip-sla-tcp)#ip sla schedule 8 life forever start-time now
R_matriz(config)#ip sla 9
```

Figura 3.100. Configuración del *router* R\_matriz



```
COM5 - PuTTY
R_matriz(config-ip-sla)#$ 2000:0:1:B::4 16835 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-jitter)#traffic-class 184
R_matriz(config-ip-sla-jitter)# threshold 500
R_matriz(config-ip-sla-jitter)# timeout 500
R_matriz(config-ip-sla-jitter)# frequency 10
R_matriz(config-ip-sla-jitter)#ip sla schedule 4 life forever start-time now
R_matriz(config)#no ip sla 4
R_matriz(config)#ip sla 4
R_matriz(config-ip-sla)#$000:0:1:B::4 16835 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-udp)#traffic-class 184
R_matriz(config-ip-sla-udp)# threshold 500
R_matriz(config-ip-sla-udp)# timeout 500
R_matriz(config-ip-sla-udp)# frequency 10
R_matriz(config-ip-sla-udp)#ip sla schedule 4 life forever start-time now
R_matriz(config)#ip sla 5
R_matriz(config-ip-sla)#$t 2000:0:1:B::4 23 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-tcp)#traffic-class 104
R_matriz(config-ip-sla-tcp)# threshold 500
R_matriz(config-ip-sla-tcp)# timeout 500
R_matriz(config-ip-sla-tcp)# frequency 20
R_matriz(config-ip-sla-tcp)#ip sla schedule 5 life forever start-time now
R_matriz(config)#ip sla 6
R_matriz(config-ip-sla)#$t 2000:0:1:B::4 21 source-ip 2000:0:1:9::1
R_matriz(config-ip-sla-tcp)# threshold 500
```

Figura 3.101. Configuración del IP SLA en el *router* R\_matriz



```
COM5 - PuTTY
R_matriz#sh ip sla configuration 1
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 500
Type of operation to perform: udp-jitter
Target address/Source address: 2000:0:1:B::4/2000:0:1:9::1
Target port/Source port: 16838/0
Traffic-Class parameter: 0x38
Flow-Label parameter: 0x0
Request size (ARR data portion): 32
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 15 (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 500
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
Percentile:
R_matriz#
```

Figura 3.102. Estadísticas del IP SLA del *router* R\_matriz

```
COM5 - PuTTY
R_matriz#sh ip sla statistics 1
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Type of operation: udp-jitter
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:02:05 UTC Wed Jul 17 2013
Latest operation return code: No connection
RTT Values:
  Number Of RTT: 0          RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
  Number of Latency one-way Samples: 0
  Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
  Number of SD Jitter Samples: 0
  Number of DS Jitter Samples: 0
  Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Over Threshold:
  Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
  Loss Source to Destination: 0
  Source to Destination Loss Periods Number: 0
  Source to Destination Loss Period Length Min/Max: 0/0
  Source to Destination Inter Loss Period Length Min/Max: 0/0
  Loss Destination to Source: 0
  Destination to Source Loss Periods Number: 0
  Destination to Source Loss Period Length Min/Max: 0/0
  Destination to Source Inter Loss Period Length Min/Max: 0/0
  Out Of Sequence: 0      Tail Drop: 0
  Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
  Calculated Planning Impairment Factor (ICPIF): 0
  Mean Opinion Score (MOS): 0
Number of successes: 0
Number of failures: 68
```

Figura 3.103. Configuración del IP SLA 1

```
COM5 - PuTTY
R_matriz#sh ip sla statistics 2
IPSLAs Latest Operation Statistics

IPSLA operation id: 2
Type of operation: udp-jitter
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:03:13 UTC Wed Jul 17 2013
Latest operation return code: No connection
RTT Values:
  Number Of RTT: 0          RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
  Number of Latency one-way Samples: 0
  Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
  Number of SD Jitter Samples: 0
  Number of DS Jitter Samples: 0
  Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Over Threshold:
  Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
  Loss Source to Destination: 0
  Source to Destination Loss Periods Number: 0
  Source to Destination Loss Period Length Min/Max: 0/0
  Source to Destination Inter Loss Period Length Min/Max: 0/0
  Loss Destination to Source: 0
  Destination to Source Loss Periods Number: 0
  Destination to Source Loss Period Length Min/Max: 0/0
  Destination to Source Inter Loss Period Length Min/Max: 0/0
  Out Of Sequence: 0      Tail Drop: 0
  Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
  Calculated Planning Impairment Factor (ICPIF): 0
  Mean Opinion Score (MOS): 0
Number of successes: 0
Number of failures: 63
Operation time to live: Forever
```

Figura 3.104. Configuración del IP SLA 2

```
COM5 - PuTTY
R_matriz#sh ip sla statistics 3
IPSLAs Latest Operation Statistics

IPSLA operation id: 3
Type of operation: udp-jitter
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:03:58 UTC Wed Jul 17 2013
Latest operation return code: No connection
RTT Values:
  Number Of RTT: 0          RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
  Number of Latency one-way Samples: 0
  Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
  Number of SD Jitter Samples: 0
  Number of DS Jitter Samples: 0
  Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
  Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Over Threshold:
  Number Of RTT Over Threshold: 0 (0%)
Packet Loss Values:
  Loss Source to Destination: 0
  Source to Destination Loss Periods Number: 0
  Source to Destination Loss Period Length Min/Max: 0/0
  Source to Destination Inter Loss Period Length Min/Max: 0/0
  Loss Destination to Source: 0
  Destination to Source Loss Periods Number: 0
  Destination to Source Loss Period Length Min/Max: 0/0
  Destination to Source Inter Loss Period Length Min/Max: 0/0
  Out Of Sequence: 0      Tail Drop: 0
  Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
  Calculated Planning Impairment Factor (ICPIF): 0
  Mean Opinion Score (MOS): 0
Number of successes: 0
Number of failures: 70
Operation time to live: Forever
```

Figura 3.105. Configuración del IP SLA 3

```
R_matriz#sh ip sla statistics 4
IPSLAs Latest Operation Statistics

IPSLA operation id: 4
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:04:28 UTC Wed Jul 17 2013
Latest operation return code: No connection
Number of successes: 0
Number of failures: 83
Operation time to live: Forever

R_matriz#sh ip sla statistics 9
IPSLAs Latest Operation Statistics

IPSLA operation id: 9
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:05:03 UTC Wed Jul 17 2013
Latest operation return code: Timeout
Number of successes: 0
Number of failures: 108
Operation time to live: Forever

R_matriz#
```

Figura 3.106. Configuración del IP SLA 4

### 3.3 ANÁLISIS DE RESULTADOS

#### 3.3.1 ESTADÍSTICAS DE TRÁFICO GENERADO

Se corrió las pruebas por tiempo aproximado de 2 horas, y se recolectaron las estadísticas correspondientes a los IP SLA configurados; obteniendo datos como latencia en una dirección, de origen a destino, y de destino a origen; latencia de ida y vuelta, paquetes perdidos y *jitter*.

Las estadísticas se obtuvieron a través del comando `show ip sla statistics`, en el modo de configuración privilegiado.

Las estadísticas (más relevantes) recopiladas son los IP SLA 1, 2 y 3 y tiene más datos ya que la configuración realizada para los 3 primeros IP SLA, son distintos a las configuraciones del resto de las IP SLA.

Al ejecutar el comando:

```
R_matriz # show ip sla 1
R_matriz # show ip sla 2
R_matriz # show ip sla 3
```

Obtenemos los siguientes datos.

**Tabla 3.18.** Estadísticas IP SLA

Estadísticas	IP SLA1	IP SLA2	IP SLA3
Pérdida de paquetes SD	1	1	1
Pérdida de paquetes DS	2	2	1
TAIL DROP	0	0	0
Fuera de secuencia	0	0	0
ICPIF	0	1	9
MOS	0	3,56	3,43

**Tabla 3.19.** Estadísticas IP SLA

Estadísticas	IP SLA1	IP SLA2	IP SLA3	IP SLA4	IP SLA5	IP SLA6	IP SLA7	IP SLA8	IP SLA9
# RTT	19	2109	1506						
RTT promedio (ms)	57	98	69	51	76	81	96	68	25
Muestras Jitter SD Sourde-Destination	18	1800	1506						
Muestras Jitter DS Destination - Source	18	1800	1506						
Jitter SD(ms)	23	25	18						
Jitter DS(ms)	14	27	16						
Muestras de Latencia	4	789	890						
Latencia Promedio SD	5	21	25						

### 3.3.2 ANÁLISIS DE RESULTADOS

El tráfico de video, voz, FTP, así como el inyectado con el generador de tráfico para que saturé la conexión LAN del *switch*, fueron generados simultáneamente, de esta manera cada tipo de tráfico competirá por el ancho de banda disponible y se hiciera uso de los métodos de encolamiento y evasión de la congestión. De acuerdo a la frecuencia configurada para los IP SLA del 6 al 9, se percibe que el tráfico generado en estos casos es mayor, para probar si la calidad del tráfico de voz fue degradada. Esto quiere decir que para el mismo tiempo de simulación, se generaron más ramas de tráfico TCP que UDP.

En cuanto a la pérdida de paquetes, de acuerdo a la Tabla 3.18, se puede apreciar que para el tráfico UDP (IP SLA 1, 2 y 3), que fue donde se obtuvieron estadísticas relacionadas, en la red IPv6 no se obtuvieron ningún tipo de pérdidas ni inconvenientes.

En IPv6 a pesar que los paquetes son de mayor tamaño, el procesamiento de los mismos es mas sencillo en los enrutadores ya que no se toma en cuenta todos los campos de la

cabecera como se hacia en IPv4, sino que se considera los campos que realmente son usados mejorando los tiempos de retardo y jitter y aminorando asi las pérdidas.

A nivel de RTT se puede apreciar un comportamiento muy similar entre los diferentes tipos de tráfico generados. El valor máximo obtenido fue de 98 ms correspondiente al IP SLA 2 (que genera tráfico similar al de una conversación g711ulaw); y el valor mínimo fue de 25 ms, correspondiente al IP SLA 9 (toma las mediciones del tráfico ICMP-echo). Observamos que el valor obtenido en IP SLA 2 (VoIP) y de IP SLA 9 (ICMP ECHO) cumplen con los requisitos de CoS especificados en la tabla 3.1 para RTT<150ms y para jitter < 30ms.

El tráfico, más sensible a las características del canal, es el de voz. Este cae dentro de la clase Premium, y debe tener un retardo  $\leq 150$  ms; *jitter*  $\leq 30$ ms; latencia  $\leq 25$ ms. Para los IP SLA 1, 2, y 3 en IPv6, se puede ver que estos parámetros caen dentro de lo establecido. El valor de RTT también está dentro del rango establecido en ambas situaciones, y el porcentaje de paquetes entregados también está dentro de lo que se debe cumplir.

Adicionalmente, para el tráfico de voz, se tienen dos medidas más: ICPIF y MOS. El parámetro ICPIF cuantificar el factor de deterioro de la calidad de la voz encontrado dentro de la red.

Upper Limit for ICPIF	Speech Communication Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

**Figura 3.107.** Niveles de calidad de acuerdo a ICPIF

MOS (*Mean Opinion Score*) es utilizado para determinar la calidad del sonido producido por un códec en específico.

<b>Mean opinion score (MOS)</b>		
<b>MOS</b>	<b>Quality</b>	<b>Impairment</b>
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

**Figura 3.108.** Rango MOS

## CAPÍTULO 4

### 4 CONCLUSIONES Y RECOMENDACIONES

#### 4.1 CONCLUSIONES

- El presente trabajo podrá servir como punto de referencia para el dimensionamiento de las capacidades requeridas por cada servicio dentro de una red convergente; y, también para la implementación de QoS en una red IPv6; los servicios que cada PYME requiera dependerá de su giro de negocio y nivel de adopción que tenga con tecnologías que agilicen los trabajos diarios, por lo que, en este documento se detallan los principales servicios: telefonía IP, video *streaming*, y transmisión de datos entre matriz y sucursales.
- El dimensionamiento de las capacidades de cada uno de los servicios que requiere una empresa, es importante para conocer las capacidades de los enlaces físicos que conectan cada sitio de la empresa, sin embargo al tratarse de redes IP, su crecimiento es flexible y escalable acorde las necesidades y crecimiento de la empresa.
- Al aplicar QoS en una red se logra optimizar los actuales recursos, en lugar de ampliar capacidades de transmisión que implica mayores costos para una empresa, con esto se logra aplazar la expansión de la capacidad de los enlaces hasta que se requiera por crecimiento de la empresa.
- La calidad de servicio permite a una empresa garantizar que las aplicaciones críticas dispongan siempre de los recursos necesarios para su correcto funcionamiento, estas aplicaciones críticas son aquellas que se transmiten en tiempo real, *streaming* de video y datos críticos; mientras que las aplicaciones de datos no críticos o de tipo mejor esfuerzo como correo electrónico e Internet, no requieren que se les garantice la disponibilidad de recursos ya que son aplicaciones tolerantes a retardos y bajas capacidades de red.
- En la presente topología se ha configurado como protocolo de enrutamiento RIP. RIP es un protocolo de vector de distancia estandarizado, diseñado para uso en redes pequeñas como la del presente diseño.
- El concepto conocido como Calidad de Servicio o QoS (*Quality of Service*) introduce mecanismos que permiten diferenciar los distintos paquetes de forma que los *routers* puedan dar un trato especial a determinados paquetes acelerando su reenvío.

- En IPv6 se han añadido nuevos campos en la cabecera que permiten proporcionar Calidad de Servicio. El formato de trama IPv6 posee campos adicionales que ayudan con la aplicación de calidad de servicio sobre su red, así como por ejemplo el campo de Etiqueta de flujo *Flow Label*, hace la distinción de los flujos de tráfico circulantes en la red, facilitando su interpretación, y manipulación. El campo *Traffic Class* distingue entre las diferentes clases o prioridades de paquetes.
- Las políticas de QoS implementadas sobre la red del presente trabajo cumplen con los parámetros establecidos para los diferentes tipos de tráfico, dándole prioridad a tráfico en tiempo real, como de voz, que son más sensibles al retardo y a *jitter*, estando dentro del rango de los parámetros tolerables: retardo  $\leq 150$  ms; *jitter*  $\leq 30$  ms; latencia  $\leq 25$  ms y entrega de paquetes de 99,0%
- Se ha implementado la modalidad DiffServ ya que presenta numerosas ventajas en cuanto a la utilización como método de QoS, entre las tantas ventajas se encuentra la de garantizar un trato homogéneo en todos los nodos de la red a cada una de las clases asignadas a los diferentes grupos de paquetes, para así tener la certeza de que los flujos tendrán la prioridad requerida por el usuario.
- La arquitectura DiffServ es un método de calidad de servicio que garantiza a los usuarios que sus flujos de datos tendrán privilegios de extremo a extremo.
- Para identificar a cada clase de tráfico, el marcado de paquetes se realizó mediante la asignación de un código específico (DiffServ CodePoint – DSCP).

## 4.2 RECOMENDACIONES

- A medida de lo posible se recomienda emplear una topología física redundante por temas de contingencia ante fallas, si bien este tipo de topologías son más costosas, minimizan la probabilidad que se quede sin servicios por problemas en los enlaces; es de potestad de cada empresa definir los recursos monetarios que se asignará al despliegue de la infraestructura de red y esta definición deberá ser consecuente con la criticidad e impacto que signifique para cada empresa, quedarse sin servicios en una de sus sucursales.
- El protocolo de enrutamiento que se recomienda en empresas pequeñas es RIP, mientras que al tratarse de una empresa mediana a grande se recomienda emplear protocolos como EIGRP u OSPF.
- El inyector de tráfico inyecta solo tráfico en IPV4, para implementaciones en IPv6 se recomienda la utilización de un generador de tráfico en IPv6.



- Las interfaces seriales que se utilizan en los *routers* del laboratorio para enlaces WAN, presentan algunas limitaciones en ancho de banda que para la aplicación de calidad de servicio, provocan que algunos umbrales tengan que ser decrementados.
- La aplicación de las políticas de calidad tanto a nivel de IPv4 como en IPv6 se expresan netamente en ambientes de congestión por lo cual se debe garantizar que a través de la red esté cursando el tráfico IP, voz, video de lo más real posible. De esta manera los datos obtenidos serán más fiables.
- Si bien el direccionamiento IPv6 está muy lejos de terminarse, para el IP Planning a nivel IPv6 de debe considerar los últimos RFC a fin de no desperdiciar direccionamiento.

## CAPÍTULO 5

### 5 REFERENCIAS BIBLIOGRÁFICAS

- [1] D. F. Alzate C y A. Cárdenas, *Retos en la transmisión de 40/100 Gb/s sobre fibra Óptica*, Revista en Telecomunicaciones e Informatica, vol. I, nº 2, pp. 23-60, 2011.
- [2] V. J. Malpartida Aranda y E. J. Sánchez Aranda, *Diseño de una red convergente basada en IPv6 para la red LAN de la Escuela de Informatica de la Universidad Nacional de Trujillo*, Repositorio UNITRU, Trujillo, Perú, 2016.
- [3] C. García García, *Propuesta de arquitectura de QoS en entorno inalámbrico 802.11 e basado en Diffserv con ajuste dinámico de parámetros*, Madrid, España: Universidad Carlos III de Madrid, 2006.
- [4] G. T. Jesús, *Alta Velocidad y calidad de servicios en redes IP*, Mexico: Universidad Autónoma de Nayarit (UAN), México, 2002.
- [5] J. Joskowicz, *Cableado Estructurado*, Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de la Republica de Montevideo, Uruguay, 2006.
- [6] Á. M. Mejía Fajardo, *Redes Convergentes*, Revista Universidad Militar Nueva Granada, vol. 14, nº 14, pp. 64-74, 2014.
- [7] J. M. Osorio, J. R. Hernandez Garibay y M. H. Almaguer Cantú, *Cableado Estructurado: Un estado del arte*, Journal of Basic Science, vol. IV, nº 2, pp. 3-8, 2006.
- [8] R. Rangel, *Medios de transmisión*, Universidad Virtual del Estado de Guanajuato, Guanajuato, Mexico, 2004.
- [9] J. Ramírez Sánchez y J. V. Días Martínez, *IIESCA - Universidad Veracruzana*, 2 12 2008. [En línea]. Available: <https://www.uv.mx/iiesca/files/2012/12/redes2008-2.pdf>.
- [10] Anónimo, *Red Informática*, [En línea]. Available: <https://www.mindomo.com/es/mindmap/proceso-tecnologico-04b04782262443dbb7121e851aa636ea>.
- [11] A. R. Alvarado, *Cable Coaxial*, [En línea]. Available: <https://slideplayer.es/slide/10158995/>.
- [12] A. S. Tanenbaum, *Redes de computadoras*, Mexico: Pearson Educación, 2003.
- [13] Anónimo, *Fiber optic cable*, Computer Hope, 10 febrero 2017. [En línea]. Available: <https://www.computerhope.com/jargon/f/fiberopt.htm>.
- [14] C. R. Sosa, *Redes de computadoras*, SEP, Escuela Superior de Ingeniería Mecánica y Eléctrica, nº 12, pp. 45-50, 2002.

- [15] S. D. Saade, C. Albaca Paraván y F. H. Lutz, *ieeexplore.ieee.org*, 10 Octubre 2016. [En línea]. Available: <https://ieeexplore.ieee.org/abstract/document/7585265/metrics>.
- [16] R. T. Anccalli, *Cableado Estructurado*, 22 octubre 2014. [En línea]. Available: <https://conocimientosdehoy.blogspot.com/2014/10/cableado-estructurado.html>.
- [17] R. M. Benites, J. L. Quiroz y R. Villafani, *Modelo Sip Seguro para una Comunicación extremo a extremo sobre IPv6*, Revista ECIPERU, vol. IIX, nº 2, pp. 63-68, 2011.
- [18] Anónimo, *IPv4-v6*, [En línea]. Available: <https://sites.google.com/site/wartj03/ipv4-v6>.
- [19] R. J. M. Tejedor, *El protocolo IPv6 (I)*, PC World nº 174, IDG Communications S.A., 2001. [En línea]. Available: [http://www.ramonmillan.com/tutoriales/ipv6\\_parte1.php#cabeceraipv6](http://www.ramonmillan.com/tutoriales/ipv6_parte1.php#cabeceraipv6).
- [20] D. Mejia, *Estructura de Capas para Telefonía IP (Cisco)*, [En línea]. Available: [https://www.researchgate.net/figure/Figura-1-Estructura-de-Capas-para-Telefonia-IP-Cisco\\_fig1\\_303381730](https://www.researchgate.net/figure/Figura-1-Estructura-de-Capas-para-Telefonia-IP-Cisco_fig1_303381730).
- [21] E. Guttierrez, *Capítulo 4 QoS – Calidad de Servicio*, [En línea]. Available: <https://slideplayer.es/slide/3831282/>.
- [22] A. O. Espinosa, *QoS Calidad de Servicio en la Red*, abril 2018. [En línea]. Available: <http://qos-informatica.blogspot.com/2015/04/arquitectura-basica-de-qos.html>.
- [23] C. N. Academy, *Introduction to Networks: Exploring the Network*, Cisco Press, 14 enero 2014. [En línea]. Available: <http://www.ciscopress.com/articles/article.asp?p=2164577&seqNum=6>.
- [24] J. C. Martinez, *Calidad de Servicio (QoS)*, Universidad Javeriana de Cali, [En línea]. Available: [http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr\\_-\\_calidad\\_de\\_servicio\\_qos\\_.pdf](http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_-_calidad_de_servicio_qos_.pdf).
- [25] Anónimo, *La cabecera IPv4*, [En línea]. Available: <http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/cabipv4.html>.
- [26] Anónimo, *Redes Convergentes - Descripción de DiffServ QoS*, [En línea]. Available: <https://slideplayer.es/slide/10370113/>.
- [27] INEC, *Directorio De Empresas Y Establecimientos*, 2016.
- [28] S. GUERRA, *Economía de Ecuador crecería este año, pero menos que en 2017*, Revista Gestión, [En línea]. Available: Disponible en línea en junio 2018: <http://www.revistagestion.ec/economia-y-finanzas-analisis/economia-de-ecuador-creceria-este-ano-pero-menos-que-en-2017>.

- [29] R. Zárate, *La telefonía y su importancia en las empresas*, 23 diciembre 2013. [En línea]. Available: <http://www.ricardozarate.es/?p=461>.
- [30] C. Onetto, *El video y sus beneficios para la colaboración empresarial*, Dinero.com, 02 diciembre 2015. [En línea]. Available: <https://www.dinero.com/opinion/columnistas/articulo/opinion-sobre-importancia-videoconferencias-empresas/216748>.
- [31] J. D. K. H. K. EVARISTO, *El impulso hacia la centralización: el péndulo vuelve a cambiar*.
- [32] R. GÓMEZ, *Arquitectura de los sistemas distribuidos*.
- [33] R. DEAL, *CCNA® Cisco® Certified Network Associate Study Guide*, McGraw-Hill, 2008.
- [34] S. Checa, *Tipos de Topología de red: malla, estrella, árbol, bus y anillo*, 17 julio 2018. [En línea]. Available: <https://www.locurainformaticadigital.com/2018/07/17/topologia-de-red-malla-estrella-arbol-bus-anillo/>.
- [35] M. Viracucha, *Esquemas de diseño*, Quito, 2019.
- [36] Anónimo, *INTRODUCCION A LA VoIP*, Google Sites. [En línea]. [Último acceso: 12 julio 2018].
- [37] YEALINK, *Sistemas de Videoconferencia*, YEALINK, [En línea]. Available: [https://www.sistek.cl/yealink/vcseries/Yealink%20VC800%20Video%20Conferenci ng%20System%20Datashet\\_ES%28LA%29.pdf](https://www.sistek.cl/yealink/vcseries/Yealink%20VC800%20Video%20Conferenci ng%20System%20Datashet_ES%28LA%29.pdf).
- [38] Anónimo, *¿Qué es el formato de codificación de video H.264 y por qué se está convirtiendo en el estándar de la industria en compresión de video?*, Black Box Network Services, [En línea]. Available: <https://www.blackbox.es/es-es/Page/38309/Recursos/Recursos-Tecnicos/black-box-explica/multimedia/Compresion-de-video-H264>.
- [39] B. Gonzalez, *Internet Speed Requirements for Video Streaming*, 09 julio 2018. [En línea]. Available: <https://www.lifewire.com/internet-speed-requirements-for-movie-viewing-1847401>.
- [40] A. Acosta y H. Serrano, *Enrutamiento con OSPF e IS-IS en redes IPv6*, Cisco, 2017.
- [41] R. Gutierrez, *Estado del Arte IPv6 (enrutamiento RIPNG, EIGRP, OSPF en Cisco)*, 2010. [En línea]. Available: <https://es.scribd.com/document/244201014/Estado-del-Arte-IPv6-enrutamiento-RIPNG-EIGRP-OSPF-en-Cisco-pdf>.

- [42] O. Salcedo, G. Narvaez y F. Puente, *Políticas de QoS para interfaces troncales de los equipos Metro y Core MPLS de una red basada en ASON*, Colombia: Universidad Distrital Francisco José de Caldas.
- [43] *Configuring IP SLAs UDP Jitter Operations for VoIP*, CISCO, [En línea]. Available: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla\\_udp\\_jitter\\_voip.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_udp_jitter_voip.pdf).
- [44] *Assured Forwarding and Expedited Forwarding*, [En línea]. Available: <https://sites.google.com/site/amitsciscozone/home/qos/assured-and-expedited-forwarding>.
- [45] *Uso del agente de la garantía de servicio de Cisco e Internetwork Performance Monitor para administrar la calidad del servicio en redes de voz sobre IP*, CISCO, [En línea]. Available: [https://www.cisco.com/c/es\\_mx/support/docs/ip/service-assurance-agent-saa/13938-csaaipm.html](https://www.cisco.com/c/es_mx/support/docs/ip/service-assurance-agent-saa/13938-csaaipm.html).
- [46] Anónimo, *Reverse DNS v6*, [En línea]. Available: <http://rdns6.com/zone>.
- [47] S. d. Luz, *Configurar un servidor DNS (Bind) en Linux Ubuntu*, RedesZone.net, 8 febrero 2013. [En línea]. Available: <https://www.redeszone.net/gnu-linux/configurar-un-servidor-dns-bind-en-linux-ubuntu/>.
- [48] *Servidor Web Apache sobre IPv6*, 11 febrero 2012. [En línea]. Available: <https://www.linuxito.com/gnu-linux/nivel-alto/4-servidor-web-apache-sobre-ipv6>.