



UNIVERSIDAD
NACIONAL
DE LOJA



Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

“Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la Provincia de Loja”

TESIS PREVIA A LA OBTENCIÓN
DEL TÍTULO DE INGENIERO EN
SISTEMAS

Autor:

- *López-Tene, Israel-Alejandro*

Director:

- *Salcedo-López, Franco-Hernán, Mg. Adm. Docente de la Carrera CIS*

Loja-Ecuador

2016

Certificación del Director

Ingeniero.

Franco Hernán Salcedo López, Mg. Adm.

DOCENTE DE LA CARRERA DE INGENIERIA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA.

CERTIFICA:

Que el presente trabajo, denominado **“Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la provincia de Loja”**, realizado por el egresado López Tene Israel Alejandro, cumple con los requisitos establecidos por las normas generales para la graduación en la Universidad Nacional de Loja, tanto en el aspecto de forma como contenido, por lo cual me permito autorizar proseguir los trámites legales para su presentación y defensa.

Loja, 07 de octubre del 2015



Ing. Franco Hernán Salcedo López, Mg. Adm.

Director de Tesis

Autoría

Yo **ISRAEL ALEJANDRO LÓPEZ TENE** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional - Biblioteca Virtual.

Firma:

Cedula: 1104069081

Fecha: 26 de octubre 2016

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **ISRAEL ALEJANDRO LÓPEZ TENE**, declaro ser el autor de la tesis titulada: **“ANÁLISIS Y EMULACIÓN DE MULTIHOMING Y DE LA PUBLICACIÓN AL INTERNET DE SERVICIOS WEB, A TRAVÉS DE UNA RED IPV6 EN LA EMPRESA XNET DE LA PROVINCIA DE LOJA”**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para la constancia de esta autorización, en la ciudad de Loja, a los veinte días del mes de octubre del dos mil dieciséis.

Firma: 

Autor: Israel Alejandro López Tene

Cédula: 1104069081

Dirección: Loja (Av. Oriental de Paso y Génova)

Correo Electrónico: israellopeztene@gmail.com

Teléfono: 072614083

Celular: 0989504535

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Franco Hernán Salcedo López, Mg. Adm.

Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

Ing. Gastón René Chamba Romero, Mg. Sc.

Dedicatoria

A mis queridos padres Efrén y Libia por ser el pilar fundamental de mi vida y estar junto a mí en todo momento, quienes con su amor y apoyo incondicional me dieron un enorme impulso e inspiración. A mis hermanos y en fin a toda la familia quienes de una u otra manera me apoyaron en la realización de este sueño.

Agradecimiento

A Dios por permitirme seguir siempre en la realización de mis sueños, mis metas y mis aspiraciones, por no dejarme caer nunca, por haberme dado una hermosa familia y la oportunidad de vivir este momento. A mis padres por su apoyo incondicional haciendo posible que concluya este objetivo trascendental de mi vida.

Expreso mi más querido agradecimiento, a la Universidad Nacional de Loja, a la carrera de Ingeniería en Sistemas, directivos personal administrativo. Quiero enfatizar mi agradecimiento al Ing. Franco Hernán Salcedo López quien en calidad de director apporto su experiencia profesional guiándome, ayudándome en la realización y culminación exitosa de este proyecto de tesis.

Agradecer así mismo a todos quienes conforman la Empresa XNET de la ciudad de Loja por permitirme recabar la información sin ningún inconveniente.

A todos ustedes muchas gracias, y que Dios los bendiga siempre.

Índice de Contenidos

1. Índice General

Certificación del Director	II
Autoría	III
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.	IV
Dedicatoria.....	V
Agradecimiento	VI
Índice de Contenidos	VII
1. Índice General	VII
2. Índice de Figuras.....	XIV
3. Índice Tablas.	XVIII
a. Título	1
b. Resumen	2
Summary	3
c. Introducción	4
d. Revisión de Literatura	5
1. Protocolo de Internet IPv6 y protocolo de enrutamiento OSPFv3, BGP-4 y Multihoming.....	5
1.1. Introducción a IPv6	5
1.2. Distribución de Recursos en Internet	6
1.3. Características de IPv6.....	8
1.3.1. Direccionamiento en IPv6	9
1.3.2. Formato de las Direcciones en IPv6.....	10
1.3.3. Representación Textual de las direcciones	10
1.3.4. Direcciones Unicast en IPv6	10

1.4. Protocolos de Gateway Interior	12
1.4.1. Protocolo OSPFv3.....	13
1.4.2. Enrutamiento por Estado de Enlace	13
1.4.3. Algoritmo SPF.....	15
1.4.4. Paquetes OSPFv3	15
1.4.5. Características del protocolo OSPFv3	16
1.4.6. Tipos de áreas de OSPFv3.....	17
1.4.7. Ventajas y desventajas del protocolo OSPFv3	17
1.5. Protocolo BGP.....	18
1.5.1. Protocolo BGP-4.....	20
1.5.2. Tipos de Mensajes BGP-4.....	20
1.6. Herramientas para emular redes	21
1.7. Estudio y aplicabilidad de Multihoming	22
1.7.1. Formas de conexión con Multihoming.....	23
1.7.2. Múltiples conexiones utilizando un solo Proveedor de servicio.....	23
1.7.3. Múltiples conexiones con varios proveedores de servicio	24
1.7.4. Multihoming en empresas pequeñas.....	26
1.7.5. Multihoming en empresas grandes.....	26
1.7.6. Problemas de Multihoming.....	26
2. Análisis de la situación actual de la Empresa.....	27
2.1.1. Misión.....	27
2.1.2. Visión.....	27
2.1.3. Propósito	27
2.2. Análisis de la infraestructura en la red de datos de la empresa XNET	28
2.2.1. Descripción.....	28
2.2.2. Proveedor de servicios de internet	29

2.3. Personal de la empresa.....	32
2.4. Planes de servicio de Internet que ofrece la Empresa	32
e. Materiales y Métodos	35
1. Materiales	35
2. Métodos	35
2.1. Técnicas	36
2.2. Metodología de Desarrollo del Proyecto.....	36
f. Resultados.....	39
1. Primera Fase.- Análisis de la red de la empresa XNET de la parroquia el sagrario.....	39
1.1. Ubicación de las antenas AirGrid M2 en la cuida de Loja	39
1.2. Descripción de dispositivos de la red.....	40
1.3. Clientes de la red sagrario	41
1.4. Direccionamiento de la red sagrario	42
1.5. Protocolo de enrutamiento de la red sagrario.....	42
1.6. Seguridad de la Red Sagrario.....	43
2. Segunda Fase.- Diseñar la red de la parroquia sagrario	44
2.1. Análisis de BGP y OSPFv3 que se implementa.....	44
2.1.1. Análisis de BGP-4	45
2.1.2. Análisis de OSPFv3.....	46
2.2. Análisis de Multihoming que se implementa	47
2.2.1. Multihoming en el router de borde Sagrario.....	47
2.2.2. Multihoming en el router de borde Valle.....	48
2.3. Topología de la Nueva red sagrario.....	49
2.4. Porque utilizamos IPv6.....	50
2.5. Direccionamiento IPv6 para la red sagrario	50
3. Tercera Fase.- Configuración en GNS3 de la topología de la red.....	53

3.1. Paso1: Configuración básica de todos los router pertenecientes a la red de la empresa:	53
3.1.1. Router céli román: Configuración básica	54
3.1.2. Router pradera: Configuración básica	54
3.1.3. Router las palmas: Configuración básica	55
3.1.4. Router de borde sagrario: Configuración básica	55
3.1.5. Router san cayetano: Configuración básica	56
3.1.6. Router samaná: Configuración básica	56
3.1.7. Router valle: Configuración básica	57
3.1.8. Router de borde valle: Configuración básica	57
3.1.9. Router proveedor 1: Configuración básica	58
3.1.10. Router proveedor 2: Configuración básica	58
3.2. Paso 2: Configuración del protocolo IPv6 a los router de la red de la empresa.	
59	
3.2.1. Router céli román: Configuración IPv6	61
3.2.2. Router pradera: Configuración IPv6	62
3.2.3. Router palmas: Configuración IPv6	62
3.2.4. Router de borde sagrario: Configuración IPv6	63
3.2.5. Router san cayetano: Configuración IPv6	64
3.2.6. Router samaná: Configuración IPv6	65
3.2.7. Router valle: Configuración IPv6	65
3.2.8. Router de borde valle: Configuración IPv6	66
3.2.9. Router proveedor 1: Configuración IPv6	66
3.2.10. Router proveedor 2: Configuración IPv6	67
3.3. Paso 3: Configuración de la interfaz loopback en los router céli román, pradera, palmas, san cayetano, samaná y valle.	67
3.3.1. Router céli román: Configuración de interfaz loopback	68

3.3.2. Router pradera: Configuración de interfaz loopback.....	69
3.3.3. Router palmas: Configuración de interfaz loopback.....	69
3.3.4. Router san cayetano: Configuración de interfaz loopback	69
3.3.5. Router samaná: Configuración de interfaz loopback.....	70
3.3.6. Router valle: Configuración de interfaz loopback.....	70
3.4. Paso 4: Configuración de protocolo OSPFv3 para los router céli román, pradera, palmas, san cayetano, samaná, valle, borde sagrario y borde valle.....	71
3.4.1. Router céli román: Configuración OSPFv3.....	72
3.4.2. Router pradera: Configuración OSPFv3	73
3.4.3. Router palmas: Configuración OSPFv3	74
3.4.4. Router san cayetano: Configuración OSPFv3.....	75
3.4.5. Router samaná: Configuración OSPFv3	76
3.4.6. Router valle: Configuración OSPFv3.....	77
3.4.7. Router borde sagrario: Configuración OSPFv3	78
3.4.8. Router borde valle: Configuración OSPFv3.....	80
3.5. Paso 5: Configuración del protocolo exterior BGP y Multihoming para los router borde sagrario, borde valle, proveedor 1 y proveedor 2	81
3.5.1. Router borde sagrario: Configuración del protocolo BGP y Multihoming	83
3.5.2. Router borde valle: Configuración del protocolo BGP y Multihoming	83
3.5.3. Router proveedor 1: Configuración del protocolo BGP y Multihoming	84
3.5.4. Router proveedor 2: Configuración del protocolo BGP y Multihoming	85
4. Cuarta Fase.- Pruebas	86
4.1. Plan de Pruebas	86
4.1.1. Propósito	86
4.1.2. Alcance de las Pruebas	86
4.1.3. Entorno y configuración de las pruebas.....	91
4.1.4. Resultados de las Pruebas.....	92

4.1.4.1. Caso 1: Exista conectividad de los dispositivos de la red de la empresa.	92
.....	
• Verificar conectividad entre los dispositivos de la red sagrario.	92
4.1.4.2. Caso 2: Verificar la configuración del Protocolo OSPFv3 en los dispositivos de la red de la empresa.	93
.....	
• Verificar adyacencia OSPFv3 entre los dispositivos.	93
• Verificar áreas configuradas	94
• Verificar rutas aprendidas del protocolo OSPFv3 en routers	96
4.1.4.3. Caso3: Verificar la configuración del protocolo BGP en los dispositivos de la red.	98
.....	
• Verificar la configuración del protocolo BGP.	99
• Verificar rutas aprendidas por medio del protocolo BGP.	100
4.1.4.4. Caso 4: Analizar las métricas de OSPFv3 y BGP.	102
.....	
4.1.4.5. Caso 5: Verificación de los paquetes de los protocolos de enrutamiento OSPFv3 y BGP.	111
.....	
4.1.4.6. Caso 6: Prueba de funcionamiento de Multihoming a la red de la empresa.	118
.....	
• Prueba de conectividad de red sagrario con red externa pruebas (prueba realizada por el enlace principal del router de borde sagrario).	118
• Verificar porque proveedor está siendo publicada la red sagrario hacia el internet.	119
• Caída del enlace principal de la red sagrario y auto levantamiento de enlace de secundario 1	120
.....	
• Verificar tabla de enrutamiento del router de borde sagrario a la caída del enlace principal.	120
.....	
• Prueba de conectividad por medio del enlace de secundario 1	121
.....	
• Caída del enlace secundario 1 de la red sagrario y auto levantamiento de enlace de secundario 2.	122
.....	

• Verificar tabla de enrutamiento del router de borde sagrario a la caída del enlace secundario 1.	123
• Prueba de conectividad por medio del enlace de respaldo.....	124
4.1.4.7. Prueba de funcionamiento de Multihoming a la red valle.....	125
• Prueba de conectividad de red valle con red externa pruebas.	125
• Verificar porque proveedor está siendo publicada nuestra red.....	126
• Caída del enlace principal de la red valle y auto levantamiento de enlace de respaldo.....	126
• Verificar tabla de enrutamiento del router de borde valle.....	127
• Prueba de conectividad por medio del enlace de respaldo.....	128
g. Discusión	130
1. Desarrollo de la propuesta	130
2. Valoración técnica económica ambiental.....	132
h. Conclusiones	134
i. Recomendaciones.....	135
j. Bibliografía	136
k. Anexos	138
Anexo 1: Encuesta al Gerente de la Empresa XNET	138
Anexo 2: Encuesta al técnico de la Empresa XNET	141
Anexo 3: Fotos de las instalaciones de los equipos de red de la Empresa.....	144
Anexo 4: Glosario de términos.....	145
Anexo 5: Licencia Creative Commons.....	147

2. Índice de Figuras

Figura 1. Imagen de la Distribución de recursos en Internet	7
Figura 2. Formato de Dirección Unicast.....	12
Figura 3. Algoritmo SPF.....	15
Figura 4. Estructura del Protocolo BGP.	19
Figura 5. Multihoming con un solo proveedor	23
Figura 6. Pérdidas de Conexión.....	24
Figura 7. Múltiples conexiones con varios proveedores de servicio	24
Figura 8. Pérdida de conexión hacia el ISP	25
Figura 9. Orgánico Estructural	28
Figura 10. Topología de red de la empresa	30
Figura 11. Distribución del MDF e IDF	31
Figura 12. Red Sagrario.....	40
Figura 13. Topología de la nueva red sagrario.....	44
Figura 14. BGP-4 en la empresa.	45
Figura 15. OSPFv3 en la empresa.....	46
Figura 16. Multihoming borde sagrario.....	47
Figura 17. Multihoming borde valle.	48
Figura 18. Topología de la red sagrario.	49
Figura 19. Configuración básica de router céli román	54
Figura 20. Configuración básica de router pradera	55
Figura 21. Configuración Básica de router las palmas	55
Figura 22. Configuración básica de router borde sagrario.....	56
Figura 23. Configuración Básica de router san cayetano.	56
Figura 24. Configuración Básica de router samaná	57
Figura 25. Configuración básica router valle	57
Figura 26. Configuración básica router borde valle	58
Figura 27. Configuración básica de router proveedor 1	58
Figura 28. Configuración básica de router proveedor 2	59
Figura 29. Interfaces de los router	60
Figura 30. Configuración IPv6 de router céli román	61
Figura 31. Configuración IPv6 de router pradera	62
Figura 32. Configuración IPv6 de router palmas.	63
Figura 33. Configuración IPv6 de router borde sagrario.....	64
Figura 34. Configuración IPv6 de router san cayetano.....	64

Figura 35. Configuración IPv6 de router samaná.....	65
Figura 36. Configuración IPv6 de router valle	65
Figura 37. Configuración IPv6 de router borde valle.	66
Figura 38. Configuración IPv6 de router proveedor 1.....	66
Figura 39. Configuración IPv6 de router proveedor 2.....	67
Figura 40. Configuración de interfaz loopback en router céli román.....	69
Figura 41. Configuración de interfaz loopback en router pradera.....	69
Figura 42. Configuración de interfaz loopback en router palmas.....	69
Figura 43. Configuración de interfaz loopback en router palmas.....	70
Figura 44. Configuración de interfaz loopback en router samaná.	70
Figura 45. Configuración de interfaz loopback en router Valle.	70
Figura 46. Configuración OSPFv3 de router céli román	73
Figura 47. Configuración OSPFv3 de router pradera.....	74
Figura 48. Configuración OSPFv3 de router palmas	75
Figura 49. Configuración OSPFv3 de router San Cayetano.....	76
Figura 50. Configuración OSPFv3 de router samaná.....	77
Figura 51. Configuración OSPFv3 de router valle.....	78
Figura 52. Configuración OSPFv3 de router borde Sagrario.....	79
Figura 53. Configuración de Id OSPFv3 de router Receptor y comando redistribute de direcciones.	79
Figura 54. Configuración OSPFv3 de router borde valle.....	80
Figura 55. Configuración de Id OSPFv3 de router borde valle y comando redistribute de direcciones.	80
Figura 56. Configuración BGP y Multihoming de router borde sagrario.....	83
Figura 57. Configuración BGP y Multihoming de router borde Valle.	84
Figura 58. Configuración BGP y Multihoming de router proveedor 1.....	84
Figura 59. Configuración BGP y Multihoming de router proveedor 2.....	85
Figura 60. Topología de la red sagrario	91
Figura 61. Conectividad de router céli román a router palmas.	92
Figura 62. Conectividad de router céli román a router samaná.....	92
Figura 63. Conectividad de router céli román a router pradera.	93
Figura 64. Verificar adyacencias de router palmas.	93
Figura 65. Verificar adyacencias de router borde sagrario.....	94
Figura 66. Verificar adyacencias de router valle.	94
Figura 67. Verificar áreas del router palmas.	95

Figura 68. Verificar áreas de router borde sagrario.....	96
Figura 69. Tabla de enrutamiento de router pradera.....	97
Figura 70. Tabla de enrutamiento de router saman.	98
Figura 71. Configuracin BGP del router borde Sagrario.	99
Figura 72. Configuracin BGP del router borde valle.	100
Figura 73. Tabla de enrutamiento de router borde sagrario.	101
Figura 74. Tabla de enrutamiento de router borde valle.....	102
Figura 75. Red Empresa.....	103
Figura 76. Tabla de enrutamiento de router saman.	104
Figura 77. Tabla de enrutamiento de router valle.....	105
Figura 78. Tabla de enrutamiento de router bordevalle.....	106
Figura 79. Tabla de enrutamiento de router bordesagrario.	107
Figura 80. Tabla de enrutamiento de router palmas.....	108
Figura 81. Red para pruebas de BGP.....	108
Figura 82. Tabla de enrutamiento de router pradera.....	109
Figura 83. Tabla de enrutamiento de router palmas.....	110
Figura 84. Tabla de enrutamiento de router bordesagrario.	111
Figura 85. Red pruebas con wireshark.	112
Figura 86. Direccin loopback de establecimiento de comunicacin.....	113
Figura 87. Paquete hello.....	113
Figura 88. Paquete DB. Description.....	114
Figura 89. Paquete LS Request.....	114
Figura 90. Paquete LS Update.....	115
Figura 91. Paquete LS Acknowledge.	115
Figura 92. Red pruebas de bgp con wireshark.....	116
Figura 93. Paquete Open.....	117
Figura 94 Paquete Keepalive.....	117
Figura 95 Paquete Update.....	117
Figura 96. Ping extendido de mquina virtual a red externa pruebas.....	118
Figura 97. Tabla de enrutamiento de router borde sagrario.	119
Figura 98. Topologa con enlace principal cado de router borde sagrario.	120
Figura 99. Adyacencias terminadas en router borde sagrario con proveedor 1.....	120
Figura 100. Taba de enrutamiento de router borde sagrario.	121
Figura 101. Prueba de conectividad de router palmas hacia red externa pruebas. ...	122
Figura 102. Topologa con enlace secundario 1 cado de router borde sagrario.	122

Figura 103. Adyacencias terminadas en router borde sagrario con proveedor 2.....	123
Figura 104. Tabla de enrutamiento de router borde sagrario.	123
Figura 105. Prueba de Conectividad por enlace alternativo de router Céli Román a red externa pruebas.....	124
Figura 106. Prueba de Conectividad por enlace alternativo de router pradera a Red Externa pruebas.	124
Figura 107. Traceroute de router san cayetano a router de red externa pruebas.....	125
Figura 108. Traceroute de router samaná a router de red externa pruebas.	125
Figura 109. Tabla de enrutamiento de router borde valle.	126
Figura 110. Topología con enlace principal caído de router borde valle.....	127
Figura 111. Adyacencias terminadas en router borde valle con proveedor 2.	127
Figura 112. Tabla de enrutamiento de router valle.....	128
Figura 113. Traceroute de enlace secundario de router san cayetano a router de red externa pruebas.....	128
Figura 114. Traceroute de enlace secundario de router samaná a router de red externa pruebas.	129

3. Índice Tablas.

TABLA I. LIMITANTES DE IPV4.....	6
TABLA II. DESCRIPCION DE LAS RIR.....	7
TABLA III. CARACTERISTICAS DE IPV6 CON RESPECTO A IPV4	8
TABLA IV. DIRECCIONES UNICAST.....	11
TABLA V. COMPARATIVA DE LOS PROTOCOLOS DE ENRUTAMIENTO DINAMICO.	12
TABLA VI. GENERALIDADES DE OSPFV3.....	14
TABLA VII. PAQUETES OSPFV3.....	15
TABLA VIII. CARACTERISTICAS DE OSPFV3.....	16
TABLA IX. VENTAJAS Y DESVENTAJAS DE OSPFV3.....	17
TABLA X. MENSAJES DE BGP-4.....	20
TABLA XI. TABLA COMPARATIVA DE GNS3 Y PACKET TRACER.....	22
TABLA XII. XPLAN PARA EL HOGAR.....	33
TABLA XIII. XPLAN EMPRESARIAL.....	33
TABLA XIV. XPLAN CYBERS.....	34
TABLA XV. MATERIALES Y MÉTODOS.....	35
TABLA XVI. DIRECCIONAMIENTO DE LA RED.....	42
TABLA XVII. BLOQUE DE DIRECCIÓN DE LA EMPRESA.....	50
TABLA XVIII. TOTAL SUBREDES DE LA EMPRESA.....	51
TABLA XIX. DIRECCIÓN PARA CADA ANTENA DE LA RED.....	52
TABLA XX. COMANDOS DE CONFIGURACIÓN BÁSICA.....	53
TABLA XXI. COMANDOS PARA CONFIGURACIÓN DE IPv6.....	59
TABLA XXII. DIRECCIONES IPV6.....	60
TABLA XXIII COMANDOS PARA CONFIGURAR LA INTERFAZ LOOPBACK.....	68
TABLA XXIV DIRECCIONES IPV6 PARA LAS INTERFACES LOOPBACK.....	68
TABLA XXV. COMANDOS CONFIGURACIÓN DE OSPFV3.....	71
TABLA XXVI. ID DE OSPFV3.....	72
TABLA XXVII. COMANDOS PROTOCOLO BGP-4 Y MULTIHOMING.....	81
TABLA XXVIII. ESTABLECER SISTEMA AUTONOMO(AS) Y ID DE CADA ROUTER.	82
TABLA XXIX. CASO DE PRUEBA DE 1.....	87
TABLA XXX. CASO DE PRUEBA 2.....	87
TABLA XXXI. CASO DE PRUEBA 3.....	88
TABLA XXXII. CASO DE PRUEBA 4.....	88

Tabla XXXIII CASO DE PRUEBA 5	89
TABLA XXXIV. CASO DE PRUEBA 6.	89
TABLA XXXV. RECURSOS HUMANOS.....	132
TABLA XXXVI. RECURSOS TÉCNICOS TECNOLÓGICOS	132
TABLA XXXVII. RECURSOS DE SERVICIOS.....	133
TABLA XXXVIII. COSTE GENERAL DE RECURSOS.....	133

a. Título

“Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la Provincia de Loja”.

b. Resumen

El análisis y emulación de Multihoming a través de una red IPv6 en la Empresa XNET de la Provincia de Loja tuvo como punto de partida el análisis de red de la empresa Xnet, tomando como base la red de la empresa se diseñó la nueva topología incluyendo recomendaciones de Multihoming para que la red de la empresa sea tolerante a fallos, se realizó la configuración de red con los protocolos de enrutamiento interno y exterior OSPFv3 y BGP respectivamente y como último se diseñó un plan de pruebas para comprobar Multihoming.

Para su desarrollo se aplicó la metodología Top-Down Network Design debido a su adaptabilidad al desarrollo de emulación de redes, misma que permitió desarrollar el proyecto de tesis acorde a los objetivos planteados.

El uso de las Técnicas y herramientas expuestas, han permitido recabar la información de la empresa para realizar las fases 1 y 2 del proyecto. La realización de la fase 3 se empleó el método sistémico puesto que tuvimos que realizar una investigación de los protocolos de enrutamiento utilizados en el desarrollo del proyecto.

Summary

The paper presents the design of a network for the company Xnet from the city of Loja, integrating Internet Protocol version 6 network design, emulation for the use of IPv6. IPv6 help advertising and development of the company, would not have to make major changes in the configuration of client computers, together with IPv6 designed to put a protocol for high availability in the edge router, as is Multihoming to help to provide uninterrupted internet service to customers.

Development for the Top-Down Network Design methodology was applied due to its adaptability to the development of network emulation, allowing develop a same network emulation according to the objectives.

The use of techniques and tools exposed, have begun to collect information from the company for phases 1 and 2 of the project. The completion of phase 3 systemic method was used since we had to conduct an investigation of the metrics used in the project.

c. Introducción

IPv6 se ha desarrollado durante los últimos años, el proceso ha sido impulsado principalmente por la futura escasez de direcciones IPv4. La crisis del espacio de direcciones IPv4 se ha visto retrasado por varios enfoques para direccionamiento IP, las más importantes son: Subneteo de red, NAT (puente) y los espacios de direcciones privadas. Estas soluciones solo posponen lo inevitable, por lo que los esfuerzos para rediseñar el protocolo IP, condujeron al protocolo IPv6. [1]

Hoy en día los Registros Regionales de Internet tienen políticas de asignación de direcciones IPv4 muy rigurosas. Se puede extender el espacio de direcciones IPv4 durante un periodo más de tiempo, pero si el resultado es que solo unos pocos privilegiados pueden obtener espacios de direcciones públicas no se convierte en la solución óptima.

La implementación de IPv6 en empresas se van tornando más comunes, decenas de implementaciones se han desplegado y utilizado, ya que no es necesario un software adicional o parches especiales, puesto que la mayoría de los sistemas operativos incluyen soporte para IPv6 y algunos incluso lo activan por defecto. IPv6 ha llegado a un punto en el que casi todo el mundo puede utilizarlo.

El uso de Multihoming en empresas proveedoras de internet ha ido en crecimiento debido a que las mismas buscan la excelencia al momento de brindar su servicio, Multihoming da un plus a la empresa que lo implemente, para así poder brindar un servicio de calidad, con la certeza de que el servicio de internet no fallara a sus clientes.

d. Revisión de Literatura

1. Protocolo de Internet IPv6 y protocolo de enrutamiento OSPFv3, BGP-4 y Multihoming

1.1. Introducción a IPv6

El Protocolo de Internet versión 6, mejor conocido como IPv6, es la versión más reciente de este protocolo y el sucesor de IPv4, la versión anterior, la cual no había sufrido cambios importantes desde 1981 cuando se dio a conocer por primera vez. Antes de adoptar este nombre, el protocolo IPv6 fue conocido como IPng (Internet Protocol next generation), y hasta la fecha existen personas que lo siguen llamando de esta manera. [1]

Al observar el salto desde IPv4 hasta IPv6 (omitiendo la opción que parecería ser más lógica, IPv5) surge la duda en cuanto a por qué no se utilizó IPv5 como el nombre para el protocolo sucesor. Y la respuesta es muy simple, IPv5 nunca fue considerado para ser la nueva versión del protocolo. El nombre IPv5 fue asignado a un protocolo experimental, cuyo objetivo era el de la transmisión de datos en tiempo real. Este protocolo fue conocido originalmente como ST-2 (Stream Protocol Versión 2), pero su función fue reemplazada eventualmente por RSVP (Resource Reservation Setup Protocol). Incluso, a raíz de este suceso, se han hecho peticiones para que en un futuro las versiones aumenten en números pares. [2]

Hasta hace algunos años, el IPv4 había resultado ser un protocolo completo y de fácil implementación. El problema es que no se anticiparon algunas situaciones que eventualmente se convertirían en limitantes para la utilización del mismo. [2]

Estas son algunas de estas situaciones, las que se muestran en la Tabla 1.

TABLA I.
LIMITANTES DE IPV4.

No.	Limitantes de Ipv4
1	El crecimiento desmedido del Internet y la reducción del espacio para asignar direcciones IP.
2	El crecimiento del Internet y la capacidad de los enrutadores pertenecientes al backbone de Internet para mantener grandes tablas de enrutamiento.
3	Herramientas que se configuraban a parte del protocolo de Internet IPv4.
4	La necesidad de un mejor soporte en la transmisión de datos en “tiempo real”, mejor conocido como “Calidad de Servicio”.

Para resolver estas limitantes, la IETF (Internet Engineering Task Force) desarrolló un grupo de protocolos y estándares conocido como IPv6. Este protocolo fue diseñado con la intención de afectar en lo más mínimo a las capas inferiores y superiores, evitando agregar características totalmente nuevas a esta versión, manteniendo así la estructura básica original del protocolo.

1.2. Distribución de Recursos en Internet

La distribución de recursos en Internet en sus inicios fue controlada por la Internet Assigned Numbers Authority (cuyo acrónimo es IANA), y que en la actualidad a partir del año 1998 fue sustituido por la Internet Corporation for Assigned Names and Numbers (ICANN). [3] Las atribuciones de la ICANN fueron dadas por el Departamento de Comercio de Estados Unidos bajo la figura de adjudicación directa y única. Las tareas de la ICANN fueron y siguen siendo la gestión de la asignación de nombres de dominio de primer nivel (el dominio de primer nivel es la parte final de un dominio de Internet, o sea las letras que siguen al punto final de cualquier nombre, por ejemplo el gt, edu, gob) y direcciones IP. [3] Para estas tareas se crearon cinco RIR (Regional Internet Registry) o registros regionales de Internet, a las cuales la IANA delega los recursos para que sean éstas quienes sub-deleguen los recursos a los ISP y organizaciones de usuarios finales. Las cinco RIR son, ARIN, RIPE, APNIC, LACNIC y AFRINIC. La imagen para la distribución de recursos en Internet se muestra en la Figura 1. [3]

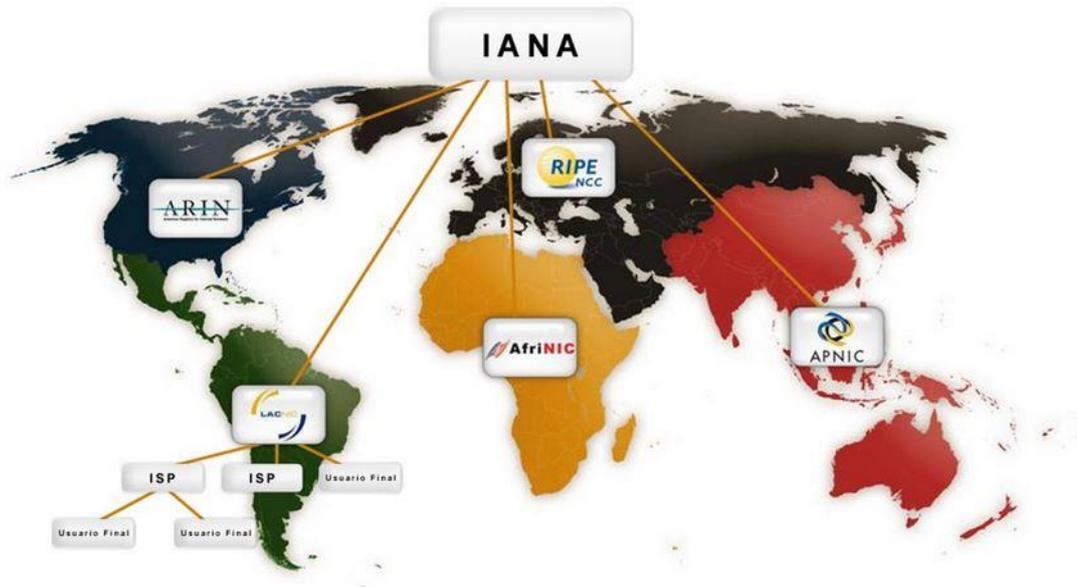


Figura 1. Imagen de la Distribución de recursos en Internet

Descripción de las RIR que cubren a todo el planeta las cuales son reguladas por la Organización ICANN. Las cuales se muestran en la Tabla 2.

TABLA II.
DESCRIPCIÓN DE LAS RIR.

Nombre de RIR	Región que cubre	Año de reconocimiento por la ICANN
La AFRINIC (African Network Information Centre).	Cubre la región de África.	En abril del 2005.
La APNIC (Asia-Pacífico Network Information Centre).	Cubre la región de Asia-Pacífico.	En enero de 1993.
La ARIN (American Registry for Internet Numbers)	Cubre la región de Canadá.	En diciembre de 1997.
La LACNIC (Latin American and Caribbean Internet Address Registry).	Cubre Latinoamérica y el Caribe.	En el año de 2001.

La RIPE NCC (Réseaux IP Européens Network Coordination Centre).	Cubre las regiones de Europa, Medio Oriente y Asia Central.	En abril de 1992.
--	---	-------------------

1.3. Características de IPv6

IPv6 presenta ciertas características que contrastan con la versión 4 de este protocolo. Estas características se listan a continuación, en la Tabla 3.

TABLA III.
CARACTERÍSTICAS DE IPV6 CON RESPECTO A IPV4

Versión	Concepto	Estructura	Ventajas	Desventajas
IPv4	Es la cuarta versión del protocolo de Internet Protocolo (IP), y la primera en ser implementada a gran escala.	Está compuesta de 4 grupos de 8 bits (32 bits), cada uno 8x4, se puede decir de 4 grupos decimales donde cada una está formado por 3 dígitos.	Formato de cabecera más grande. Configuración manual y dinámica. Direcciones Broadcast. IPv4 utiliza direcciones de 32 bits de longitud, lo que ofrece un total de 4.294.967.296 direcciones IP diferentes. La actual población mundial se estima en alrededor de 6.700 millones de personas, fácilmente advertimos lo ajustado de la situación.	Elevada demanda de direcciones IP. No tiene seguridad. Limita el crecimiento de Internet.
IPv6	Es la versión 6 del protocolo de Internet	Está compuesto de ocho grupos de 4 caracteres cada uno.	Formato de cabecera más sencillo. Direcciones multicast. IPv6 considera en su misma estructura las funcionalidades que actualmente se agregan a	Para estar enlazada al universo IPv6 durante la fase de transición, todavía se

(Internet protocol) un estándar en desarroll o del nivel de red encargad o de dirigir y encamin ar los paquetes a través de una red.	Además se complica un poco, ya que los grupos en vez de expresarse en notación decimal lo harán en hexadecimal y la separación no se la hará por un (.), sino por (:).	IPv4 con la implementación de IPSec. Configuración estática, configuración dinámica utilizando DHCPv6, y autoconfiguración dinámica. El procedimiento de configuración dinámica simplifica enormemente la implementación de direccionamiento dinámico en redes pequeñas, eliminando el requerimiento de un servidor DHCP, permitiendo así brindar una dirección IPv6 con la ayuda de la dirección MAC.	necesita una dirección IPv4 o algún tipo de NAT.
--	--	--	--

En vista a las ventajas que proporciona IPv6, y teniendo una visión hacia el futuro de la empresa, en cuanto a su crecimiento de usuarios, se ha optado por adoptar el protocolo IPv6 para realizar el proyecto fin de carrera.

1.3.1. Direccionamiento en IPv6

Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados.

1. **Unicast.-** Esta es una dirección que identifica a una sola interface. Un paquete enviado a una dirección de este tipo es entregado a la interface que se identifica con esa dirección.
2. **Anycast.-** Esta es una dirección que identifica a un grupo de interfaces que típicamente pertenecen a diferentes nodos. Un paquete enviado a una dirección de este tipo es entregado a una de las interfaces identificadas con esa dirección, y se entrega a la interface más cercana (en relación a métricas de distancia de los protocolos de enrutamiento).

3. **Multicast.**- Esta es una dirección que identifica a un grupo de interfaces que típicamente pertenecen a diferentes nodos. Un paquete enviado a una dirección de este tipo es entregado a todas las interfaces identificadas con esa dirección.

1.3.2. Formato de las Direcciones en IPv6

La técnica de representación de las direcciones en IPv6 es muy parecida al que se utiliza en el formato de IPv4. En IPv4 se utilizan 4 campos de 8 bits y cada campo estaba en sistema decimal. Ahora en IPv6 se utilizan 8 campos pero en sistema hexadecimal.

1.3.3. Representación Textual de las direcciones

Las direcciones en IPv6 están representadas por 8 campos de números en base hexadecimal y cada campo está compuesto de 16 bits o sea 4 dígitos hexadecimales, separados en lugar de un “.” como en IPv4 por “:”. Algunas reglas que se pueden aplicar para hacer la representación de una dirección son las siguientes: [4]

1. No hay diferencia entre letras mayúsculas y minúsculas, por ejemplo “EF01” equivale a “ef01”.
2. Es opcional dejar o no los ceros en un campo. Por ejemplo “00e1” es equivalente a “e1”.
3. Una sucesión de ceros puede ser representada por “::” pero únicamente una vez en una dirección.

Por ejemplo la siguiente dirección:

- 00AA:0000:FFF9:0000:0000:5555:ABCD:0012
- Puede ser representada usando la regla 1. por:
00aa:0000:fff9:0000:0000:5555:abcd:0012
- Que a la vez puede ser comprimida usando la regla 2. por:
aa:0:fff9:0:0:5555:abcd:12
- Que además usando la regla 3. puede ser representada como:
aa:0:fff9::5555:abcd:12

1.3.4. Direcciones Unicast en IPv6

Se muestra las direcciones Unicast en la Tabla 4, las mismas que se dividen en:

TABLA IV.
DIRECCIONES UNICAST.

Direcciones Unicast IPv6	
Identificadores de Interfaz	Los identificadores de interface en direcciones IPv6 Unicast son usadas para identificar una interfaz en un enlace. Es requerido que sean únicas en un prefijo de subred. Es recomendado que el mismo identificador de interface no sea asignado a diferentes nodos en un enlace. Usualmente el identificador de interface se deriva de la dirección MAC, es por ello que se dice que las direcciones de los nodos IPv6 están basados en el formato IEEE EUI-64. El RFC 2373 incluye un apéndice donde se explica cómo crear los identificadores de interfaces. El mismo identificador de interface puede ser utilizado en múltiples interfaces de un mismo nodo, mientras que las interfaces estén unidas a diferentes subredes.
Direcciones sin Especificar	La dirección con la forma 0:0:0:0:0:0:0:0 es llamada la dirección sin especificar, y nunca debe ser asignada a un nodo, pues ésta indica la ausencia de una dirección. Esta dirección tampoco debe ser utilizada como dirección destino ni en una cabecera de enrutamiento IPv6. Un paquete IPv6 con una dirección origen sin especificar nunca debe de ser reenviado por un enrutador.
Direcciones Loopback	En IPv6 estas direcciones están definidas como "0:0:0:0:0:0:0:1" o de manera simplificada como "::1". Esta dirección es utilizada para que un nodo IPv6 se envíe un paquete a sí mismo tal como en IPv4. Esta dirección no debe de ser usada como dirección origen en los paquetes IPv6 que son enviadas fuera de un nodo, y nunca debe de ser reenviado por un enrutador.
Direcciones Globales Unicast	Las direcciones globales son utilizadas para comunicar los nodos con Internet. Estas direcciones, llamadas direcciones globales Unicast, están actualmente asignadas como "001" en los tres últimos bits de la izquierda de la dirección. Esto corresponde a direcciones desde 2000:: hasta 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, o sea un espacio 2000:: /3. Este espacio de direcciones está definido para usar los 64 bits de la izquierda para el prefijo de la red y los 64 bits de la derecha para la parte de nodos.

El formato de una dirección Unicast se muestra en la Figura 2.

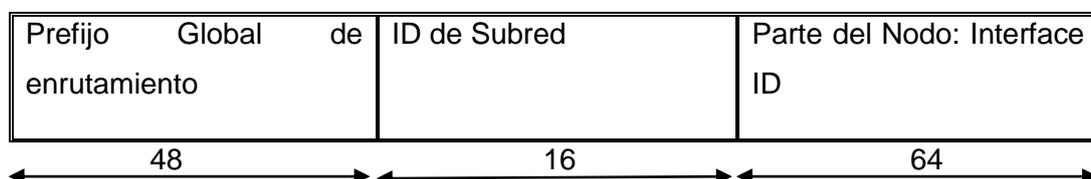


Figura 2. Formato de Dirección Unicast

Donde el prefijo global de enrutamiento tiene una longitud de 48 bits y el prefijo es asignado por el proveedor a un grupo de subredes o sitio. La parte del identificador de subred tiene una longitud de 16 bits y contiene los números de la subred dentro de un sitio, 216 subredes son permitidas. La parte de la derecha es de una longitud de 64 bits y contiene la parte del nodo, que también es llamada identificador de interface. Esta parte identifica el nodo dentro de una subred. 264 direcciones para nodos son permitidas en cada subred. [4]

1.4. Protocolos de Gateway Interior

Realizaremos un cuadro comparativo de los protocolo de enrutamiento dinámicos de Gateway Interior, para identificar el protocolo de enrutamiento dinámico que más nos convenga para realizar el Proyecto, el cual se muestra en la Tabla 5.

TABLA V.
COMPARATIVA DE LOS PROTOCOLOS DE ENRUTAMIENTO DINAMICO.

Protocolo	RIPv1	RIPv2	OSPFV3	EIGRP
Nombre	Routing Internet Protocol	Routing Internet Protocol	Open Short Path First	Enhanced Interior Gateway Routing Protocol
Clase	Vector Distancia	Vector Distancia	Estado de enlace	Vector Distancia
Tipo	IGP	IGP	IGP	IGP
Distancia Administrativa	120	120	110	5(rutas sumariadas), 90 (Rutas internas), 170 (Rutas externas)
Métrica	Conteo de Saltos	Conteo de Saltos	Costo	Compuesta (Ancho de banda más retraso)
Modo	Clasfull	Clasless	Clasless	Clasless
Algoritmo	Bellman-Ford	Bellman-Ford	Dijkstra (SPF)	Dual
Convergencia	Lenta	Lenta	Rápida	Rápida

Soporta VLSM y CIDR	No	Si	Si	Si
Temporizadores (Valor por defecto en segundos)	Update (30) Invalid (180) Holdown (180) Flush (240)	Update (30) Invalid (180) Holdown (180) Flush (240)	Hello (10) Dead Interval (4 veces el tiempo de Hello)	Hello (5 seg en redes multiacceso) Hold-down (3 veces tiempo de Hello)
Formula cálculo de costo	Conteo de saltos	Conteo de saltos	100.000.000/ Ancho de banda en bps	Ancho de banda en bps+ retraso del enlace
Tipos de paquete	Query Reply	Query Reply	Hello Database Description (DBD) Link State Request (LSR) Link State Update (LSU) Link State Ack (LSAck)	Hello Update Query Reply Ack

Se revisó las características de cada protocolo de Enrutamiento de Gateway Interior y se escogió para realizar el proyecto al protocolo OSPFv3 puesto que nos brinda mejor adaptabilidad a los objetivos del Proyecto Fin de Carrera.

1.4.1. Protocolo OSPFv3

OSPFv3 es un protocolo de enrutamiento Estado-Enlace, el cual fue descrito por primera vez en el RFC 2740. El protocolo OSPFv3 trabaja con direcciones IPv6, distribuyendo por la red solamente el prefijo de estas direcciones. No posee soporte para direcciones IPv4, razón por la cual si se desea tener dentro de la misma red direcciones IPv6 y direcciones IPv4 se deben configurar tanto el protocolo OSPF como su versión 3. [5]

El protocolo de enrutamiento OSPFv3 se basa en el algoritmo de estado de enlace primero el camino más corto, por ese motivo es conveniente revisar el funcionamiento de este algoritmo.

1.4.2. Enrutamiento por Estado de Enlace

Los protocolos de estado de enlace construyen tablas de enrutamiento fundamentándose en la base de datos de la topología de la red. Esta base de datos se construye con los paquetes de estado de enlace que se pasan entre todos los routers para describir así el estado de una red. De esta manera se tiene conocimiento total de la red. [5]

Estos algoritmos de estado de enlace utilizan las siguientes características las cuales se muestran en la Tabla 6.

TABLA VI.
GENERALIDADES DE OSPFV3.

El protocolo OPSF utiliza	
Publicaciones de estado de enlace (LSA).	Una publicación de estado de enlace es un paquete de información pequeño sobre el enrutamiento, usado para realizar un seguimiento de todos los routers en el área donde se encuentra la red. Estas publicaciones proporcionan actualización de estados de enlace de redes conectadas a otros routers. Cuando existe una falla o se produce un cambio en la topología de la red, las publicaciones con enviadas en multicast. Cada router copia el estado de enlace (LSA), para proceder a la actualización de la base de datos de los estados de enlace o de la topología y luego envía la LSA a sus vecinos. Las LSA provocan que cada router dentro del área vuelva a calcular las rutas.
Bases de datos de Topología.	La base de datos está formada por la recopilación de los estados de enlace.
Algoritmo SPF y el árbol SPF resultante.	El algoritmo Primero la ruta más corta (SPF) realiza cálculos en la base de datos, y da como resultado el árbol SPF. El algoritmo SPF determina si existe conectividad en la red.
Tabla de enrutamiento con sus rutas y puertos de cada red.	El router elabora una lista de las mejores rutas a las redes destino y de las interfaces que permiten llegar a ella. Esta información se incluye en la tabla de enrutamiento.

1.4.3. Algoritmo SPF

OSPFv3 utiliza el algoritmo SPF, éste determina la mejor ruta hacia el destino. SPF añade los costes, definido como un valor basado en el ancho de banda. SPF fue creado por un informático Alemán (Edsger Dijkstra) en 1959. SPF calcula una ruta más corta y libre de bucles. [5]

Calcula costos a lo largo de cada ruta, desde el origen hasta el destino, este costo es calculado por cada router hacia cada destino en la topología. Como se muestra en la Figura 3.

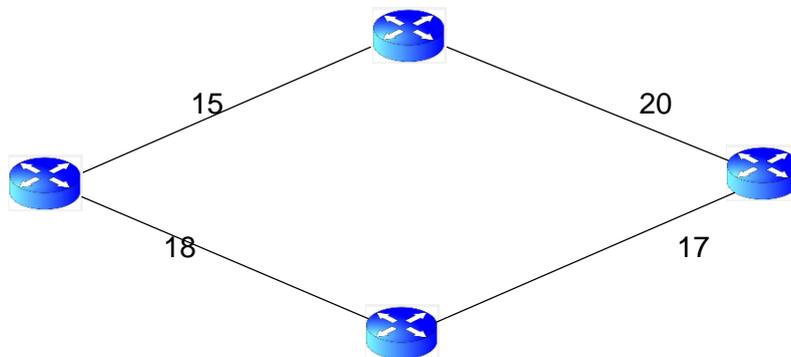


Figura 3. Algoritmo SPF

1.4.4. Paquetes OSPFv3

OSPFv3 posee 5 tipos de paquetes OSPFv3, dichos paquetes se encargan de lo concerniente al establecimiento y mantenimiento de rutas, determinación de DR y otros aspectos del protocolo. Los paquetes mencionados se muestran en la Tabla 7.

TABLA VII.
PAQUETES OSPFV3.

Nombre	Descripción
Hello	Descubre los vecinos y construye adyacencias entre ellos.
Descripción de la Base de Datos (DBD)	Controla la sincronización de la bases de datos entre los routers.
Link- State Request (LSR)	Solicita registros específicos de link- state de router a router.

Link – State Update (LSU)	Envía los registros de link-state específicamente solicitados.
Link – State Acknowledgement (LSAck)	Reconoce los demás tipos de paquetes

1.4.5. Características del protocolo OSPFv3

Características más importantes del protocolo OSPFv3, las cuales se muestran en la Tabla 8.

TABLA VIII.
CARACTERÍSTICAS DE OSPFV3.

Nombre	Descripción
Respuesta rápida y sin bucles de enrutamiento	El algoritmo SPF sobre el que se basa OSPFv3, permite un tiempo de respuesta muy rápido al momento de calcular la topología de la red. Posee un mismo mapa de toda la red el cual impide la generación de bucles de enrutamiento ni conteos.
Seguridad ante los cambios	El protocolo OSPFv3 especifica que todos los intercambios entre routers deben ser autenticados. Permite una variedad de esquemas de autenticación así como también la elección de esquemas diferentes entre un área y otra. La idea detrás de la autenticación es garantizar que solo los routers confiables difundan información de enrutamiento.
Soporte de múltiples métricas	Al momento de evaluar el camino entre dos nodos en base a diferentes métricas. Una vez elegida una métrica para el enrutamiento de un paquete, esta métrica será siempre la misma para ese paquete.
Balance de carga en múltiples caminos	OSPFv3 permite el balance de carga cuando existe más de un camino con igual costo hacia un mismo destino.

1.4.6. Tipos de áreas de OSPFv3

OSPFv3 es un protocolo complejo y requiere mucho estudio para poder comprender bien cómo funciona, y mucha práctica para poder dominarlo. Uno de los conceptos más importantes dentro de OSPF es el diseño y funcionamiento de las distintas áreas, las mismas que veremos a continuación.

- Estándar.- Es el área por defecto y permite actualización de enlaces, sumarización de rutas internas y rutas externas.
- Backbone.- Es el área principal de una topología OSPFv3. Es obligatorio que exista y todas las demás áreas deben estar conectadas a ella. Se etiqueta como área 0 y tiene las mismas características de un área estándar.
- Stub área.- Este tipo de área no acepta información acerca de rutas externas al sistema autónomo (redistribución), tales como rutas desde orígenes no OSPF. Si los routers necesitan enrutar hacia redes ubicadas fuera del sistema autónomo OSPF, utilizan una ruta por defecto (0.0.0.0/0).
- Totally stubby área.- Esta área es propietaria de Cisco y no acepta rutas de sistemas autónomos externos (redistribución).
- Not-so-stubby área (NSSA).- Casi el peor nombre del mundo escogieron para denominar este tipo. En esta área existen los LSA de tipo 7. Son similares al área Stub ya que no aceptan información de rutas externas al sistema autónomo.

1.4.7. Ventajas y desventajas del protocolo OSPFv3

El protocolo OSPFv3 Presenta las siguientes ventajas y desventajas, las cuales se muestran en la Tabla 9. [6]

TABLA IX.
VENTAJAS Y DESVENTAJAS DE OSPFv3.

Tipo	Descripción	Tipo	Descripción
	OSPFv3 ofrece rápida convergencia y escalabilidad en redes de gran tamaño.		Conlleva un alto costo de CPU y memoria del router.

Ventajas	Al ser un estándar abierto soporta dispositivos de todos los fabricantes.	Desventajas	Solo soporta el conjunto de protocolos TCP/IP.
	Cada router posee una imagen completa y sincronizada de la red.		Requiere un diseño de red jerárquico estricto para que una red se pueda dividir en áreas más pequeñas, a fin de reducir el tamaño de las tablas de topología y enrutamiento.

El protocolo OSPFv3 brinda convergencia y escalabilidad de la red de datos, es de estándar abierto y soporta dispositivos de todos los fabricantes. Permite un balance de carga de las rutas que deben ser escogidas por el router.

1.5. Protocolo BGP

Los protocolos de router externo son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de router externo la prioridad era buscar rutas óptimas atendiendo únicamente al criterio de minimizar la distancia medida en términos de la métrica elegida para la red. [7]

La selección de rutas entre sistemas autónomos plantea un problema diferente, ya que la cuestión no se reduce a la selección de la ruta óptima sino que se debe atender a criterios externos de tipo político, económico, administrativo, etc. Dependiendo de las necesidades y objetivos de la empresa.

Hasta 1990 se utilizaba como protocolo de routing externo en la Internet el denominado EGP (Exterior Gateway Protocol). Este protocolo no fue capaz de soportar el crecimiento de la Red y entonces se desarrolló un nuevo protocolo de routing externo denominado BGP. Desde entonces se ha producido 4 versiones de BGP, las especificaciones ahora vigentes de BGP-4 se encuentran en el RFC 1771.

BGP ES un protocolo de transporte fiable. Esto elimina la necesidad de llevar a cabo la fragmentación de actualización explícita, la retransmisión, el reconocimiento, y secuenciación. [7]

Es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

Por ejemplo, como se muestra en la Figura 4, los ISP registrados en Internet suelen componerse de varios sistemas autónomos (en este caso de dos redes OSPFv3 e OSPF) y para este caso es necesario un protocolo como BGP.

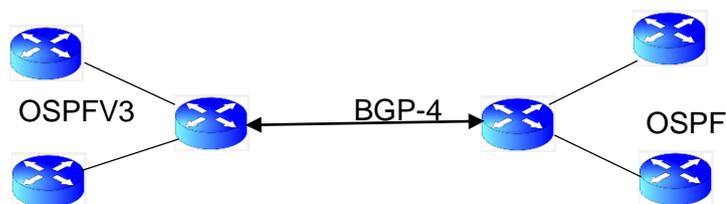


Figura 4. Estructura del Protocolo BGP.

El protocolo BGP es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. Para enviar un paquete por una ruta o por otra.

Un router BGP da a conocer sus direcciones IP a los enrutadores BGP y esta información se difunde por los enrutadores BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre enrutadores, no utiliza RIP.

Cuando se dice BGP suele hacerse referencia a la versión 4 del protocolo, en la realización del Presente Proyecto Fin de Carrera se Utilizara la versión más reciente que es BGP-4.

1.5.1. Protocolo BGP-4

BGP-4 es un protocolo propuesto como estándar. Los principales cambios se aplican al soporte de supernetting o CIDR. En particular BGP-4 soporta prefijos IP y agregación de rutas.

Los principales cambios de BGP-4 son:

- El número de versión en la cabecera es 4.
- CIDR elimina el concepto de clase de red del encaminamiento inter-dominio, sustituyéndolo por el prefijo IP.
- La lista de redes en un mensaje UPDATE se sustituyen por el NLRI.
- BGP-4 permite la negociación del valor "Hold Time" por cada conexión de modo que los extremos de la misma usen el mismo valor.

1.5.2. Tipos de Mensajes BGP-4

BGP-4 utiliza cinco tipos de mensaje para negociar sus parámetros, intercambiar la información de encaminamiento o indicar los errores. Los cuales se muestran en la Figura 10. Cada mensaje tiene un tamaño de entre 19 y 4096 bytes, y depende del TCP/IP para su entrega, secuencia miento y fragmentación. Esto implica que los mensajes múltiples BGP-4 se pueden enviar en un segmento TCP. Todos los mensajes incluyen una cabecera común de 19 bytes, y a continuación datos adicionales dependiendo del tipo de mensaje. En los mensajes BGP-4 se suele codificar la información con el formato Tipo-Longitud-Valor (TLV) para proporcionar flexibilidad, extensibilidad y facilidad en el proceso de los mensajes y de sus datos. [7]

TABLA X.
MENSAJES DE BGP-4.

Nombre	Descripción
Mensaje Open-Abrir	El primer mensaje BGP-4 que se envía después de que la conexión TCP se ha establecido es el mensaje OPEN. Este tipo de mensaje se emplea para intercambiar información de configuración y negociar los parámetros comunes de la sesión punto a punto.

Mensaje Update-Actualización	Los mensajes UPDATE se utilizan para distribuir información de encaminamiento en BGP-4, y son enviados únicamente con posterioridad al establecimiento de la sesión. Un mensaje UPDATE puede ser usado para eliminar rutas existentes, añadir nuevas rutas o ambas cosas.
Mensaje Keepalive	Los mensajes KEEPALIVE son enviados periódicamente para indicar que el enlace punto a punto se encuentra todavía operativo. Se usa para mantener activa la sesión BGP-4. El mensaje contiene sólo cabecera y ningún tipo de datos.
Mensaje Notificación	El mensaje de notificación, se envía cuando el protocolo BGP-4 detecta que se ha producido un error, después del cual se ha cerrado la sesión y la conexión TCP. La causa del error se envía al otro extremo para ser depurada.

1.6. Herramientas para emular redes

Nos permite configurar unidades virtuales de (Routers, Switches, Hosts, entre otras cosas), para poder observar el comportamiento del envío y recepción de información a través de la red, ya sea en una pequeña red LAN o algo tan extenso como el internet. [8]

Para utilizar Gns3 debemos seleccionar la imagen del tipo de router que utilizaremos en nuestra topología, GNS3 permite utilizar diferentes tipos de routers que van desde el c1700 hasta el c7200, debido que al momento de la instalación de Gns3 no viene instalado por defecto las imágenes iso. [8]

Tabla comparativa de Packet Tracer y Gns3, la cual se mostrara en la Tabla 11.

TABLA XI.
TABLA COMPARATIVA DE GNS3 Y P. T.

Es un simulador de redes	Es un simulador de redes
Fácil de usar	Fácil de usar
Fácil instalación	Fácil instalación
Gratuito	Gratuito
Trabaja con sistemas IOS reales, y no distribuye los IOS de CISCO por lo que los usuarios deben adquirirlo aparte del software GNS3	Permite la configuración global en el IOS que provee CISCO.
Apropiado para simular grandes redes, ya que permite que un cliente GNS3 pueda correr en una maquina diferente al que contiene el emulador repartiendo el procesamiento entre varios PCs.	No necesita tener dispositivos como computadoras, router, cables, etc. Para conocer el comportamiento físico y real de una red.
Viene con todas las características propias de los router, como los son las características de BGP-4-4 con IPv6.	Permite simular grandes cantidades de router y switches en un mismo computador sin inconvenientes.
Para su correcto funcionamiento requiere de un computador con altos recursos.	Permite la ejecución de la simulación en un computador con recursos básicos.

Con la información recolectada, se establece que la mejor alternativa es utilizar el emulador de redes GNS3 debido a que nos ofrecen las características totales de cada router, como los son las características de los router para utilizar BGP-4 con IPv6.

1.7. Estudio y aplicabilidad de Multihoming

El termino Multihoming se refiere a la práctica que se tiene con los proveedores de la red y los proveedores de acceso a internet, cuando se conecta con más de un enlace. Un sistema autónomo con Multihoming mantiene la conexión a internet, cuando se tiene un fallo o pérdida en una de las conexiones y es capaz de dirigir al tráfico a cualquier

destino por medio de otra conexión, entregando un servicio igual y previendo la saturación. [9]

Se emplea especialmente para fines en los que se requiere la implementación de redundancia, con perspectivas de garantizar la calidad en el servicio. Las empresas necesitan cada vez más de una conectividad hacia el internet, lo que conlleva a la necesidad de considerar adquirir un nivel de redundancia de proveedores de acceso (Multihoming), con el fin de asegurar la conectividad hacia internet cuando se necesite.

1.7.1. Formas de conexión con Multihoming

Las diferentes formas de conexiones que existe para comunicar a los proveedores de servicio de Internet con sus Clientes, se las describirá a continuación.

1.7.2. Múltiples conexiones utilizando un solo Proveedor de servicio

Consiste en la conexión de un único proveedor de servicio de internet al cual se conectan una o varias conexiones solicitando servicio de conexión a internet. Tal como se muestra en la Figura 5.

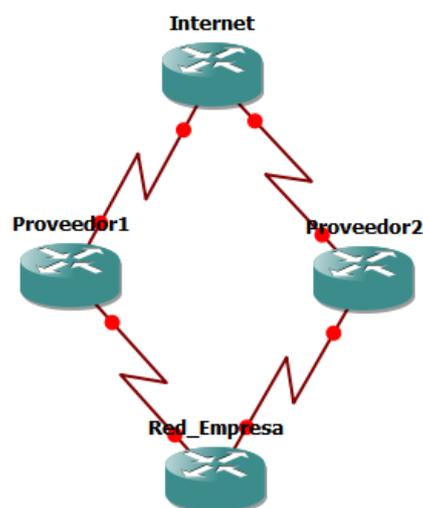


Figura 5. Multihoming con un solo proveedor

En el momento en que la conexión al proveedor de servicio de internet o el enlace físico se pierde el internet deja de funcionar, la empresa se queda incomunicada y sin acceso

a internet, convirtiéndose en una pérdida para le empresa, tal como se muestra en la Figura 6.

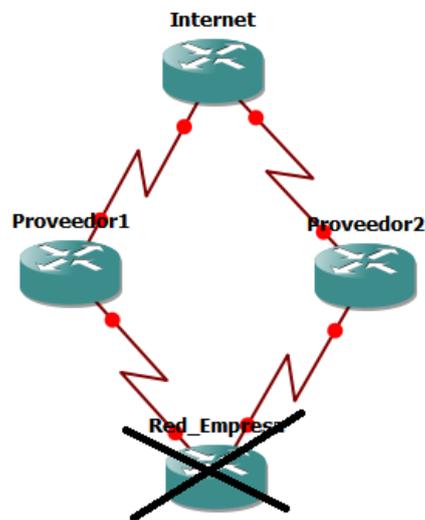


Figura 6. Pérdidas de Conexión

1.7.3. Múltiples conexiones con varios proveedores de servicio

Con el fin de dar redundancia a la red hacia el internet y evitar la pérdida de conexión, o reducir la probabilidad de que se dé la pérdida de paquetes, se utiliza una conexión a varios ISPs, lo que garantiza una alta disponibilidad de servicio de internet, ya que es menos probable que dos o más servicios totalmente independientes colapsen al mismo tiempo. Como se muestra en la Figura 7.

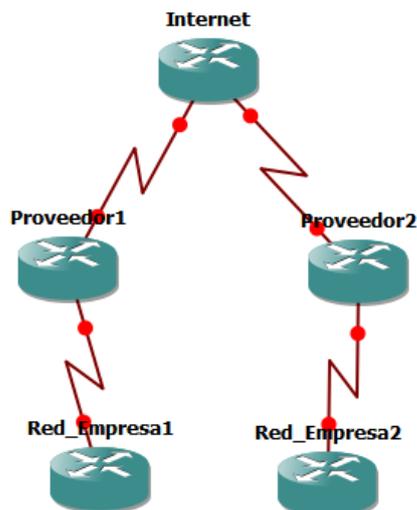


Figura 7. Múltiples conexiones con varios proveedores de servicio

Con el uso de topología mostrada en la Figura 7, si el enlace en uno de los proveedores falla, la empresa continúa con la conexión hacia el internet a través de los otros ISPs, ya que de manera automática el protocolo selecciona otra vía de comunicación hacia el internet. La pérdida de conexión de uno de los proveedores no nos dejaría sin el servicio de internet. Como se muestra en la Figura 8.

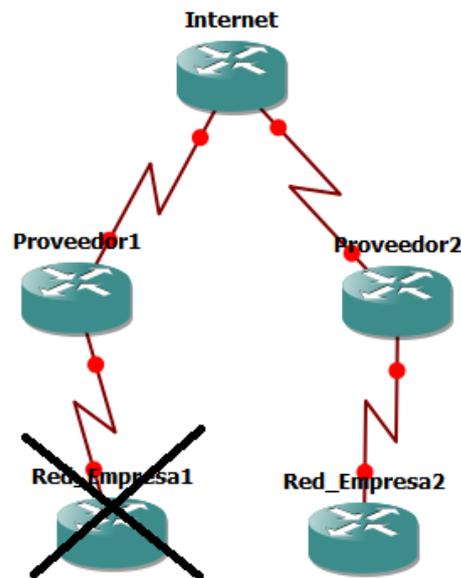


Figura 8. Pérdida de conexión hacia el ISP

Se utiliza Multihoming para brindar un plus a la empresa Xnet, utilizando al máximo las características de Multihoming, brindando así redundancia a la red de la empresa con múltiples conexiones de salida al internet.

La creciente utilización sobre Internet de aplicaciones con valor crítico, tales como la gestión de una cadena de suministros, e-commerce, transacciones financieras y comunicaciones interactivas (voz sobre IP o videoconferencia), ha sido la causa de que cada vez más empresas prefieran disponer de redes Multihoming, y de esta forma no arriesgar, al delegar todo el servicio de conectividad en un solo operador. Con la redundancia en los nodos se garantiza la conexión a Internet, y esta solución resuelve cualquier incidencia en las conexiones ya que el tráfico se distribuye entre las redes de los diferentes ISPs, con lo que el posible fallo de una queda solventado por la otra.

Según Jack Fleitman, autor del libro "Negocios Exitosos", las características principales de la pequeña y grande empresa son las siguientes: [10]

1.7.4. Multihoming en empresas pequeñas

Se debe considerar los siguientes puntos para trabajar con organizaciones pequeñas, los cuáles son:

- No pueden acceder a estos servicios porque los costos son muy altos, y su implementación es difícil.
- La comunicación se puede cortar debido a las modificaciones en los estados de los enlaces.
- Se cuenta con algunos recursos adicionales, pero muy limitados.

1.7.5. Multihoming en empresas grandes

Se debe considerar algunos puntos que son importantes al trabajar con organizaciones grandes como son:

- Multihoming con IPv6 se aplica por lo general para empresas grandes, aunque no es una restricción, se tiene que tomar en cuenta las necesidades de la organización.
- Facilita un número mayor de direcciones (128 bits), seguridades y calidad de servicio (QoS), entre algunas de sus características.
- Los diferentes fabricantes tanto de hardware como de los sistemas operativos han permitido una mejora en las aplicaciones.

1.7.6. Problemas de Multihoming

- Los costos son muy altos, debido a que la adquisición de las direcciones es elevada y los proveedores han incrementado sus valores.
- Se ha impuesto restricciones en la conectividad, estas solo deben aplicarse a los puntos de acceso de los dominios o a toda la red en la que se va aplicar Multihoming.
- La actualización del software es importante, ya que es una nueva técnica que necesita nuevas versiones del mismo.
- Se debe capacitar a los usuarios, para lograr un mejor desempeño de la aplicación.
- El tráfico de retorno no puede controlarse de manera eficaz a pesar de que se maneja calidad de servicio (QoS).

2. Análisis de la situación actual de la Empresa

La empresa XNET brinda servicio de internet, cámaras IP, mantenimiento y reparación de computadoras, se encuentra ubicada en las calles Segundo Cueva Céli Y Clodoveo Carrión de la cuida de Loja.

Historia misión visión de la empresa.

La Empresa XNET fue fundada por el Ing. Monfilio Sanmartín, el 21 de julio del 2011, comenzó brindando internet a sus vecinos, viendo en ello una forma de ayudar a la colectividad y ganar dinero, pensó en expandirse para brindar internet a la ciudadanía.

2.1.1. Misión

Proveer del acceso a las tecnologías de la información usando infraestructura de telecomunicaciones de última generación, gestionado por personal calificado para brindar un servicio acorde a las necesidades de nuestros usuarios, comprometidos al desarrollo del país y orientados a superar los desniveles culturales, económicos y sociales.

2.1.2. Visión

Ser una empresa líder en el mercado de las telecomunicaciones con innovación, servicio y dedicación a sus clientes, liderando la preferencia en la provisión de servicios de última tecnología e Internet en el país, con recursos técnicos, financieros y humanos calificados.

2.1.3. Propósito

Proveer del servicio de acceso a internet, diseño e implementación de sistemas de telecomunicaciones acorde a las necesidades del cliente, con tecnología de punta y sin limitaciones geográficas en la ciudad de Loja.

Nuestros servicios son especialmente diseñados para cubrir las necesidades de comunicación, enfocados en usuarios particulares y empresariales, con una atención

personalizada que le aseguran confiabilidad y seriedad en nuestros servicios. El orgánico estructural de la empresa Xnet de la ciudad de Loja se muestra en la figura 9.

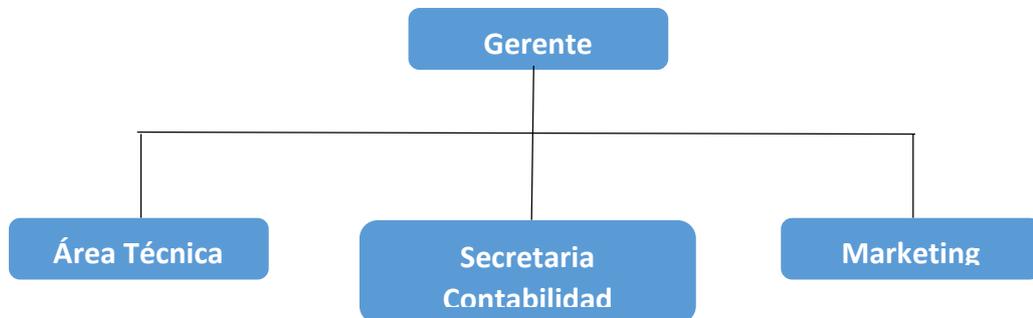


Figura 9. Orgánico Estructural

2.2. Análisis de la infraestructura en la red de datos de la empresa XNET

La Empresa Xnet Proveedor de Internet de la ciudad de Loja, ha ido creciendo en los últimos tiempos, buscando así mejorar toda su infraestructura tanto física como tecnológica, tratando así mantenerse en el auge de las empresas que proveen servicio de internet.

Actualmente la Empresa, cuenta con una Área Técnica, desde donde se lleva a cabo métodos y técnicas para mantener la infraestructura de la red de datos en óptimas condiciones en lo referente a que se encuentre activa y funcional para la transmisión de datos, voz y video. Área de secretaría y contabilidad la cual es encargada de registrar nuevos clientes, receptar el cobro de mensualidades por el pago del servicio de internet y realizar las actividades relacionadas con la contabilidad de la empresa. Área de marketing la cual es la encargada de la publicidad de la empresa, brindar al público una imagen de calidad de la empresa en cuanto a los servicios y calidad de servicio de internet que ofrece.

2.2.1. Descripción

El servicio de internet proveniente de TELCONET, llega al domicilio del gerente de la empresa el cual es conectado al router de borde, la misma que se conecta con la antena AirGrid M2 ubicada en el barrio las Palmas, esta es la antena principal de toda la conexión de la red de la empresa XNET. Desde la antena del barrio las Palmas se realiza una conexión punto multipunto con las demás antenas pertenecientes a la empresa, las mismas que están ubicadas en puntos clave de la urbe lojana para brindar internet de calidad, las fotos de las antenas se las puede ver en Anexo 3.

Cada antena cubre un área específica de la urbe lojana, las mismas que actúan como punto multipunto con los clientes conectadas a la misma, la conexión de los clientes con la antena es vía ondas electromagnéticas, las mismas que son recibidas por una mini antena ubicada en el domicilio del cliente, de la mini antena baja un cable y se conecta a la corriente eléctrica para de ahí salir un cable UTP para ser conectado al ordenador del cliente.

La empresa utiliza el protocolo de enrutamiento estático, para las antenas asignándoles así una dirección fija y constante a cada una de las mismas, pudiendo así diferenciarlas con la dirección IP. La empresa tiene un servidor central DHCP el cual asigna las direcciones dinámicas a los clientes que se conectan a la red de la empresa.

2.2.2. Proveedor de servicios de internet

El proveedor de servicios de Internet (ISP), es la empresa TELCONET-NEDETEL, que garantiza a la empresa la conexión de internet, el cual llega a la empresa mediante fibra óptica y es convertido a UTP por el conversor de fibra óptica-Ethernet, transportado al router de borde, todos estos equipos pertenecientes a TELCONET-NEDETEL. A continuación se muestra la Figura 10, la misma que muestra la topología de red de la empresa XNET de la ciudad de Loja.

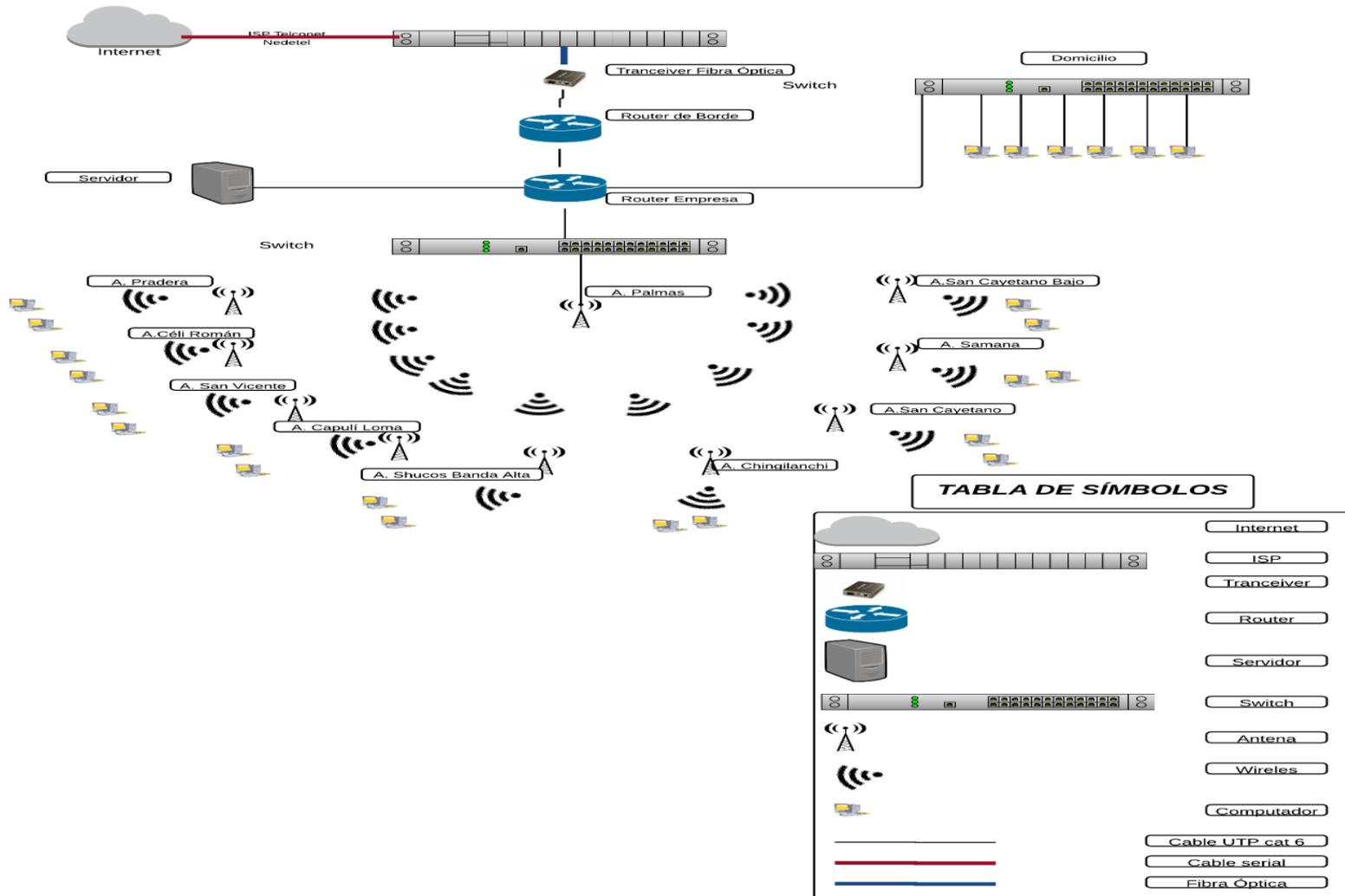


Figura 10. Topología de red de la empresa

Se muestra el backbone de la infraestructura de la red de datos, en donde se visualizan las antenas conectadas vía ondas electromagnéticas, cada antena tiene un router que le permite administrar el servicio de internet dedicado a los usuarios conectados a la misma. Cada router en la antena tiene una caja solar que le protege de los rayos solares y la lluvia.

2.2.2.1. Distribuidor central MDF (Main Distribution Frame)

En base a la información recopilada se determinó los componentes del distribuidor central (MDF) y los componentes de la distribución intermedia IDF, los mismos que se conectan con cable UTP Cat6a la misma se puede observar en el Anexo 3. El distribuidor central se encuentra en un cuarto pequeño con un área de 3,50 x 5,20 m, la cual está ubicada en el domicilio del gerente.

En la actualidad el MDF, cuenta con un sistema de alimentación eléctrica ininterrumpida (UPS) de 5KVA que provee energía eléctrica en caso de un cese de fluido eléctrico. A continuación se muestra en la Figura 11 los elementos que conforman el MDF, los IDF se encuentran en cada torre de la empresa, protegidos del agua y sol por una caja solar.

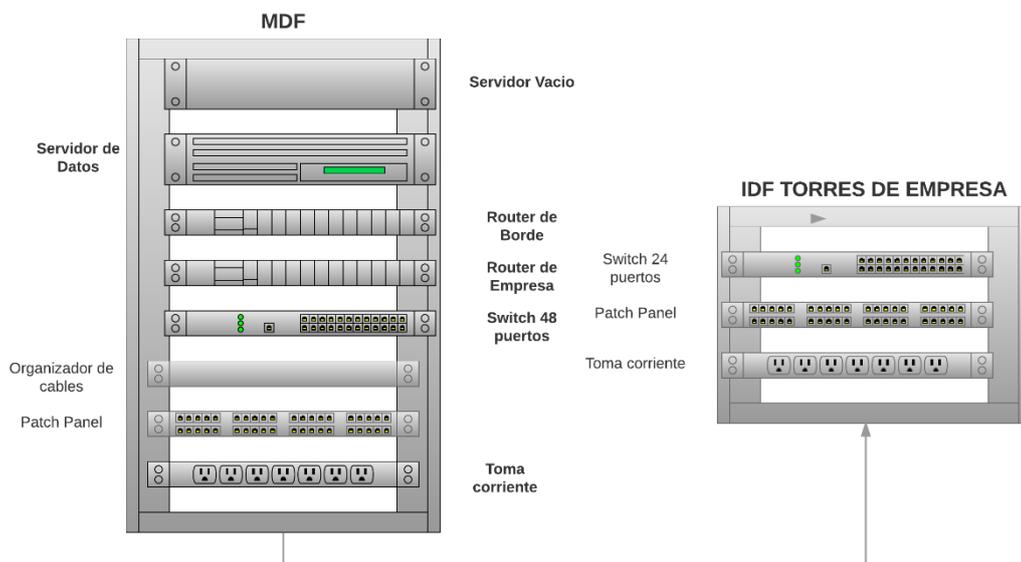


Figura 11. Distribución del MDF e IDF

2.3. Personal de la empresa

Las siguientes personas desarrollan sus actividades laborales en la empresa Xnet.

Gerente.

Funciones:

- Planificar, ejecutar, controlar y evaluar actividades de desarrollo dentro de la empresa, para que faciliten la gestión de los diversos procesos dentro de la misma.
- Brindar asesoría y asistencia técnica en la adquisición de hardware y software para la empresa.
- Monitorear el correcto funcionamiento de la redes de la empresa.
- Capacitar al personal que se integre a laborar a la empresa.
- Realizar instalaciones de nuevos clientes.

Técnico de soporte y mantenimiento

Funciones:

- Realizar instalaciones de servicio de internet, cámaras IP a los clientes.
- Realizar el marketing de la empresa por medio de redes sociales.
- Brindar mantenimiento a equipos de la empresa.
- Brindar asesoría de los servicios que ofrece la empresa a los clientes.

Secretaria/Contabilidad

Funciones:

- Realizar los cobros de los servicios que brinda la empresa.
- Mantener la agenda al día del gerente.
- Realizar la contabilidad de la empresa.

2.4. Planes de servicio de Internet que ofrece la Empresa

Los planes de servicio de internet que ofrece la empresa, se adaptan a las necesidades de los clientes, puesto que la empresa brinda varios planes de internet. Los planes que la empresa brinda son:

- **xPlan para el Hogar.-** En el cual ofrecen planes de Internet ilimitado residencial con la mejor velocidad y al menor precio. Ofrecen descuentos a las personas que

contratasen el servicio y que fuesen personas discapacitadas legalmente establecidas. A continuación se muestran los planes en la Tabla 12.

TABLA XII.
XPLAN PARA EL HOGAR.

Velocidad/Ancho de Banda	Nivel de compartición	Costo Mensual
2 Mbps	6:1	\$ 17.00
2.5 Mbps	6:1	\$ 25.80
3 Mbps	6:1	\$ 39.80
3.5 Mbps	6:1	\$ 58.80
4 Mbps	6:1	\$ 89.80

- **xPlan Empresarial.-** En el cual ofrecen planes de Internet ilimitado con un nivel de compartición más bajo que puede ser útil para empresas, hoteles, centros educativos, condominios, departamentos, casas de arriendo etc. Ofrecen descuentos a las personas que contratasen el servicio y que fuesen personas discapacitadas legalmente establecidas. A continuación se muestran los planes en la Tabla 13.

TABLA XIII.
XPLAN EMPRESARIAL.

Velocidad/Ancho de Banda	Nivel de compartición	Costo Mensual
1 Mbps	1:3	\$ 45.50
1.5 Mbps	1:3	\$ 54.50
2 Mbps	1:3	\$ 89.80

- **xPlan Cybers.-** En el cual ofrecen planes de Internet ilimitado con un nivel de compartición más bajo para Cybers y pymes para conexión a servidores de juegos locales, servidores TeamSpekers, para salas de conferencia y cursos en línea mediante VOIP, con las latencias más bajas para que no haya interrupción de servicios. Ofrecen descuentos a las personas que contratasen el servicio y que fuesen personas discapacitadas legalmente establecidas. A continuación se muestran los planes en la Tabla 14.

TABLA XIV.
XPLAN CYBERS.

Velocidad/Ancho de Banda	Nivel de Compartición	Costo Mensual
1 Mbps	1:1	\$ 125.00
2 Mbps	1:1	\$ 240.00

La empresa cuenta con una página de Facebook la cual es <https://www.facebook.com/internetxnet?fref=ts> y también tiene una página web que es <http://www.xnet.net.ec/> en la cual se puede consultar todo tipo de duda acerca del servicio que presta la empresa.

e. Materiales y Métodos

1. Materiales

Para realizar el Proyecto Fin de Carrera se utilizan los recursos materiales y humanos descritos en la siguiente Tabla 15.

TABLA XV.
MATERIALES Y MÉTODOS.

Talento Humano			
Rol	Tiempo (Horas)	Valor Hora (\$)	Valor Total (\$)
Investigador	350	3.00	1050.00
Subtotal (\$)			1050.00
Recursos Técnicos			
Recursos Hardware			
Descripción	Cantidad	Valor Unitario (\$)	Valor Total (\$)
Computador P.	400 horas	2.00	700.00
Pendrive	2	10.00	20.00
Subtotal (\$)			720.00
Recursos Software			
Descripción	Cantidad	Valor Unitario (\$)	Valor Total (\$)
Latex	1	0.00	0.00
GanttProject	1	0.00	0.00
Herramienta de emulación GNS3.	1	0.00	0.00
Subtotal (\$)			0.00
Recursos Materiales			
Servicios			
Descripción	Cantidad	Valor Unitario (\$)	Valor Total (\$)
Transporte	400 días	0.60	240.00
Internet	140 días	0.50	70
Subtotal (\$)			310.00
Materiales			
Descripción	Cantidad	Valor Unitario (\$)	Valor Total (\$)
Impresiones	300	0.15	45.00
Varios	1	30.00	20.00
Subtotal (\$)			65.00
Tota (\$)			2020.00

2. Métodos

Se utilizan los siguientes métodos para el análisis de la información de la empresa XNET, los cuales se describen a continuación.

Método Sistemático.- Entender las características primordiales del sistema bajo estudio como lo son elementos de la red, medios de transmisión que se utiliza en la empresa, el entorno de la estructura general de la empresa, herramienta para la emulación GNS3, comandos para la configuración de la topología, direccionamiento IPv6 el entendimiento de estos complementos nos ayudan a realizar el Proyecto Fin de Carrera.

Método Deductivo.- Ayudó a tener una perspectiva general sobre el impacto que provocara la implementación del sistema de la red implementándolo con Multihoming junto con el direccionamiento IPv6, en la empresa Xnet de la ciudad de Loja.

Método Inductivo.- Permitió conocer a detalle los problemas que acarrea la falta de un sistema que brinde redundancia al proveedor ISP de la empresa y los beneficios que nos podría brindar a la empresa en el ámbito publicitario y el prestigio a la misma.

2.1. Técnicas

Entrevista: Se aplicó al gerente de la empresa Xnet de la ciudad de Loja, al técnico encargado de la parte de mantenimiento e instalación del servicio, para obtener información sobre cómo se realizan los procesos internos y externos de la empresa y los procesos correspondientes al manejo de la red.

Observación Directa.- Se utilizó para determinar los problemas que ocasiona no contar con un sistema Multihoming integrado; a través de las fichas de observación se establecieron los procesos y el manejo de la red de la empresa.

2.2. Metodología de Desarrollo del Proyecto.

Se eligió la metodología Top-Down porque permite al diseñador de red conocer las solicitudes, requerimientos del usuario primero para luego moverse en espiral hacia abajo según las exigencias requeridas. Con la metodología Top-Down Network Design se diseña una red en base a la popularización, encapsulación o segmentación empezando de arriba hacia abajo. La cual propone 4 fases que se describen a continuación en la tabla 16.

TABLA XVI
METODOLOGÍA TOP-DOWN NETWORK DESIGN.

Metodología Top-Down Network Design [11]	Metodología aplicada al proyecto
<p>Primera Fase.- Analizar metas del negocio, Analizar la red existente, explorar el tráfico de la red.</p>	<p>Primera Fase.- Se realizó el levantamiento de información a través de la observación directa a las instalaciones físicas de la institución, además se aplicó una entrevista al gerente y técnico de la empresa, para conocer la situación actual de la empresa, las entrevistas se encuentran en el anexo 1 y 2.</p>
<p>Segunda Fase.- Diseñar una topología de la red, diseñar direccionamiento IP, seleccionar protocolo de enrutamiento.</p>	<p>Segunda Fase.- Una vez obtenida la información se diseñó la propuesta de la topología de la red para la parroquia sagrario con su direccionamiento IPv6, sus protocolos OSPFv3 y BGP adaptados con IPv6 y se realizó un análisis de Multihoming que se aplicara.</p>
<p>Tercera fase.- Configuración de la topología. Utilizando los protocolos de enrutamiento y direccionamiento expuestos en la segunda fase.</p>	<p>Tercera Fase.- Se realizó la configuración de la topología en GNS3 de la red de la parroquia Sagrario. Utilizando el protocolo de internet IPv6, protocolo de enrutamiento OSPFv3 y protocolo de enrutamiento Exterior BGP-4 con Multihoming.</p>
<p>Cuarta fase.- Probar el diseño de la red, documentar el diseño de la red.</p>	<p>Cuarta Fase.- Se diseñó un plan de pruebas, para verificar si la red cumple con el propósito por el cual fue creada, se prueba la funcionalidad del protocolo OSPFv3, BGP-4 y Multihoming realizando ping de conectividad de direcciones virtuales de nuestra red a direcciones virtuales de una red alterna</p>

	<p>creada específicamente para las pruebas. Para la prueba de funcionamiento de Multihoming se desactivara un enlace del router receptor de la red de la empresa al router proveedor que por defecto se ha configurado, levantándose así automáticamente el enlace de respaldo que se tiene, para que así no se pierda la conectividad de internet de la empresa, y así se probara con el otro router de borde.</p>
--	---

f. Resultados

Corresponde al desarrollo práctico del proyecto de investigación, para lo cual se sigue la metodología Top-Down Network Design, la cual consta de las siguientes 4 fases.

1. Primera Fase.- Análisis de la red de la empresa XNET de la parroquia el sagrario.

En esta fase se describe la situación actual de la red de la parroquia sagrario, los datos obtenidos son el resultado de la información proporcionada por el gerente y técnico en las entrevistas que se realizó, las cuales se muestran en el Anexo 1 y 2.

La red de la parroquia sagrario, está compuesta de tres antenas AirGrid M2, las mismas que tienen una capacidad de alcance de 5 km, acaparando así a todo cliente ubicado en ese sector. Cada antena actúa como punto multipunto con los clientes conectados a la misma, a cada cliente se le proporciona una mini antena para que con esta sea capaz de recibir la señal de internet enviada por la antena. Para que la conexión del cliente tenga buena señal la visibilidad de la antena de la empresa con la mini antena del cliente no debe tener obstáculos obstruyendo su conexión visual. La obstrucción visual de la antena AirGrid M2 con la mini antena del cliente producirá que la señal que normalmente debería llegar, no la haría de la misma forma, puesto que la obstrucción mermaría la señal normal de internet que se le brinda al cliente.

1.1. Ubicación de las antenas AirGrid M2 en la cuida de Loja

La ubicación de las antenas se las ha realizado por medio de un análisis posicional de acuerdo a la geografía de la urbe lojana y en particular a la de la parroquia Sagrario, tomando como referencia los puntos más altos de la Parroquia, la cual se muestra en la Figura 12. La visibilidad de la antena con la mini antena del cliente debe ser nítida sin obstáculos. La antena ubicada en el barrio céli román esta en las calles José miguel friofrío y ramón burneo, la antena ubicada en el barrio las palmas esta en las calles segundo cueva céli y Daniel Álvarez Burneo y la antena ubicada en el barrio san cayetano esta en las calles Checoslovaquia y Moscú.

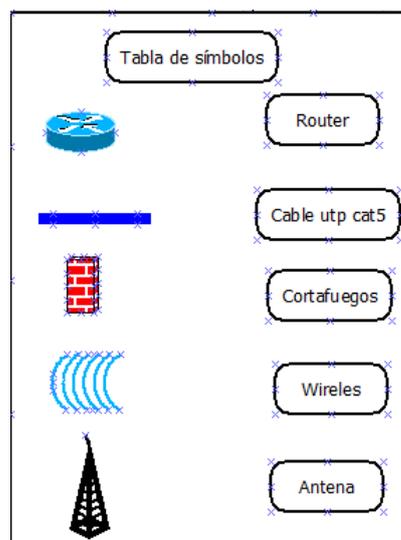
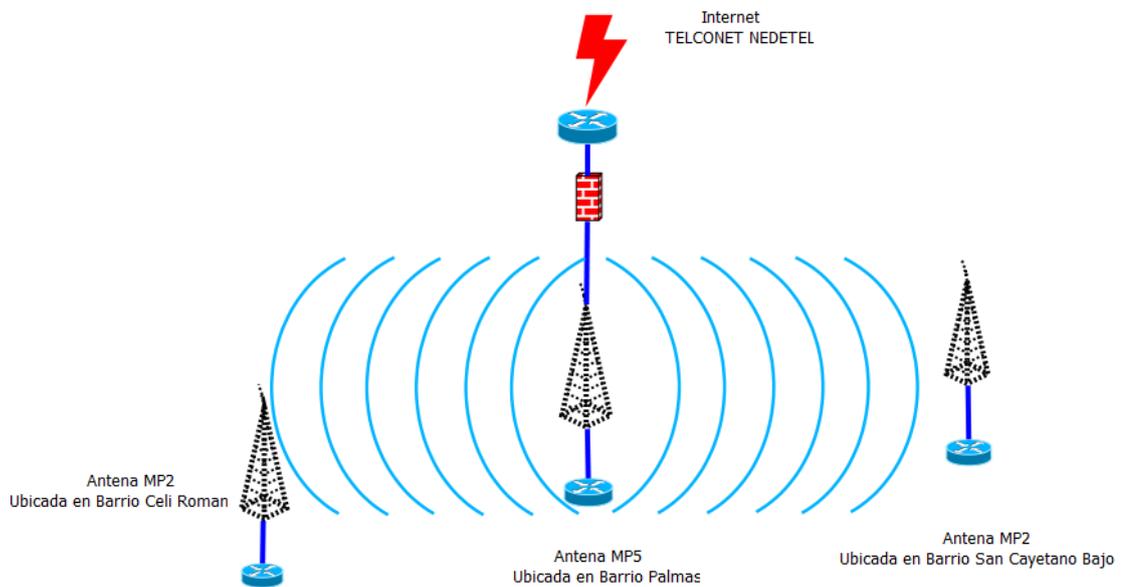


Figura 12. Red Sagrario

Las antenas palmas, celi román y pradera, esta ubicadas en viviendas de usuarios, las mismas que trabajan con luz de las propias viviendas, siendo esta una de las falencias que tiene las antenas, ya que si se fuera la luz en la vivienda por algún acontecimiento fuera de lo normal, se dejaría sin servicio de internet a los clientes conectados a la antena. La solución sería implementar un UPS en cada antena de la red, pudiendo así rescatar el servicio de internet para esos clientes, hasta que se arregle el problema de la luz eléctrica.

1.2. Descripción de dispositivos de la red

Se realizó una descripción de los dispositivos principales que tiene la red Sagrario.

- **Router Receptor.-** Este router recibe el internet del proveedor Telconet NEDETEL, y a su vez se conecta con el router Palmas. Este ruteador facilita la interconexión de las diferentes redes con las que cuenta la empresa determinando cual es la mejor ruta que deben tomar los paquetes para llegar a su destino. Es la puerta de entrada y salida de los paquetes de la empresa hacia el internet.
- **Antena del router Palmas.-** Es la encargada de primero recibir la señal del router Receptor, segundo transmitir la señal que recibe del router receptor a las demás torres de la red Sagrario actuando como antena multipunto con las demás antenas de la red Sagrario.
- **Antena de céli román y san cayetano.-** La función es recibir la señal de la antena palmas para así brindar servicio de internet a los clientes que se conecten a la misma. Estas antenas tienen la función de punto multipunto, actuando como antena emisora de la señal de internet para los clientes que se conecten a ella.
- **Router de la antena palmas.-** Este router es el principal de la empresa, puesto que actúa como punto multipunto con los demás router de las antenas de la empresa, tiene incorporado las IPTables para realizar el control del tráfico de la red.
- **Router de las antenas céli román, palmas y san cayetano.-** Son los receptores de la señal de internet proveniente del Router palmas, y a su vez actúa como punto multipunto con los clientes que le corresponde en la parroquia.

Los mismos que se encuentran protegidos por una caja solar para protegerlos del medio ambiente, evitando así daños relacionados al sol, lluvia, polvo, etc.

1.3. Clientes de la red sagrario

La red de la parroquia sagrario cuenta con un aproximado 150 clientes conectados a la red de la empresa. Tiene 130 clientes conectados con el plan xPlan para el Hogar, que es para clientes residenciales. También tiene 12 clientes que les brinda el servicio de XPlan Empresarial que es dedicado a empresas y hoteles de la ciudad. Tenemos 8 clientes que se les brinda el xPlan Cyber que es con un nivel de compartición más alto para Cybers y pymes para conexión a servidores de juegos, a cada cliente del plan se le proporciona una router para que pueda administrar el plan de internet a sus clientes.

1.4. Direccionamiento de la red sagrario

La red de la parroquia Sagrario tiene un direccionamiento IPv4, con el cual abastece de direcciones IPs a los clientes de la red. El bloque de direcciones que tiene la empresa esta subneteadado, se la ha asignado a cada antena una subred específica con el fin de que se pueda identificar de una mejor manera las antenas de la red sagrario. Se muestra en la tabla 17 el direccionamiento IPv4 de la empresa XNET.

TABLA XVII.
DIRECCIONAMIENTO DE LA RED.

Antena	Dirección Ipv4
Pradera	192.168.X.X
Céli Román	192.168.X.X
San Vicente	192.168.X.X
Capulí Loma	192.168.X.X
Shucos Banda Alta	192.168.X.X
Chingilanchi	192.168.X.X
San Cayetano	192.168.X.X
Samaná	192.168.X.X
Palmas	192.168.X.X
Valle	192.168.X.X

1.5. Protocolo de enrutamiento de la red sagrario.

El protocolo de enrutamiento que se utiliza en la red sagrario para la distribución interna de la red es el protocolo OSPF, soporta VLSM y CIDR. La red está dividida en dos áreas, el área 0 es la principal en la cual está el router de borde y a la cual se conecta el área 1 que son los demás router de la red.

Para que OSPF tenga actualizada la tabla de enrutamiento entre los nodos de la red, utiliza los paquetes. Paquete **Hello** los cuales se envían periódicamente a sus vecinos, el cual contiene el listado de vecinos activos del router. Paquete **LSA** son los cambios en el estado de los enlaces de los router. En la empresa XNET se tiene dividida la red mediante áreas las mismas que nos permiten ordenar de acuerdo a las redes internas de la empresa. El router receptor actúa como router límite de sistema autónomo ASBR. El router palmas actúa como router ABR que es el encargado de generar los enlaces de resúmenes para así diseminar la información entre los routers de la empresa.

Los router internos de la red Sagrario (Palmas, San Cayetano y Céli Román), son capaces de encaminar cualquier paquete a cualquier punto del área que está asociadas. En la red tenemos un Router Fronterizo del AS (ASBR), que es el Router Receptor, que nos permite encaminar paquetes fuera del sistema autónomo de la red Sagrario.

1.6. Seguridad de la Red Sagrario

La seguridad de la red es un factor importante que tiene implementada la empresa. Tiene incorporado WPA2 como control de Acceso, proporciona a los clientes de la red un alto nivel de seguridad en el que sólo los usuarios autorizados pueden acceder a la red. Basado en el estándar IEEE 802.11i ratificado, verifica los usuarios de la red a través de un servidor. La herramienta utilizada a nivel de software para levantar el firewall en los servicios de internet (dns, dhcp, proxy, router, http, smtp, pop, ect) es: IPTables que viene preinstalada en la distribución de Centos v. 5.4, IPTables incluye un módulo que permite a los administradores de red inspeccionar y restringir conexiones a servicios disponibles en la red.

En iptables las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes ip. Existen tres cadenas básicas INPUT (entrada), OUTPUT (salida) y FORWARD (reenvió), al administrador puede crear tantas como desee.

2. Segunda Fase.- Diseñar la red de la parroquia sagrario

El diseño de la topología, implica adaptar los equipos de la red al ambiente de trabajo, de tal manera que los recursos de la red sean aprovechados optimizando recursos y dinero. Para diseñar la nueva red se tomó como base el posicionamiento de las antenas de la red anterior como se muestra en la Figura 13, en esta red implementaremos para los router internos de la empresa el protocolo OSPFv3, y para los router externos el Protocolo BGP.

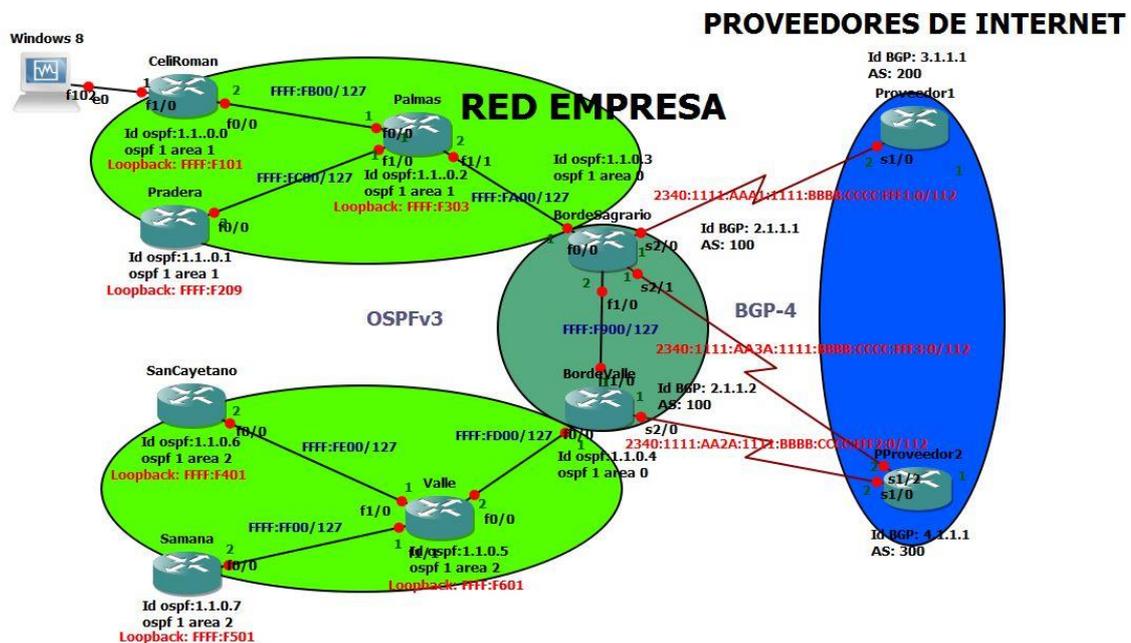


Figura 13. Topología de la nueva red sagrario

La propuesta que se realizó tiene dos routers de borde, dos proveedores de internet, permitiendo así brindar redundancia a la red de la empresa, la utilización de varios ISP brinda un plus, un extra a la empresa para poder brindar el servicio de internet redundante a fallos y fiable para sus clientes.

2.1. Análisis de BGP y OSPFv3 que se implementa

Estos son los protocolos que sirven para el enrutamiento externo e interno de la red de la empresa.

2.1.1. Análisis de BGP-4

El protocolo BGP-4 sirve para la comunicación de la red de la empresa con redes externas y permite comunicación entre sistemas autónomos como se muestra en la Figura 14.

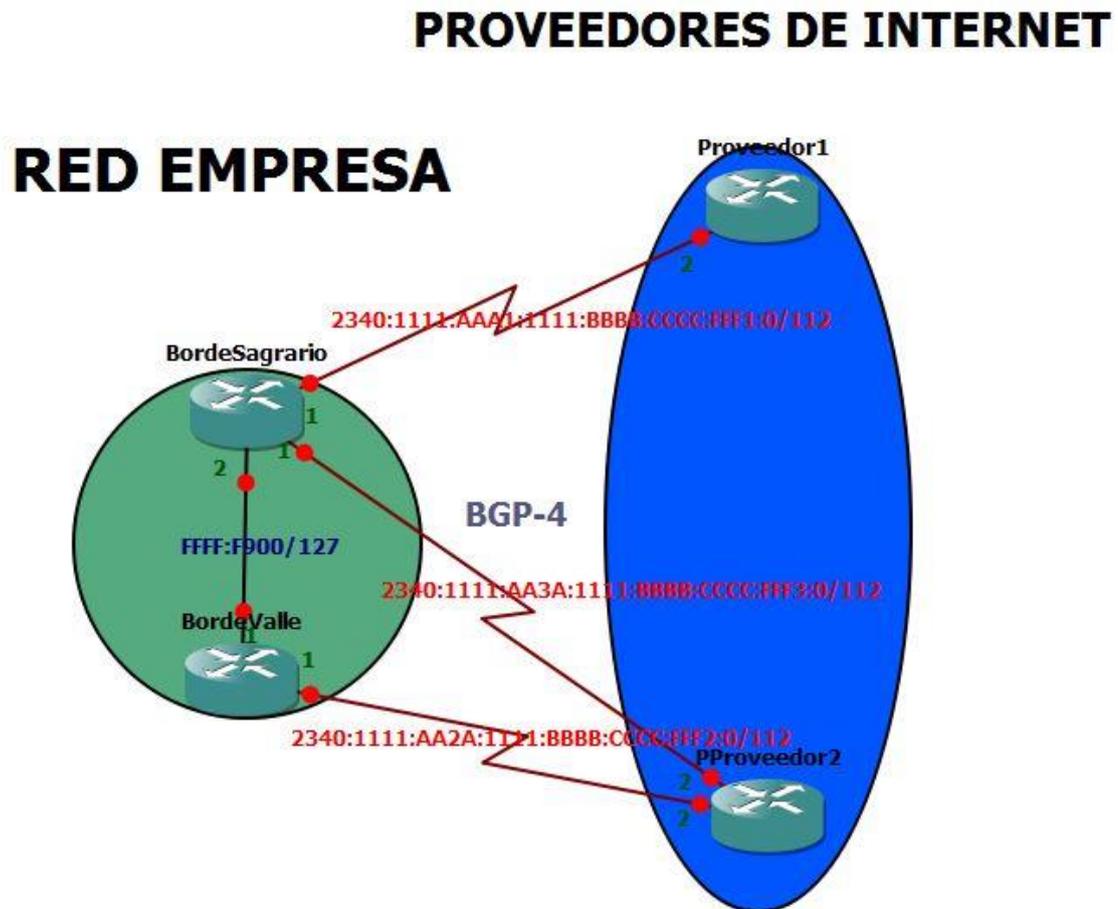


Figura 14. BGP-4 en la empresa.

La configuración de BGP-4 tiene dos routers de borde, el router de borde sagrario tiene implementado una salida principal que es hacia el router proveedor 1 y dos salidas secundarias que son hacia el router proveedor 2 y router borde valle. El router de borde valle tiene implementado una salida principal que es hacia el router proveedor 2 y una salida secundaria hacia el router de borde sagrario. La publicación de las rutas desde la red de la empresa hacia el internet será total, permitiendo así la salida de todas las subredes de la empresa.

2.1.2. Análisis de OSPFv3

El protocolo OSPFv3 nos sirve para la comunicación interna de la red como se muestra en la Figura 15.

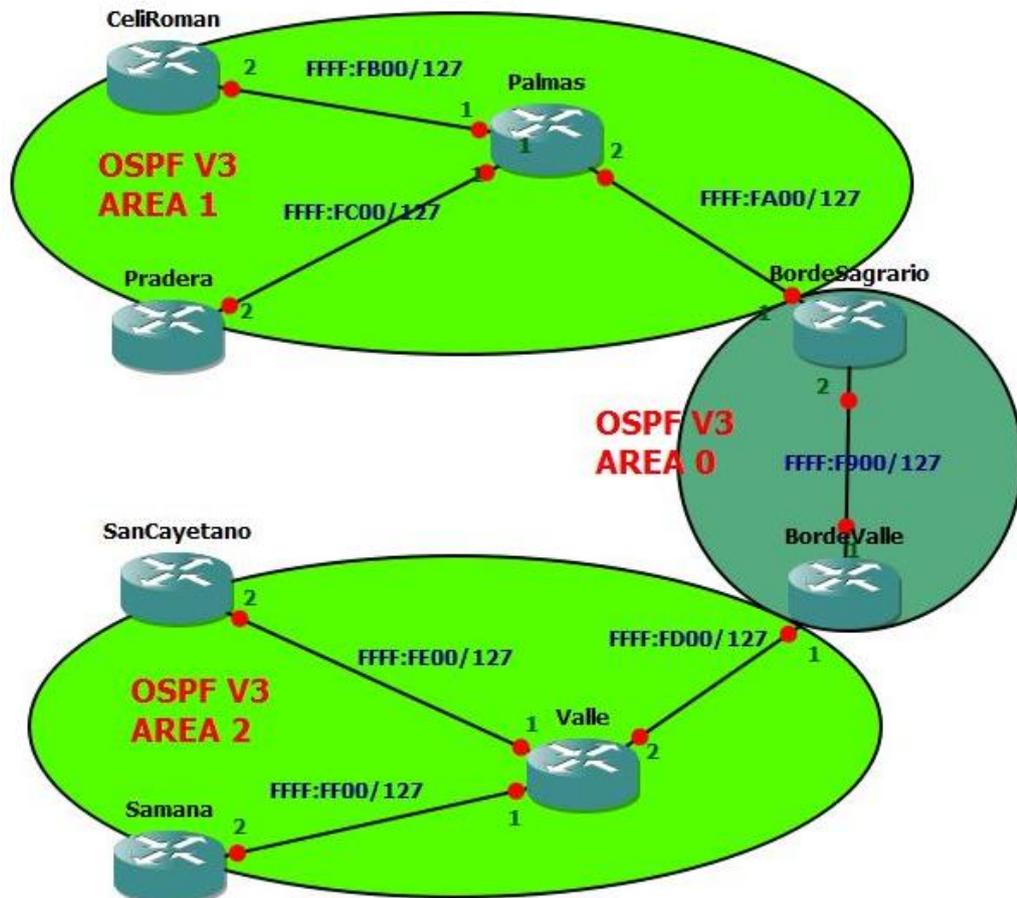


Figura 15. OSPFv3 en la empresa.

En la red de la empresa se configura el protocolo de enrutamiento dinámico OSPFv3 que es el que soporta el protocolo de internet IPv6, con esta configuración cada router puede elegir la mejor ruta para alcanzar cada destino dentro del sistema autónomo. Tiene configurado un área central o backbone, es el área principal de la topología y todas las áreas están conectadas a ella. El área 1 comprende a los routers que se conecta al router de bordesagrario, y permite controlar las actualizaciones de estado de enlace y la inundación de paquetes dentro de la red. El área 2 comprende a los routers que se conectan al router bordevalle, y permite controlar las actualizaciones de estado de enlace y la inundación de paquetes dentro de la red.

2.2. Análisis de Multihoming que se implementa

La red de la empresa que se diseño trabaja con 2 dos proveedores de internet, los cuales están conectados a los router de borde de la red de la empresa. La configuración de Multihoming se realizó en los router de borde y los proveedores de internet.

2.2.1. Multihoming en el router de borde Sagrario

En el router bordeSagrario está configurado Multihoming el cual permite tener tres caminos de salida hacia el exterior, los caminos se muestran en la Figura 16.

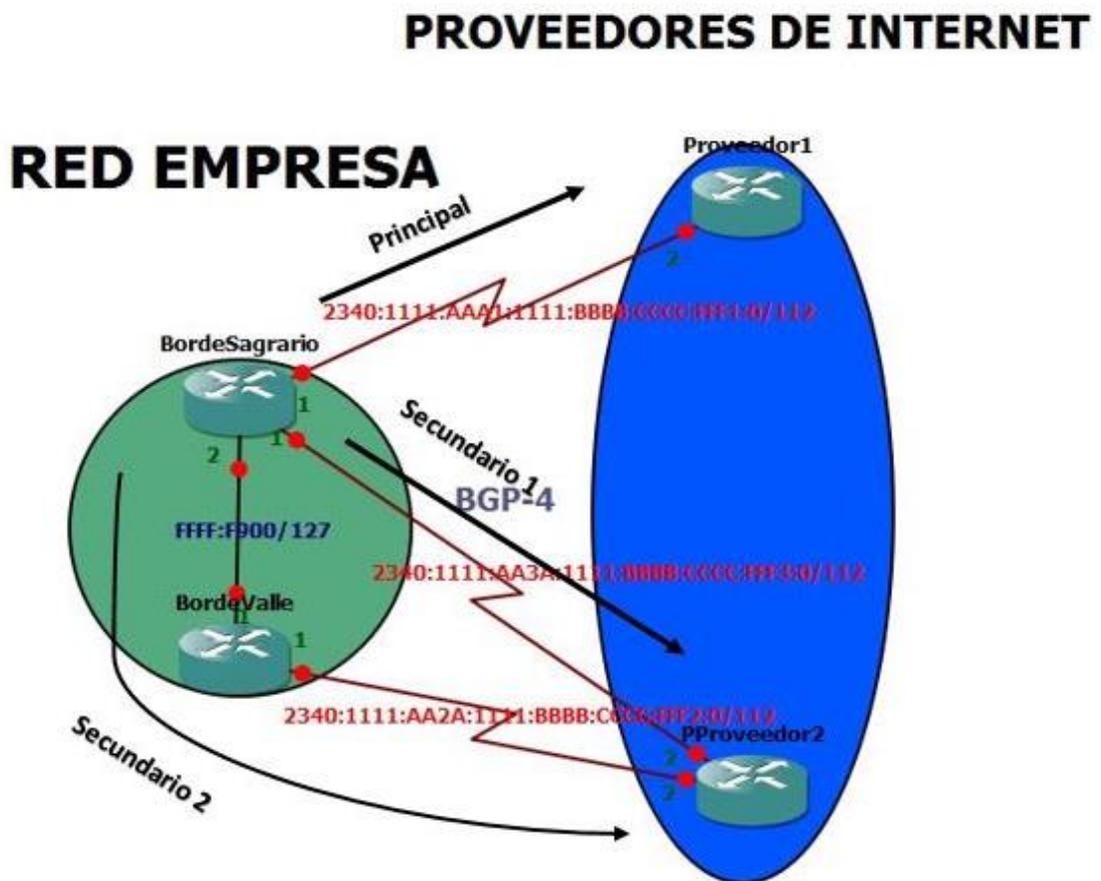


Figura 16. Multihoming borde sagrario.

La salida principal hacia el exterior es la que va dirigida hacia el router proveedor 1, al momento que ocurra algún fallo en el enlace principal, automáticamente se establecerá el enlace secundario 1 como principal, el enlace secundario 1 es la que está dirigida hacia el router proveedor 2 y todo el tráfico de la red sagrario se dirigirá hacia el mismo, la tabla de enrutamiento del router borde sagrario se actualizara con la vía de salida por

el router proveedor 2. Si ocurre una falla en el enlace secundario 1, automáticamente se establecerá el enlace secundario 2 como principal, el enlace secundario 2 es la que está dirigida hacia el router de borde valle y todo el tráfico de la red sagrario se dirigirá hacia el exterior por medio del router borde valle, la tabla de enrutamiento del router borde sagrario se actualizara con la vía de salida por el router de borde valle.

2.2.2. Multihoming en el router de borde Valle

En el router bordevalle está configurado Multihoming el cual nos permite tener dos caminos de salida hacia el exterior, los caminos se muestran en la Figura 17.

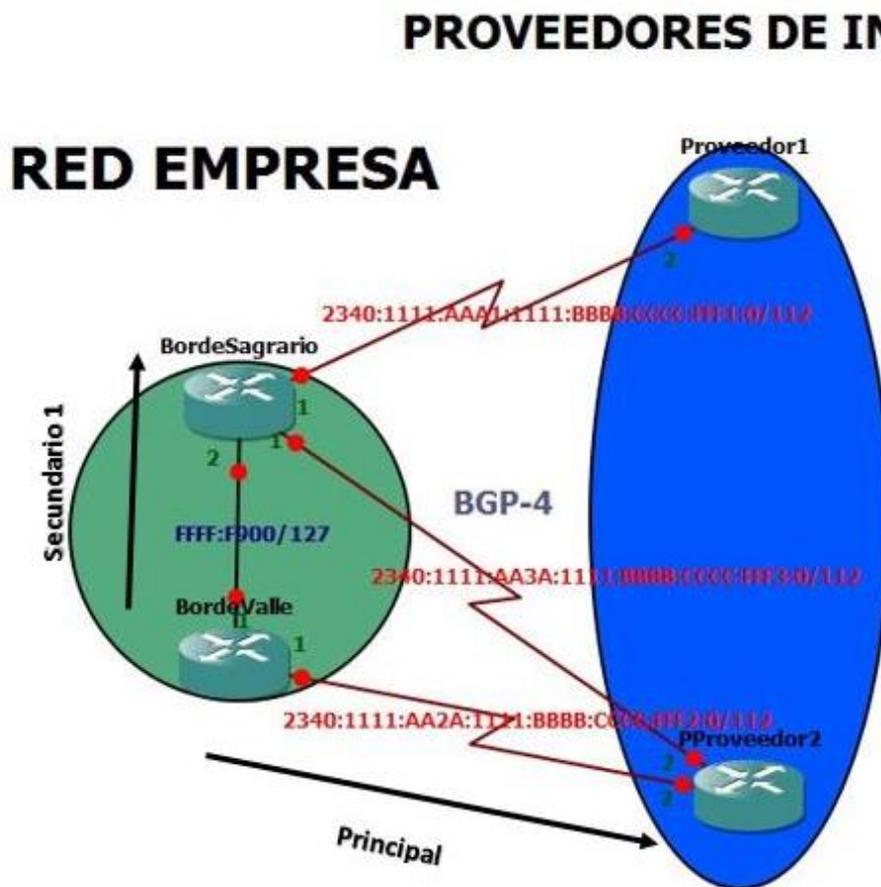


Figura 17. Multihoming borde valle.

La salida principal hacia el exterior es la que va dirigida hacia el router proveedor 2, al momento que ocurra algún fallo en el enlace principal, automáticamente se establecerá el enlace secundario como principal, el enlace secundario es la que está dirigida hacia el router de borde sagrario y todo el tráfico de la red valle se dirigirá hacia el exterior por

medio del router borde sagrario, la tabla de enrutamiento del router borde valle se actualizara con la vía de salida por el router de borde sagrario.

2.3. Topología de la Nueva red sagrario

La topología que se propone es con dos routers de borde dividiendo las antenas en dos grupos de acuerdo a la ubicación. Como se muestra en la figura 18.

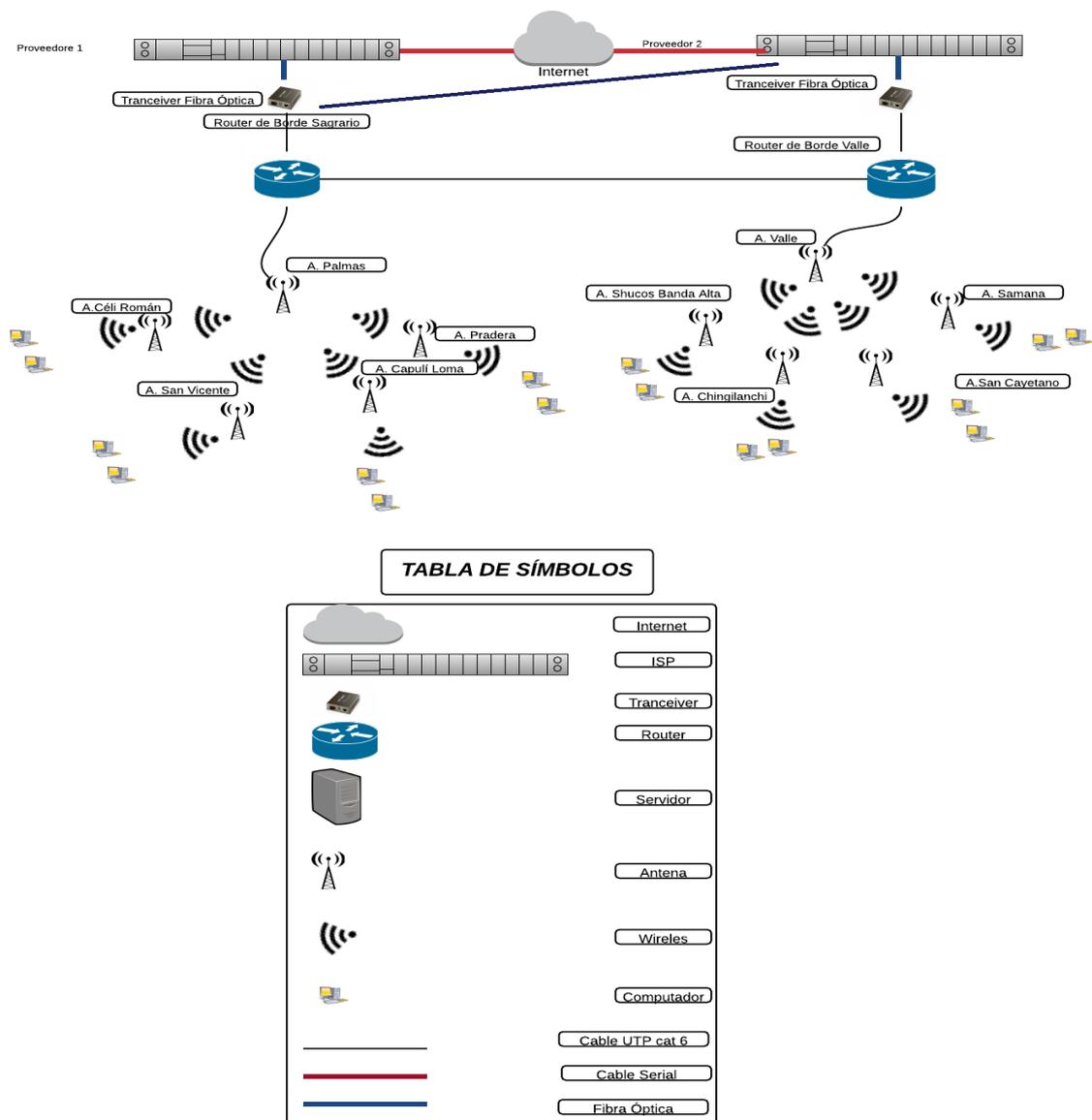


Figura 18. Topología de la red sagrario.

La topología que se propone es en forma de árbol, tiene los router de borde que son a los cuales llega el internet y desde los cuales se distribuye el servicio de internet a los demás routers de la empresa.

2.4. Porque utilizamos IPv6

La cantidad de los clientes cada día va en aumento en la empresa XNET, teniendo esto en mente, nos abordamos en el mundo de IPv6. Por la cantidad de IPs que nos proporcionan, las seguridad incorporada en la misma dirección y se da un paso al avance de servicio de internet, un paso al futuro, innovar en la provincia siendo los primeros en brindar el servicio de internet con el protocolo de Internet IPv6.

Para pedir un bloque de direcciones de IPv6 la empresa deberá cumplir con 3 peticiones que son: Primera llenar un formulario que sirve como solicitud para pedir el bloque de direcciones, segundo deberá proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses. Tercero se realiza planes de direccionamiento por al menos un año y elaborar una descripción detallada de la topología de la red.

De acuerdo al número de clientes que actualmente maneja la red de la empresa Xnet que es de 500 clientes, lo que se quiere en la empresa es aumentar el número de clientes, promoviendo y publicitando que la empresa va a brindar servicio de internet con el Protocolo IPv6, adoptando así todos los beneficios del protocolo IPv6, pudiendo así brindar un servicio proyectado al futuro de los ISP.

2.5. Direccionamiento IPv6 para la red sagrario

De acuerdo a los requerimientos de la empresa se ha elaborado el siguiente bloque de dirección IPv6 que es una dirección unicast global enrutable, el cual se Muestra en la tabla 18.

TABLA XVIII.
BLOQUE DE DIRECCIÓN DE LA EMPRESA.

Bloque de Dirección que se asigna a la empresa
2340:1111:aaaa:1111:bbbb:cccc:ffff:f/120

Teniendo para uso de la empresa los tres últimos dígitos del bloque de la dirección asignada. De los tres últimos dígitos escogemos 1 digito para que se para las subredes y los últimos dos para que sirva para los host de la empresa. Teniendo las siguientes subredes, las cuales se muestran en la tabla 19.

TABLA XIX.
TOTAL SUBREDES DE LA EMPRESA.

Número	Dirección
1	2340:1111:aaaa:1111:bbbb:cccc:ffff:f000/120
2	2340:1111:aaaa:1111:bbbb:cccc:ffff:f100/120
3	2340:1111:aaaa:1111:bbbb:cccc:ffff:f200/120
4	2340:1111:aaaa:1111:bbbb:cccc:ffff:f300/120
5	2340:1111:aaaa:1111:bbbb:cccc:ffff:f400/120
6	2340:1111:aaaa:1111:bbbb:cccc:ffff:f500/120
7	2340:1111:aaaa:1111:bbbb:cccc:ffff:f600/120
8	2340:1111:aaaa:1111:bbbb:cccc:ffff:f700/120
9	2340:1111:aaaa:1111:bbbb:cccc:ffff:f800/120
10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f900/120
11	2340:1111:aaaa:1111:bbbb:cccc:ffff:fa00/120
12	2340:1111:aaaa:1111:bbbb:cccc:ffff:fb00/120
13	2340:1111:aaaa:1111:bbbb:cccc:ffff:fc00/120
14	2340:1111:aaaa:1111:bbbb:cccc:ffff:fd00/120
15	2340:1111:aaaa:1111:bbbb:cccc:ffff:fe00/120
16	2340:1111:aaaa:1111:bbbb:cccc:ffff:ff00/120

Las direcciones que se muestran en la tabla 19, ya están divididas de acuerdo a las necesidades y requerimientos de la empresa, las cual dan un total de 16 subredes para añadir y subdividir a las redes de acuerdo a la conveniencia de la empresa, y tener 256 direcciones para host como máximo por cada subred.

De estas direcciones que se muestran en la tabla 20, se ha asignado a cada antena una dirección. Las direcciones restantes se reservan para el incremento de nuevas antenas en la empresa.

TABLA XX.
DIRECCIÓN PARA CADA ANTENA DE LA RED.

Nombre de Antena	Dirección
Céli Román	2340:1111:aaaa:1111:bbbb:cccc:ffff:f100/120
Pradera	2340:1111:aaaa:1111:bbbb:cccc:ffff:f200/120
Capulí Loma	2340:1111:aaaa:1111:bbbb:cccc:ffff:f300/120
San Vicente	2340:1111:aaaa:1111:bbbb:cccc:ffff:f400/120
Palmas	2340:1111:aaaa:1111:bbbb:cccc:ffff:f500/120
Valle	2340:1111:aaaa:1111:bbbb:cccc:ffff:f600/120
Shucos Banda Alta	2340:1111:aaaa:1111:bbbb:cccc:ffff:f700/120
Chingilanchi	2340:1111:aaaa:1111:bbbb:cccc:ffff:f800/120
San Cayetano	2340:1111:aaaa:1111:bbbb:cccc:ffff:f900/120
Samaná	2340:1111:aaaa:1111:bbbb:cccc:ffff:fa00/120

3. Tercera Fase.- Configuración en GNS3 de la topología de la red.

La configuración se realiza por partes, primero se configura los nombres del router y claves de seguridad del mismo, segundo la configuración del protocolo de internet IPv6, tercero la configuración del protocolo de enrutamiento OSPFv3 de los router de la empresa, cuarto se realiza la configuración de BGP con Multihoming de los router de borde de la empresa y de los router proveedores de internet.

3.1. Paso1: Configuración básica de todos los router pertenecientes a la red de la empresa:

Se realiza la configuración básica de todos los router con los comandos descritos a continuación en la siguiente Tabla 21.

TABLA XXI.
COMANDOS DE CONFIGURACIÓN BÁSICA

Comando	Descripción
Router# configure terminal	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Router(config)# hostname nombre	Permite agregar un nombre al router.
Router(config)# enable secret clave	Permite poner una clave de acceso al modo de configuración global.
Router(config)# line vty 0 4 Router(config-line)# password clave Router(config-line)# login	Permite establecer una clave para el acceso remoto al router. El comando login se debe poner obligatoriamente para validar la configuración.
Router(config)# line console 0 Router(config-line)# password clave Router(config-line)# login	Permite establecer una clave de acceso para la conexión al puerto de consola. El comando login se debe poner obligatoriamente para validar la configuración.
Router(config t)# Banner motd &#####&	El mensaje del día (motd) es un mensaje que se configura para que aparezca

	cuando alguien intenta ingresar al equipo por cualquier medio
Router# wr	Realiza una copia de la información. La información se guarda de la memoria RAM del router, en la memoria NVram del router.

En el manual de usuario en la configuración básica del router esta detallado paso a paso como se configura los nombres y contraseñas del router.

3.1.1. Router céli román: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la Figura 19.

```

line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 06161D20484B1B18
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 12091716160E1E05
  login
!
```

Figura 19. Configuración básica de router céli román

3.1.2. Router pradera: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 20.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1502190D002F3925
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 044B19070B245E4F
  login
!

```

Figura 20. Configuración básica de router pradera

3.1.3. Router las palmas: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 21.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1313161E0709
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 01050708570E
  login
!

```

Figura 21. Configuración Básica de router las palmas

3.1.4. Router de borde sagrario: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 22.

```

line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 06161D20484B1B18
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 12091716160E1E05
  login
!
```

Figura 22. Configuración básica de router borde sagrario.

3.1.5. Router san cayetano: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 23.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1502190D002F3925
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 044B19070B245E4F
  login
!
```

Figura 23. Configuración Básica de router san cayetano.

3.1.6. Router samaná: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 24.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1313161E0709
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 01050708570E
  login
!

```

Figura 24. Configuración Básica de router samaná

3.1.7. Router valle: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 25.

```

line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 06161D20484B1B18
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 12091716160E1E05
  login
!

```

Figura 25. Configuración básica router valle

3.1.8. Router de borde valle: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 26.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1502190D002F3925
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 044B19070B245E4F
  login
!

```

Figura 26. Configuración básica router borde valle

3.1.9. Router proveedor 1: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 27.

```

!
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 1313161E0709
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 01050708570E
  login
!

```

Figura 27. Configuración básica de router proveedor 1

3.1.10. Router proveedor 2: Configuración básica

Se realiza la configuración con los comandos descritos en la tabla 21, se escribe en la consola del router el comando **show running-config**, se visualiza los cambios en la figura 28.

```

line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 06161D20484B1B18
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 12091716160E1E05
  login
!

```

Figura 28. Configuración básica de router proveedor 2

3.2. Paso 2: Configuración del protocolo IPv6 a los router de la red de la empresa.

Se configura IPv6 en las interfaces de los router de la red de la empresa, los comandos utilizados en la configuración se muestran a continuación en la Tabla 22.

TABLA XXII.
COMANDOS PARA CONFIGURACIÓN DE IPv6.

Comando	Descripción
Router()# configure terminal	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Router(config)# IPv6 unicast-routing	El comando habilita la característica de IPv6 unicast para una única interfaz.
Router(config)# interface fa 0/1	Permite ingresar a la configuración específica de la interfaz.
Router(config)# interface s 1/1	Permite ingresar a la configuración específica de la interfaz serial.
Router(config-if)# no shutdown	Habilita la interfaz físicamente para la comunicación con otros dispositivos.

Router(config-if)# IPv6 enable	Habilita el protocolo IPv6.
Router(config-if)# IPv6 address aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa	Ingreso de la dirección IPv6 a la interfaz en cuestión.

Para realizar las configuraciones del protocolo de internet IPv6 se debe conocer las interfaces de cada router, para asignar cada IPv6 a su correspondiente interfaz, las interfaces se muestran en la figura 29.

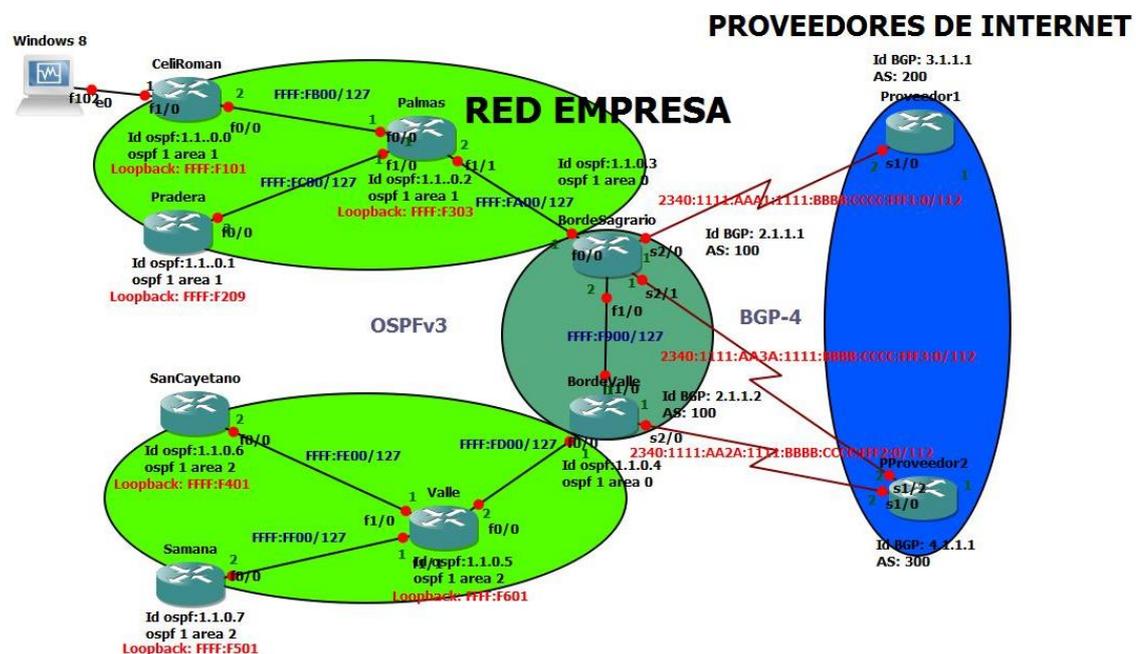


Figura 29. Interfaces de los router

Para la configuración de IPv6 en la interfaces FastEthernet y seriales, se utilizan las siguientes direcciones IPv6 que se muestran el Tabla 23.

TABLA XXIII.
DIRECCIONES IPV6.

Router Inicio	Router Destino	Interfaz	IPv6
Céli Román	Palmas	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fb02/127
Palmas	Céli Román	FA0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fb01/127
Pradera	Palmas	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fc02/127
Palmas	Pradera	FA 1/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fc01/127
Palmas	Borde Sagrario	FA 1/1	2340:1111:aaaa:1111:bbbb:cccc:ffff:fa02/127

Borde Sagrario	Palmas	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fa01/127
Borde Sagrario	Proveedor 1	S 2/0	2340:1111:aaa1:1111:bbbb:cccc:fff1:1/112
Borde Sagrario	Proveedor 2	S 2/1	2340:1111:aa3a:1111:bbbb:cccc:fff3:1/112
Proveedor 1	Borde Sagrario	S 1/0	2340:1111:aaa1:1111:bbbb:cccc:fff1:2/112
Borde Sagrario	Borde Valle	FA 1/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:f902/127
Borde Valle	Borde Sagrario	FA 1/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:f901/127
San Cayetano	Valle	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fe02/127
Valle	San Cayetano	FA 1/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fe01/127
Samaná	Valle	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:ff02/127
Valle	Samaná	FA 1/1	2340:1111:aaaa:1111:bbbb:cccc:ffff:ff01/127
Valle	Borde Valle	FA 0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fd02/127
Borde Valle	Valle	FA0/0	2340:1111:aaaa:1111:bbbb:cccc:ffff:fd01/127
Borde Valle	Proveedor 2	S 2/0	2340:1111:aa2a:1111:bbbb:cccc:fff2:1/112
Proveedor 2	Borde Valle	S 1/0	2340:1111:aa2a:1111:bbbb:cccc:fff2:2/112
Proveedor 2	Borde Sagrario	S 1/2	2340:1111:aa3a:1111:bbbb:cccc:fff3:2/112

En el manual de usuario en la configuración del protocolo IPv6 esta detallado paso a paso como se configura la activación del router para IPv6 y como se ingresa la dirección IPv6 en la interfaz.

3.2.1. Router céli román: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar la interfaz FastEthernet del router céli román, por el cual se comunica hacia el router las palmas. Se escribe en la consola del router céli román el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 30.

```
!
interface FastEthernet0/0
  description Conexion hacia router Palmas
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127
  ipv6 enable
CeliRoman#sh run
```

Figura 30. Configuración IPv6 de router céli román

3.2.2. Router pradera: Configuración IPv6

Con los comandos descritos en la tabla 22 se procede a configurar la interfaz FastEthernet del router pradera, por el cual se comunica hacia el router las palmas. Se escribe en la consola del router pradera el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 31.

```
!
interface FastEthernet0/0
  description cenexion hacia router Palmas
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127
  ipv6 enable
Pradera#sh run
```

Figura 31. Configuración IPv6 de router pradera

3.2.3. Router palmas: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar las interfaces FastEthernet del router las palmas, por las cuales se comunica hacia los router céli román, router pradera y router borde sagrario. Se escribe en la consola del router las palmas el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la Figura 32.

```

!
interface FastEthernet0/0
  description conexion hacia router Celiroman
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB01/127
  ipv6 enable
!
interface FastEthernet1/0
  description conexion hacia router Pradera
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC01/127
  ipv6 enable
!
interface FastEthernet1/1
  description conexion hacia router BordeSagrario
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127
  ipv6 enable
!
Palmas#sh run

```

Figura 32. Configuración IPv6 de router palmas.

3.2.4. Router de borde sagrario: Configuración IPv6

Con los comandos descritos en la tabla 22 se procede a configurar las interfaces FastEthernet del router de borde sagrario, por las cuales se comunica hacia los router las palmas, router borde valle, proveedor 1 y proveedor 2. Se escribe en la consola del router borde sagrario el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 33.

```

interface FastEthernet0/0
  description conexion hacia router Palmas
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet1/0
  description conexion hacia router BordeValle
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127
  ipv6 enable
  ipv6 ospf 1 area 0
!
interface Serial2/0
  description conexion hacia router proveedor 1
  no ip address
  ipv6 address 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:1/112
  ipv6 enable
  serial restart-delay 0
  no dce-terminal-timing-enable
!
interface Serial2/1
  description conexion hacia router proveedor 2
  no ip address
  ipv6 address 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:1/112
  ipv6 enable
bordeSagrario#sh run

```

Figura 33. Configuración IPv6 de router borde sagrario.

3.2.5. Router san cayetano: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar la interfaz FastEthernet del router san cayetano, por el cual se comunica hacia el router valle. Se escribe en la consola del router san cayetano el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 34.

```

!
interface FastEthernet0/0
  description conexion hacia router Valle
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE02/127
  ipv6 enable
SanCayetano#sh run

```

Figura 34. Configuración IPv6 de router san cayetano.

3.2.6. Router samaná: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar la interfaz FastEthernet del router samaná, por el cual se comunica hacia el router valle. Se escribe en la consola del router samaná el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 35.

```
!
interface FastEthernet0/0
  description conexion hacia router Valle
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF02/127
  ipv6 enable
Samana#sh run
```

Figura 35. Configuración IPv6 de router samaná

3.2.7. Router valle: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar las interfaces FastEthernet del router valle, por las cuales se comunica hacia los router san cayetano, router samaná y router borde valle. Se escribe en la consola del router valle el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 36.

```
!
interface FastEthernet0/0
  description conexion hacia router bordeValle
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD02/127
  ipv6 enable
!
interface FastEthernet1/0
  description conexion hacia router san Cayetano
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE01/127
  ipv6 enable
!
interface FastEthernet1/1
  description conexion hacia router samana
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF01/127
  ipv6 enable
!
Valle#sh run
```

Figura 36. Configuración IPv6 de router valle

3.2.8. Router de borde valle: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar las interfaces FastEthernet del router de borde valle, por las cuales se comunica hacia los router valle, router borde sagrario y proveedor 2. Se escribe en la consola del router borde valle el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 37.

```
interface FastEthernet0/0
  description conexion hacia router valle
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet1/0
  description conexion hacia router bordeSagrario
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901/127
  ipv6 enable
  ipv6 ospf 1 area 0
!
interface Serial2/0
  description conexiona hacia router proveedor 2
  no ip address
  ipv6 address 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:1/112
  ipv6 enable
BordeValle#sh run
```

Figura 37. Configuración IPv6 de router borde valle.

3.2.9. Router proveedor 1: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar las interfaces seriales del router proveedor 1, por las cuales se comunica hacia el router de borde sagrario. Se escribe en la consola del router proveedor 1 el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 38.

```
!
interface Serial1/0
  description conexion hacia router bordeSagrario
  no ip address
  ipv6 address 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2/112
  ipv6 enable
proveedor1#sh run
```

Figura 38. Configuración IPv6 de router proveedor 1

3.2.10. Router proveedor 2: Configuración IPv6

Con los comandos descritos en la Tabla 22 se procede a configurar las interfaces seriales del router proveedor 2, por las cuales se comunica hacia el router de borde valle y al router borde sagrario. Se escribe en la consola del router proveedor 2 el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 39.

```
interface Serial1/0
  no ip address
  ipv6 address 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2/112
  ipv6 enable
  serial restart-delay 0
  no dce-terminal-timing-enable
!
interface Serial1/1
  no ip address
  ipv6 address 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:1/112
  ipv6 enable
  serial restart-delay 0
  no dce-terminal-timing-enable
!
interface Serial1/2
  description CONEXION HACIA ROUTER !!!!! BORDE SAGRARIO !!!!!
  no ip address
  ipv6 address 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2/112
  ipv6 enable
  serial restart-delay 0
  no dce-terminal-timing-enable
!
proveedor2#sh run
```

Figura 39. Configuración IPv6 de router proveedor 2

3.3. Paso 3: Configuración de la interfaz loopback en los router céli román, pradera, palmas, san cayetano, samaná y valle.

Las interfaces loopback son interfaces virtuales, utilizadas para simular interfaces físicas en cada router, en nuestro caso simula los clientes conectados a cada router de la red de la empresa.

Se utiliza los siguientes comandos que se muestran la tabla 24, para configurar la interfaz Loopback.

TABLA XXIV
COMANDOS PARA CONFIGURAR LA INTERFAZ LOOPBACK.

Comando	Descripción
Router()# configure terminal	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Router(config)# interfaz lo número	Se ingresa a la interfaz virtual loopback.
Router(config-lo)# IPv6 enable	Se habilita IPv6 para la interfaz virtual loopback.
Router(config-lo)# IPv6 address x:x:x:x::/	Se ingresa la dirección virtual IPv6 designada para esta interfaz.
Router(config)#exit	Se vuelve a la configuración principal.

A continuación se detalla en la tabla 25, de las direcciones IPv6 que utiliza cada router para las interfaces virtuales loopback.

TABLA XXV
DIRECCIONES IPV6 PARA LAS INTERFACES LOOPBACK.

Router	Interfaz Loopback	Dirección IPv6
Céli Román	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f101/120
Pradera	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f209/120
Palmas	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f303/120
San Cayetano	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f401/120
Samaná	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f501/120
Valle	Interfaz lo 10	2340:1111:aaaa:1111:bbbb:cccc:ffff:f601/120

En el manual de usuario en la configuración de la interfaz loopback esta detallado pasó a paso como se configura la interfaz.

3.3.1. Router céli román: Configuración de interfaz loopback

Con los comandos descritos en la Tabla 24 se procede a configurar la interfaz Loopback del router céli román, se escribe en la consola del router el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 40.

```
!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/120
  ipv6 enable
CeliRoman#sh run
```

Figura 40. Configuración de interfaz loopback en router céli román

3.3.2. Router pradera: Configuración de interfaz loopback

Con los comandos descritos en la Tabla 24 se procede a configurar la interfaz loopback del router pradera, se escribe en la consola del router el comando show running-config, para visualizar los cambios, los mismos que se muestran en la figura 41.

```
!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/120
  ipv6 enable
Pradera#sh run
```

Figura 41. Configuración de interfaz loopback en router pradera.

3.3.3. Router palmas: Configuración de interfaz loopback

Con los comandos descritos en la Tabla 24 se procede a configurar la interfaz loopback del router Palmas, se escribe en la consola del router el comando show running-config, para visualizar los cambios, los mismos que se muestran en la figura 42.

```
!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/120
  ipv6 enable
Palmas#sh run
```

Figura 42. Configuración de interfaz loopback en router palmas.

3.3.4. Router san cayetano: Configuración de interfaz loopback

Con los comandos descritos en la tabla 24 se procede a configurar la interfaz loopback del router san cayetano, se escribe en la consola del router el comando show running-config, para visualizar los cambios, los mismos que se muestran en la figura 43.

```
!  
interface Loopback10  
  no ip address  
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/120  
  ipv6 enable  
  
SanCayetano#sh run
```

Figura 43. Configuración de interfaz loopback en router palmas.

3.3.5. Router samaná: Configuración de interfaz loopback

Con los comandos descritos en la tabla 24 se procede a configurar la interfaz loopback del router samaná, se escribe en la consola del router el comando show running-config, para visualizar los cambios, los mismos que se muestran en la figura 44.

```
!  
interface Loopback10  
  no ip address  
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501/120  
  ipv6 enable  
  
Samana#sh run
```

Figura 44. Configuración de interfaz loopback en router samaná.

3.3.6. Router valle: Configuración de interfaz loopback

Con los comandos descritos en la tabla 24 se procede a configurar la interfaz loopback del router valle, se escribe en la consola del router el comando show running-config, para visualizar los cambios, los mismos que se muestran en la figura 45.

```
!  
interface Loopback10  
  no ip address  
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/120  
  ipv6 enable  
  
Valle#sh run
```

Figura 45. Configuración de interfaz loopback en router Valle.

3.4. Paso 4: Configuración de protocolo OSPFv3 para los router céli román, pradera, palmas, san cayetano, samaná, valle, borde sagrario y borde valle.

Se configura el protocolo de enrutamiento dinámico OSPFv3 en los routers de la red con los comandos descritos en la tabla 26.

TABLA XXVI.
COMANDOS CONFIGURACIÓN DE OSPFV3.

Comando	Descripción
Router# configure terminal	Permite ingresar al modo de configuración global y usar los comandos generales del router.
Router(config)# IPv6 router OSPFv3 N°	Es el comando utilizado para habilitar OSPFV3. El número 1 puede tomar el valor de 1-65535, el valor que se le pone aquí debe tener todos los router configurados dentro de esta red.
Router(config-rtr)# router-id x.x.x.x	El comando se utiliza para definir de forma manual el router dentro del dominio OSPFV3, esta definición identifica al router dentro del dominio OSPFV3.
Router(config-rtr)#log-adjacency-changes	Muestra en consola si existe algún cambio o mensaje, dentro de la topología.
Router(config)# interface FastEthernet N°interfaz	Se ingresa a la interfaz en cuestión para poderla activar el protocolo OSPFV3.
Router(config-if)# IPv6 OSPFv3 N° area N°	Se activa OSPFv3 en la interfaz, se debe poner con el número de OSPFv3 y número de área.
Router(config)# interface lo N°Loopback	Se ingresa a la interfaz loopback, la cual se activa automáticamente sin la necesidad de el comando no shutdown
Router(config-if)# IPv6 OSPFv3 N° area N°	Se activa OSPFv3 en la interfaz, se debe poner con el número de OSPFv3 y número de área.

Para la configuración del protocolo de enrutamiento dinámico OSPFv3 se requiere establecer los id de cada router, puesto que con los id se puede identificar a cada router dentro de la red, especificar las q tendrá la red, que son tres. El área 1 consta de los routers pertenecientes a la red Sagrario, el área 2 consta de los router pertenecientes a la red valle y el área 0 o backbone a la cual se conectan todas las área consta de los router de borde sagrario y borde valle, los cuales se muestran en la siguiente tabla 27.

TABLA XXVII.
ID DE OSPFV3.

Router	OSPFV3 v3 Área	Router -id
Céli Román	Área 1	1.1.0.0
Pradera	Área 1	1.1.0.1
Palmas	Área 1	1.1.0.2
San Cayetano	Área 2	1.1.0.6
Samaná	Área 2	1.1.0.7
Valle	Área 2	1.1.0.5
Borde Sagrario	Área 0	1.1.0.3
Borde Valle	Área 0	1.1.0.4

En el manual de usuario en la configuración del protocolo OSPFv3 esta detallado paso a paso como se activa OSPF para el router, poner el router id y activar OSPF para la interfaz determinada.

3.4.1. Router céli román: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router céli román, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz tanto FastEthernet como loopback y se activa el protocolo OSPFv3, se escribe en la consola del router Céli Román el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 46.

```

!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/120
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.0
  log-adjacency-changes
!
CeliRoman#sh run

```

Figura 46. Configuración OSPFv3 de router celi román

3.4.2. Router pradera: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router pradera, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz tanto FastEthernet como loopback y se activa el protocolo OSPFv3, se escribe en la consola del router pradera el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 47.

```

!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/120
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.1
  log-adjacency-changes
!
Pradera#sh run

```

Figura 47. Configuración OSPFv3 de router pradera.

3.4.3. Router palmas: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router palmas, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz FastEthernet y se activa el protocolo OSPFv3, se escribe en la consola del router palmas el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 48.

```

interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/120
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB01/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet1/0
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC01/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet1/1
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.2
  log-adjacency-changes
Palmas#sh run

```

Figura 48. Configuración OSPFv3 de router palmas

3.4.4. Router san cayetano: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router san cayetano, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz FastEthernet y se activa el protocolo OSPFv3, se escribe en la consola del router san cayetano el comando

show running-config, para visualizar los cambios, los mismos que se muestran en la figura 49.

```
!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/120
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE02/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
ip classless
no ip http server
no ip http secure-server
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.6
  log-adjacency-changes
!
SanCayetano#sh run
```

Figura 49. Configuración OSPFv3 de router San Cayetano.

3.4.5. Router samaná: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router samaná, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz FastEthernet y se activa el protocolo OSPFv3, se escribe en la consola del router samaná el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 50.

```

!
interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501/120
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF02/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.7
  log-adjacency-changes
!
Samana#sh run

```

Figura 50. Configuración OSPFv3 de router samaná.

3.4.6. Router valle: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en el router valle, se debe tener cuidado con el Id de cada router, puesto que es el identificador de cada router en la red, se ingresa a cada interfaz FastEthernet y se activa el protocolo OSPFv3, se escribe en la consola del router valle el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 51.

```

interface Loopback10
  no ip address
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/120
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD02/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet1/0
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE01/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
interface FastEthernet1/1
  no ip address
  duplex auto
  speed auto
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF01/127
  ipv6 enable
  ipv6 ospf 1 area 2
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.5
  log-adjacency-changes
!
Valle#sh run

```

Figura 51. Configuración OSPFv3 de router valle.

3.4.7. Router borde sagrario: Configuración OSPFv3

Con los comandos descritos en la tabla 26 se procede a configurar el protocolo OSPFv3 en la interfaz, la configuración se visualiza con el comando **show running-config**, los mismos que se muestran en la figura 52.

```

!
interface FastEthernet0/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01/127
  ipv6 enable
  ipv6 ospf 1 area 1
!
interface FastEthernet1/0
  no ip address
  duplex half
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127
  ipv6 enable
  ipv6 ospf 1 area 0
!
bordeSagrario#sh run

```

Figura 52. Configuración OSPFv3 de router borde Sagrario.

Seguido se realiza la configuración del Id del router borde sagrario, puesto que es el identificador de cada router en la red, en este router se procede a ingresar a la configuración de OSPFv3, seguido se ingresa el comando **redistribute BGP-4 100**, el cual nos indica que dentro de la configuración de OSPFv3 que tiene se distribuya las rutas q ingresan por medio del protocolo BGP a los router que están trabajando con el protocolo OSPFv3 en la red, se escribe en la consola del router borde Sagrario el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 53.

```

!
logging alarm informational
no cdp log mismatch duplex
ipv6 router ospf 1
  router-id 1.1.0.3
  log-adjacency-changes
  redistribute bgp 100
!
bordeSagrario#sh run

```

Figura 53. Configuración de Id OSPFv3 de router Receptor y comando redistribute de direcciones.

3.4.8. Router borde valle: Configuración OSPFv3

Con los comandos descritos en la Tabla 26 se procede a configurar el protocolo OSPFv3 en la interfaz, la configuración se visualiza con el comando **show running-config**, los mismos que se muestran en la Figura 54.

```
!  
interface FastEthernet0/0  
  no ip address  
  duplex half  
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01/127  
  ipv6 enable  
  ipv6 ospf 1 area 2  
!  
interface FastEthernet1/0  
  no ip address  
  duplex half  
  ipv6 address 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901/127  
  ipv6 enable  
  ipv6 ospf 1 area 0  
!  
BordeValle#sh run
```

Figura 54. Configuración OSPFv3 de router borde valle.

Seguido se realiza la configuración del Id del router borde valle, puesto que es el identificador de cada router en la red, en este router se procede a ingresar a la configuración de OSPFv3, seguido se ingresa el comando **redistribute BGP 100**, el cual nos indica que dentro de la configuración de OSPFv3 que tiene se distribuya las rutas q ingresan por medio del protocolo BGP-4 a los router que están trabajando con el protocolo OSPFv3 en la red, se escribe en la consola del router borde valle el comando **show running-config**, para visualizar los cambios, los mismos que se muestran en la figura 55.

```
!  
logging alarm informational  
no cdp log mismatch duplex  
ipv6 router ospf 1  
  router-id 1.1.0.4  
  log-adjacency-changes  
  redistribute bgp 100  
!  
BordeValle#sh run
```

Figura 55. Configuración de Id OSPFv3 de router borde valle y comando redistribute de direcciones.

3.5. Paso 5: Configuración del protocolo exterior BGP y Multihoming para los router borde sagrario, borde valle, proveedor 1 y proveedor 2

Se configura el protocolo de enrutamiento de Gateway exterior BGP para los router borde sagrario, borde valle, proveedor1 y proveedor2, el id del router BGP debe ser único, los comandos utilizados se muestran a continuación en la tabla 28.

TABLA XXVIII.
COMANDOS PROTOCOLO BGP-4 Y MULTIHOMING.

Comando	Descripción
Router# Config t	Se ingresa al modo de configuración global.
Router(config)#router BGP N°AS	Se identifica el sistema autónomo BGP que tendrá el router dentro de la red.
Router(config-router)#BGP router id x.x.x.x	El id del router identifica de forma exclusiva un router dentro de un dominio. El comando se utiliza para definir de forma manual el identificador del router.
Router(config-router)#no BGP default ipv4-unicast	Se desactiva la opción para unicast IPv4.
Router(config-router)#neighbor x.x.x.x.x.x.x.x remote-as N°AS	Se agrega un sistema autónomo a BGP, al especificar la IP y número de sistema autónomo.
Router(config-router)#neighbor x.x.x.x.x.x.x.x eBGP-multihop x	Es utilizado para indicar que existe más de un camino para llegar a un mismo destino.
Router(config-router)#adres-family IPv6	Se ingresa al modo de configuración específica de BGP correspondiente al protocolo IPv6.
Router(config-router-af)#neighbor x.x.x.x.x.x.x.x activate	Se activa la sesión en el punto local de las interfaces que son vecinas al router en cuestión, adicional la sesión también debe ser activada en el vecino.

Router(config-router-af)#neighbor x.x.x.x.x.x.x.x weight xxx	Se utiliza para la selección de la mejor ruta, se la realiza de forma manual y la ruta con mayor peso, se diría que es la mejor ruta. Y x la cual la tabla de enrutamiento por defecto va a dirigir y aprender las rutas de entrada y salida.
Router(config-router-af)#network x.x.x.x.x.x.x.x/x	Hace referencia a la red que se encuentran dentro del sistema autónomo y que se desea publicar al exterior.
Router(config-router-af)#redistribute OSPF x	Anuncia a los prefijos aprendidos de forma dinámica a los router vecinos de BGP, mediante el protocolo OSPF.
Router(config-router-af)#exit-address-family	Salida del modo de configuración específica de BGP para IPv6.

Para la configuración del protocolo BGP se requiere establecer los id de cada router, puesto que con los id se puede identificar a cada router dentro de la red, los cuales se los establece en la siguiente tabla 29.

TABLA XXIX.
ESTABLECER SISTEMA AUTONOMO(AS) Y ID DE CADA ROUTER.

Router	AS BGP	Router -id
Borde Sagrario	100	2.1.1.1
Borde Valle	100	2.1.1.2
Proveedor1	200	3.1.1.1
Proveedor2	300	4.1.1.1

En el manual de usuario en la configuración del protocolo exterior BGP y Multihoming esta detallado paso a paso como se activa BGP para el router con su respectivo sistema autónomo, poner el router id, añadir los sistemas autónomos adyacentes, activar los sistemas autónomos adyacentes y ponerles un peso específico a las rutas de salida

3.5.1. Router borde sagrario: Configuración del protocolo BGP y Multihoming

Con los comandos descritos en la tabla 28 se procede a configurar el protocolo BGP en el router borde sagrario, se debe tener cuidado con el Id y el sistema autónomo de cada router, puesto que es el identificador de cada router en la red, para ingresarlo sin tener errores se debe tomar el Id de la Tabla 28. Se escribe en la consola del router borde sagrario el comando **show running-config | section router BGP 100**, para visualizar los cambios, los mismos que se muestran en la figura 56.

```
bordeSagrario#show running-config | section router bgp 100
router bgp 100
  bgp router-id 2.1.1.1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 remote-as 300
  neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 ebgp-multihop 6
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 remote-as 200
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 ebgp-multihop 4
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 remote-as 100
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 ebgp-multihop 2
  !
  address-family ipv6
    neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 activate
    neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 weight 800
    neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 activate
    neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 weight 1000
    neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 activate
    neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 weight 500
    network 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F/116
  redistribute ospf 1
  no synchronization
  exit-address-family
bordeSagrario#
```

Figura 56. Configuración BGP y Multihoming de router borde sagrario.

3.5.2. Router borde valle: Configuración del protocolo BGP y Multihoming

Con los comandos descritos en la tabla 28 se procede a configurar el protocolo BGP en el router borde valle, se debe tener cuidado con el Id y el sistema autónomo de cada router, puesto que es el identificador de cada router en la red, para ingresarlo sin tener errores se debe tomar en cuenta la tabla 29. Se escribe en la consola del router borde

valle el comando **show running-config | section router BGP 100**, para visualizar los cambios, los mismos que se muestran en la figura 57.

```
BordeValle#show running-config | section router bgp 100
router bgp 100
  bgp router-id 2.1.1.2
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 remote-as 300
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 ebgp-multihop 4
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 remote-as 100
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 ebgp-multihop 2
  !
  address-family ipv6
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 activate
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 weight 1000
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 activate
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 weight 500
  network 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F/116
  redistribute ospf 1
  no synchronization
  exit-address-family
BordeValle#
```

Figura 57. Configuración BGP y Multihoming de router borde Valle.

3.5.3. Router proveedor 1: Configuración del protocolo BGP y Multihoming

Con los comandos descritos en la tabla 28 se procede a configurar el protocolo BGP en el proveedor1, se debe tener cuidado con el Id y el sistema autónomo de cada router, puesto que es el identificador de cada router en la red, para ingresarlo sin tener errores se debe tomar en cuenta la Tabla 29 para el Sistema Autónomo. Se escribe en la consola del router proveedor 1 el comando **show running-config | section router BGP 200**, para visualizar los cambios, los mismos que se muestran en la figura 58.

```
Proveedor1#show running-config | section router bgp 200
router bgp 200
  bgp router-id 3.1.1.1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:1 remote-as 100
  neighbor 2340:1111:AAA2:1111:BBBB:CCCC:FFA1:2 remote-as 400
  !
  address-family ipv6
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:1 activate
  neighbor 2340:1111:AAA2:1111:BBBB:CCCC:FFA1:2 activate
  exit-address-family
Proveedor1#
```

Figura 58. Configuración BGP y Multihoming de router proveedor 1.

3.5.4. Router proveedor 2: Configuración del protocolo BGP y Multihoming

Con los comandos descritos en la tabla 28 se procede a configurar el protocolo BGP en el proveedor 2, se debe tener cuidado con el Id y el sistema autónomo de cada router, puesto que es el identificador de cada router en la red, para ingresarlo sin tener errores se debe tomar en cuenta la tabla 29. Se escribe en la consola del router proveedor 2 el comando **show running-config | section router BGP 300**, para visualizar los cambios, los mismos que se muestran en la figura 59.

```
proveedor2#show running-config | section router bgp 300
router bgp 300
  bgp router-id 4.1.1.1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 remote-as 400
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:1 remote-as 100
  neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:1 remote-as 100
  !
  address-family ipv6
  neighbor 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 activate
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:1 activate
  neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:1 activate
  exit-address-family
proveedor2#
```

Figura 59. Configuración BGP y Multihoming de router proveedor 2.

4. Cuarta Fase.- Pruebas

Para realizar las pruebas de funcionamiento de la red de la empresa, se ha establecido un plan de pruebas que consta de cuatro puntos. Primer punto se establece los objetivos que se deben cumplir. Segundo punto se diseña los casos de pruebas que ayuden a comprobar si la configuración realizada cumple con los objetivos. Tercer punto se especifica la topología que se utiliza para implementar la fase de pruebas. Cuarto punto se realiza las pruebas de acorde a los casos de prueba anteriormente realizados.

4.1. Plan de Pruebas

Se diseñó el plan de pruebas para el proyecto el cual consta de los siguientes puntos.

4.1.1. Propósito

Una vez realizada la configuración de la red Sagrario se procede a elaborar las pruebas de funcionamiento de la red, las cuales permiten comprobar que la red de la empresa cumple los objetivos para la cual fue creada, a continuación, los objetivos que deberá cumplir el plan de pruebas son:

- Exista conectividad de los equipos de la red con el protocolo IPv6.
- Verificar la configuración del Protocolo OSPFv3 en los dispositivos de la red Sagrario.
- Verificar la configuración del protocolo BGP en los dispositivos de la red.
- Analizar las métricas de OSPFv3 y BGP.
- Analizar los paquetes de OSPFv3 y BGP con Wireshark.
- Prueba de funcionamiento de Multihoming a la red de la empresa.

4.1.2. Alcance de las Pruebas

Se diseñó los casos de pruebas que ayudan a comprobar si la configuración realizada cumple con los requerimientos.

Prueba de funcionamiento de que si existe conectividad de los equipos de la red con el protocolo IPv6. La cual se muestra en la Tabla 30.

TABLA XXX.
CASO DE PRUEBA DE 1.

Caso 1	
Nombre de Prueba	Medios para Solución
Exista conectividad de los equipos de la red con el protocolo IPv6.	Para verificar la conexión de los equipos de la red Sagrario se realiza una petición con el comando ping x:x:x:x:x:x:x , informándonos así si existe o no conexión.

Prueba de funcionamiento para verificar la configuración del protocolo OSPFv3 en los dispositivos de la red. La cual se muestra en la tabla 31.

TABLA XXXI.
CASO DE PRUEBA 2.

Caso 2	
Nombre de Prueba	Solución Prueba
Verificar la configuración del protocolo OSPF en los dispositivos de la red.	<ul style="list-style-type: none"> • Para verificar la adyacencia de los dispositivos de la red se procede a verificar los id de vecinos. Con el comando show IPv6 OSPF neighbor. • Para verificar las rutas aprendidas de cada router se procede a verificar su tabla de enrutamiento con el comando show IPv6 route.

Prueba de funcionamiento para verificar la configuración del protocolo BGP en los dispositivos de la red Sagrario. La cual se muestra en la tabla 32.

TABLA XXXII.
CASO DE PRUEBA 3.

Caso 3	
Nombre de Prueba	Solución de Prueba
Verificar la configuración del protocolo BGP en los dispositivos de la red.	<ul style="list-style-type: none"> Se verifica la configuración del Protocolo BGP-4 con el comando show running-config section BGP as. Verificar rutas aprendidas por medio del Protocolo BGP con el comando show ipv6 route.

Prueba de distancias administrativas de los protocolos OSPFv3 e BGP en los routers de la red. La cual se muestra en la tabla 33.

TABLA XXXIII.
CASO DE PRUEBA 4

Caso 4	
Nombre de Prueba	Medios para Solución
Constatar las distancias administrativas de OSPFv3 de los router internos de la red (router pradera, samaná).	<ul style="list-style-type: none"> Para verificar la distancia administrativa de OSPFv3, se escribe el comando show ipv6 route en la consola de los router indicados. Verificar las distancias administrativas que se han aprendido.
Constatar las distancias administrativas BGP de los router (router borde sagrario y borde valle).	<ul style="list-style-type: none"> Para verificar la distancia administrativa de BGP, se escribe el comando show ipv6 route en la consola de los router indicados. Verificar las distancias administrativas que se han aprendido.

Prueba para verificar el establecimiento de comunicación con los protocolo OSPFv3 y BGP, la cual me muestra en la tabla 34

Tabla XXXIV
CASO DE PRUEBA 5

Caso 5	
Nombre de Prueba	Medios para Solución
Verificar los paquetes de comunicación de los router palmas con bordesabragio a través del protocolo OSPFv3, con la herramienta Wireshark.	<ul style="list-style-type: none"> • Verificar que direcciones IPv6 se envían al momento de establecer la comunicación. • Verificación del uso de los paquetes que utiliza OSPFv3 para su comunicación.
Verificar los paquetes de comunicación de los router bordesabragio con proveedor 1 a través del protocolo BGP, con la herramienta Wireshark.	<ul style="list-style-type: none"> • Verificar que protocolos utiliza BGP para la comunicación. • Verificación el uso de los paquetes que utiliza BGP para la comunicación.

Prueba para verificar el funcionamiento de Multihoming en la red de la empresa. La cual se muestra en la Tabla 35.

TABLA XXXV.
CASO DE PRUEBA 6.

Caso 6	
Nombre de Prueba	Solución de Prueba
Prueba de funcionamiento de Multihoming red sagrario.	<ul style="list-style-type: none"> • Realizar una prueba de conectividad con el comando ping a una interfaz virtual ubicada en una red externa pruebas previamente configurada. • Comprobar que se está publicando por el proveedor principal a la red externa, con el comando show ipv6 route. • Se realiza la caída del enlace principal, de la red sagrario, seguido se revisa el levantamiento de enlace secundario 1 que tenemos configurado. Se verifica la tabla de enrutamiento del router borde sagrario y se observa cual es la nueva ruta de

	<p>salida hacia al exterior con el comando show ipv6 route.</p> <ul style="list-style-type: none"> • Prueba de conectividad por medio del enlace de respaldo. Se realiza una prueba de eco desde los router céli román y pradera hasta la red externa pruebas. • Se realiza la caída del secundario 1, de la red sagrario, seguido se revisa el levantamiento de enlace secundario 2 que está configurado. Se verifica la tabla de enrutamiento del router borde sagrario y se observa cual es la nueva ruta de salida hacia al exterior con el comando show ipv6 route. • Prueba de conectividad por medio del enlace de respaldo. Se realiza una prueba de eco desde los router céli román y pradera hasta la red externa pruebas.
<p>Prueba de funcionamiento de Multihoming red Valle.</p>	<ul style="list-style-type: none"> • Realizar una prueba de conectividad con el comando ping a una interfaz virtual ubicada en una red externa pruebas previamente configurada. • Comprobar que se está publicando por el proveedor principal a la red externa, con el comando show ipv6 route. • Se realiza la caída del enlace principal, de la red Sagrario, seguido se revisa el levantamiento de enlace de respaldo que está configurado. Se verifica la tabla de enrutamiento del router borde Valle y se observa cual es la nueva ruta de salida hacia al exterior con el comando show ipv6 route. • Prueba de conectividad por medio del enlace de respaldo. Se realiza una prueba de eco desde los router san cayetano y samaná hasta la red externa pruebas.

4.1.4. Resultados de las Pruebas

Se realiza las pruebas de funcionamiento basándonos en el alcance de las pruebas previamente realizadas.

4.1.4.1. Caso 1: Exista conectividad de los dispositivos de la red de la empresa.

Las pruebas de conectividad son muy importantes puesto que verifican si existe conectividad entre los dispositivos de la red.

- **Verificar conectividad entre los dispositivos de la red sagrario.**

Se realiza la verificación con el comando **ping x:x:x:x:x:x:x:x** de router a router, la verificación se efectúa entre las direcciones loopback de cada router.

En la consola del router céli román, se procede a teclear el comando **ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f303**, la dirección tecleada es la dirección loopback configurada en router palmas. Se observa en la consola **Success rate is 100 percent (5/5)**, que significa que la conexión fue exitosa que tuvo el 100% de conectividad con router palmas. La cual se muestra en la figura 61.

```
CeliRoman#ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f303
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/571/720 ms
CeliRoman#
```

Figura 61. Conectividad de router céli román a router palmas.

En la consola del router céli román, se procede a teclear el comando **ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f501**, la dirección tecleada es la dirección loopback configurada en router samaná. Se observa en la consola **Success rate is 100 percent (5/5)**, que significa que la conexión fue exitosa que tuvo el 100% de conectividad con router samaná. La cual se muestra en la figura 62.

```
CeliRoman#ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f501
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1324/1664/1932 ms
CeliRoman#
```

Figura 62. Conectividad de router céli román a router samaná.

En la consola del router san cayetano, se procede a teclear el comando **ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f209**, la dirección tecleada es la dirección

loopback configurada en router pradera. Se observa en la consola **Success rate is 100 percent (5/5)**, que significa que la conexión fue exitosa que tuvo el 100% de conectividad con router pradera. La cual se muestra en la figura 63.

```
SanCayetano#ping 2340:1111:aaaa:1111:bbbb:cccc:ffff:f209
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1384/1457/1512 ms
SanCayetano#
```

Figura 63. Conectividad de router céli román a router pradera.

4.1.4.2. Caso 2: Verificar la configuración del Protocolo OSPFv3 en los dispositivos de la red de la empresa.

El protocolo OSPFv3 permite la comunicación interna de la red sagrario, permitiendo crear adyacencias de vecinos para su comunicación.

- **Verificar adyacencia OSPFv3 entre los dispositivos**

Para verificar la adyacencia de los dispositivos de la red se procede a teclear el comando **show IPv6 OSPFv3 neighbor**.

En la consola del router palmas, se procede a teclear el comando **show IPv6 OSPF neighbor**, el cual nos indica los Id de los router que se conectan directamente por medio de OSPFV3 al router. Se observa en la consola en **Neighbor ID**, el id 1.1.0.3, 1.1.0.1, 1.1.0.0, que es el identificador OSPFv3 del router borde sagrario, san cayetano y céli román respectivamente, el cual indica que son router adyacentes. La cual se muestra en la figura 64.

```
Palmas#sh ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.0.3          1    FULL/DR         00:00:33   4             FastEthernet1/1
1.1.0.1          1    FULL/BDR        00:00:33   4             FastEthernet1/0
1.1.0.0          1    FULL/BDR        00:00:35   4             FastEthernet0/0
Palmas#
```

Figura 64. Verificar adyacencias de router palmas.

En la consola del router borde Sagrario, se procede a teclear el comando **show IPv6 OSPF neighbor**, el cual nos indica los Id de los router que se conectan directamente por medio de OSPFv3 al router. Se observa en la consola en **Neighbor ID**, el id 1.1.0.4, 1.1.0.2, que es el identificador OSPFv3 del router borde valle y palmas respectivamente, el cual indica que son router adyacentes. La cual se muestra en la figura 65.

```
bordeSagrario#sh ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.0.4          1    FULL/BDR        00:00:38   5             FastEthernet1/0
1.1.0.2          1    FULL/BDR        00:00:36   6             FastEthernet0/0
bordeSagrario#
```

Figura 65. Verificar adyacencias de router borde sagrario.

En la consola del router valle, se procede a teclear el comando **show IPv6 OSPF neighbor**, el cual nos indica los Id de los router que se conectan directamente por medio de OSPFv3 al router. Se observa en la consola en **Neighbor ID**, el id 1.1.0.7, 1.1.0.6, 1.1.0.4, que es el identificador OSPFv3 del router samaná, san cayetano y borde valle respectivamente, el cual indica que son router adyacentes. La cual se muestra en la figura 66.

```
Valle#sh ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.0.7          1    FULL/BDR        00:00:33   4             FastEthernet1/1
1.1.0.6          1    FULL/BDR        00:00:31   4             FastEthernet1/0
1.1.0.4          1    FULL/DR         00:00:34   4             FastEthernet0/0
Valle#
```

Figura 66. Verificar adyacencias de router valle.

- **Verificar áreas configuradas**

Para verificar las áreas configuradas se procede a teclear el comando **show IPv6 OSPF 1** en la consola de routers de la red.

En la consola del router palmas, se procede a teclear el comando **show IPv6 OSPF 1**, en el cual se verifica que tiene el área 1 configurado, 4 interfaces activas con el protocolo OSPFv3 conectadas a ella y se ha ejecutado el protocolo SPF 3 veces que es el encargado de buscar el mejor camino de las rutas, se ejecuta 3 veces, porque tiene 3 interfaces de salida una hacia cada router vecino. La cual se muestra en la Figura 67.

```

Palmas#sh ipv6 ospf 1
Routing Process "ospfv3 1" with ID 1.1.0.2
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Area 1
    Number of interfaces in this area is 4
    SPF algorithm executed 3 times
    Number of LSA 32. Checksum Sum 0x1174E7
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
Palmas#

```

Figura 67. Verificar áreas del router palmas.

En la consola del router borde sagrario, se procede a teclear el comando **show IPv6 OSPF 1**, en el cual se verifica que tiene el área 0 configurado, 1 interfaz activa con el protocolo OSPFv3 conectada a ella y se ha ejecutado el protocolo SPF 3 veces que es el encargado de buscar el mejor camino de las rutas, se ejecuta 3 veces, porque tiene 3 interfaces de salida una hacia cada router vecino. El área 1 configurado, 1 interfaces activas con el protocolo OSPFv3 conectadas a ella y se ha ejecutado el protocolo SPF 2 veces que es el encargado de buscar el mejor camino de las rutas, se ejecuta 2 veces, porque tiene 2 interfaces de salida una hacia cada router vecino La cual se muestra en la Figura 68.

```

bordeSagrario#sh ipv6 ospf 1
Routing Process "ospfv3 1" with ID 1.1.0.3
It is an area border and autonomous system boundary router
Redistributing External Routes from,
  bgp 100
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    SPF algorithm executed 3 times
    Number of LSA 16. Checksum Sum 0x062C65
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
  Area 1
    Number of interfaces in this area is 1
    SPF algorithm executed 2 times
    Number of LSA 15. Checksum Sum 0x069C9F
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 4
bordeSagrario#

```

Figura 68. Verificar áreas de router borde sagrario.

- **Verificar rutas aprendidas del protocolo OSPFv3 en routers**

Para verificar las rutas aprendidas de cada router se procede a verificar su tabla de enrutamiento con el comando **show IPv6 route**.

En la consola del router pradera, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la legenda que nos indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Las direcciones que tienen al inicio la letra **O** que están subrayadas con rojo, que significa que fueron aprendidas dentro de la misma área por medio del protocolo OSPFv3 y también rutas aprendidas entre áreas las cuales tienen al inicio las letras **OI** son las que están subrayadas con azul. La cual se muestra en la Figura 69.

```

via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/4]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/3]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/3]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/2]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/2]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/2]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/2]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/1]
via ::, FastEthernet0/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127 [0/0]
via ::, FastEthernet0/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/128 [0/0]
via ::, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD00/127 [110/4]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD02/127 [110/4]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE00/127 [110/5]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE02/127 [110/5]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF00/127 [110/5]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF02/127 [110/5]
via FE80::C803:10FF:FEA0:1C, FastEthernet0/0
Pradera#

```

Figura 69. Tabla de enrutamiento de router pradera.

En la consola del router samaná, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la leyenda que nos indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Las direcciones **OE2** que están subrayadas con blanco son las rutas externas que se aprendieron del protocolo BGP-4, las direcciones que tienen al inicio la letra **O** que están subrayadas con rojo que significa que fueron aprendidas dentro de la misma área por medio del protocolo OSPFv3 y también tenemos rutas aprendidas entre áreas las cuales tienen al inicio las letras **OI** son las que están subrayadas con azul. La cual se muestra en la Figura 70.

```

IPv6 Routing Table - 27 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [110/1]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [110/1]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [110/1]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/128 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/128 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/128 [110/4]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/128 [110/2]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F500/120 [0/0]
    via ::, Loopback10
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501/128 [0/0]
    via ::, Loopback10
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/1]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/3]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/3]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/4]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/4]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127 [110/5]
    via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
Samana#

```

Figura 70. Tabla de enrutamiento de router samaná.

4.1.4.3. Caso3: Verificar la configuración del protocolo BGP en los dispositivos de la red.

El protocolo BGP nos permite la comunicación entre sistemas autónomos.

- **Verificar la configuración del protocolo BGP.**

Se verifica la configuración del Protocolo BGP-4 con el comando **show running-config | section BGP 100**, el cual muestra solo la configuración BGP del router.

En la consola del router borde sagrario, se procede a teclear el comando **show running-config | section BGP 100**, el cual indica solo la configuración BGP que se ha realizado. La cual se muestra en la Figura 71.

```
bordeSagrario#sh running-config | section router bgp 100
router bgp 100
  bgp router-id 2.1.1.1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 remote-as 200
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 ebgp-multihop 4
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 remote-as 100
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 ebgp-multihop 2
  !
  address-family ipv6
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 activate
  neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 weight 1000
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 activate
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 weight 500
  network 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F/116
  redistribute ospf 1
  no synchronization
  exit-address-family
bordeSagrario#
```

Figura 71. Configuración BGP del router borde Sagrario.

En la consola del router borde valle, se procede a teclear el comando **show running-config | section BGP 100**, el cual indica solo la configuración BGP que se ha realizado. La cual se muestra en la Figura 72.

```

BordeValle#show running-config | section bgp 100
router bgp 100
  bgp router-id 2.1.1.2
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 remote-as 300
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 ebgp-multihop 4
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 remote-as 100
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 ebgp-multihop 2
  !
  address-family ipv6
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 activate
  neighbor 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 weight 1000
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 activate
  neighbor 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 weight 500
  network 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F/116
  redistribute ospf 1
  no synchronization
  exit-address-family
  redistribute bgp 100
BordeValle#

```

Figura 72. Configuración BGP del router borde valle.

- **Verificar rutas aprendidas por medio del protocolo BGP.**

En la consola del router borde sagrario, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la legenda que indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Las direcciones que tienen al inicio la letra B que está subrayadas con rojo, significa que fueron aprendidas por el protocolo BGP y que son rutas externas de otros sistemas autónomos. La cual se muestra en la Figura 73.

```
bordeSagrario#sh ipv6 route
IPv6 Routing Table - 29 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [20/0]
  via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [20/0]
  via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [20/0]
  via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
C 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:0/112 [0/0]
  via ::, Serial2/0
L 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:1/128 [0/0]
  via ::, Serial2/0
O 2340:1111:AAA1:1111:BBBB:CCCC:FFFF:F101/128 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAA1:1111:BBBB:CCCC:FFFF:F209/128 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAA1:1111:BBBB:CCCC:FFFF:F303/128 [110/1]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
OI 2340:1111:AAA1:1111:BBBB:CCCC:FFFF:F401/128 [110/3]

bordeSagrario#sh ipv6 route
```

Figura 73. Tabla de enrutamiento de router borde sagrario.

En la consola del router borde valle, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la leyenda que nos indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Las direcciones que tienen al inicio la letra **B** que están subrayadas con rojo, que significa que fueron aprendidas por el protocolo BGP y que son rutas externas de otros sistemas autónomos. La cual se muestra en la Figura 74.

```

BordeValle#sh ipv6 route
IPv6 Routing Table - 29 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2340:1111:AA2A:1111:BBBB:CCCC:FFF2:0/112 [0/0]
    via ::, Serial2/0
L   2340:1111:AA2A:1111:BBBB:CCCC:FFF2:1/128 [0/0]
    via ::. Serial2/0
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [20/0]
    via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [20/0]
    via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [20/0]
    via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
OI  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/128 [110/3]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/128 [110/3]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/128 [110/2]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
O   2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/128 [110/2]

BordeValle#

```

Figura 74. Tabla de enrutamiento de router borde valle.

4.1.4.4. Caso 4: Analizar las métricas de OSPFv3 y BGP.

Se analiza las distancias administrativas y métricas en las direcciones aprendidas por los protocolos de enrutamiento.

Distancias administrativas y métrica del protocolo OSPF

De acuerdo al aprendizaje de cada ruta en el router, la distancia administrativa tiene un valor establecido. Como se utilizó el protocolo OSPFv3 para todos los router internos de la red, la distancia administrativa será general para todas la cual es 110. La métrica que utiliza OSPF es el ancho de banda que tendrá cada enlace de router a router, este se calcula con la siguiente formula $\frac{1000000}{\text{Ancho banda}}$, en nuestro caso como se utilizó FastEthernet, sería de la siguiente forma $\frac{100000}{100000}$, la métrica de router a router tiene el valor de 1.

A continuación se describe el recorrido que tiene que hacer el router samaná para llegar al router céli román tomando en cuenta las métricas. Se muestra la red de la empresa y se señala los routers desde los cuales se hará el recorrido, como se muestra en la en la figura 75.

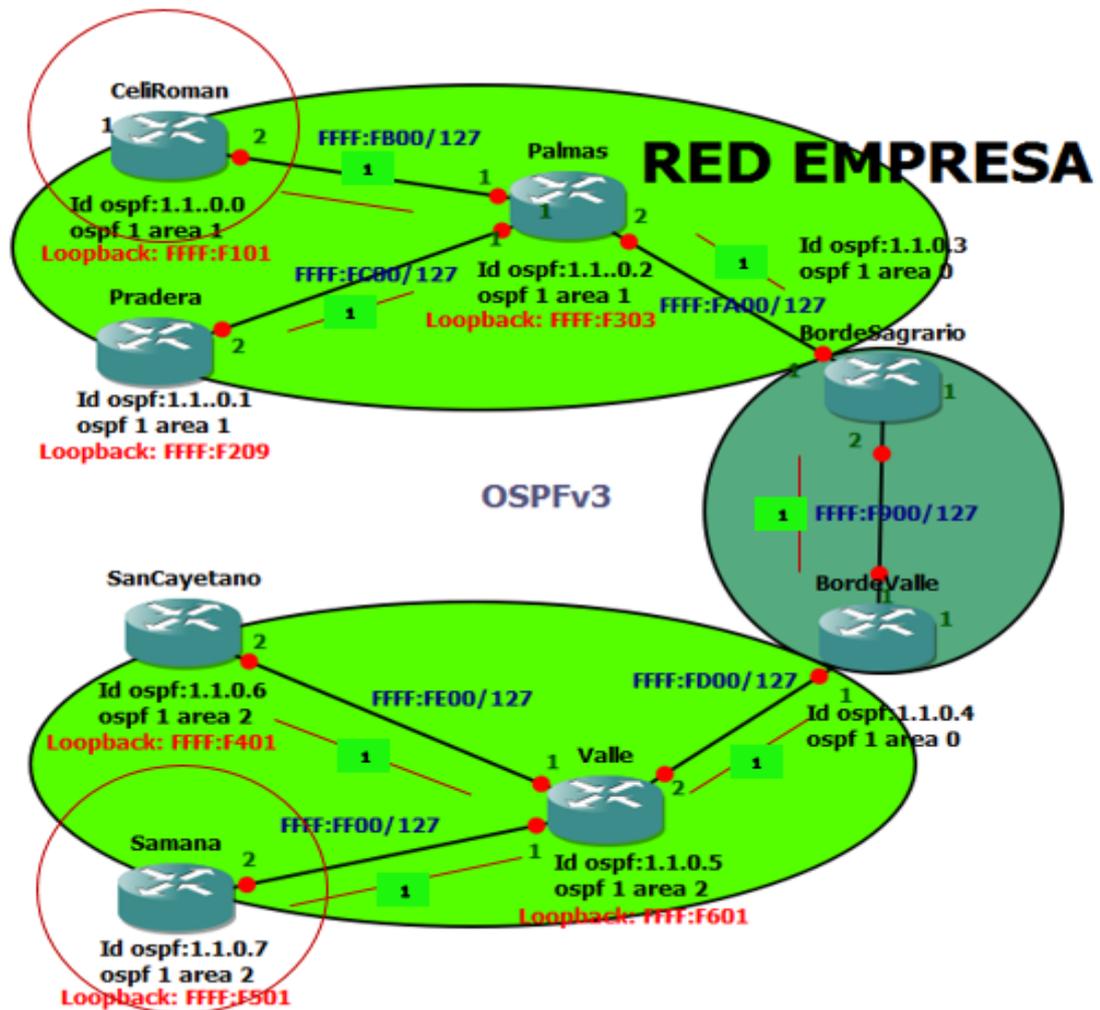


Figura 75. Red Empresa

A continuación se muestra la ruta de routers que debe pasar para que se puedan comunicar el router samaná y céli román.

Tabla de enrutamiento de router samaná.- Se muestra la tabla de enrutamiento del router samaná con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router céli román, la cual indica la distancia administrativa de ospf que es 110 y la métrica que tiene para llegar hacia el router céli román que es 5. El número 5 nos indica la métrica que utiliza el router samaná para llegar hacia el router céli román la cual se ha calculado sumando todas las métricas de los enlaces hasta llegar al router céli román. El router samaná siempre mostrara la métrica más baja para llegar a un destino. Como se muestra en la figura 76.

```

O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/1]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/3]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/3]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/4]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/4]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/5]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/5]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/5]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127 [110/5]
  via FE80::C806:13FF:FEB0:1D, FastEthernet0/0

Samana#

```

Figura 76. Tabla de enrutamiento de router samaná.

Tabla de enrutamiento del router Valle.- Se muestra la tabla de enrutamiento del router valle con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router céli román, la cual indica la distancia administrativa de ospf que es 110 y la métrica que tiene para llegar hacia el router céli román que es 4. El número 4 indica la métrica que utiliza el router samaná para llagar hacia el router céli román la cual se ha calculado sumando todas las métricas de los enlaces hasta llegar al router céli román. El router valle siempre mostrara la métrica más baja para llegar a un destino. Como se muestra en la figura 77.

```

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F100/120 [110/5]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/128 [110/4]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/128 [110/3]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501/128 [110/1]
  via FE80::C808:10FF:FEF0:0, FastEthernet1/1
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F600/120 [0/0]
  via ::, Loopback10
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [0/0]
  via ::, Loopback10
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F801/128 [110/4]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/2]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/2]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/3]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/3]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/4]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/4]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/4]
  via FE80::C805:15FF:FEDC:0, FastEthernet0/0
Valle#sh ipv6 route

```

Figura 77. Tabla de enrutamiento de router valle.

Tabla de enrutamiento del router Bordevalle.- Se muestra la tabla de enrutamiento del router valle con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router céli román, indica la distancia administrativa de ospf que es 110 y la métrica que tiene para llegar hacia el router céli román que es 3. El número 3 indica la métrica que utiliza el router Bordevalle para llagar hacia el router céli román la cual se ha calculado sumando todas las métricas de los enlaces hasta llegar al router céli román. El router Bordevalle siempre mostrara la métrica más baja para llegar a un destino. Como se muestra en la figura 78

```

O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/1]
  via FE80::C806:13FF:FEB0:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F801/128 [110/3]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [0/0]
  via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901/128 [0/0]
  via ::, FastEthernet1/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/1]
  via ::, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/2]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/2]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/3]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/3]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/3]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127 [110/3]
  via FE80::C804:FF:FE30:1C, FastEthernet1/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD00/127 [0/0]
  via ::, FastEthernet0/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01/128 [0/0]

BordeValle#

```

Figura 78. Tabla de enrutamiento de router bordevalle.

Tabla de enrutamiento del router Bordesagrario.- Se muestra la tabla de enrutamiento del router Bordesagrario con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router céli román, indica la distancia administrativa de ospf que es 110 y la métrica que tiene para llegar hacia el router céli román que es 2. El número 2 indica la métrica que utiliza el router Bordesagrario para llagar hacia el router céli román la cual se ha calculado sumando todas las métricas de los enlaces hasta llegar al router céli román. El router Bordesagrario siempre mostrara la métrica más baja para llegar a un destino. Como se muestra en la figura 79.

```

C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [0/0]
  via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/128 [0/0]
  via ::, FastEthernet1/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [0/0]
  via ::, FastEthernet0/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01/128 [0/0]
  via ::, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [110/1]
  via ::, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC02/127 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD00/127 [110/2]
  via FE80::C805:15FF:FEDC:1C, FastEthernet1/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD02/127 [110/2]

```

Figura 79. Tabla de enrutamiento de router bordesagrario.

Tabla de enrutamiento del router Palmas.- Se muestra la tabla de enrutamiento del router Palmas con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router céli román, indica la distancia administrativa de ospf que es 110 y la métrica que tiene para llegar hacia el router céli román que es 1. El número 1 indica la métrica que utiliza el router Palmas para llagar hacia el router céli román la cual se ha calculado sumando todas las métricas de los enlaces hasta llegar al router céli román. El router Palmas siempre mostrara la métrica más baja para llegar a un destino. Como se muestra en la figura 80.

```

via FE80::C804:FF:FE30:0, FastEthernet1/1
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F801/128 [110/1]
via FE80::C801:11FF:FE98:0, FastEthernet0/0
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/2]
via FE80::C804:FF:FE30:0, FastEthernet1/1
OI 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/2]
via FE80::C804:FF:FE30:0, FastEthernet1/1
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA00/127 [110/1]
via ::, FastEthernet1/1
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/127 [0/0]
via ::, FastEthernet1/1
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA02/128 [0/0]
via ::, FastEthernet1/1
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB00/127 [0/0]
via ::, FastEthernet0/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB01/128 [0/0]
via ::, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB02/127 [110/1]
via ::, FastEthernet0/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC00/127 [0/0]
via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FC01/128 [0/0]

Palmas#sh ipv6 route

```

Figura 80. Tabla de enrutamiento de router palmas.

Distancias administrativas y métrica de protocolo BGP.

En el protocolo bgp la distancia administrativa es 20, en cuanto a la métrica el protocolo bgp toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

A continuación se describe el recorrido que tiene que hacer el router pradera para llegar a la red pruebas por medio del router bordesagrario con el proveedor 1 como salida principal. Como se muestra en la figura 81.

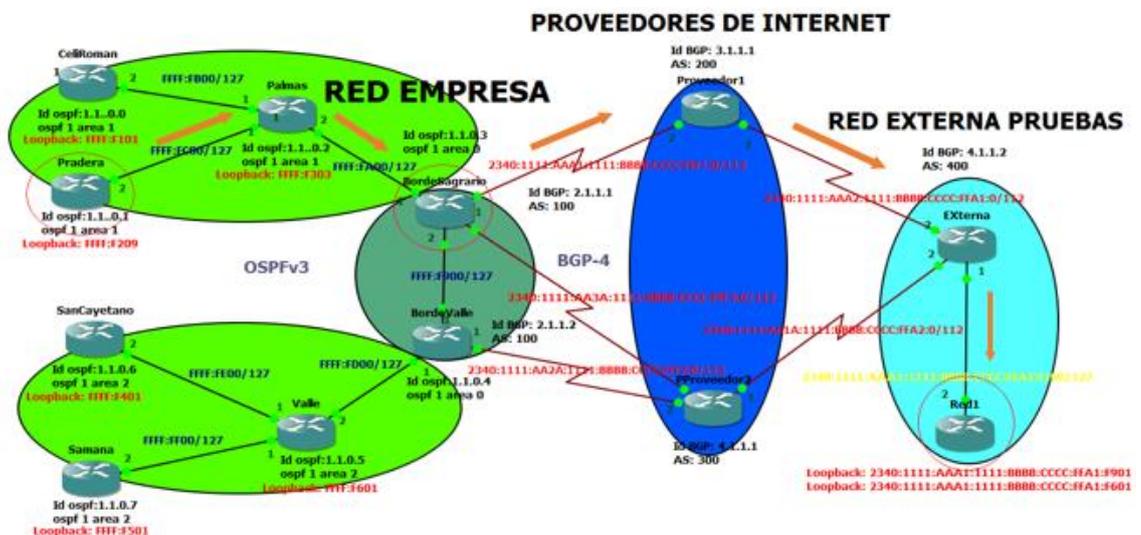


Figura 81. Red para pruebas de BGP.

A continuación se muestra las tablas de enrutamiento de los router pradera, palmas, bordesagrario, que son los nodos por los cuales saldrá la petición eco hacia la red 1.

Tabla de enrutamiento de router pradera.- Se muestra la tabla de enrutamiento del router pradera con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router Red 1, indica la distancia administrativa de bgp que es 20, en cuanto a la métrica se mantiene la misma de cuando llego redistribuida al router bordesagrario la cual es 1 esta métrica es por defecto que se mantiene en 1 cuando se redistribuye la ruta con OE2. Como se muestra en la figura 82.

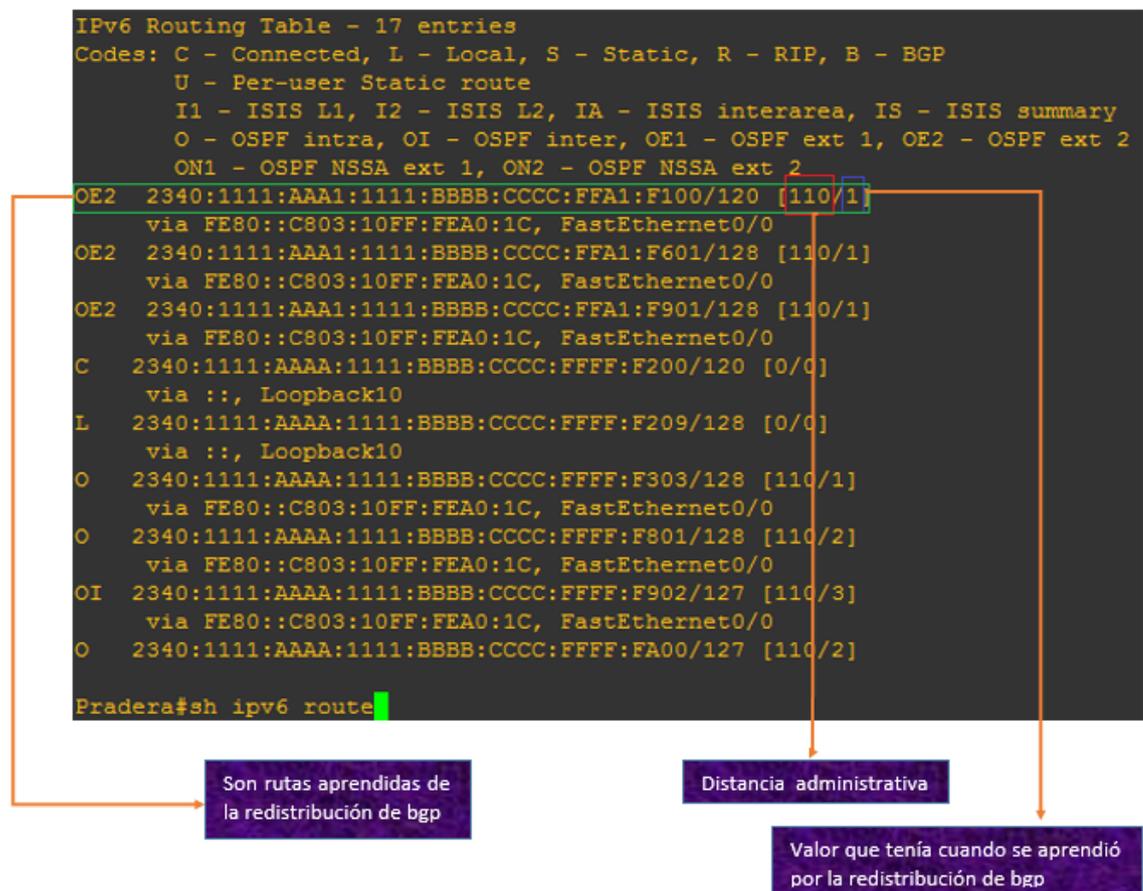


Figura 82. Tabla de enrutamiento de router pradera.

Tabla de enrutamiento de router palmas.- Se muestra la tabla de enrutamiento del router palmas con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router Red 1, en el cuadro rojo nos indica la distancia administrativa de BGP que es 20 y en el cuadro azul esta métrica que es la

que se mantiene cuando llega redistribuida al router borde/agregador la cual es 1 y no suma el costo interno del trayecto. Como se muestra en la figura 83.

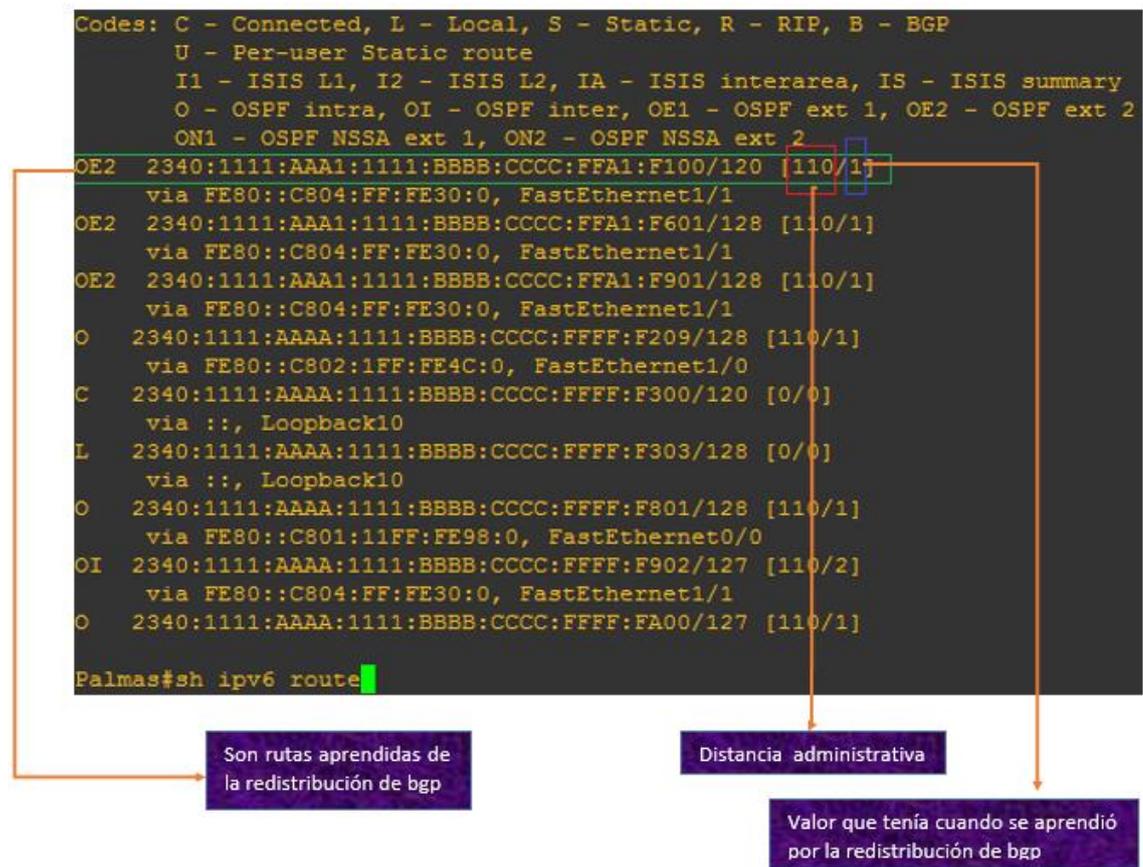


Figura 83. Tabla de enrutamiento de router palmas.

Tabla de enrutamiento de router borde/agregador.- Se muestra la tabla de enrutamiento del router borde/agregador con el comando **show ipv6 route**, la sección que se encuentra en el cuadro verde corresponde a la subred del router Red 1, en el cuadro rojo nos indica la distancia administrativa de BGP que es 20 y en el cuadro azul indica la métrica que en este caso es 0 es la métrica por defecto que adquiere. En el cuadro amarillo esta la dirección que tiene configurada de salida hacia el router proveedor 1. Como se muestra en la figura 84.

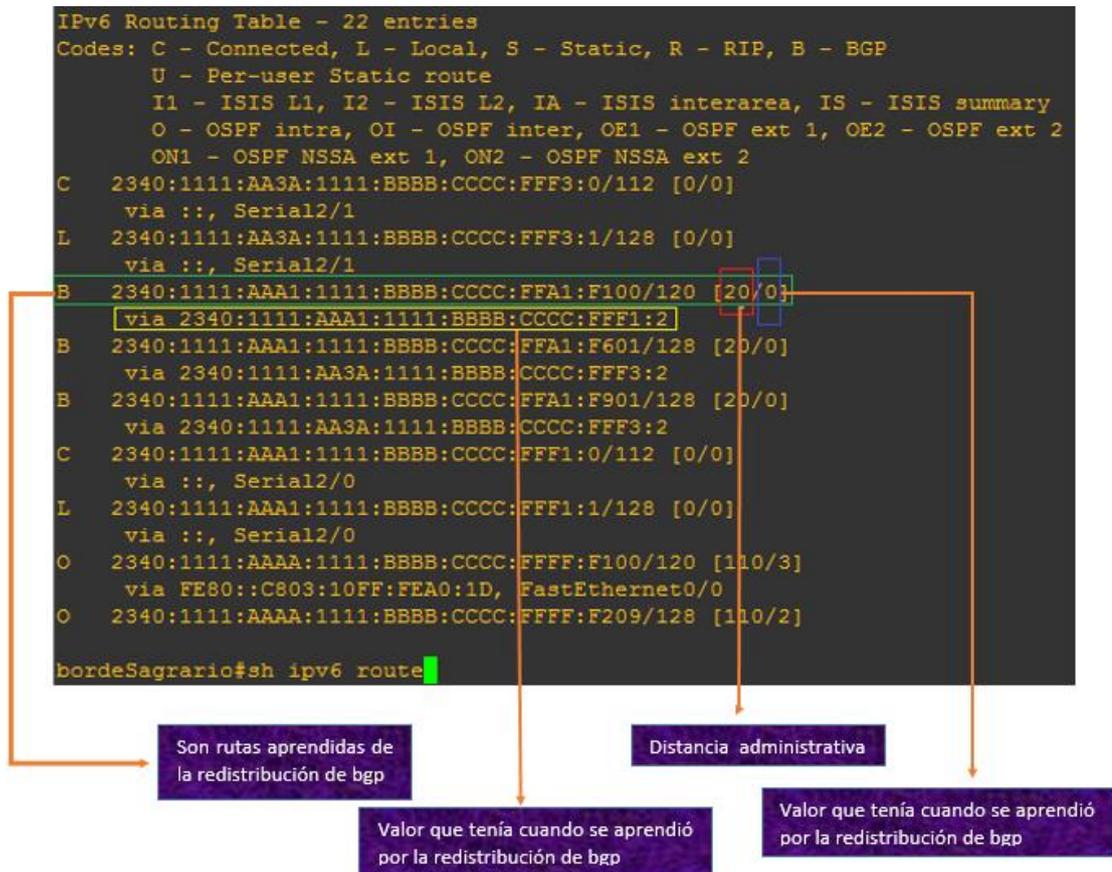


Figura 84. Tabla de enrutamiento de router bordeSagrario.

4.1.4.5. Caso 5: Verificación de los paquetes de los protocolos de enrutamiento OSPFv3 y BGP.

Análisis del enlace de los router palmas y bordeSagrario del protocolo OSPFv3 con wireshark

Para el establecimiento de comunicación de los routers adyacentes, el protocolo OSPFv3 utiliza los siguientes paquetes, que se muestran en la tabla 35.

Tabla XXXVI
PAQUETES DE COMUNICACIÓN DE OSPFV3.

Tipo	Nombre paquete	Utilización
1	Hello	Se envía periódicamente para establecer las adyacencias entre los router vecinos.
2	Data Base Description	Se intercambia este paquete cuando una adyacencia se está inicializando.
3	Link State Request	Es la respuesta que envía el router con el cual se está inicializando la comunicación y contiene la actualización de la base de datos de la topología.
4	Link State Update	Se implementa con el envío de los paquetes Link State Request.
5	Link State Acknowledgment	Es el paquete de confirmación del Link State Update.

Se muestra la figura 85 en la cual se ha señalado con el cuadrado rojo el enlace que se está capturando el tráfico por medio de wireshark.

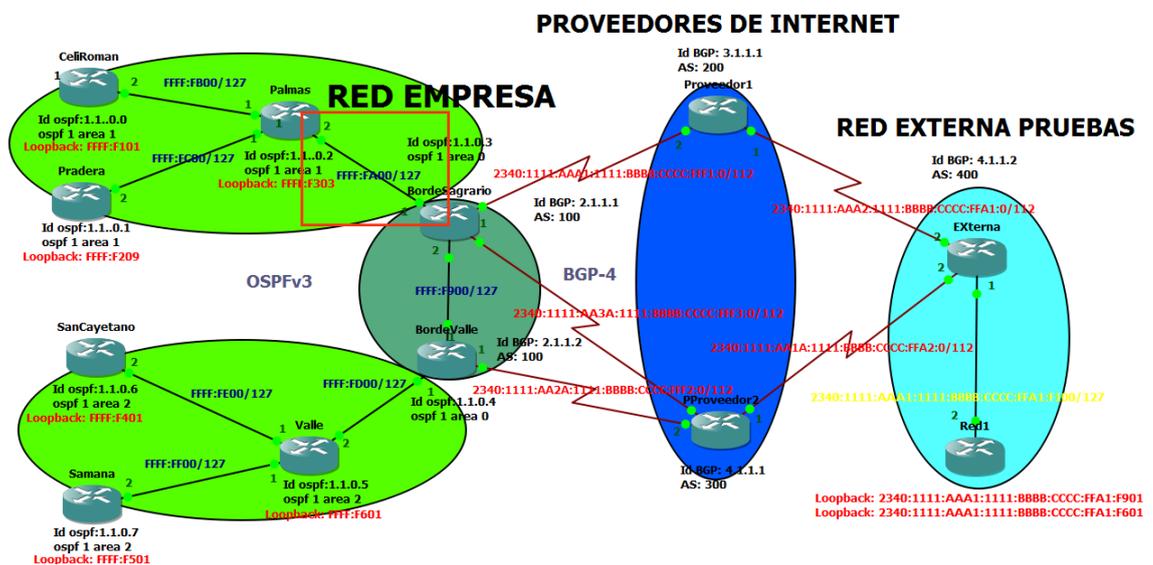


Figura 85. Red pruebas con wireshark.

Se realizó la captura en el wireshark, observamos la captura N° 1, en la paleta **source** tenemos la dirección loopback (::) que indica que esta se envía cuando se está estableciendo por primera vez la conexión. Como se muestra en la figura 86.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	::	ff02::1:ffa0:1d	ICMPv	78	Neighbor Solicitation for fe8
2	0.04686600	::	ff02::16	ICMPv	90	Multicast Listener Report Mes
3	0.04697600	::	ff02::16	ICMPv	90	Multicast Listener Report Mes
4	0.66878300	fe80::c803:10ff:fea0:1d	ff02::1	ICMPv	86	Neighbor Advertisement fe80::
5	0.69738800	fe80::c803:10ff:fea0:1d	ff02::16	ICMPv	90	Multicast Listener Report Mes
6	0.71071200	fe80::c803:10ff:fea0:1d	ff02::16	ICMPv	90	Multicast Listener Report Mes
7	0.72996700	fe80::c803:10ff:fea0:1d	ff02::16	ICMPv	90	Multicast Listener Report Mes
8	0.73006800	::	ff02::1:ffff:fa02	ICMPv	78	Neighbor Solicitation for 234
9	0.85085700	::	ff02::1:ff30:0	ICMPv	78	Neighbor Solicitation for fe8
10	1.58541400	2340:1111:aaaa:1111:bbbb:cccc:ff02::1	ff02::1	ICMPv	86	Neighbor Advertisement 2340:1
11	2.37273900	fe80::c803:10ff:fea0:1d	ff02::16	ICMPv	90	Multicast Listener Report Mes

Figura 86. Dirección loopback de establecimiento de comunicación.

En la línea N° 14 tiene el protocolo OSPF el cual es de tipo de paquete Hello, este paquete se envía a todas las interfaces adyacentes para establecer vecindades, en **Destination** ff02::5 está dirección se utiliza para enlaces locales y trabaja propiamente con OSPF. En el subrayado con rojo indica la versión de OSPF que se está utilizando en este caso 3, el tipo de mensaje utilizado que es Hello tipo 1 y el área es 1. Como se muestra en la figura 87.

No.	Time	Source	Destination	Protocol	Length	Info
14	3.12365500	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	90	Hello Packet
29	4.42094500	fe80::c804:ff:fe30:0	ff02::5	OSPF	90	Hello Packet
38	13.06846000	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet
40	14.32355100	fe80::c804:ff:fe30:0	ff02::5	OSPF	94	Hello Packet
44	23.07676000	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet
46	24.38276300	fe80::c804:ff:fe30:0	ff02::5	OSPF	94	Hello Packet
49	33.13543200	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet
51	34.34937100	fe80::c804:ff:fe30:0	ff02::5	OSPF	94	Hello Packet
55	43.10975900	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet

Open Shortest Path First

- OSPF Header
 - Version: 3
 - Message Type: Hello Packet (1)
 - Packet Length: 36
 - Source OSPF Router: 1.1.0.2 (1.1.0.2)
 - Area ID: 0.0.0.1 (0.0.0.1)
 - Checksum: 0x24c5 [correct]
 - Instance ID: IPv6 unicast AF (0)
 - Reserved: 00
- OSPF Hello Packet
 - Interface ID: 6

Figura 87. Paquete hello.

En la línea N° 64 se tiene el protocolo OSPF el cual es de tipo de paquete DB Description, este paquete se intercambió para inicializar la adyacencia con el router bordesagrario con el Id: 1.1.0.3. En el subrayado con rojo indica la versión de OSPF que se está utilizando en este caso 3, el tipo de mensaje utilizado que es DB Description tipo 2 y el área configurada que es 1. Como se muestra en la figura 88.

No.	Time	Source	Destination	Protocol	Length	Info
60	44.359053000	fe80::c804:11:fe30:0	ff02::5	OSPF	94	Hello Packet
63	44.468849000	fe80::c803:10ff:fea0:1d	fe80::c804:ff:fe30:0	OSPF	142	DB Description
64	44.530835000	fe80::c804:ff:fe30:0	fe80::c803:10ff:fea0:1d	OSPF	162	DB Description
65	44.530948000	fe80::c804:ff:fe30:0	fe80::c803:10ff:fea0:1d	OSPF	106	LS Request

<

[] Frame 64: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
 [] Ethernet II, Src: ca:04:00:30:00:00 (ca:04:00:30:00:00), Dst: ca:03:10:a0:00:1d (ca:03:10:a0:00:1d)
 [] Internet Protocol Version 6, Src: fe80::c804:ff:fe30:0 (fe80::c804:ff:fe30:0), Dst: fe80::c803:10ff:fea0:1d (fe80::c803:10ff:fea0:1d)
 [] Open Shortest Path First
 [] OSPF Header
 Version: 3
 Message Type: DB Description (2)
 Packet Length: 108
 Source OSPF Router: 1.1.0.3 (1.1.0.3)
 Area ID: 0.0.0.1 (0.0.0.1)

Figura 88. Paquete DB. Description.

En la línea N° 65 se tiene el protocolo OSPF el cual es de tipo de paquete LS Request, una vez iniciada la adyacencia se actualiza la topología de la base de datos del router. En el subrayado con rojo indica la versión de OSPF que se está utilizando en este caso 3, el tipo de mensaje utilizado que es LS Request tipo 3 y el área configurada que es 1. Como se muestra en la figura 89.

No.	Time	Source	Destination	Protocol	Length	Info
64	44.530835000	fe80::c804:ff:fe30:0	fe80::c803:10ff:fea0:1d	OSPF	162	DB Description
65	44.530948000	fe80::c804:ff:fe30:0	fe80::c803:10ff:fea0:1d	OSPF	106	LS Request
66	44.655925000	fe80::c803:10ff:fea0:1d	fe80::c804:ff:fe30:0	OSPF	82	DB Description

<

[] Frame 65: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
 [] Ethernet II, Src: ca:04:00:30:00:00 (ca:04:00:30:00:00), Dst: ca:03:10:a0:00:1d (ca:03:10:a0:00:1d)
 [] Internet Protocol Version 6, Src: fe80::c804:ff:fe30:0 (fe80::c804:ff:fe30:0), Dst: fe80::c803:10ff:fea0:1d (fe80::c803:10ff:fea0:1d)
 [] Open Shortest Path First
 [] OSPF Header
 Version: 3
 Message Type: LS Request (3)
 Packet Length: 52
 Source OSPF Router: 1.1.0.3 (1.1.0.3)
 Area ID: 0.0.0.1 (0.0.0.1)

Figura 89. Paquete LS Request.

Seleccionando la línea N° 121 de la imagen, la cual tiene como protocolo OSPF y como tipo de paquete a LS Update que son los que implementan el envío de los LS Request actualizando la tabla de topología, se observa la información del paquete la cual indica que OSPF es la versión 3, el tipo de mensaje que se utiliza es 4 y se observa el router id del router borde sagrario 1.1.0.3 que es con el cual se está realizando el intercambio de información. Como se muestra en la figura 90.

No.	Time	Source	Destination	Protocol	Length	Info
121	108.48710500	fe80::c804:ff:fe30:0	ff02::5	OSPF	118	LS Update
123	111.08518200	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	90	LS Acknowledge
124	113.06887400	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet


```

Payload length: 64
Next header: OSPF IGP (89)
Hop limit: 1
Source: fe80::c804:ff:fe30:0 (fe80::c804:ff:fe30:0)
Destination: ff02::5 (ff02::5)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Open Shortest Path First
  OSPF Header
    Version: 3
    Message Type: LS Update (4)
    Packet Length: 64
    Source OSPF Router: 1.1.0.3 (1.1.0.3)
    Area ID: 0.0.0.1 (0.0.0.1)
    Checksum: 0x0292 [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  LS Update Packet
  
```

Figura 90. Paquete LS Update.

En la línea N° 123 se tiene el protocolo OSPF el cual es de tipo de paquete LS Acknowledge, una vez actualizada la topología con LS Update se confirma la actualización con este paquete. En el subrayado con rojo indica la versión de OSPF que se está utilizando en este caso 3, el tipo de mensaje utilizado que es LS Acknowledge tipo 5 y el área configurada que es 1. Como se muestra en la figura 91.

No.	Time	Source	Destination	Protocol	Length	Info
123	111.08518200	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	90	LS Acknowledge
124	113.06887400	fe80::c803:10ff:fea0:1d	ff02::5	OSPF	94	Hello Packet


```

Frame 123: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: ca:03:10:a0:00:1d (ca:03:10:a0:00:1d), Dst: IPv6mcast_05 (33:33:00:00:00:05)
Internet Protocol Version 6, Src: fe80::c803:10ff:fea0:1d (fe80::c803:10ff:fea0:1d), Dst: ff02::5 (ff02::5)
Open Shortest Path First
  OSPF Header
    Version: 3
    Message Type: LS Acknowledge (5)
    Packet Length: 36
    Source OSPF Router: 1.1.0.2 (1.1.0.2)
    Area ID: 0.0.0.1 (0.0.0.1)
    Checksum: 0xd76f [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  LSA Header
    LS Age: 1 seconds
    Do Not Age: False
    LS Type: AS-External-LSA (0x4005)
    Link State ID: 0.0.0.0
    Advertising Router: 1.1.0.3 (1.1.0.3)
  
```

Figura 91. Paquete LS Acknowledge.

Análisis del enlace de los routers bordesagrario y proveedor 1 del protocolo BGP con wireshark

El protocolo BGP maneja diferentes tipos de paquetes los cuales sirven para realizar la comunicación entre los routers, los cuales se muestran en la tabla 36.

Tabla XXXVII
PAQUETES DE COMUNICACIÓN DE BGP

Nombre del paquete	Utilización
Open	Es el primero en enviarse tras la comunicación TCP.
Keepalive	Sirve como confirmación de unos mensajes open, si el tiempo es ilimitado de la conexión BGP se envía este paquete periódicamente.
Update	Se envía solo si se produce algún cambio en la topología.

Se muestra la figura 92 en la cual se ha señalado con el cuadrado rojo el enlace que se está capturando el tráfico de paquetes por medio de wireshark.

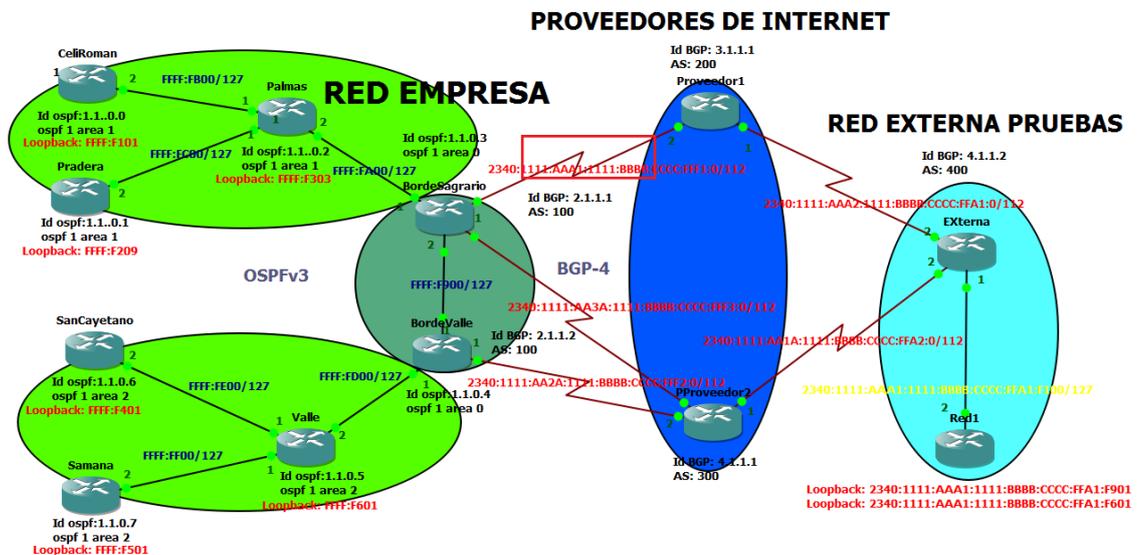


Figura 92. Red pruebas de bgp con wireshark

En la línea N° 8 tenemos el protocolo BGP el cual es de tipo de paquete OPEN, es el primero en enviarse tras la comunicación tcp. En el subrayado rojo indica el tipo de mensaje que es 1, la versión del protocolo que es 4, el sistema autónomo que es 100 y el id del router proveedor 1 que es 2.1.1.1. Como se muestra en la figura 93.

No.	Time	Source	Destination	Protocol	Length	Info
8	19.814797000	2340:1111:aaal:1111:bbbb:cccc:2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	109	OPEN Message
9	19.866465000	2340:1111:aaal:1111:bbbb:cccc:2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	128	OPEN Message


```

Frame 8: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
Cisco HDLC
Internet Protocol Version 6, Src: 2340:1111:aaal:1111:bbbb:cccc:fff1:1 (2340:1111:aaal:1111:bbbb:cccc:fff1:1), Dst: 2340:1111:aaal:1111:bbbb:cccc:fff1:2 (2340:1111:aaal:1111:bbbb:cccc:fff1:2)
Transmission Control Protocol, Src Port: 25795 (25795), Dst Port: 179 (179), Seq: 1, Ack: 1, Len: 45
Border Gateway Protocol - OPEN Message
Marker: ffffffffffffffffffffffffffffffffff
Length: 45
Type: OPEN Message (1)
Version: 4
My AS: 100
Hold Time: 180
BGP Identifier: 2.1.1.1 (2.1.1.1)

```

Figura 93. Paquete Open.

En la línea N° 145 tenemos el protocolo BGP el cual es de tipo de paquete KEEPALIVE, sirve como confirmación a un mensaje OPEN. En el subrayado rojo indica la versión del protocolo de internet utilizado, el puerto por el cual se está publicando y el tipo de mensaje. Como se muestra en la figura 94.

No.	Time	Source	Destination	Protocol	Length	Info
142	260.369952000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	ICP	64	0UL3/-1/9 [ACK] St
143	260.370125000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	109	OPEN Message
144	260.470002000	2340:1111:aaal:1111:bbbb:cccc:fff1:2	2340:1111:aaal:1111:bbbb:cccc:fff1:1	BGP	128	OPEN Message, KEEP
145	260.538196000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	83	KEEPALIVE Message
146	260.538330000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	377	UPDATE Message, UP


```

Frame 145: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Cisco HDLC
Internet Protocol Version 6, Src: 2340:1111:aaal:1111:bbbb:cccc:fff1:1 (2340:1111:aaal:1111:bbbb:cccc:fff1:1), Dst: 2340:1111:aaal:1111:bbbb:cccc:fff1:2 (2340:1111:aaal:1111:bbbb:cccc:fff1:2)
Transmission Control Protocol, Src Port: 60137 (60137), Dst Port: 179 (179), Seq: 46, Ack: 65, Len: 19
Border Gateway Protocol - KEEPALIVE Message
Marker: ffffffffffffffffffffffffffffffffff
Length: 19
Type: KEEPALIVE Message (4)

```

Figura 94 Paquete Keepalive.

En la línea N° 146 tenemos el protocolo BGP el cual es de tipo de paquete UPDATE, sirve para intercambiar las rutas de encaminamiento y solo se envía si se produce algún cambio. En el subrayado rojo indica la versión del protocolo de internet utilizado, el puerto por el cual se está publicando y el tipo de mensaje. Como se muestra en la figura 95.

No.	Time	Source	Destination	Protocol	Length	Info
143	260.370125000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	109	OPEN Message
144	260.470002000	2340:1111:aaal:1111:bbbb:cccc:fff1:2	2340:1111:aaal:1111:bbbb:cccc:fff1:1	BGP	128	OPEN Message, KEEPALIVE Message
145	260.538196000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	83	KEEPALIVE Message
146	260.538330000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	377	UPDATE Message, UPDATE Message
147	260.606075000	2340:1111:aaal:1111:bbbb:cccc:fff1:1	2340:1111:aaal:1111:bbbb:cccc:fff1:2	BGP	102	KEEPALIVE Message, KEEPALIVE Me


```

Frame 146: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface 0
Cisco HDLC
Internet Protocol Version 6, Src: 2340:1111:aaal:1111:bbbb:cccc:fff1:1 (2340:1111:aaal:1111:bbbb:cccc:fff1:1), Dst: 2340:1111:aaal:1111:bbbb:cccc:fff1:2 (2340:1111:aaal:1111:bbbb:cccc:fff1:2)
Transmission Control Protocol, Src Port: 60137 (60137), Dst Port: 179 (179), Seq: 65, Ack: 65, Len: 313
Border Gateway Protocol - UPDATE Message
Marker: ffffffffffffffffffffffffffffffffff
Length: 81
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 58
Path attributes

```

Figura 95 Paquete Update.

4.1.4.6. Caso 6: Prueba de funcionamiento de Multihoming a la red de la empresa.

Para poner a prueba Multihoming se recrea escenarios posibles que se pueden presentar en la red de la empresa.

- **Prueba de conectividad de red sagrario con red externa pruebas (prueba realizada por el enlace principal del router de borde sagrario).**

Se realiza la prueba de conectividad con el comando ping extendido de los routers de la red Sagrario a la red externa.

En la consola de la máquina virtual, se hace ping a las dos interfaces virtuales loopback que están configuradas en el router de la red externa de pruebas, escribimos el comando **ping -t 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901** que es la primer interfaces virtual y la segunda es **ping -t 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f601** las direcciones tecleadas son las Interfaces virtuales (loopback) del router de red externa. Se Observa en la consola **0% perdidos**, que significa que la conexión fue exitosa que tuvo el 100% de conectividad con el router red1 de la red externa de pruebas. La cual se muestra en la figura 96.

```
C:\Windows\system32\cmd.exe
C:\Users\Ezequiel>ping -n 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901
Debe especificar la dirección IP.
C:\Users\Ezequiel>ping -t 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901
Haciendo ping a 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901 con 32 bytes de datos:
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=845ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=773ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=789ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=868ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=789ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=811ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=763ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=875ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=980ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=552ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=568ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=651ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=698ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=525ms
Respuesta desde 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901: tiempo=559ms
Estadísticas de ping para 2340:1111:aaa1:1111:bbbb:cccc:fffa1:f901:
    Paquetes: enviados = 15, recibidos = 15, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 525ms, Máximo = 988ms, Media = 736ms
Control-C
^C
C:\Users\Ezequiel>_
```

Figura 96. Ping extendido de máquina virtual a red externa pruebas.

- **Verificar porque proveedor está siendo publicada la red sagrario hacia el internet.**

Se realiza una revisión de la tabla de enrutamiento del router borde sagrario, la cual enseña la ruta establecida por defecto que tenemos para la salida al exterior de las direcciones de la red sagrario.

En la consola del router borde sagrario, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa primero la leyenda que nos indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Seguido se observa las direcciones que tienen la letra B son las que por medio del protocolo BGP se han aprendido, la vía por la cual se han aprendido estas rutas es por medio de las q están subrayadas con rojo y es la dirección de la interfaz serial del router proveedor 1. La cual se muestra en la figura 97.

```

bordeSagrario#sh ipv6 route
IPv6 Routing Table - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B  2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [20/0]
   via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
B  2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [20/0]
   via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
B  2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [20/0]
   via 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2
C  2340:1111:AAA1:1111:BBBB:CCCC:FFF1:0/112 [0/0]
   via ::, Serial2/0
L  2340:1111:AAA1:1111:BBBB:CCCC:FFF1:1/128 [0/0]
   via ::, Serial2/0
O  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/128 [110/2]
   via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/128 [110/2]
   via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/128 [110/1]
   via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
C  2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [0/0]

bordeSagrario#

```

Figura 97. Tabla de enrutamiento de router borde sagrario.

- **Caída del enlace principal de la red sagrario y auto levantamiento de enlace de secundario 1**

Seguido de la caída del enlace principal se revisa el levantamiento del enlace secundario 1. Se observa la Figura 98 que muestra la caída del enlace principal de la red sagrario.

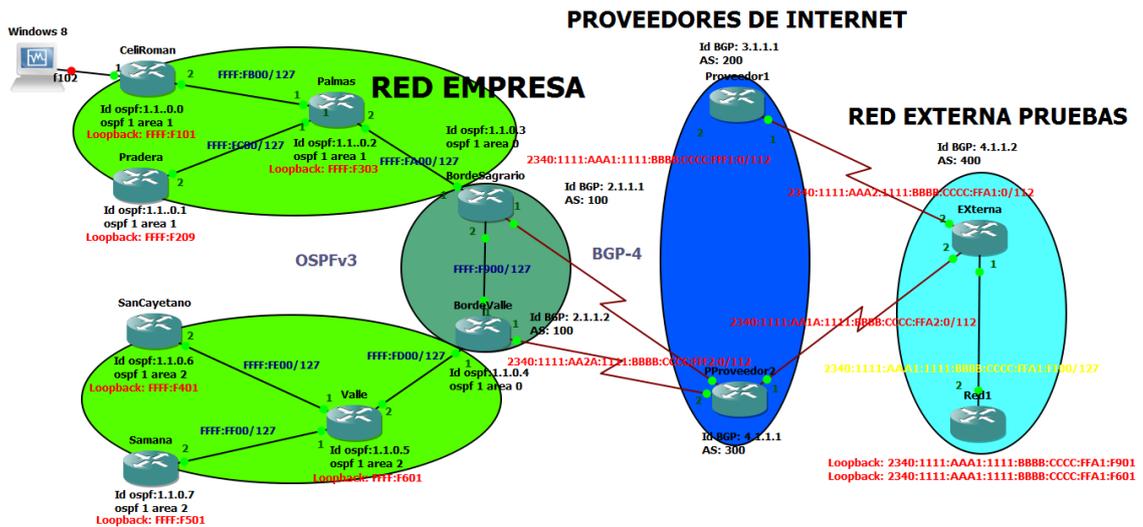


Figura 98. Topología con enlace principal caído de router borde sagrario.

Al momento de la caída del enlace router de borde sagrario con el proveedor 1, se desactivan las adyacencias entre estos routers la cual se evidencia en la figura 80 en la línea que esta subrayada con rojo, también muestra que el tiempo de vida del enlace ha expirado la cual se observa en el subrayado azul de la figura 99.

```
*May 12 16:49:17.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
bordeSagrario#
bordeSagrario#
*May 12 16:50:50.327: %BGP-5-ADJCHANGE: neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 Down BGP Notification sent
bordeSagrario#
*May 12 16:50:50.327: %BGP-3-NOTIFICATION: sent to neighbor 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 4/0 (hold time expired) 0 bytes
```

Figura 99. Adyacencias terminadas en router borde sagrario con proveedor 1.

- **Verificar tabla de enrutamiento del router de borde sagrario a la caída del enlace principal.**

Al momento de la caída del enlace del router borde sagrario con el proveedor 1 la tabla de enrutamiento del router borde sagrario cambia, la ruta que tenía para la entrada y salida de paquetes del internet se cambió por la ruta hacia el proveedor 2.

En la consola del router borde sagrario, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la leyenda que indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Seguido se observa las direcciones que tienen la letra B son las que por medio del protocolo BGP se han aprendido, la vía por la cual se han aprendido estas rutas es por medio de las que están subrayadas con rojo y es la dirección de la interfaz serial del router proveedor 2. La cual se muestra en la figura 100.

```

bordeSagrario#show ipv6 route
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2340:1111:AA3A:1111:BBBB:CCCC:FFF3:0/112 [0/0]
    via ::, Serial2/1
L   2340:1111:AA3A:1111:BBBB:CCCC:FFF3:1/128 [0/0]
    via ::, Serial2/1
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [20/0]
    via 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [20/0]
    via 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2
B   2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [20/0]
    via 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2
O   2340:1111:AAA:1111:BBBB:CCCC:FFFF:F303/128 [110/1]
    via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
C   2340:1111:AAA:1111:BBBB:CCCC:FFFF:F902/127 [0/0]
    via ::, FastEthernet1/0
L   2340:1111:AAA:1111:BBBB:CCCC:FFFF:F902/128 [0/0]
    via ::, FastEthernet1/0
C   2340:1111:AAA:1111:BBBB:CCCC:FFFF:FA00/127 [0/0]

bordeSagrario#

```

Figura 100. Taba de enrutamiento de router borde sagrario.

- **Prueba de conectividad por medio del enlace de secundario 1**

Se realiza la prueba por medio del comando **TRACEROUTE** para poder observar los saltos que tiene la petición hasta llegar a su destino. Se escribe el comando **traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601** y en el marco rojo observamos los saltos que va dando de router a router hasta llegar a su destino, los saltos indican que va por el enlace secundario 1, que esta subrayado de color verde el cual es la dirección del router proveedor 2. La cual se muestra en la figura 101.

```

Palmas#traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601

Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601

 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01 88 msec 92 msec 108 msec
 2 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 172 msec 264 msec 184 msec
 3 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 276 msec 356 msec 276 msec
 4 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 348 msec 368 msec 400 msec

```

Figura 101. Prueba de conectividad de router palmas hacia red externa pruebas.

- **Caída del enlace secundario 1 de la red sagrario y auto levantamiento de enlace de secundario 2**

Seguido de la caída del enlace secundario 1 se revisa el levantamiento del enlace secundario 2. Se observa la figura 102 que muestra la caída del enlace secundario 1 de la red sagrario.

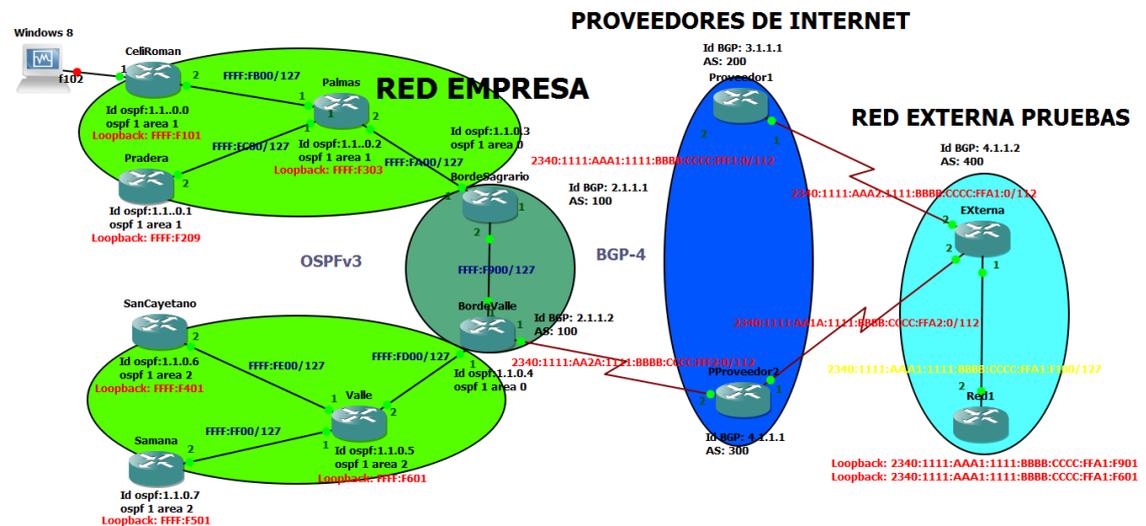


Figura 102. Topología con enlace secundario 1 caído de router borde sagrario.

Al momento de la caída del enlace router de borde sagrario con el enlace secundario 1, se desactivan las adyacencias entre estos routers la cual se evidencia en la figura 85 en la línea que esta subrayada con rojo, también muestra que el tiempo de vida del enlace ha expirado la cual se observa en el subrayado azul de la figura 103.

```

bordeSagrario#
*Jun 30 01:27:17.507: %BGP-5-ADJCHANGE: neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 Down BGP Notification sent
bordeSagrario#
*Jun 30 01:27:17.507: %BGP-3-NOTIFICATION: sent to neighbor 2340:1111:AA3A:1111:BBBB:CCCC:FFF3:2 4/0 (hold time expired) 0 bytes
bordeSagrario#

```

Figura 103. Adyacencias terminadas en router borde sagrario con proveedor 2

- **Verificar tabla de enrutamiento del router de borde sagrario a la caída del enlace secundario 1.**

Al momento de la caída del enlace del router borde sagrario con el proveedor 2 la tabla de enrutamiento del router borde sagrario cambia, la ruta que tenía para la entrada y salida de paquetes del internet se cambió por la ruta hacia el router de borde valle.

En la consola del router borde sagrario, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la leyenda que indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Seguido se observa las direcciones que tienen la letra **OE2**, que indican que el router aprendió las rutas externas por medio del protocolo OSPFv3. Las rutas son redistribuidas por medio del protocolo OSPF del router borde valle hacia el router borde sagrario. Las cual se observan en la Figura 104.

```

bordeSagrario#sh ipv6 route
IPv6 Routing Table - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [110/1]
    via FE80::C805:15FF:FEDC:1C, FastEthernet1/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [110/1]
    via FE80::C805:15FF:FEDC:1C, FastEthernet1/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [110/1]
    via FE80::C805:15FF:FEDC:1C, FastEthernet1/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F101/128 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F209/128 [110/2]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F303/128 [110/1]
  via FE80::C803:10FF:FEA0:1D, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [110/1]
  via ::, FastEthernet1/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [0/0]
  via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/128 [0/0]
bordeSagrario#

```

Figura 104. Tabla de enrutamiento de router borde sagrario.

- **Prueba de conectividad por medio del enlace de respaldo**

Se realiza la prueba por medio del comando **TRACEROUTE** para poder observar los saltos que tiene la petición hasta llegar a su destino. Se escribe el comando **tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601** y en el marco rojo se observa los saltos que va dando de router a router hasta llegar a su destino, los saltos indican que va por el enlace secundario del router borde sagrario que es por el router de borde valle. La cual se muestra en la figura 105.

```
CeliRoman#tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601
 0 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 196 msec 224 msec 148 msec
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FB01 452 msec 596 msec 588 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01 876 msec 684 msec 804 msec
 3 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 968 msec 1068 msec 1164 msec
 4 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 1540 msec 868 msec 1472 msec
 5 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 1468 msec 1664 msec 1740 msec
 6 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601
CeliRoman#
```

Figura 105. Prueba de Conectividad por enlace alternativo de router Céli Román a red externa pruebas.

Se realiza la prueba por medio del comando **TRACEROUTE** para poder observar los saltos que tiene la petición hasta llegar a su destino. Se escribe el comando **tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601** y en el marco rojo se observa los saltos que va dando de router a router hasta llegar a su destino, los saltos indican que va por el enlace secundario del router borde sagrario que es por el router de borde valle. La cual se muestra en la figura 106.

```
Pradera#tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601
 0 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 324 msec 196 msec 96 msec
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FA01 392 msec 392 msec 484 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901 680 msec 680 msec 684 msec
 3 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 864 msec 772 msec 864 msec
 4 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 1064 msec 1352 msec 1260 msec
 5 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 1456 msec 1456 msec 1560 msec
Pradera#
```

Figura 106. Prueba de Conectividad por enlace alternativo de router pradera a Red Externa pruebas.

4.1.4.7. Prueba de funcionamiento de Multihoming a la red valle.

Para poner a prueba Multihoming en el router bordevalle se recrea los escenarios posibles que pueda existir.

- **Prueba de conectividad de red valle con red externa pruebas.**

Se realiza la prueba de conectividad con el comando ping de los routers de la red sagrario a la red externa.

En la consola del router san cayetano se tecléa el comando **traceroute 2340:1111:aaa1:1111:bbbb:cccc:ff2:f901**, que indican los saltos que va realizando de router en router hasta llegar a su destino, en este caso se va dirigiendo por la salida principal que se tiene configurada que es por el proveedor 1, como se muestra en el subrayado azul de la figura 107.

```
SanCayetano#traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f901
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE01 144 msec 136 msec 136 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01 276 msec 272 msec 272 msec
 3 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 680 msec 544 msec 612 msec
 4 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 616 msec 684 msec 692 msec
 5 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901 828 msec 684 msec 892 msec
SanCayetano#
```

Figura 107. Traceroute de router san cayetano a router de red externa pruebas.

En la consola del router samaná se tecléa el comando **traceroute 2340:1111:aaa1:1111:bbbb:cccc:ff2:f601**, que indican los saltos que va realizando de router en router hasta llegar a su destino, en este caso se va dirigiendo por la salida principal que se tiene configurada que es por el proveedor 1, como se muestra en el subrayado azul de la figura 108.

```
Samana#traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF01 336 msec 300 msec 292 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01 600 msec 576 msec 592 msec
 3 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2 780 msec 792 msec 788 msec
 4 2340:1111:AA1A:1111:BBBB:CCCC:FFA2:2 988 msec 988 msec 1080 msec
 5 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 1256 msec 1464 msec 1448 msec
Samana#
Samana#
```

Figura 108. Traceroute de router samaná a router de red externa pruebas.

- **Verificar porque proveedor está siendo publicada nuestra red.**

Se realiza una revisión de la tabla de enrutamiento del router borde valle, la cual muestra la ruta establecida por defecto que tiene para la salida al exterior de las direcciones de la red valle.

En la consola del router borde valle, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa primero la legenda que indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Seguido se observa las direcciones que tienen la letra B son las que por medio del protocolo BGP se han aprendido, la vía por la cual se han aprendido estas rutas es por medio de las que están subrayadas con rojo y es la dirección de la interfaz serial del router proveedor 2. La cual se muestra en la figura 109.

```

BordeValle#sh ipv6 route
IPv6 Routing Table - 17 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:0/112 [0/0]
  via ::, Serial2/0
L 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:1/128 [0/0]
  via ::, Serial2/0
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [20/0]
  via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [20/0]
  via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
B 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [20/0]
  via 2340:1111:AA2A:1111:BBBB:CCCC:FFF2:2
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/128 [110/2]
  via FE80::C806:13FF:FE80:0, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/1]
  via FE80::C806:13FF:FE80:0, FastEthernet0/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [0/0]
  via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901/128 [0/0]
BordeValle#

```

Figura 109. Tabla de enrutamiento de router borde valle.

- **Caída del enlace principal de la red valle y auto levantamiento de enlace de respaldo**

Seguido de la caída del enlace se evidencia el levantamiento de enlace de respaldo que está configurado. Se verifica la tabla de enrutamiento del router borde valle y se observa cual es la nueva ruta de salida hacia al exterior de la red valle. En la figura 110 muestra la caída del enlace principal de la red sagrario.

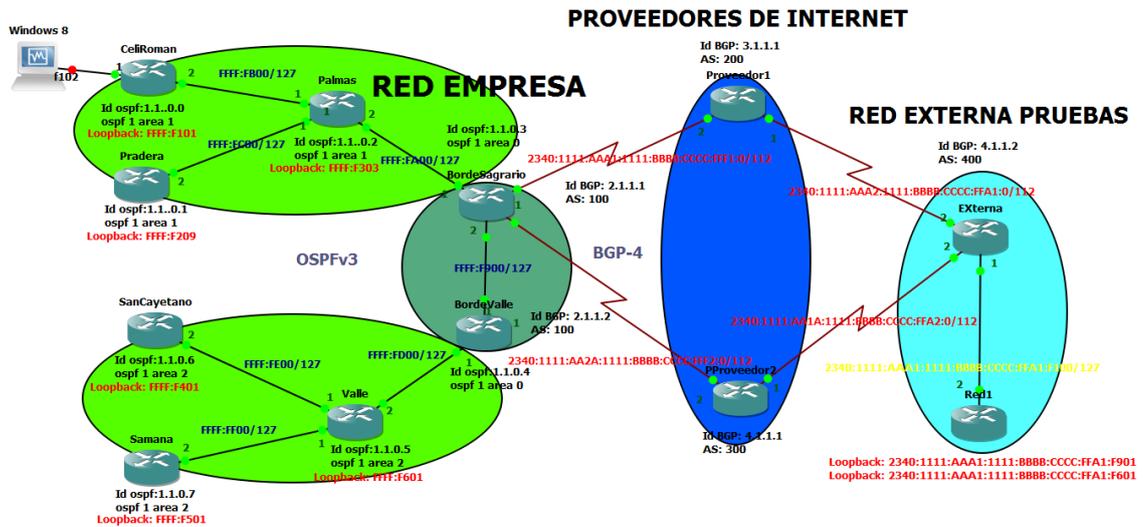


Figura 110. Topología con enlace principal caído de router borde valle.

Al momento de la caída del enlace router de borde valle con el proveedor 2, se desactivan las adyacencias entre estos routers y se ve evidenciado en la figura 111 en la línea que esta subrayada con rojo, el tiempo de vida del enlace ha expirado.

```
*May 12 23:28:31.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial
2/0, changed state to down
BordeValle#
*May 12 23:30:06.631: %BGP-5-ADJCHANGE: neighbor 2340:1111:AA2A:1111:BBBB:CC
CC:FFF2:2 Down BGP Notification sent
BordeValle#
*May 12 23:30:06.631: %BGP-3-NOTIFICATION: sent to neighbor 2340:1111:AA2A:1
111:BBBB:CCCC:FFF2:2 4/0 (hold time expired) 0 bytes
```

Figura 111. Adyacencias terminadas en router borde valle con proveedor 2.

- **Verificar tabla de enrutamiento del router de borde valle.**

Al momento de la caída del enlace del router borde valle con el proveedor 2 la tabla de enrutamiento del router borde valle cambia.

En la consola del router borde valle, se procede a teclear el comando **show IPv6 route**, el cual indica la tabla de enrutamiento del router. Se observa en la consola primero la legenda que nos indica de acuerdo a una letra el modo de aprendizaje de cada dirección IPv6. Seguido se observa las direcciones que tienen la letra **OE2**, que indican que el router aprendió las rutas externas por medio del protocolo OSPFv3. Las cual se observan en la Figura 112.

```

BordeValle#sh ipv6 route
IPv6 Routing Table - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F100/120 [110/1]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601/128 [110/1]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
OE2 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901/128 [110/1]
    via FE80::C804:FF:FE30:1C, FastEthernet1/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F401/128 [110/2]
  via FE80::C806:13FF:FEB0:0, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F501/128 [110/2]
  via FE80::C806:13FF:FEB0:0, FastEthernet0/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F601/128 [110/1]
  via FE80::C806:13FF:FEB0:0, FastEthernet0/0
C 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F900/127 [0/0]
  via ::, FastEthernet1/0
L 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F901/128 [0/0]
  via ::, FastEthernet1/0
O 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902/127 [110/1]

BordeValle#

```

Figura 112. Tabla de enrutamiento de router valle.

- **Prueba de conectividad por medio del enlace de respaldo**

Se realiza la prueba por medio del comando **TRACEROUTE** para poder observar los saltos que tiene la petición hasta llegar a su destino. Se escribe el comando **tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f901** en la consola del router san cayetano y en el marco rojo observamos los saltos que va dando de router a router hasta llegar a su destino, los saltos indican que va por el enlace secundario del router borde valle que es por el router de borde sagrario. La cual se muestra en la figura 113.

```

SanCayetano#tracert 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f901
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901
 0 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901 [110/1]
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FE01 388 msec 212 msec 196 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01 396 msec 400 msec 388 msec
 3 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 596 msec 700 msec 592 msec
 4 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 920 msec 1056 msec 1180 msec
 5 2340:1111:AAA2:1111:BBBB:CCCC:FFA1:2 1444 msec 1712 msec 1484 msec
 6 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F901 1188 msec 1280 msec 1284 msec

SanCayetano#

```

Figura 113. Traceroute de enlace secundario de router san cayetano a router de red externa pruebas.

Se realiza la prueba por medio del comando **TRACEROUTE** para poder observar los saltos que tiene la petición hasta llegar a su destino. Se escribe el comando **traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601** en la consola del router samaná y en el marco rojo observamos los saltos que va dando de router a router hasta llegar a su destino, los saltos indican que va por el enlace secundario del router borde valle que es por el router de borde sagrario. La cual se muestra en la figura 114.

```
Samana#traceroute 2340:1111:aaa1:1111:bbbb:cccc:ffa1:f601
Type escape sequence to abort.
Tracing the route to 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601
 0 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 0 msec 0 msec 0 msec
 1 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FF01 392 msec 396 msec 388 msec
 2 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:FD01 800 msec 788 msec 780 msec
 3 2340:1111:AAAA:1111:BBBB:CCCC:FFFF:F902 1188 msec 1180 msec 1184 msec
 4 2340:1111:AAA1:1111:BBBB:CCCC:FFF1:2 1592 msec 1572 msec 1576 msec
 5 2340:1111:AAA2:1111:BBBB:CCCC:FFA1:2 1956 msec 2220 msec 2040 msec
 6 2340:1111:AAA1:1111:BBBB:CCCC:FFA1:F601 2124 msec 2380 msec 2380 msec
Samana#
```

Figura 114. Traceroute de enlace secundario de router samaná a router de red externa pruebas.

g. Discusión

En el proyecto fin de carrera se realiza el análisis y emulación de una red Multihoming con los protocolos de Enrutamiento BGP y OSPFv3, a través de una red IPv6 en la empresa XNET de la provincia de Loja.

1. Desarrollo de la propuesta

Objetivo 1: Investigar cómo funcionan las diferentes métricas, políticas de configuración de BGP, OSPF bajo el protocolo IPv6, herramienta de emulación GNS3 y Multihoming.

Para cumplir con este objetivo se investigó cómo funcionan los protocolos de enrutamiento OSPFv3 Y BGP con el protocolo de internet versión 6, los cuales son los comandos que se utilizan para la configuración. Se Utiliza GNS3 para la configuración porque brinda todas las utilidades que tiene un router en la configuración real. Además se analizó Multihoming para los diversos tipos de empresas en donde se puede aplicar.

Objetivo 2: Se analiza la estructura de la red de parroquia Sagrario.

Tomando en cuenta las encuestas aplicadas al gerente y técnico de la empresa, se realizó el análisis de la red teniendo como resultado que tienen una topología tipo árbol jerárquico, que utilizan para la comunicación interna de la red, antenas AirGrid, routers que sirven para la comunicación entre las diferentes torres que tiene la empresa y los clientes. Tienen implementado un sistema de seguridad tipo WPA2 que proporciona protección a las redes inalámbricas, tienen implementado el protocolo de enrutamiento OSPF para la distribución interna de la red, utilizan el protocolo de internet IPv4. Así mismo que la red de la empresa no cuenta con una configuración de redundancia de red lo que implica que pueden existir caídas de servicio de internet por parte del servidor de internet o a su vez el fallo del router receptor de la empresa.

Diseñar la Topología de red de parroquia Sagrario.- Se diseñó la topología en base a la ubicación de las torres de la red sagrario puesto que la empresa ha realizado un estudio de acuerdo a la geografía de la parroquia para abastecer a todos clientes de la

misma, se analizó el protocolo BGP-4 y OSPFv3 siendo ellos los protocolos de enrutamiento que se configura en la red, el protocolo OSPFv3 es para la configuración interna, el protocolo BGP-4 es para la configuración externa de los router borde sagrario y valle hacia los routers proveedores de internet, se realizó el direccionamiento IPv6 para la red de la empresa, y se asignó a cada antena una dirección. La propuesta que se realizó tiene dos routers de borde, dos proveedores de internet, permitiendo así brindar redundancia a la red de la empresa, la utilización de varios ISP brinda un plus, un extra a la empresa para poder brindar el servicio de internet redundante a fallos y fiable para sus clientes.

Objetivo 3: Emulación de la red con Multihoming de la empresa XNET

Se realiza la configuración básica de los router de la red Sagrario y de los proveedores la cual consiste en poner los hostname de cada router, poner las contraseñas para el acceso al router. Se realiza la configuración IPv6 de la red, en base en el direccionamiento que está definido para cada antena de la red. Se configuro el Protocolo OSPFv3 que soporta en específico IPv6, en las interfaces de los router de la red interna, el área número 1 es para la red sagrario, el área 2 es para la red valle y el área 0 (backbone) esta los dos router de borde de la empresa. Se configuró interfaces loopback en los router céli román, pradera, san cayetano y samaná para poder realizar las pruebas de funcionamiento. Se configura con el Protocolo BGP-4 a los router de borde sagrario, borde valle, Proveedor 1 y Proveedor 2 en los cuales se definió el AS y el id que tendrá cada uno de ellos.

Pruebas.- Se realizó las pruebas de funcionamiento de la red de acuerdo al Plan de pruebas que consta en la Fase 4. Primero se establecen los objetivos que se cumplen en la fase de pruebas. Segundo se verifica la configuración del Protocolo OSPFv3 en los dispositivos de la red, revisando sus tablas de vecinos. Tercero verificar la configuración del protocolo BGP-4 en los dispositivos de la red, revisando su tabla de enrutamiento. Cuarto se realiza las pruebas de funcionamiento de Multihoming a la red, se tiene dos router de salida hacia el internet cada uno de ellos tiene un salida principal hacia el internet las pruebas se las realiza emulando la caída de cada uno de los enlaces principales y presenciando así como se realiza el auto levantamiento del router de respaldo.

2. Valoración técnica económica ambiental

Dentro de la valoración técnica en el desarrollo del trabajo investigativo se recurrió a gastos necesarios para poder alcanzar los objetivos propuestos, todos estos gastos se materializan en un plan lógico que se detalla a continuación.

La tabla 38 hace referencia a los recursos humanos empleados para realizar el desarrollo del proyecto. Cabe señalar que además se contó con el continuo asesoramiento del director de tesis, lo cual permitió que se lleve a cabo el correcto desarrollo del presente trabajo. En la tabla 41 se calcula el total de la valoración técnica económica.

TABLA XXXVIII. RECURSOS HUMANOS

Rol	Equipo de trabajo	Horas	Costo/Hora \$	Costo total \$
Tesista	Israel Alejandro López Tene	400	5.00	2000.00
Gerente de la empresa XNET	Ing. Monfilio Sanmartín	10	10.00	100.00
			Subtotal	2100.00

TABLA XXXIX. RECURSOS TÉCNICOS TECNOLÓGICOS

Hardware				
Recurso	Cantidad	Nº Horas	C. Hora	C. Total
DELL VOSTRO	1	400	1.00	400.00
Comunicaciones				
Internet	-	100h	0.70 x hora	70.00
Llamadas celular	-	5h	0.18 x hora	54.00
			Subtotal	524.00

TABLA XL. RECURSOS DE SERVICIOS

Descripción	Cantidad	C. Unitario	C. Total
Impresiones	2000 hojas	0.10	200.00
Trasporte de bus	100	0.25	25.00
Taxi	5	1.25	7.25
		Subtotal	232.25

TABLA XLI. COSTE GENERAL DE RECURSOS

Descripción	Total
Recurso humano	2100.00
Recurso técnico/tecnológico	524.00
Recurso de servicio	232.25
Subtotal	2856.25
Imprevistos (10%)	285.40
Total	3139.40

El desarrollo del presente trabajo se considera factible, pues se dispone de los recursos económicos necesarios para solventar los costos del desarrollo del proyecto, ya que el coste económico se adjudicó al autor del trabajo, debido a que la investigación se considera de carácter formativo y permitirá la obtención del título profesional, exceptuando el costo del recurso humano del director de proyecto que fue adjudicado por la universidad.

h. Conclusiones

De acuerdo a la información recolectada en la empresa XNET, a la configuración que se realizó y las pruebas realizadas para el presente proyecto de tesis, se ha podido concluir que:

- Debido al incremento de clientes en la empresa Xnet, se realizó la petición de un bloque de dirección IPv6 que satisfaga el incremento de direcciones IP que pueda tener la empresa, el cual es `2340:1111:aaaa:1111:bbbb:cccc:ffff:f/120`. Obteniendo así 16 subredes y cada una con un máximo de 256 direcciones asignables que ayudan al crecimiento de la empresa.
- Se utilizó los protocolos OSPFv3 y BGP-4 debido a que se basan en estado de enlace para descubrir vecinos, distribuir información de los enlaces, realizar administración de la topología. OSPFv3 nos permite tener segmentadas la distribución de paquetes con la utilización de las áreas y así ayudar a los router a no tener que propagar todos los mensajes que no sean de su misma área.
- La emulación de una red Multihoming es posible gracias al protocolo BGP-4 y a la manipulación de sus Path Attributes. Es factible combinar varios Path Attributes para que el resultado se acople a los requerimientos de cada red en particular.
- El uso de OSPFv3 dentro del sistema autónomo es óptimo para escenarios en los que se requiere escalabilidad, su habilidad para reaccionar y adaptarse sin perder calidad en la red es propia del protocolo y con el uso de IPv6 se aporta mayor seguridad a la red ya que dentro de sus características se incluye compatibilidad con IPSec.
- El protocolo OSPFv3 se adapta de mejor manera a las redes jerárquicas ya que dentro de cada área se puede definir el tipo de información y rutas que se va a propagar a sus vecinos. Se evita también la ejecución de tiempo de CPU de los router propagando mensajes que solo deberían publicarse en el área específica.
- La aplicación de Multihoming en la red de la empresa mejora enormemente la confiabilidad de los clientes, teniendo una redundancia de red de hasta 3 conexiones de internet en los routers de borde, consolidando así una red de la empresa robusta y tolerante a fallos.

i. Recomendaciones

- Para la elección del protocolo IGP a utilizarse dentro del sistema autónomo, el administrador de la red debe evaluar los requerimientos de la red, si el protocolo es compatible con la versión de IP, si soporta VLSM y CIDR, si necesita que la red sea dinámica.
- Brindar a cada torre de la empresa un UPS de emergencia para soportar hasta un día de carga eléctrica, para cuando se vaya la luz por cualquier acontecimiento en las viviendas, para que se pueda seguir brindando el servicio a los clientes.
- Para la configuración de los Path Attribute de BGP-4 Multihoming se debe evaluar las necesidades de la red, con el fin de escoger las configuraciones que se adapten a las necesidades del sistema autónomo.
- En el uso de BGP, se recomienda que para la configuración de un AS Multihoming este AS, no funcione como sistema autónomo (AS) de tránsito para el tráfico que proviene de internet, de manera que toda la información que viaje por el AS sea local. Para ello, no se debe anunciar hacia el exterior ninguna ruta que no tenga origen en este AS, ya que anunciar una ruta implica aceptar todo el tráfico que tenga como destino esa ruta.
- Como alcance del proyecto se recomienda la instalación del servidor Smokeping cuya funcionalidad permite medir la pérdida de paquetes y latencia en la red, así como obtener estadísticas mensuales de rendimiento, con esto se lograría evaluar el comportamiento de las salidas de la red.
- Se debe trabajar con el emulador GNS3 debido a que emula todos los módulos de un router, en el programa de Packet Tracer no me permitía configurar los comandos de bgp con ipv6, debido a ese inconveniente se trabajó con GNS3.

j. Bibliografía

- [1] C. SOLORZANO, «TRANSICION DE IPV4 A IPV6,» 30 ABRIL 2013. [En línea]. Available: <http://repositorio.ucsg.edu.ec:8080/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf>. [Último acceso: 05 Abril 2015].
- [2] U. T. D. NORTE, «Análisis del Protocolo IPv6 su evolución y aplicabilidad,» 15 01 2014. [En línea]. Available: <http://repositorio.utn.edu.ec/bitstream/123456789/1109/4/04%20ISC%20061%20CAPI TULO2.pdf>. [Último acceso: 31 abril 2015].
- [3] G. J. MALBUISSON, «Distribución de Recursos en Internet,» 15 03 2009. [En línea]. Available: <http://www.internetsociety.org/sites/default/files/Un%20buen%20equilibrio%20Distri bucio%CC%81n%20de%20recursos%20nume%CC%81ricos%20de%20Internet%20y%20 descentralizacio%CC%81n.pdf>. [Último acceso: 06 05 2015].
- [4] U. D. S. C. D. GUATEMALA, «Migración del Protocolo IPv4 a IPv6 en una red, beneficios y seguridad que conlleva este cambio,» 09 08 2009. [En línea]. Available: http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.pdf. [Último acceso: 04 05 2015].
- [5] J. M. CARRASCO, «Análisis e implementación del Protocolo OSPF para IPv6,» 16 02 2013. [En línea]. Available: <http://comunidad.udistrital.edu.co/revistavinculos/files/2013/09/An%C3%A1lisis-e- implementaci%C3%B3n-del-protocolo-de-enrutamiento.pdf>. [Último acceso: 06 05 2015].
- [6] R. S. T. CAIZA, «Implementación de un Sistema Mediante el Protocolo OSPF,» 29 08 2009. [En línea]. Available: <http://bibdigital.epn.edu.ec/bitstream/15000/1760/1/CD-2355.pdf>. [Último acceso: 31 03 2015].
- [7] U. P. SALESIANA, «Utilizando IPv6 realizar el cámcio de red con el protocolo BGP,» 20 10 2010. [En línea]. Available: <http://dspace.ups.edu.ec/bitstream/123456789/4417/1/UPS-ST000230.pdf>. [Último acceso: 09 05 2015].
- [8] A. C. T. TORRES, «Comparativa de GNS3 y Packet Tracer,» 07 09 2013. [En línea]. Available: <http://dspace.utpl.edu.ec/bitstream/123456789/4254/3/Tesis%20de%20Torres%20Tor res%20Andrea%20Cecilia.pdf>. [Último acceso: 16 04 2015].
- [9] Z. T. F. ORLANDO FLORES DUQUE, «Multihomig IPv6 caso Practico,» 23 10 2007. [En línea]. Available: <http://repositorio.espe.edu.ec/bitstream/21000/418/1/T-ESPE-021826.pdf>. [Último acceso: 17 04 2016].

- [10] J. Fleitman, *Negocios Exitosos*, Mexico: Mc Graw Hill Interamericana Editores, 2000.
- [11] Edgar Callisalla, <<Metodologías para el diseño de redes,>> 21 10 2014. [En línea].
Available:
https://www.academia.edu/8893403/METODOLOGIAS_PARA_EL_DISE%3%91O_DE_REDES_Contentido [Último acceso: 17 09 2016]

k. Anexos

Anexo 1: Encuesta al Gerente de la Empresa XNET

Universidad Nacional de Loja


1859

Área de la Energía las Industrias y los Recursos Naturales no Renovables
Carrera de Ingeniería en Sistemas

Esta encuesta se la realiza con finalidad de obtener información para realizar el tema "Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la provincia de Loja".

Nombre: Monfilio San Martín Fecha: 03-05-2015
Cargo: Gerente Institución: Xnet

Señale con un visto la sección correspondiente.

1. ¿Cuál es la topología con la que esta implementada la red de la empresa XNET?

Tipo bus

Tipo estrella

Tipo anillo

Tipo árbol

Tipo malla

Tipo mixta

Otros _____

2. ¿Cuál es el Nombre del proveedor ISP de su empresa?

TELCONET NEDETEL

3. ¿Cuál es el Protocolo de internet con que cuenta la empresa XNET?

Protocolo IPv4

Protocolo IPv6

4. ¿Cuáles son los Protocolos de enrutamiento que tiene la red de la parroquia el sagrario?

Protocolos de enrutamiento Dinámico

RIP

IGRP

OSPFV3

IS-IS

EIGRP

BGP-4

Otros OSPF

5. ¿Cuál es la marca y modelo de router que utiliza en su empresa?

CISCO

DLINK

OTROS _____

6. ¿Cuál es la marca y modelo de Switch que utiliza, en su empresa?

CISCO

DLINK

OTROS _____

7. ¿Cuáles son los servicios que presta la empresa XNET?

Internet, Camaras IP, voz IP, mantenimiento y Reparacion de Computadores

8. ¿Qué tipo de Firewall tiene la empresa?

IP Tables

9. ¿Cuál es la Misión y Visión de la Empresa XNET?

Misión - Proveer del acceso a las tecnologías de la información usando infra-estructura de telecomunicaciones de última generación, gestionado por personal calificado para brindar un servicio acorde a las necesidades de nuestros usuarios.

10. ¿Cuál es la fecha de creación de la Empresa?

31 de julio del 2011

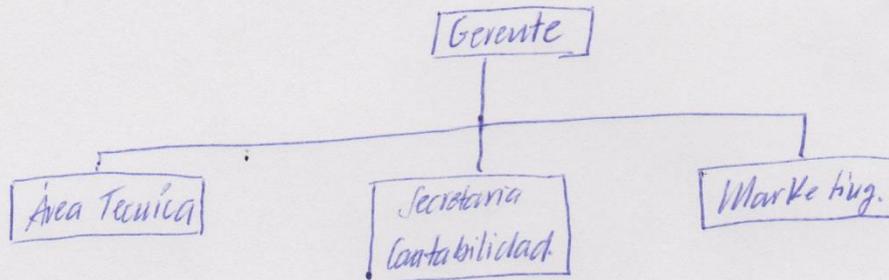
11. ¿Tiene incorporado en su red un sistema de redundancia hacia los servidores de internet?

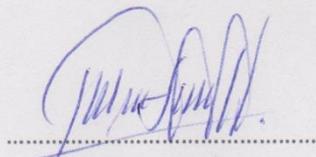
No tiene

12. ¿Qué sistema de seguridad tiene incorporado en la red wifi de la empresa?

Usa encriptación WEP/WPA, establece número máximo de dispositivos que se pueden conectar.

13. Como está estructurado el orgánico estructural de su Empresa.




Firma

Gracias por su colaboración

Anexo 2: Encuesta al técnico de la Empresa XNET

Universidad Nacional de Loja


1859

Área de la Energía las Industrias y los Recursos Naturales no Renovables
Carrera de Ingeniería en Sistemas

Esta encuesta se la realiza con finalidad de obtener información para realizar el tema "Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la provincia de Loja".

Nombre: Manfilio San Martin Fecha: 03-05-2015
Cargo: Eerente Institución: Xnet

Señale con un visto la sección correspondiente.

1. ¿Cuál es la topología con la que esta implementada la red de la empresa XNET?

Tipo bus

Tipo estrella

Tipo anillo

Tipo árbol

Tipo malla

Tipo mixta

Otros _____

2. ¿Cuál es el Nombre del proveedor ISP de su empresa?

TELCONET NEDETEL

3. ¿Cuál es el Protocolo de internet con que cuenta le empresa XNET?

Protocolo IPv4

Protocolo IPv6

4. ¿Cuáles son los Protocolos de enrutamiento que tiene la red de la parroquia el sagrario?

Protocolos de enrutamiento Dinámico

RIP

IGRP

OSPFV3

IS-IS

EIGRP

BGP-4

Otros OSPF

5. ¿Cuál es la marca y modelo de router que utiliza en su empresa?

CISCO

DLINK

OTROS _____

6. ¿Cuál es la marca y modelo de Switch que utiliza, en su empresa?

CISCO

DLINK

OTROS _____

7. ¿Cuáles son los servicios que presta la empresa XNET?

Internet, Camaras IP, voz IP, mantenimiento y Reparacion de computadores

8. ¿Qué tipo de Firewall tiene la empresa?

IP Tables

9. ¿Cuál es la Misión y Visión de la Empresa XNET?

Misión- Proveer del acceso a las tecnologías de la información usando infraestructura de telecomunicaciones de ultima generacion, gestionado por personal calificado para brindar un servicio acorde a las necesidades de nuestros usuarios.

10. ¿Cuál es la fecha de creación de la Empresa?

31 de julio del 2011

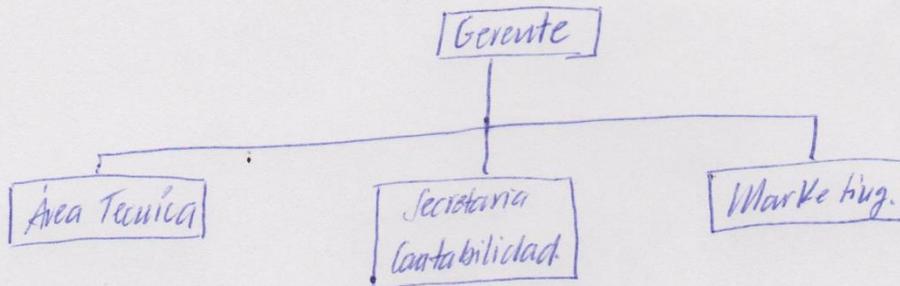
11. ¿Tiene incorporado en su red un sistema de redundancia hacia los servidores de internet?

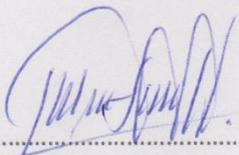
No tiene

12. ¿Qué sistema de seguridad tiene incorporado en la red wifi de la empresa?

usa encriptación WEP/WPA, establece número máximo de dispositivos que se pueden conectar

13. Como está estructurado el orgánico estructural de su Empresa.




.....
Firma

Gracias por su colaboración

Anexo 3: Fotos de las instalaciones de los equipos de red de la Empresa.



Figura 1: Caja solar protectora.



Figura 2: Torre principal de Las Palmas

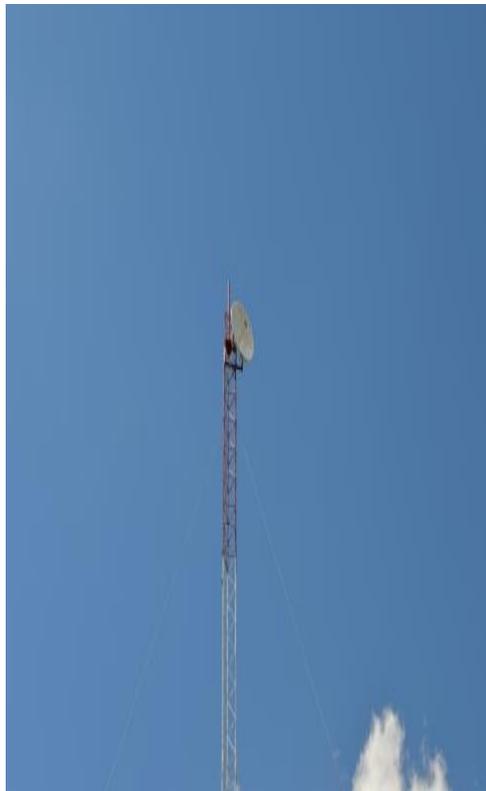


Figura 3: Torre de Céli Román



Figura 4: Rack parte delantera.

Anexo 4: Glosario de términos.

- **Backbone:** La palabra backbone se refiere a las principales conexiones troncales de internet.
- **Direccionamiento:** Permite la transmisión de datos entre host de la misma red o redes diferentes.
- **DHCP:** Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
- **Enrutamiento:** Busca un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. También es el proceso usado por el router para enviar paquetes a la red de destino.
- **Firewall (Muro de fuego-Cortafuego):** Es un elemento de software o hardware de seguridad utilizados en la red para prevenir algunos tipos de comunicaciones prohibidas, según las políticas de red que se hayan definido en función de las necesidades de la empresa.
- **Gateway:** Puerta de enlace, acceso, pasarela. Nodo en una red informática que sirve como punto de acceso a otra red.
- **Paquete:** Grupo de bits que incluye datos e información. Es la unidad de transmisión de la capa 3 del modelo OSI.
- **Ping:** Comprueba el estado de conexión con los equipos remotos por medio de los paquetes de solicitud eco y de respuesta de eco. Para determinar si un sistema IP específico es accesible en una red.
- **Router:** Aparato que reenvía un grupo de datos de un tipo especial de protocolo, desde una red lógica hacia otra red lógica, basado en la tabla de enrutamiento y el protocolo.
- **Antena (Punto multipunto):** Se aplica para una arquitectura más amplia sirviendo así como conexión para muchos clientes que se conectan a ella.
- **Antena (Punto a Punto):** Las redes punto a punto se aplican para un tipo de arquitectura de red específica, en la que cada canal de datos se usa para comunicar únicamente dos nodos.
- **ISP:** Es un proveedor de servicio de internet.
- **Hostname:** Identificador en donde se le cambia de nombre al router

- **Nat:** Permite alargar el tiempo de vida de las direcciones IPv4, permitiéndoles asignar direcciones privadas a redes para que después pueden salir al internet por medio de una IP pública.
- **Subneteo:** Dividir una dirección de red en subredes más pequeñas.
- **Router de Borde:** Router límite de la configuración interna de la red con la redes eternas.
- **Router red Externa:** Router creado para realizar las pruebas de funcionamiento de la red de la empresa XNET.
- **AS:** Sistema autónomo de una red.
- **Path Attribute:** Son los atributos de ruta del protocolo BGP.
- **P.T.:** Aplicación para emular redes.
- **IPSec:** Asegura las comunicaciones sobre el protocolo de internet. Viene incorporado en IPv6.

Anexo 5: Licencia Creative Commons.



Análisis y Emulación de Multihoming y de la publicación al Internet de servicios web, a través de una red IPv6 en la Empresa XNET de la Provincia de Loja by Israel Alejandro López is licensed under a Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional License.