



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

**“ESTUDIO DE LAS METODOLOGÍAS DE MIGRACIÓN DE IPv4 A IPv6
APLICADA A UNA PROPUESTA TÉCNICA PARA EL ISP FASTNET CIA.LTDA”**

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

PRESENTADO POR:

Danilo Santiago Hidalgo Villavicencio

Luis Rodrigo García Machado

Riobamba – Ecuador

2013

Mi agradecimiento infinito, a mí querida hermana Janeth, quien me ayudo en mi formación académica y por el apoyo incondicional e inmensurable.

Rodrigo

Mi agradecimiento a Dios por todas las oportunidades que me ha dado, a mi familia y a todas las personas que con sus palabras de aliento supieron brindarme fuerza en momentos de dificultad.

Danilo

La presente investigación está dedicada a la empresa Fastnet, por permitirnos tomar el nombre de la misma y realizar esta valiosa aportación y así culminar nuestra carrera académica.

Rodrigo

Dedico esta investigación a la Escuela Superior Politécnica del Chimborazo por el conocimiento brindado en sus aulas y a mi madre María que con su esfuerzo y sacrificio me permitió finalizar mis estudios

Danilo

FIRMA

FECHA

ING. IVÁN MENES

DECANO FACULTAD

DE INFORMÁTICA Y ELECTRÓNICA

ING. WILSON BALDEÓN

DIRECTOR ESCUELA DE INGENIERÍA

ELECTRÓNICA EN TELECOMUNICACIONES

Y REDES

ING. EDWIN ALTAMIRANO

DIRECTOR DE TESIS

ING. ALBERTO ARELLANO

MIEMBRO DEL TRIBUNAL

DIRECTOR CENTRO DOCUMENTACIÓN

NOTA DE TESIS

© DERECHOS DE AUTOR

"Nosotros, Danilo Santiago Hidalgo Villavicencio, Luis Rodrigo García Machado, somos responsables de las ideas doctrinas y resultados expuestos en esta tesis de grado, y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo".

ÍNDICE GENERAL

PORTADA

AGRADECIMIENTO

DEDICATORIA

ÍNDICE GENERAL

ÍNDICE DE ABREVIATURAS

ÍNDICE FIGURAS

ÍNDICE TABLAS

INTRODUCCIÓN

CAPÍTULO I 22

MARCO REFERENCIAL 22

1.1. ANTECEDENTES DE LA INVESTIGACIÓN 22

1.2. JUSTIFICACIÓN DE LA INVESTIGACIÓN 23

1.3. OBJETIVOS 24

1.4. OBJETIVOS GENERAL 24

1.4.1. OBJETIVOS ESPECÍFICOS..... 25

1.4.2. HIPÓTESIS..... 25

CAPÍTULO II 28

TECNOLOGÍA DE ACCESO DE BANDA ANCHA INALÁMBRICO E INTRODUCCIÓN AL PROTOCOLO IPV6 28

2.1. TECNOLOGÍAS DE ACCESO A LA BANDA ANCHA 27

2.1.1. TECNOLOGÍAS INALÁMBRICAS 28

2.2. PROTOCOLO IPV6..... 31

2.2.1. CARACTERÍSTICAS 32

2.2.2. DIRECCIONAMIENTO IPV6..... 34

2.2.2.1. DIRECCIONES UNICAST 35

2.2.2.1.1. LAS DIRECCIONES LOCALES DE ENLACE ("LINK-LOCAL"). 35

2.2.2.1.2. LAS DIRECCIONES SITE-LOCAL 36

2.2.2.1.3. LAS DIRECCIONES GLOBALES 37

2.2.2.2. DIRECCIONES MULTICAST..... 38

2.2.2.3. DIRECCIONES ANYCAST..... 41

2.2.2.4. DIRECCIONES COMPATIBLES..... 41

2.2.2.5. DIRECCIONES IPV6 PRESENTES EN HOST Y ROUTER 42

2.2.3. PLAN DE DIRECCIONAMIENTO 42

2.2.3.1.	DISTRIBUCIÓN Y ASIGNACIÓN	43
2.2.3.2.	POLÍTICAS PARA DISTRIBUCIÓN Y ASIGNACIÓN	45
2.2.4.	MECANISMOS DE TRANSICIÓN/COEXISTENCIA	46
2.2.4.1.	DUAL STACK (DOBLE PILA)	47
2.2.4.2.	TÉCNICAS DE TÚNELES	48
2.2.4.2.1.	6TO4	50
2.2.4.2.2.	6 RD.....	53
2.2.4.2.3.	TEREDO	53
2.2.4.2.4.	CARRIER-GRAY NAT	55
2.2.4.2.5.	TUNNEL BROKER (TB)	56
2.2.4.2.6.	SOFTWIRES	59
2.2.4.2.7.	6OVER4	61
2.2.4.2.8.	ISATAP	63
2.2.4.3.	TÉCNICAS DE TRADUCCIÓN	64
2.2.4.3.1.	NAT64	64
2.2.5.	RESUMEN DE TÉCNICAS EN TUNELES	69
2.2.5.1.	DESCRIPCIÓN DE CRITERIO.....	70
2.3.	HOME OFFICE.....	72
2.3.1.	CONSTRUYENDO UN SOHO CON IPv6	72
2.2.1.1.	IDENTIFICANDO LAS PARTES DE UN SOHO	72
2.3.1.1.1.	IDENTIFICACIÓN DE EQUIPOS.....	73
2.3.1.1.2.	IDENTIFICACIÓN DE SISTEMAS OPERATIVOS.....	73
2.3.1.1.3.	IDENTIFICACIÓN DE APLICACIONES	74
2.3.2.	IDENTIFICACIÓN DE LOS COMPONENTES QUE REQUIEREN CONFIGURACIÓN.	74
2.3.3.	CONFIGURANDO LOS COMPONENTES SOHO CON IPv6	75
2.2.3.1.	CONFIGURACIÓN DE LA RED INTERNA.....	76
2.2.3.2.	CONFIGURACIÓN DE LA CONEXIÓN CON EL EXTERIOR (INTERNET) .	79
CAPÍTULO III		82
METODOLOGÍAS DE MIGRACIÓN A IPV6.....		82
3.1.	ESTRATEGIAS PARA LA COEXISTENCIA Y ADOPCIÓN DE IPV6 EN ECUADOR (IETF IPV6.EC)	83
3.1.1.	ESTRATEGIAS.....	84
3.1.2.	METODOLOGÍA POR EL MINISTERIO DE TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN	84
3.2.	LACNIC- PLANIFICACIÓN IPV6	86
3.2.1.	PRE-PROYECTO.....	86
3.2.1.1.	INFORMARSE.....	86
3.2.1.2.	RELEVAMIENTO DEL IMPACTO	88
3.2.1.3.	PRIMERA EXPERIENCIA	90
3.2.1.4.	APOYO INTERNO	90
3.2.2.	DISEÑO	90
3.2.1.5.	DIRECCIONAMIENTO	91

3.2.1.6.	ENRUTAMIENTO	93
3.2.1.7.	SERVICIOS	94
3.2.1.8.	CAPACITACIÓN	95
3.2.3.	IMPLEMENTACIÓN	95
3.3.	ESCENARIOS DE ANÁLISIS PARA LA INTRODUCCIÓN DE IPv6 EN LA RED DE UN ISP (RFC 4029)	95
3.3.1.	ESCENARIOS	96
3.2.1.1.	LANZAMIENTO	96
3.2.1.2.	BACKBONE	96
3.2.1.3.	CONEXIÓN AL CLIENTE	97
3.2.1.4.	COMPLETAMENTE IPv6	97
3.3.2.	TRANSICIÓN	97
3.2.2.1.	TRANSICIÓN EN EL BACKBONE	98
3.2.2.2.	TRANSICIÓN EN LA CONEXIÓN DEL CLIENTE	98
3.2.2.3.	TRANSICIÓN EN LA RED Y EN LOS SERVICIOS	98
3.4.	IPv6 EN 3 PASOS	101
3.4.1.	PUBLICAR LAS DIRECCIONES OBTENIDAS EN INTERNET	101
3.4.2.	DESPLIEGUE EN EL BACKBONE DEL ISP	102
3.4.3.	IPv6 EN EL USUARIO FINAL	103
3.5.	MODELO SISTEMÁTICO DE MIGRACIÓN HACIA EL PROTOCOLO IPv6	104
CAPÍTULO IV		111
ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA PROVEEDORA DE INTERNET FASTNET CIA. LTDA.		111
4.1.	IPv6 EN MIKROTIK	112
4.2.	ARQUITECTURA	114
4.3.	ENLACE PRINCIPAL	115
4.4.	ESTRUCTURA DE LA RED DE CORE	115
4.5.	ESTRUCTURA DE LA RED DE DISTRIBUCIÓN	117
4.6.	ESTRUCTURA DE LA RED DE ACCESO	119
4.7.	SERVICIOS	121
4.8.	CENTRO DE OPERACIONES DE LA RED (NOC)	122
CAPÍTULO V		125
APLICACIÓN/ PROCESO DE MIGRACIÓN		125
5.1.	ETAPA 1 TODO IPv4	126
5.1.1.	EVALUACIÓN DE EQUIPOS	126
5.1.2.	ESCENARIO EN CUAL SE ENCUENTRA EL ISP FASTNET	130
5.1.3.	ALCANCE DEL PROYECTO DE IMPLEMENTACIÓN	130
5.1.4.	CAMBIO DE TECNOLOGÍA	130
5.1.5.	CAPACITACIÓN DEL PERSONAL	131
5.1.6.	COSTOS DE IMPLEMENTACIÓN	132
5.2.	ETAPA 2 TÚNELES IPv6 PARA PRUEBAS Y PARA CLIENTES OBJETIVO	135
5.2.1.	ACTUALIZACIÓN	135

5.2.2.	TUNELIZACIÓN	140
5.2.2.1.	EN EL CORE	140
5.2.2.2.	EN LOS CLIENTES	144
5.2.3.	PRUEBAS INICIALES EN LA RED	144
5.3.	ETAPA 3 IMPLEMENTACIÓN DEL NÚCLEO DUAL STACK	148
5.3.1.	ADQUISICIÓN DE UN PREFIJO DE RED IPv6	148
5.3.2.	PLAN DE CONMUTACIÓN	149
5.3.3.	CONECTIVIDAD CON EL PROVEEDOR DE NIVEL SUPERIOR.....	149
5.3.4.	PLAN DE DIRECCIONAMIENTO	152
5.3.4.1.	DIRECCIONAMIENTO NIVEL 1	153
5.3.4.2.	DIRECCIONAMIENTO NIVEL 2	156
5.3.5.	SERVICIOS	157
5.3.5.1.	ACTIVAR IPv6 EN CENTOS.....	157
5.3.5.2.	SERVIDOR MAIL	159
5.3.5.3.	SERVIDOR WEB	160
5.3.6.	HERRAMIENTA DE MONITOREO.....	161
5.4.	ETAPA 4 PROPORCIONAR CONECTIVIDAD IPV6 A LOS NODOS Y CLIENTES EXISTENTES.....	162
5.4.1.	DIRECCIONES IPv6 ESTÁTICAS	162
5.4.1.1.	ROUTER DE CORE.....	163
5.4.1.2.	SERVICIOS	164
5.4.1.3.	NODO TERRAZA HOSPITAL SAN JUAN	165
5.4.1.4.	NODO CACHA	166
5.4.1.5.	GUAMOTE.....	170
5.4.1.6.	NODO DOLOROSA	172
5.4.1.7.	NODO POLITÉCNICA	173
5.5.	ETAPA 5 EXPANDIR IPv6 A TRAVÉS DE LA RED	175

COMPROBACIÓN DE LA HIPÓTESIS176

CONCLUSIONES

RECOMENDACIONES

RESUMEN

SUMMARY

GLOSARIO

ANEXOS

CAPÍTULO VI

BIBLIOGRAFÍA

ÍNDICE DE ABREVIATURAS

AAA	Authentication, Authorization, Accounting
ADSL	Asimétric Digital Subscriber Line
AEPROVI	Asociación de empresas proveedoras de servicios de Internet
AFRINIC	African Network Information Centre
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
CATV	Televisión por cable
CMTS	Sistema de Terminación de Cable módems
CONATEL	Consejo Nacional de Telecomunicaciones
CPE	Equipo Local del Cliente
DHCPv6	Dynamic Host Configuration Protocol Version 6
DNS	Domain Name System / Service
DSL	Digital Subscriber Line
EDGE	Enhanced Data Rates
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
HFC	Hybrid Fiber Coaxial
HSDPA	High Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Corporación de Internet para la Asignación de Nombres y Números
ICMP	Protocolo de Mensajes de Control de Internet
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPng	Internet Protocol New Generation
IPsec	Internet Protocol security
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Proveedor de servicio de internet
LACNIC	Latin American and Caribbean

LAN	Local Area Network
MAC	Media Access Control
MDBA	Modulación Digital de Banda Ancha
MINTEL	Ministerio de Telecomunicaciones
MPLS	Multiprotocol Label Switching
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NOC	Centro de operaciones de Red
PDA	Personal Digital Assistant
PoP	Point of Present (Punto de presencia de la red un ISP)
RFC	Request For Comments
RIPE NCC	Centro de Coordinación de redes IP europeas
RIR	Regional Internet Registry
S.O	Sistema Operativo
SOHO	Small Office Home Office
SSH	Secure Shell
SUPERTEL	Superintendencia de Telecomunicaciones
SVA	Servicio de Valor Agregado
TCP	Transmission Control Protocol
Telnet	TELEcommunication NETwork
TFTP	Protocolo de transferencia de archivos trivial
TIC	Tecnologías de la Información y comunicación
UDP	User Datagram Protocol
UIT	Unión Internacional de Telecomunicaciones
UMTS	Universal Mobile Telecommunications System
WAN	Redes de área amplia
WLAN	Wireless Local Area Network

ÍNDICE DE FIGURAS

FIGURA II. 1 MODELO DE SISTEMA PUNTO A PUNTO. FUENTE (AUTORES).....	29
FIGURA II. 2 MODELO SISTEMA PUNTO-MULTIPUNTO. FUENTE (AUTORES).....	29
FIGURA II. 3 DIRECCIONES IPV6 RESERVADA. FUENTE: WWW.FREEBSD.ORG (FREEBSD, 2010).....	34
FIGURA II. 4 FORMATO EUI-64. FUENTE: INTRODUCCIÓN A IPV6 (PALET, 2009)	36
FIGURA II. 5 ESTRUCTURA DIRECCIÓN SITE-LOCAL. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012).....	36
FIGURA II. 6 ESTRUCTURA DIRECCIÓN GLOBAL. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012).....	37
FIGURA II. 7 JERARQUÍA DE DIRECCIONES UNICAST GLOBALES. FUENTE: DIRECCIONES "UNICAST" GLOBALES (RAMÍREZ MOSQUERA DANILO ENRIQUE, 2010).....	38
FIGURA II. 8 ESTRUCTURA DIRECCIÓN MULTICAST. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012).....	38
FIGURA II. 9 VALORES DEL CAMPO S. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012)	39
FIGURA II. 10 DIRECCIONES DE MULTICAST PREDETERMINADO. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012)	39
FIGURA II. 11 DIRECCIÓN DE NODO-SOLICITADO. FUENTE: REVISTA INSTITUCIONAL N°14 (SUPERTEL, 2012).....	40
FIGURA II. 12 ORGANISMOS DE ADMINISTRACIÓN DE DIRECCIONES. FUENTE: HTTP://LACNIC.NET (LACNIC, 2012).....	44
FIGURA II. 13 ASIGNACIÓN DE DIRECCIONES IP. FUENTE: HTTP://LACNIC.NET (LACNIC, 2012)	45
FIGURA II. 14 DUAL STACK. FUENTE: HERRAMIENTAS DE TRANSICIÓN (CONSULINTEL & 6DEPLOY, 2008).....	47
FIGURA II. 15 TÚNEL ROUTER A ROUTER. FUENTE: ESTUDIO PARA LA MIGRACIÓN DE IPV4 A IPV6 PARA LA EMPRESA PROVEEDORA DE INTERNET (MILLTEC S.A-DAVID NÚÑEZ LARA, 2009).....	48
FIGURA II. 16 TÚNEL HOST A ROUTER Y ROUTER A HOST. FUENTE: ESTUDIO PARA LA MIGRACIÓN DE IPV4 A IPV6 PARA LA EMPRESA PROVEEDORA DE INTERNET (MILLTEC S.A-DAVID NÚÑEZ LARA, 2009)	49
FIGURA II. 17 TÚNEL HOST A HOST. FUENTE: ESTUDIO PARA LA MIGRACIÓN DE IPV4 A IPV6 PARA LA EMPRESA PROVEEDORA DE INTERNET (MILLTEC S.A-DAVID NÚÑEZ LARA, 2009)	49
FIGURA II. 18 ENRUTAMIENTO 6TO4. FUENTE: (AUTORES).....	52
FIGURA II. 19 ENFOQUE CGN CON LA REDIPV4 DEL ISP. FUENTE: IETF (RFC 6264, 2011).....	56
FIGURA II. 20 MODELO DEL TÚNEL BROKER. FUENTE: IETF (RFC 3053, 2001)	57
FIGURA II. 21 TÚNEL SOFTWARE. FUENTE: HERRAMIENTAS DE TRANSICIÓN (CONSULINTEL & 6DEPLOY, 2008).....	61
FIGURA II. 22 CONFIGURACIÓN 6OVER4.FUENTE: (AUTORES)	63
FIGURA II. 23 CONFIGURACIÓN 6OVER4. FUENTE:IETF (RFC 5214,, 2008).....	64
FIGURA II. 24 LONGITUD DEL PREFIJO. FUENTE:IETF (RFC 6052, 2010).....	65
FIGURA II. 25 REPRESENTACIÓN DE DIRECCIONES IPV4 INCRUSTADAS EN DIRECCIONES IPV6 USANDO EL PREFIJO NETWORK-SPECIFIC. FUENTE:IETF (RFC 6052, 2010)	67
FIGURA II. 26 REPRESENTACIÓN DE DIRECCIONES IPV4 INCRUSTADAS EN DIRECCIONES IPV6 USANDO EL PREFIJO WELL-KNOW. FUENTE: IETF (RFC 6052, 2010).....	67
FIGURA II. 27 SOHO (SMALL OFFICE HOME OFFICE). FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009).....	72
FIGURA II. 28 PUNTO DE DEMARCACIÓN. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009).....	75
FIGURA II. 29 RED CON ENLACE DEDICADO. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009)	77
FIGURA II. 30 RED CON ENLACE DEDICADO. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009)	78
FIGURA II. 31 AUTOCONFIGURACIÓN. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009).....	78
FIGURA II. 32 SERVIDOR PARA LA AUTOCONFIGURACIÓN. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009)	79
FIGURA II. 33 ASIGNACIÓN DE PREFIJOS CASO A. FUENTE: IPV6 PARA TODOS (PALET, Y OTROS, 2009).....	80
FIGURA III. 1 METODOLOGÍA DE COEXISTENCIA Y TRANSICIÓN EN EL ECUADOR. FUENTE: IPV6 EN ECUADOR (MINTEL, 2012).....	85
FIGURA III. 2 PLANIFICACIÓN LACNIC. FUENTE: (AUTORES)	86
FIGURA III. 3 IPV6 SOBRE MPLS. FUENTE: HERRAMIENTAS DE TRANSICIÓN (CONSULINTEL & 6DEPLOY, 2008).....	102
FIGURA III. 4 IPV6 EN DUAL STACK. FUENTE: : HERRAMIENTAS DE TRANSICIÓN (CONSULINTEL & 6DEPLOY, 2008).....	103
FIGURA III. 5 ETAPAS DE DESARROLLO PARA LA MIGRACIÓN. FUENTE (AUTORES).....	106
FIGURA III. 6 SEGMENTO DE RED DE PRUEBAS EN EL ISP FASTNET. FUENTE (AUTORES).....	107
FIGURA III. 7 MODELO SISTEMÁTICO DE TRANSICIÓN PARA EL ISP FASTNET	110
FIGURA IV. 1 ARQUITECTURA DE LA RED FASTNET. FUENTE: (AUTORES)	114
FIGURA IV. 2 RED DE CORE	115
FIGURA IV. 3 NÚCLEO DE LA RED. FUENTE: (AUTORES)	116
FIGURA IV. 4 COBERTURA DE FASTNET. FUENTE: (AUTORES)	117
FIGURA IV. 5 ESTRUCTURA DE ACCESO EN EL CLIENTE PARA ACCEDER AL ISP. FUENTE: (AUTORES).....	119
FIGURA IV. 6 SERVICIOS ALOJADOS EN FASTNET. FUENTE (AUTORES).....	121
FIGURA IV. 7 CENTRO DE OPERACIONES DE FASTNET. FUENTE (EL AUTOR).....	122
FIGURA IV. 8 ADMINISTRACIÓN POR DUDE (MIKROTIK.). FUENTE: NOC FASTNET CIA. LTDA.	123
FIGURA V. 1 PRESENCIA DEL PROTOCOLO IPV6 EN LOS EQUIPOS DE LA CAPA DE ACCESO. FUENTE: (AUTORES).....	126
FIGURA V. 2 PORCENTAJE DE EQUIPOS EN LA CAPA DE DISTRIBUCIÓN FUENTE: (AUTORES).....	127
FIGURA V. 3 PORCENTAJE DE EQUIPOS EN LA CAPA DE ACCESO. FUENTE: (AUTORES).....	128
FIGURA V. 4 PORCENTAJE DE EQUIPOS PRESENTES EN LOS CLIENTES. FUENTE: AUTOR.....	129

EN LA FIGURA V.5 SE MUESTRA DETALLES DE LA CAPACITACIÓN QUE HEMOS CONSIDERADO FAVORABLE PARA EL PERSONAL DE FASTNET.	132
FIGURA V. 6 PROPUESTA DE CAPACITACIÓN POR NETSOSE. FUENTE: HTTP://WWW.NETSOSE.COM/IPV6ADMINISTRADORES.HTML	132
FIGURA V. 7 ACTUALIZACIÓN DE ROUTER DE DISTRIBUCIÓN. FUENTE: (AUTORES).	136
FIGURA V. 8 DUAL STACK EN EL EQUIPO. FUENTE (AUTORES)	136
FIGURA V. 9 OPCIONES DE RUTEO. FUENTE (AUTORES)	137
FIGURA V. 10 CARACTERÍSTICAS IPV6 PARA TÚNELES.	137
FIGURA V. 11 INGRESO VÍA WINBOX. FUENTE: (AUTORES).....	138
FIGURA V. 12 ACTUALIZACIÓN DE ROUTER DE ACCESO FUENTE: (AUTORES)	138
FIGURA V. 13 PRESENCIA DEL PAQUETE IPV6 EN ROUTER MIKROTIK. FUENTE (AUTORES).	139
FIGURA V. 14 ACTUALIZACIÓN DE FIRMWARE. FUENTE (AUTORES)	139
FIGURA V. 15 INCOMPATIBILIDAD IPV6 CON UBIQUITI. FUENTE (AUTORES).....	139
FIGURA V. 16 CONFIGURACIÓN DE CPE TP-LINK TL-WDR3500. FUENTE (AUTORES).....	140
FIGURA V. 17 IP 6TO4 PÚBLICA. FUENTE(AUTORES).....	141
FIGURA V. 18 PSEUDO INTERFACE PARA 6TO4. FUENTE (AUTORES).	141
FIGURA V. 19 CONFIGURACIÓN DE IPV6 EN LA INTERFAZ TÚNEL. FUENTE (AUTORES).	142
FIGURA V. 20 CONFIGURACIÓN DE RUTA IPV6. FUENTE (AUTORES)	142
FIGURA V. 21 RESPUESTA DE DNS DE GOOGLE. FUENTE (AUTORES).	143
FIGURA V. 22 TRÁFICO IPV6 GENERADO. FUENTE (AUTORES).	143
FIGURA V. 23 ESTRUCTURA DE LA RED DE PRUEBAS. FUENTE (AUTORES).	145
FIGURA V. 24 CONFIGURACIÓN DE IP'S EN EL DISTRIBUIDOR. FUENTE (AUTORES).	146
FIGURA V. 25 CONFIGURACIÓN DE LA ANTENA DE IRRADIACIÓN. FUENTE (AUTORES).	146
FIGURA V. 26 CONFIGURACIÓN ANTENA EN MODO AP. FUENTE (AUTORES)	147
FIGURA V. 27 RUTA ESTÁTICA POR DEFECTO EN ROUTER DE ACCESO.	147
FIGURA V. 28 RED ASIGNADA A FASTNET. FUENTE: HTTP://BGP.HE.NET/AS27947#_PREFIXES6	148
FIGURA V. 29 PROPAGACIÓN DE RUTAS IPV6 EN TELCONET. FUENTE: HTTP://BGP.HE.NET/AS27947#_GRAPH6	148
FIGURA V. 30 CONECTIVIDAD CON EL PROVEEDOR DE NIVEL SUPERIOR. FUENTE (AUTORES).	150
FIGURA V. 31 PING A DNS IPV6 GOOGLE DESDE EL ROUTER TELCONET.....	151
FIGURA V. 32 /ETC/MODPROBE.CONF. FUENTE: (AUTORES).	158
FIGURA V. 33 /ETC/MODPROBE.CONF. FUENTE: (AUTORES).	158
FIGURA V. 34 /ETC/SYSCONFIG/NETWORK. FUENTE (AUTORES).	158
FIGURA V. 35 /ETC/SYSCONFIG/NETWORK-SCRIPTS/IFCFG-ETH0. FUENTE: (AUTORES).	158
FIGURA V. 36 LÍNEA DE COMANDOS PARA REINICIAR EL SISTEMA. FUENTE (AUTORES).....	158
FIGURA V. 37 /ETC/POSTFIX/MAIN.CF. FUENTE (AUTORES).	159
FIGURA V. 38 LÍNEA DE COMANDO PARA REINICIAR EL SERVICIO POSTFIX. FUENTE(AUTORES).	159
FIGURA V. 39 /ETC/DOVECOT.CONF. FUENTE: (AUTORES).	160
FIGURA V. 40 LÍNEA DE COMANDOS PARA REINICIAR EL SERVICIO DOVECOT. FUENTE (AUTORES).	160
FIGURA V. 41 /ETC/HTTPD/CONF/HTTPD.CONF. FUENTE: (AUTORES).	160
FIGURA V. 42 /ETC/HTTPD/CONF/HTTPD.CONF. FUENTE: (AUTORES).	161
FIGURA V. 43 LÍNEA DE COMANDOS PARA REINICIAR EL SERVICIO HTTPD. FUENTE (AUTORES).	161
FIGURA V. 44 EQUIPOS EN EL NODO HOSPITAL SAN JUAN. FUENTE (AUTORES).	165
FIGURA V. 45 EQUIPOS EN EL NODO CACHA. FUENTE (AUTORES).	167
FIGURA V. 46 EQUIPOS EN EL NODO GUAMOTE. FUENTE (AUTORES).	171
FIGURA V. 47 EQUIPOS EN EL NODO DOLOROSA. FUENTE (AUTORES).	172
FIGURA V. 48 EQUIPOS EN EL NODO POLITÉCNICA. FUENTE (AUTORES)	174

ÍNDICE DE TABLAS

TABLA II. I FRECUENCIA DE MODULACIÓN DIGITAL DE BANDA ANCHA. FUENTE: WWW.CONATEL.GOB.EC (SUPERTEL, 2010)	28
TABLA II. II RESUMEN TÉCNICA DE TÚNELES. FUENTE (AUTORES)	69
TABLA III. I RECURSOS DISPONIBLES DE INVESTIGACIÓN PARA EL ESTUDIO DE IPV6 PLANIFICANDO IPV6 (LACNIC, 2012)	86
TABLA III. II SEGUNDA ETAPA EN EL DISEÑO DE UN PRE PROYECTO IPV6. FUENTE: PLANIFICANDO IPV6 (LACNIC, 2012)	89
TABLA III. III EQUIPOS CON SOPORTE IPV6. FUENTE: PLANIFICANDO IPV6 (LACNIC, 2012)	90
TABLA III. IV PLAN DE DIRECCIONAMIENTO. FUENTE: PLANIFICANDO IPV6 (LACNIC, 2012)	91
TABLA III. V PLAN DE ENRUTAMIENTO FUENTE: PLANIFICANDO IPV6 (LACNIC, 2012)	94
TABLA III. VI SERVICIOS PRESENTES EN UNA RED. FUENTE (AUTORES)	95
TABLA III. VII HERRAMIENTAS DE MONITORIZACIÓN PARA IPV6. FUENTE: (AUTORES)	100
TABLA III. VIII TÉCNICAS DE MIGRACIÓN PARA UN ISP. FUENTE (AUTORES)	105
TABLA IV. I SOPORTE IPV6 POR PARTE DE MIKROTIK. FUENTE (AUTORES)	112
TABLA IV. II SOPORTE DE EQUIPOS EN EL NÚCLEO. FUENTE (AUTORES)	116
TABLA IV. III ANTENAS UBNT EN LA RED DE DISTRIBUCIÓN. FUENTE (AUTORES)	118
TABLA IV. IV RUTEADORES PRESENTES EN LA RED DE DISTRIBUCIÓN . FUENTE (AUTORES)	118
TABLA IV. V EQUIPOS DE ACCESO Y SOPORTE IPV6. FUENTE (AUTORES)	120
TABLA IV. VI CANTIDAD DE CUENTAS EN FASTNET. FUENTE(HTTP://SUPERTEL.GOB.EC)	120
TABLA IV. VII EQUIPOS CPE PRESENTES EN LOS USUARIOS. FUENTE (AUTOR)	120
TABLA IV. VIII Dns FASTNET. FUENTE (AUTORES)	121
TABLA IV. IX SOPORTE IPV6 EN LOS SERVIDORES. FUENTE (AUTORES)	122
TABLA IV. X SOPORTE IPV6 EN EL SOFTWARE. FUENTE (AUTORES)	124
TABLA V. I CANTIDAD DE ROUTERS PARA CAMBIO. FUENTE (AUTORES)	133
TABLA V. II CPE'S MODELO/PRECIO. FUENTE (AUTORES)	133
TABLA V. III COSTOS DE CAPACITACIÓN. FUENTE (AUTORES)	134
TABLA V. IV COSTO INVERSIÓN INICIAL	134
TABLA V. V IP'S EN EL EQUIPO DE DISTRIBUCIÓN. FUENTE (AUTORES)	145
TABLA V. VI DIRECCIONES IPV6 EN EL ROUTER DE ACCESO. FUENTE (AUTORES)	147
TABLA V. VII DIRECCIÓN IPV6 UNICAST GLOBAL. FUENTE (AUTORES)	149
TABLA V. VIII ASIGNACIÓN DE DIRECCIONES EN EL ROUTER TELCONET. FUENTE (AUTORES)	150
TABLA V. IX DIRECCIONES IPV6 EN EL ROUTER CORE FASTNET. FUENTE (AUTORES)	151
TABLA V. X CÁLCULO DE SUBREDES IPV6. FUENTE (AUTORES)	153
TABLA V. XI NÚMEROS DE DIRECCIONES IPV6'S ASIGNADO PARA USO EN LA INFRAESTRUCTURA. FUENTE (AUTORES)	156
TABLA V. XII DIRECCIONES IPV6 ROUTER CORE HOSPITAL SAN JUAN. FUENTE (AUTORES)	164
TABLA V. XIII DIRECCIONES IPV6 EN LOS SERVIDORES. FUENTE (AUTORES)	165
TABLA V. XIV ASIGNACIÓN DE DIRECCIONES. FUENTE (AUTORES)	166
TABLA V. XV ASIGNACIÓN DE DIRECCIONES NODO CACHA. FUENTE (AUTORES)	167
TABLA V. XVI ASIGNACIÓN DE DIRECCIONES EN EL NODO GUANO. FUENTE (AUTORES)	169
TABLA V. XVII ASIGNACIÓN DE DIRECCIONES EN EL NODO CHAMBO. FUENTE (AUTORES)	169
TABLA V. XVIII DIRECCIONES IPV6 EN ROUTER TELCONET. FUENTE (AUTORES)	170
TABLA V. XIX ASIGNACIÓN DE DIRECCIONES EN EL NODO GUAMOTE. FUENTE (AUTORES)	171
TABLA V. XX DIRECCIONES IPV6 EN ROUTER TELCONET. FUENTE (AUTORES)	172
TABLA V. XXI ASIGNACIÓN DE DIRECCIONES EN EL NODO DOLOROSA. FUENTE (AUTORES)	173
TABLA V. XXII DIRECCIONES IPV6 EN ROUTER TELCONET. FUENTE (AUTORES)	174
TABLA V. XXIII ASIGNACIÓN DE DIRECCIONES DEL NODO POLITÉCNICA FUENTE (AUTORES)	175

INTRODUCCIÓN

El protocolo IPv6 nace como el sucesor de IPv4, llenando la necesidad de incrementar direcciones IP en el internet ya que el crecimiento vertiginoso de dispositivos en la red así lo demanda, esta oportunidad de crear un nuevo protocolo también ha sido tomado en cuenta para mejorar aspectos de conectividad, seguridad y movilidad.

En el Ecuador los Carrier de Telecomunicaciones¹ soportan tránsito IPv6 pero los ISP de nivel medio empiezan a desarrollar planes para el soporte del nuevo protocolo ante las políticas Nacionales.

El ISP² FASTNET Cia. Ltda. tomará la iniciativa de involucrarse en el deployment IPv6, por esta razón la presente investigación tiene como objetivo principal estudiar las metodologías de migración de IPv4 a IPv6 para aplicarla a una propuesta técnica para el desarrollo de IPv6 en la red del ISP.

Esta investigación consta de 5 capítulos distribuidos de la siguiente manera:

El capítulo uno es el marco referencial que describe la importancia de la investigación y los antecedentes del nuevo protocolo.

El capítulo dos, menciona los aspectos teóricos necesarios para comprender la arquitectura del ISP y del nuevo protocolo, que posteriormente servirá para el desarrollo de la metodología.

El capítulo tres, describe las metodologías de migración hacia IPv6, que son las mejores prácticas expuestas por la comunidad involucrada en el desarrollo tecnológico de las comunicaciones.

¹ **Carrier de Telecomunicaciones:** Son empresas que proporcionan transporte de telefonía, video y datos.

² **ISP:** Un proveedor de servicios de Internet o ISP, es una empresa que brinda conexión a Internet a sus clientes a través de un medio alámbrico, inalámbrico u óptico.

El capítulo cuatro, analiza la situación actual del ISP FASTNET, describiendo si el hardware y el software presente soportan IPv6, para posteriormente ubicarlo en el escenario de transición más adecuado con referencia a las metodologías.

El capítulo cinco, propone una metodología a seguir para migrar hacia IPv6 en la infraestructura del ISP, del cual se desprende que el mecanismo DUAL STACK estará presente en la red.

La propuesta técnica finaliza con una red completamente IPv6, con el cambio de equipos en sitios en los que actualmente no soportan el nuevo protocolo.

Finalmente se espera que el presente documento se convierta en una metodología de migración al nuevo protocolo de internet a ser implementado totalmente en el ISP Fastnet y aquellos ISP que en su infraestructura manejen tecnología inalámbrica de tipo Mikrotik³ y Ubiquiti⁴, que cabe mencionar en la zona centro del país, están presentes en un número considerable.

³ **Mikrotik:** Se dedica principalmente a la venta de productos de hardware de red como routers denominados RouterBoard y switches también conocidos por el software que lo integra, denominado RouterOS y SwOS.

⁴ **Ubiquiti:** Ubiquiti Networks provee equipamiento en hardware y software orientado a comunicaciones inalámbricas, presenta varias plataformas AirMax™, Unifi™, AirFiber™, airVision™, MFI™ y EdgeMAX™

CAPÍTULO I

MARCO REFERENCIAL

1.1. ANTECEDENTES DE LA INVESTIGACIÓN

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA) del Departamento Estadounidense de Defensa.

Internet comenzó siendo una red informática de ARPA llamada ARPA net que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. Ya por 1989 World Wide Web se desarrolló por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN).

Cuando se creó el protocolo IP en los años 70, no se pensó en el éxito que iba tener el internet en todo el mundo, por lo tanto no se provisionó el agotamiento de direcciones IPv4.

Para solucionar en parte el consumo de direcciones IPv4 se crearon técnicas de uso eficiente, traducción de direcciones y rangos de direcciones privadas, así:

En 1993 se publica el RFC 1519 que da las pautas para la implementación de CIDR.

En 1994 se publica el RFC 1631 que introduce el protocolo NAT.

En 1996 se acuerda el RFC 1918 que especifica los espacios de direccionamiento IP "privados".

A partir del 2001 el espacio de direccionamiento IPv4 empezó a agotarse ya para el 2005 se alcanza la asignación del 75% del espacio de direccionamiento IPv4 posible.

Para el 2009 comienzan las dificultades para el mantenimiento del crecimiento de Internet en los llamados países desarrollados.

A pesar que desde 1998 la IETF adoptó el protocolo IPv6 desarrollado por Steve Deering y Craig Mudge, su utilización estuvo por mucho tiempo ajustada a unas pocas redes, en su mayoría de carácter universitario o de investigación, pero esto empezó a cambiar con el advenimiento de sistemas operativos que traen IPv6 habilitado por defecto y especialmente en el 2012, con la realización el "IPv6 Launch", coordinado por la Internet Society (ISOC) en donde los proveedores de contenido (Facebook, Yahoo, Akamai, Google, Microsoft, entre otras) habilitaron acceso por IPv6 en sus redes/portales de forma indefinida.

1.2. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Con relación a los acuerdos ministeriales del Ministerio de Telecomunicaciones del Ecuador y políticas regionales en el ámbito de las telecomunicaciones y la implantación de IPv6 en el Ecuador, Fastnet por ser un ISP de servicios Home debe admitir en su red y plataforma el curso normal del tráfico de Ipv6 en coexistencia con IPV4 ya que en la actualidad de los 176 proveedores de algún servicio de telecomunicaciones tan solo 3 permiten aquella tecnología en sus redes, SUPERTEL (10).

Por lo que es necesario de manera apremiante el emprendimiento de metas y estrategias conjuntas para la adopción del nuevo protocolo de Internet (IPv6) en proveedores de servicios de internet, de forma que se promueva una correcta coexistencia y transición y se impulse el desarrollo de nuevas plataformas y contenidos que originen el adelanto económico y la

promoción del conocimiento en la región, favoreciendo también en aspectos técnicos como expansión, seguridad, velocidad en servicios multimedia y oportunidad para la mejora de su conectividad.

Al mismo tiempo la transición hacia IPv6, será una oportunidad para el estado de promover nuevas formas de negocios para el sector empresarial, basados en la generación de conocimiento y apropiación de tecnologías disponibles para la comunicación y aprendizaje sobre Internet.

Además FASTNET pretende establecer sus planes de direccionamiento e iniciar los trámites para la solicitud de recursos de direccionamiento IPv6 ya que la implantación de normas conjuntas y estandarizadas en el ámbito de la adopción de IPv6, se vuelve imperiosa debido a la necesidad de unificar criterios para el acceso a Internet en la región y desarrollo de nuevas tecnologías, en donde los ingenieros de las TICs deben enfocar sus esfuerzos diseñando metodologías para la convivencia así como para la transición dando con esto y lo mencionado anteriormente la relevancia del caso a esta investigación ya que además la incorporación de este nuevo protocolo es impulsado por el programa "*Recursos de banda ancha*", que forma parte del **Plan Nacional de Banda Ancha** del Ecuador.

Finalmente nuestra investigación radica particularmente en los pasos de transición a IPv6 de toda una infraestructura de un proveedor de servicios de internet que brinda internet a usuarios comunes, llegando así a determinar una proyección técnica debidamente sustentada, para dejar de usar el protocolo IPv4.

1.3. OBJETIVOS

1.4. OBJETIVOS GENERAL

- Estudiar las metodologías de migración de IPv4 a IPv6 para aplicar a una propuesta técnica para el ISP Fastnet Cia. Ltda.

1.4.1. OBJETIVOS ESPECÍFICOS

- Analizar las metodologías de transición para fundamentarnos en las mejores prácticas de migración para un ISP.
- Crear un modelo sistemático de migración de acuerdo a las necesidades y requerimientos del ISP.
- Elaborar una propuesta técnica y económica para la migración a ipv6 de la infraestructura de Fastnet Cía. Ltda.

1.4.2. HIPÓTESIS

El análisis de las metodologías de migración a ipv6 permitirá elaborar un modelo sistemático de migración acorde a los requerimientos del ISP Fastnet Cía. Ltda.

CAPÍTULO II

TECNOLOGÍA DE ACCESO DE BANDA ANCHA INALÁMBRICO E INTRODUCCIÓN AL PROTOCOLO IPv6

Entre los varios identificadores que se manejan en Internet tenemos el Protocolo de Internet (IP, "Internet Protocol") conocido como "dirección IP". Estas direcciones permiten identificar unívocamente cualquier interfaz dentro de una red que utiliza IP, como es el caso de Internet. Estos identificadores son números binarios con un número limitado de bits, 32 en el caso de las direcciones IPv4, es decir 4200 millones de direcciones posibles, descontando algunos rangos reservados para usos especiales, la cantidad de direcciones realmente utilizable se reduce a alrededor de 3700 millones de direcciones IPv4. Esa cantidad de direcciones pareció ser suficiente en los albores del Internet donde la cantidad de redes y computadores interconectados era relativamente poca, pero el vertiginoso crecimiento de la penetración mundial de Internet (hoy con una población de más de 7.000 millones de personas) han hecho que esa cantidad quede corta.

Estudios económicos demuestran que un incremento del 10% en la penetración del acceso a

Internet en un país genera un crecimiento del 1% en el PIB⁵, además el internet es considerado como un instrumento habilitante de derechos humanos fundamentales como la libertad de expresión, de ahí que el plan de gobierno de muchos países considera alguna medida para lograr la masificación del Internet, SUPERTEL (10).

Por otra parte, muchos dispositivos que antes funcionaban sin conexión de red requieren o requerirán de direcciones IP para aprovechar al máximo nuevas funcionalidades, conformando así lo que hoy se conoce como el "*Internet de las cosas*", es decir, dispositivos que se comunican entre sí o hacia Internet para cumplir ciertas tareas sin necesidad de intervención humana, por ejemplo: celulares actualizando aplicaciones, televisores actualizando/bajando programación, cámaras de video y sensores de movimiento informando/grabando la presencia de intrusos, refrigeradores informando del estado de los víveres, etc.

Por lo mencionado anteriormente es una necesidad imperiosa la transición a un protocolo ip de nueva generación para el desarrollo y la expansión de los servicios de telecomunicaciones en todo el planeta que sea capaz de integrar las tecnologías actuales y aquellas que se están desarrollando.

2.1.TECNOLOGÍAS DE ACCESO A LA BANDA ANCHA

En el Ecuador las definiciones, parámetros y obligaciones de un SVA⁶, está establecidas en la Resolución 216-09-CONATEL-2009 del 29 de junio de 2009, en donde se establece como banda ancha las velocidades de 256 Kbps (bajada)/128 Kbps (subida).

Según la UIT⁷, las tecnologías de las telecomunicaciones de banda ancha se pueden clasificar en alámbricas e inalámbricas, UIT (10).

⁵ **PIB:** Es una medida macroeconómica que expresa el valor monetario de la producción de bienes y servicios de demanda final de un país durante un período determinado de tiempo (normalmente un año), además El PIB es usado como una medida del bienestar material de una sociedad.

⁶ **SVA:** Son las siglas del servicio de valor agregado estos son aquellos que utilizan servicios finales de telecomunicaciones (SMA, Telefonía Fija) y/o servicios portadores de telecomunicaciones para llegar a sus usuarios finales, e incorporan aplicaciones que permiten transformar el contenido de la información transmitida. Ejemplo de servicio de valor agregado es el acceso a Internet.

⁷ **UIT:** La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de Telecomunicaciones de la Organización de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Las tecnologías alámbricas comprenden las líneas telefónicas tradicionales; líneas de cable coaxial; y líneas de fibra óptica.

Las inalámbricas pueden dividirse en celular y fija, las de corta distancia a alta velocidad, las ópticas en el espacio libre y las satelitales.

La banda ancha, puede utilizar una sola tecnología o una combinación de las mencionadas anteriormente para ofrecer al usuario acceso a Internet a alta velocidad.

A continuación se describe aquella de interés en esta investigación pues el ámbito involucrado es la tecnología inalámbrica.

2.1.1. TECNOLOGÍAS INALÁMBRICAS

Esta tecnología es quizás la de mayor crecimiento gracias a sus bajos costos y fácil despliegue, por lo que es una de las opciones más viables para un gran número de regiones y países como el nuestro, en vías de desarrollo, que buscan acceso a alta velocidad. Algunas tecnologías inalámbricas de acceso de banda ancha, se describen a continuación:

A) SISTEMAS MDBA

La tecnología de red de área local inalámbrica es la de mayor crecimiento con los enlaces de **Modulación Digital de Banda Ancha (MDBA)**, en las bandas de frecuencia de 2.4 GHz y de 5.8 GHz, generalmente utilizados en la red de acceso, Supertel (13).

Tabla II. I Frecuencia de Modulación Digital de Banda Ancha. Fuente: www.conatel.gob.ec (Supertel, 2010)

BANDA (MHz)
902 - 928
2400 - 2483.5
5150 - 5250
5250 - 5350
5470 - 5725

Los sistemas con técnicas de modulación digital de banda ancha pueden operar en las siguientes configuraciones:

1. SISTEMAS PUNTO-PUNTO

Es un sistema de radiocomunicación que permite enlazar dos estaciones fijas distantes, empleando antenas direccionales en ambos extremos, estableciendo comunicación unidireccional o bidireccional.



Figura II. 1 Modelo de sistema punto a punto. Fuente (Autores).

2. SISTEMAS PUNTO-MULTIPUNTO

Sistema de radiocomunicación que permite enlazar una estación fija central con varias estaciones fijas distantes. Las estaciones fijas distantes emplean antenas direccionales para comunicarse en forma unidireccional o bidireccional con la estación fija central.

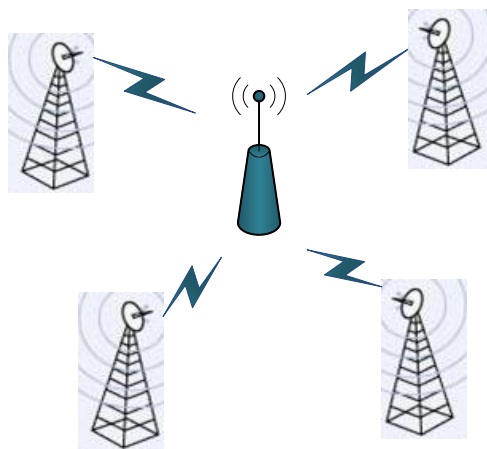


Figura II. 2 Modelo sistema punto-multipunto. Fuente (Autores).

3. SISTEMAS MÓVILES

Los sistemas móviles son sistemas de radiocomunicaciones que permiten enlazar una estación fija central con una o varias estaciones destinadas a ser utilizadas en movimiento o mientras estén detenidas en puntos no determinados.

B) SISTEMAS DE ACCESO INALÁMBRICO EN BANDA ANCHA FIJOS

Las redes de área local inalámbricas (WLAN) ofrecen acceso a banda ancha inalámbrica a distancias más cortas y con frecuencia se usan para ampliar el alcance de una conexión por línea telefónica de última milla o la conexión de banda ancha inalámbrica fija de un hogar, edificio o campus universitario. Las redes de fidelidad inalámbrica (Wi-Fi) usan dispositivos para espectro de uso común y pueden diseñarse para el acceso privado dentro de un hogar o empresa, o pueden emplearse para proporcionar acceso público a Internet en "hot spots"⁸ como restaurantes, cafeterías, hoteles, aeropuertos, centros de convenciones y parques de las ciudades.

C) SISTEMAS DE ACCESO INALÁMBRICO EN BANDA ANCHA MÓVIL

Si bien con anterioridad a la tecnología móvil de tercera generación existía la posibilidad de transferir datos a través de las redes de telefonía móvil (GPRS, EDGE), las velocidades de transmisión y el costo que importaba su uso, eran obstáculos ineludibles para el desarrollo de esta vía de acceso a Internet.

De aquí que la gran revolución en términos de acceso a Internet en redes de telefonía móvil se identifica a partir del surgimiento de la tecnología UMTS⁹ y su posterior evolución en la tecnología HSDPA, las cuales permiten velocidades de transferencia de datos superiores al megabit por segundo.

⁸ **HOT SPOTS:** Es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

⁹ **UMTS:** Sistema Universal de Telecomunicaciones Móviles, es una tecnología usada por los móviles de tercera generación 3G, pertenece al estándar de comunicaciones inalámbricas de tercera generación IMT 2000, iniciativa de la ITU.

Estos sistemas utilizan en el país las mismas bandas de frecuencia de la telefonía móvil para la transferencia de datos tanto en equipos móviles de telefonía así como también es posible proveer del servicio de acceso a Internet en computadoras portátiles (notebooks, laptops, tablets, etc.) actualmente ya traen el socket para el SIM, y en otros casos conectando un módem USB 3G, el cual contiene una tarjeta SIM dedicada en forma exclusiva a la prestación de este servicio, es decir que no puede utilizarse el chip de un módem USB 3G para el servicio de telefonía, Supertel (13).

2.2.PROTOCOLO IPv6

IPv6 es el protocolo ip de la siguiente generación (IPng) definido en el RFC 2460, este fue diseñado por la "IETF" (Internet Engineering Task Force.) como el sucesor al protocolo IPv4.

Creado para atender las limitaciones de IPv4 en las redes actuales en cuestiones de espacio de direcciones ip, ruteo ineficiente, uso de NAT, demanda de mayor tiempo de respuesta y disponibilidad de ancho de banda en aplicaciones multimedia, así como de seguridad.

El nuevo protocolo IPv6, dispone de **40.282.366.920.938.463.463.374.607.431.768.211.456** (2^{128} o **340 sextillones de direcciones**), lo que hace que la cantidad de direcciones IPv4 parezcan insignificante.

Con el mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes. También es probable que la "Era IPv6" genere una nueva innovación en las aplicaciones y las ofertas de servicios ya que, termina con la necesidad de direcciones compartidas.

IPv6 también considerado un protocolo más eficiente en aspectos como, su facilidad para la autoconfiguración, facilidad para la gestión/delegación de las direcciones, espacio para más niveles de jerarquía y para la agregación de rutas, así como habilidad para las comunicaciones extremo-a-extremo con IPsec, Palet (9).

Debemos decir que IPv6 se está implementando en todo el mundo pero coexistirá con IPv4 por muchos años en esta transición. Si bien el trabajo técnico relacionado con el protocolo, en gran medida, se ha completado, lo que resta mayoritariamente es su despliegue en las redes de los proveedores de servicios de internet.

2.2.1. CARACTERÍSTICAS

Los principales cambios del nuevo protocolo IP radican en los siguientes aspectos, *Silva (14)*.

- **Un nuevo formato de cabecera que agiliza el enrutamiento.** Con el objetivo de mejorar el proceso de enrutamiento IPv6 simplifica el encabezado del paquete de 12 elementos que se emplea en IPv4 a solo 8 elementos. Esto reduce el proceso de enrutamiento debido a que se utiliza una cabecera fija de información de control la cual es más simple ya que consta con la mitad de campos lo cual disminuye el procesamiento de los equipos de ruteo.

La cabecera fija implica una mayor facilidad para su proceso en routers y conmutadores, incluso mediante hardware, lo que implica mayores prestaciones, ya que el hecho de tener los campos alineados a 64 bits permite que las nuevas generaciones de procesadores y micro controladores de 64 bits puedan procesar mucho más eficazmente la cabecera IPv6

- **Espacio más grande para las direcciones.** IPv6 se compone por 8 segmentos de 2 bytes cada uno que suma un total de espacio de 128 bits para direcciones de origen y de destino lo que permite tener 3.4×10^{38} posibles direcciones.
- **Autoconfiguración.** Un aspecto útil que implementa IPv6 es su capacidad para configurarse automáticamente sin utilizar un protocolo de configuración dinámica como DHCP. El protocolo IPv6 puede asignar una dirección local de vínculo para cada interfaz. Mediante el descubrimiento de los routers, un host envía una solicitud de Link-Local usando Multicast pidiendo los parámetros de configuración, si los routers se encuentran configurados para esto, responderán este requerimiento con un "anuncio de router" que contiene los parámetros de configuración de la capa de red.

- **Multicast.** La habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. IPv6 no implementa broadcast, el mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local (all hosts). Muchos ambientes no tienen, sin embargo, configuradas sus redes para rutear paquetes multicast, por lo que en éstas será posible hacer "multicasting" en la red local, pero no necesariamente en forma global.
- **Seguridad.** El protocolo para cifrado y autenticación IP forma parte integral del protocolo IPv6. El soporte IPsec se vuelve obligatorio en IPv6; a diferencia de IPv4, donde su uso era opcional. Hay dos cabeceras específicas que se utilizan como mecanismo de seguridad en IPv6. Estas cabeceras son la Cabecera de Autenticación "CA" (RFC 2402) y la Cabecera de Encapsulado de Contenidos de Seguridad "CECS" (RFC 2406). La cabecera de Autenticación está diseñada para proporcionar integridad y autenticación a los datagramas IP, mientras que la cabecera de Encapsulado de Contenidos de Seguridad proporciona integridad y confidencialidad a los datagramas.
- **Calidad de Servicio (QoS).** IPv6 implementa en su estructura dos nuevos campos que implementan un mecanismo de control de flujo y de asignación.

Los nuevos campos son:

- Traffic Class, también denominado Prioridad, podría ser más o menos equivalente TOS en IPv4.
- Flow Label permite tráficos con requisitos de tiempo real.

Estos dos campos, como se puede suponer, son los que nos permiten las Calidad de Servicio y Clase de servicio propiedades intrínsecas que se pretenden en el nuevo protocolo ip.

- **Neighbor Discovery Protocol.** Se desarrolló un nuevo protocolo para interactuar con los vecinos. Los protocolos ARP y "Router Discovery" son reemplazados por este nuevo protocolo que ya no utiliza "broadcast" para propagarse por la red, en vez de ello utiliza "multicast".
- **Movilidad.** La implementación de IPv6 está pensada para soportar la movilidad en forma nativa a través del protocolo especializado en la movilidad ip MIPv6, Díaz (4).

En MIPv6 se definen tres agentes para la movilidad: Home Agent (AH), Mobile Node (MN) Correspondent Node (CN).

HA es un agente que se despliega en la red del operador que expande el servicio de movilidad. Es el encargado de tener registrada la "verdadera posición" del nodo móvil. Por su parte, el MN es el dispositivo del usuario que cuando se encuentra en la red de su operador tiene una dirección IPv6 denominada Home of Address (HoA) y cuando se desplaza y se encuentra en una red visitada adquiere una dirección diferente, denominada Care of Address (CoA). Por último, el CN es un nodo que pretende contactar con el MN y que en principio si no sabe cuál es su posición real trata de contactar usando la HoA del MN.

2.2.2. DIRECCIONAMIENTO IPv6

En la Figura II.3 se presenta todas las direcciones reservadas para IPv6.

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	Sin especificar	Como 0.0.0.0 en IPv4
::1	128 bits	Dirección de bucle local (loopback)	Como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96 bits	Direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones "empotradas."
::ff:xx:xx:xx:xx	96 bits	Direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
fe80::	10 bits	Direcciones link-local	El prefijo de <i>enlace local</i> (<i>link local</i>) especifica que la dirección sólo es válida en el enlace físico local.
fec0::	10 bits	Dirección site - local	Equivale al Direccionamiento privado IPv4
ff::	8 bits	Multicast	
001 (base 2)	3 bits	Direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son "001".

Figura II. 3 Direcciones IPv6 reservada. Fuente: www.freebsd.org (FreeBSD, 2010)

2.2.2.1. DIRECCIONES UNICAST

Estas direcciones identifican de manera única a cada nodo de la red, permitiendo la comunicación punto a punto entre ellos.

La nueva característica que trae IPv6 es la ubicación de las direcciones Unicast dentro de contextos, cada uno de los cuales define un dominio lógico o físico de la red.

Los tipos de contextos que se tienen son:

2.2.2.1.1. LAS DIRECCIONES LOCALES DE ENLACE (“LINK-LOCAL”).

Se diseñaron para direccionar un único enlace para cumplir con los propósitos de auto configuración mediante los identificadores de interfaz, descubrimiento de los nodos vecinos o situaciones en las que no se cuente con un router. De esta manera los ruteadores no necesitan transmitir ningún paquete con direcciones fuente destino entre hosts que se encuentra en un enlace local (su ámbito está limitado a la red local).

La estructura de una dirección local al enlace es “fe80:0:0:0:<identificador de interfaz>”. El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64. Ejemplo:

MAC: 39:A7:D3:F9:61:A1

Dir. IPv6: fe80:0:0:0:039A7:D3FF:FEF9:61A1

Siendo FF: FE partes de la dirección que siempre se repiten en todas las direcciones que siguen el formato EUI-64.

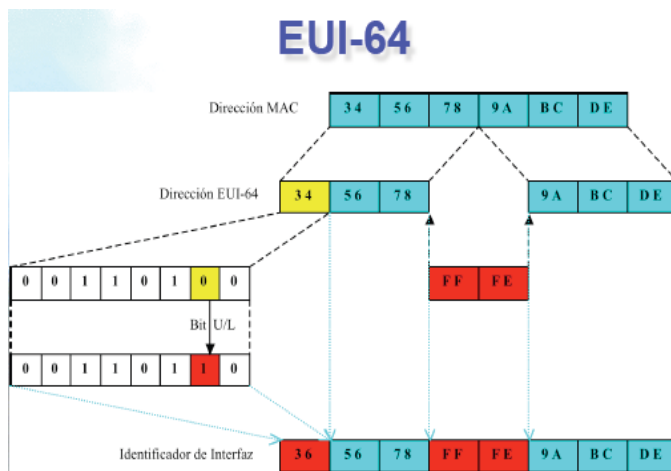


Figura II. 4 Formato EUI-64. Fuente: Introducción a IPv6 (Palet, 2009)

2.2.2.1.2. LAS DIRECCIONES SITE-LOCAL

Equivalen a las direcciones privadas que se definen en IPv4 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Las direcciones site-local no son accesibles desde sitios ubicados fuera del enlace local, disminuyendo el tráfico que se genera en los routers. Estas direcciones son utilizadas dentro de las intranets en host que no tienen una conexión directa al internet a través de IPv6.

La estructura de una dirección local única es la siguiente:

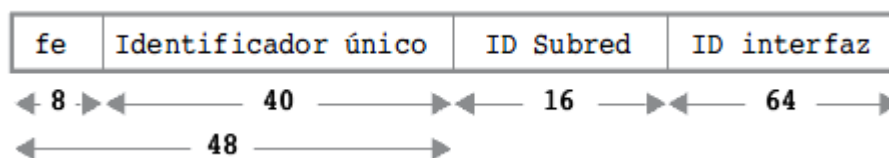


Figura II. 5 Estructura dirección site-local. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

Identificador único: Campo de 40 bits que identifica a un sitio en particular. Dado que este tipo de direcciones no son publicadas en Internet, pueden existir distintos sitios con el mismo identificador.

Identificador subred: Permite crear un plan de direccionamiento jerárquico, identificando a cada una de las 216 posibles subredes en un sitio.

Identificador de interfaz: Individualiza a una interfaz presente en una determinada subred del sitio. A diferencia de las direcciones locales al enlace, este identificador no se genera automáticamente.

Las direcciones site y link local están disponibles para uso privado interno y no necesitan ser asignadas por autoridades públicas de registro.

Las direcciones site-local constituyen un mecanismo flexible para que las redes de una misma empresa u organización con un ámbito bien definido se comuniquen entre sí. Si se cambian de ISP, por ejemplo el direccionamiento site-local permanece exactamente igual porque no está directamente relacionado con el mundo exterior.

Las direcciones link-local pueden utilizarse para aplicaciones que están limitadas a un determinado enlace y también para el proceso de arranque a través de la red antes que las máquinas reciban una dirección identificativa global.

2.2.2.1.3. LAS DIRECCIONES GLOBALES

Las direcciones "Unicast Globales" son usadas para comunicar 2 nodos a través de Internet; son equivalentes a las direcciones públicas en IPv4. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet.

El espacio reservado actualmente para este tipo de direcciones es de 2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3).

Todas las subredes en el espacio de direccionamiento "unicast global" tienen un prefijo de red fijo e igual a /64. Esto implica que los primeros 64 [bit] corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo.

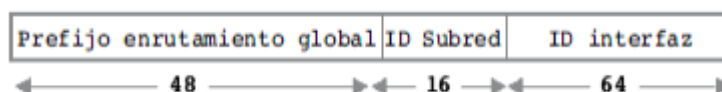


Figura II. 6 Estructura dirección global. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

El prefijo de enrutamiento global es aquel que identifica a un sitio conectado a Internet. Dicho prefijo sigue una estructura jerárquica, con el fin de reducir el tamaño de la tabla de enrutamiento global en Internet.



Figura II. 7 Jerarquía de Direcciones Unicast Globales. Fuente: Direcciones "unicast" Globales (Ramírez Mosquera Danilo Enrique, 2010)

Cada una de los Registros Regionales maneja direcciones con prefijo /23, y otorgan a cada ISP direcciones con prefijo /32, y estos a su vez dan direcciones con prefijo /48, permitiendo a cada sitio u organización el tener 2^{16} subredes, cada una con 2^{64} usuarios.

2.2.2.2. DIRECCIONES MULTICAST

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos.

Un nodo puede pertenecer a uno o varios grupos multicast.

La estructura de una dirección multicast IPv6 es el siguiente:

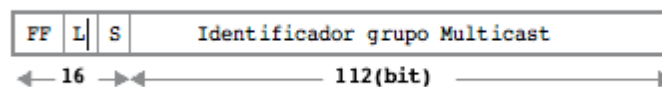


Figura II. 8 Estructura dirección multicast. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

Primeros Campos: Son dos campos de 8 [bits] cada uno y que siempre llevan los valores de "FF" [en hexadecimal].

Campo L: Indica el tiempo de vida de un grupo "multicast". Si se coloca el valor de '0' cuando es un grupo permanente y '1' cuando es un grupo "multicast" temporal.

Campo S: Indica el contexto o alcance del grupo. Ya existen valores predeterminados para este campo; los mismos que a continuación se detallan:

Valor [en decimales]	Contexto de Grupo
1	Nodo
2	Enlace
5	Sitio
8	Organización
E	Global
Otros valores	Sin asignar o reservado

Figura II. 9 Valores del Campo S. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

Con estos dos campos se pueden crear varios grupos de direcciones para cada tipo de contexto y con diferente duración, pero también ya existen grupos Multicast predeterminados como:

Dirección IPv6	Descripción
FF01::1	Todos las interfaces en un nodo
FF02::1	Todos los nodos en el enlace
FF01::2	Todos los routers en la interfaz
FF02::2	Todos los routers en el enlace
FF05::2	Todos los routers en el sitio

Figura II. 10 Direcciones de multicast Predeterminado. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

Las Direcciones Multicast no deben aparecer como direcciones origen en ningún paquete, así como tampoco deben estar presentes en las tablas de enrutamiento.

Existe además una clase especial de dirección Multicast llamada "Dirección de Nodo-Solicitado", ésta cumple con la función de asociar las direcciones "Unicast" y "Anycast" configuradas en las interfaces de un Nodo. Esta dirección tiene como prefijo predeterminado:

'FF02:0:0:0:0:1:FF00::/104'

Por lo que el rango de direcciones Multicast de Nodo-Solicitado son:

FF02:0:0:0:0:1:FF00:0000 hasta FF02:0:0:0:0:1:FFFF:FFFF

La forma en que se arman estas direcciones es la siguiente:



Figura II. 11 Dirección de Nodo-Solicitado. Fuente: Revista Institucional N°14 (SUPERTEL, 2012)

Los primeros 104 [bits] de la dirección siempre serán fijos, mientras que los últimos 24 [bits] son tomados de las direcciones IPv6 Unicast y Anycast que tenga configurado el Nodo. Por ejemplo:

Se tiene la dirección IPv6:

4037::01:800:200E:8C6C

Su dirección Multicast de Nodo-Solicitado es:

FF02::1:FF0E:8C6C

Las direcciones Multicast de Nodo-Solicitado son usadas para obtener las direcciones MAC de los Nodos presentes en un mismo Enlace, para ello se envía un paquete con la dirección Multicast del Nodo-Solicitado, para que éste responda con su respectiva dirección MAC.

2.2.2.3. DIRECCIONES ANYCAST

Es aquella que identifica a un grupo de interfaces. Los paquetes enviados a una dirección Anycast son reenviados por la infraestructura de enrutamiento hacia la interfaz más cercana al origen del paquete que posea una dirección Anycast perteneciente al grupo.

Con el fin de facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces que están asociadas a una dirección Anycast y su distancia en métricas de enrutamiento, para que se envíen siempre al nodo más cercano o de menor métrica.

Una dirección Anycast se crea al asignar una misma dirección Unicast a varias interfaces de distintos Nodos. Una dirección Anycast no puede ser nunca una dirección de origen.

Un uso de direcciones Anycast es el identificar a los routers que pertenecen a una organización y que proveen de servicio de internet.

2.2.2.4. DIRECCIONES COMPATIBLES

Las direcciones compatibles se diseñaron con la finalidad de permitir la migración y coexistencia entre los protocolos IPv4 e IPv6, las principales direcciones son:

Direcciones IPv4 compatibles, direcciones 6over4, direcciones 6to4 y direcciones ISATAP.

- Las direcciones IPv4 compatibles son usadas por nodos que se encuentran configurados con direcciones IPv6 e IPv4 que se comunican con redes IPv6 sobre una infraestructura IPv6 pública.
- Las direcciones 6over4 al igual que las direcciones 6to4 son usadas para representar la interfaz de los host en el mecanismo de transición tipo túnel (tunneling).
- Las direcciones ISATAP son usadas para representar a un nodo para el mecanismo de asignación de direcciones entre nodos con doble pila.

2.2.2.5. DIRECCIONES IPv6 PRESENTES EN HOST Y ROUTER

Por lo general, a un elemento de red que cuenta con una sola interfaz de red se le puede asignar tan solamente una dirección IPv4, pero a un elemento de red que se encuentra configurado con IPv6 se le puede asignar múltiples direcciones por cada interfaz las direcciones que pueden ser asignadas a un host o router que usa IPv6 son las siguientes:

- Una dirección unicast link-local por cada interfaz
- Una dirección unicast adicional que puede ser site-local o de dirección global por cada interfaz.
- La dirección de loopback (::1) para la interfaz de loopback.

Los hosts y ruteadores que se tiene configurado IPv6 pueden tener al menos 2 direcciones; además cada interfaz está pendiente de escuchar el tráfico multicast.

2.2.3. PLAN DE DIRECCIONAMIENTO

El espacio de direcciones IPv6 es un recurso público que debe ser administrado de manera prudente teniendo en cuenta los intereses de internet a largo plazo, (LACNIC, 2012) .

Una administración responsable del espacio de direcciones permitirá cumplir objetivos como:

A: UNICIDAD

La asignación de direcciones debe ser única en todo el mundo para que cada host público en Internet pueda ser identificado unívocamente.

B: REGISTRO

Se llevara una base de datos con los registros de las asignaciones accesible por los organismos de regulación del internet para garantizar la unicidad.

C: AGRUPACIÓN

Las direcciones se distribuirán en forma jerárquica de acuerdo a la topología de la red, permitiendo así la agregación de información de ruteo por parte de los ISP's, y para limitar la expansión de las tablas de ruteo en Internet.

D: CONSERVACIÓN

Aunque IPv6 provee un espacio de direcciones extremadamente grande, las políticas de direcciones deberían evitar su desperdicio innecesario y así se evitar la acumulación de direcciones no utilizadas.

E: EQUIDAD

Las políticas y buenas prácticas del uso del espacio de direcciones públicas se deberán aplicarse a toda la comunidad de Internet, independientemente de su ubicación, nacionalidad, tamaño o cualquier otro factor.

2.2.3.1. DISTRIBUCIÓN Y ASIGNACIÓN

La administración de los recursos IP actualmente tiene una estructura jerárquica, una entidad central llamada IANA¹⁰ administra todo el espacio de direccionamiento disponible y es la encargada de entregar bloques de direcciones a organizaciones regionales denominadas RIRs ("Regional Internet Registry") conforme a demanda, quienes a su vez se encargan de la distribución/ asignación a los proveedores de Internet. El espacio IPv4 disponible en IANA se agotó definitivamente en febrero de 2011 y en abril del mismo año APNIC (el RIR para la región de Asia Pacífico) empezó a asignar direcciones IPv4 desde su último bloque de direcciones, en RIPE (el RIR para la región de Europa medio oriente y Asia central) se agotaron las direcciones el 14 de septiembre del 2012, en ARIN (el RIR para la región de Norte América) el agotamiento sucederá el 15 de septiembre del 2013, para AFRINIC (el RIR para la región de África) el agotamiento acontecerá el 1 de septiembre del 2019 y en LACNIC (RIR para la región de América Latina y Caribe) se terminaran las direcciones el 14 de junio del 2015, SUPERTEL (10).

¹⁰ **IANA:** Internet Assigned Numbers Authority es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

La responsabilidad de la administración del espacio de direcciones de IP está distribuida globalmente de acuerdo con la estructura jerárquica que se muestra a continuación.

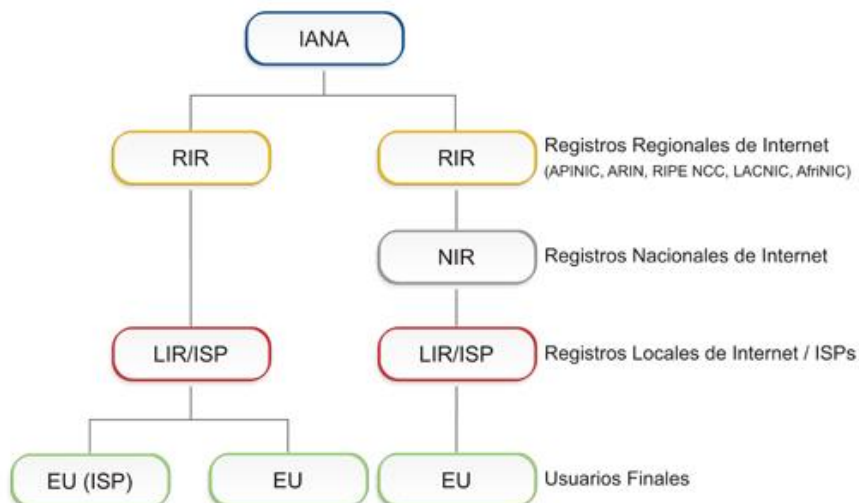


Figura II. 12 Organismos de Administración de direcciones. Fuente: <http://lacnic.net> (LACNIC, 2012)

IANA (Internet Assigned Number Authority)

IANA es responsable de distribuir parte del espacio global de las direcciones IP y los números de sistemas autónomos a Registros Regionales de acuerdo a necesidades establecidas.

REGISTRO DE INTERNET (IR)

Un Registro de Internet (IR) es una organización responsable del registro y distribución de espacios de direcciones IP a sus miembros o clientes. Los IRs están clasificados de acuerdo a su función principal y alcance territorial dentro de la estructura jerárquica.

REGISTRO DE INTERNET REGIONAL (RIR)

Los Registros de Internet Regionales (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir los recursos de Internet dentro de las respectivas regiones.

REGISTRO DE INTERNET NACIONAL (NIR)

Un Registro de Internet Nacional (NIR) distribuye, principalmente, los recursos de Internet a sus miembros o constituyentes, los cuales generalmente son LIRs.

REGISTRO DE INTERNET LOCAL (LIR)

Registro de Internet Local (LIR) es un IR que a su vez asigna recursos de Internet a usuarios de los servicios de red que éste provee. Los LIRs son generalmente ISP's, cuyos clientes son principalmente usuarios finales y posiblemente otros ISP's.

PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

Un Proveedor de Servicios de Internet asigna principalmente espacio de direcciones IP a los usuarios finales de los servicios de red que éste provee. Sus clientes pueden ser otros ISP's. Los ISP's no tienen restricciones geográficas como lo tienen los NIRs.

SITIO FINAL O USUARIO FINAL (EU)

Un end site es definido como un usuario final (suscriptor) que tiene una relación de negocios con un proveedor de servicios Internet.

2.2.3.2. POLÍTICAS PARA DISTRIBUCIÓN Y ASIGNACIÓN

LACNIC es el RIR para Latinoamérica y el Caribe encargado de la asignación de direcciones IPv4 e IPv6 a los países miembros de su jurisdicción.

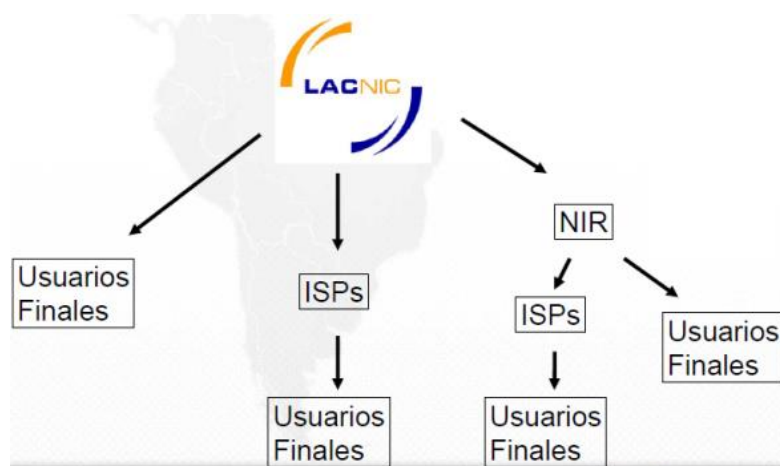


Figura II. 13 Asignación de direcciones IP. Fuente: <http://lacnic.net> (LACNIC, 2012)

DISTRIBUCIONES DE DIRECCIONES IPv6 A LIR O ISP.

LACNIC realizará una distribución de un /32 al recibir una solicitud de direccionamiento IPv6 por parte de un LIR o ISP con distribuciones previas de IPv4. En caso de requerir una distribución inicial más grande que un /32, el LIR o ISP deberá presentar la documentación que justifique el requerimiento.

ASIGNACIONES POR PARTE DE LOS ISP´S

Las asignaciones deben ser realizadas de acuerdo con las recomendaciones existentes [RFC3177], las cuales resumimos aquí:

/48 en el caso general, excepto para suscriptores muy grandes.

/64 cuando se conoce por diseño que una y sólo una subred es necesaria.

/128 cuando se conoce absolutamente que uno y sólo un dispositivo se está conectando, IETF (24).

ASIGNACIÓN A LA INFRAESTRUCTURA DEL OPERADOR

Una organización (ISP/LIR) puede asignar un /48 por PoP¹¹ como un servicio de infraestructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

2.2.4. MECANISMOS DE TRANSICIÓN/COEXISTENCIA

Debemos mencionar algunas razones por las que se desarrollaron estos mecanismos:

- Toda la estructura de Internet está basada en IPv4.
- Un cambio inmediato de protocolo es inviable debido al tamaño y a la proporción que tiene la red.
- La adopción de IPv6 se debe realizar de manera gradual.

¹¹ **PoP:** En el contexto de internet, un point-of-presence (PoP) es un acceso a internet. Es la ubicación física donde están los servidores, routers, switches ATM y demás dispositivos que permiten dicho acceso.

- Inicialmente habrá un período de transición y de coexistencia entre los dos protocolos.
- Las redes IPv4 necesitarán comunicarse con las redes IPv6 y viceversa.

Un amplio abanico de técnicas ha sido identificadas e implementadas, pero básicamente tenemos tres categorías, Palet (9).

- 1) Doble-pila para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes
- 2) Técnicas de túneles, para evitar dependencias cuando se actualizan hosts, routers o regiones. Los más utilizados y útiles son: 6to4, teredo, túnel broker
- 3) Técnicas de traducción, para permitir la comunicación entre dispositivos que son solo IPv6 y aquellos que son solo IPv4.

2.2.4.1. DUAL STACK (DOBLE PILA)

Todos los sistemas operativos modernos soportan IPv6 (Windows XP/2003/Vista,8 Linux, BSD, IOS de Cisco), además al añadir IPv6, no elimina la pila IPv4.

Las aplicaciones escogen la versión de IP a utilizar, por ejemplo en función de la respuesta DNS (destino con registro AAAA usa IPv6, caso contrario IPv4).

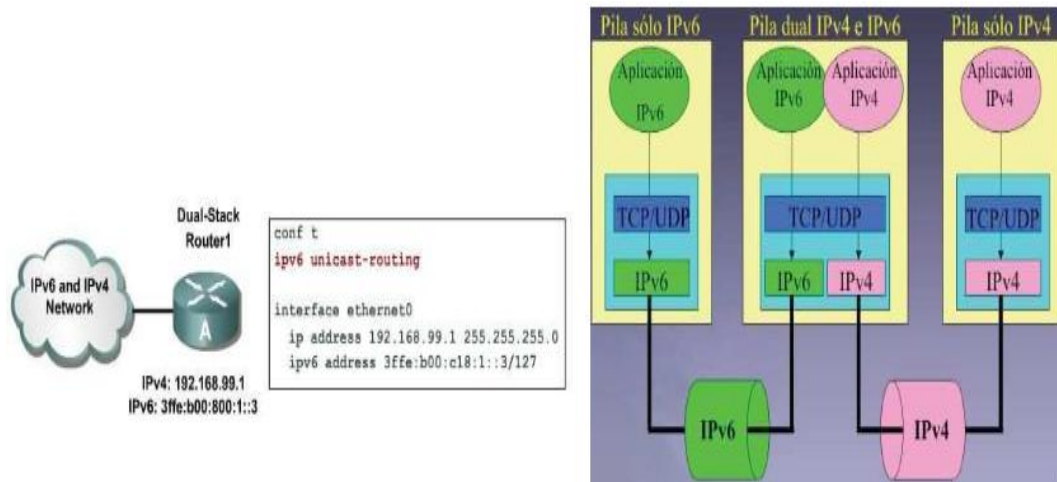


Figura II. 14 Dual Stack. Fuente: Herramientas de transición (ConsulIntel & 6Deploy, 2008)

Una red de doble pila es una infraestructura capaz de encaminar tanto paquetes IPv4 como IPv6, sin embargo se debe considerar el análisis de algunos aspectos como:

- Configuración de los servidores DNS cambio en los registros
- Configuración de los protocolos de enrutamiento
- Configuración de los Firewalls
- Cambios en la administración de las redes

2.2.4.2. TÉCNICAS DE TÚNELES

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 está siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4. Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado de paquetes. Estos túneles pueden ser utilizados de formas diferentes, Tutorial IPv6 (28).

ROUTER A ROUTER. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.

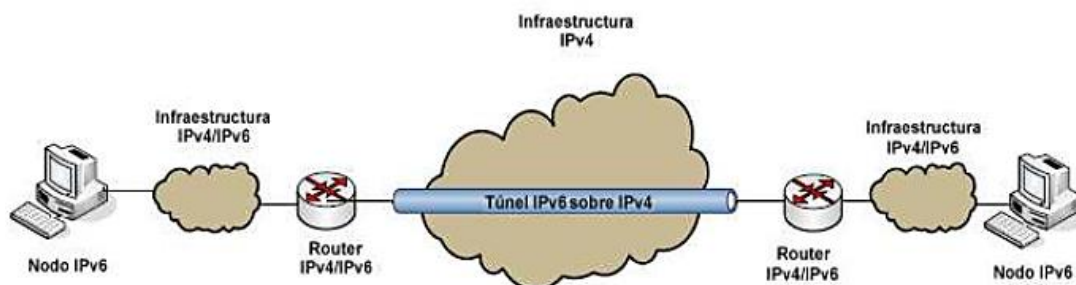


Figura II. 15 Túnel Router a Router. Fuente: Estudio para la migración de IPV4 a IPV6 para la empresa proveedora de internet (Milltec S.A-David Núñez Lara, 2009)

HOST A ROUTER. Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.

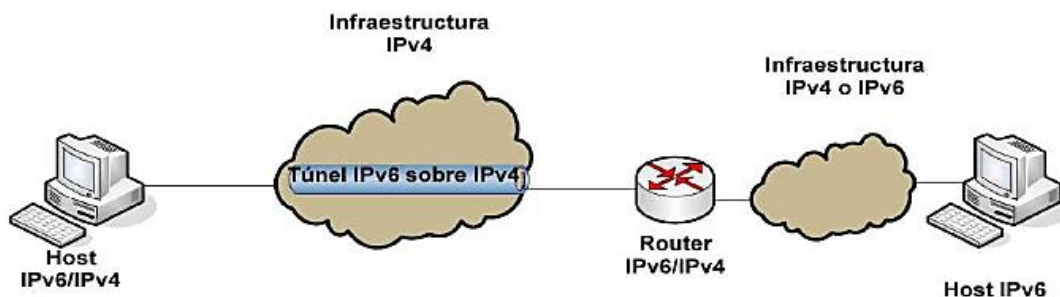


Figura II. 16 Túnel Host a Router y Router a host. Fuente: Estudio para la migración de IPV4 a IPV6 para la empresa proveedora de internet (Milltec S.A-David Núñez Lara, 2009)

HOST A HOST. Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.

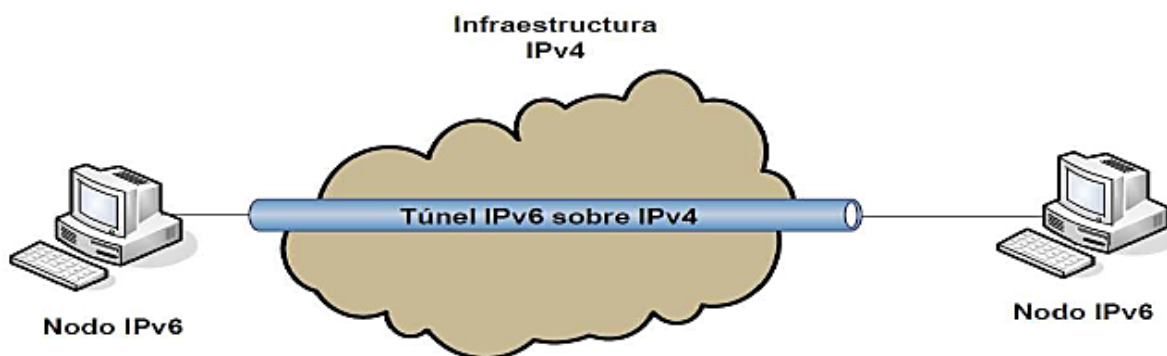


Figura II. 17 Túnel host a host. Fuente: Estudio para la migración de IPV4 a IPV6 para la empresa proveedora de internet (Milltec S.A-David Núñez Lara, 2009)

ROUTER A HOST. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

2.2.4.2.1. 6TO4

Los túneles 6to4 son un mecanismo que permiten que dispositivos IPv6 que solo están conectados a redes IPv4, puedan alcanzar otras redes IPv6. Para lograr esto, trabaja con un grupo de direcciones preestablecidos por la IANA para túneles 6to4: el bloque *2002::/16*, Palet (9).

Así, el mecanismo de túneles 6to4 trabaja de la siguiente manera: un dispositivo, que dispone de una dirección IPv6, quiere comunicarse con otra dirección IPv6 que está por fuera de su red. Para ello, debe disponer de un router que soporte pseudo-interfaces 6to4 y que sea capaz de rutear el prefijo *2002::/16*.

Además, necesitará también de al menos una dirección IPv4 pública de forma tal de calcular la dirección 6to4 para el router a partir de ésta. Este cálculo se realiza de la siguiente manera:

- 1) Se descompone la dirección IPv4 en notación nibble, por ejemplo:

Si disponemos de la dirección IPv4 *192.0.2.1*, su descomposición en nibbles sería:

192 ----> C0
0 ----> 00
2 ----> 02
1 ----> 01

- 2) Construimos la primer parte de la dirección del router utilizando el prefijo que antes mencionamos para las direcciones 6to4, de la siguiente manera: *2002:C000:0201::/48*

- 3) Ya tenemos el prefijo para nuestro router, ahora elegimos cualquier identificador de interfaz, por ejemplo: *2002:C000:0201::1/128*

Siguiendo con el desarrollo del funcionamiento de los túneles 6to4, además del dispositivo que intenta comunicarse con una red IPv6 y del router (generalmente de borde) con la pseudo-interfaces 6to4, necesitaremos un router en Internet contra el cual levantar el túnel.

Existen en el internet varios de estos dispositivos que responden a las peticiones de túnel con una dirección de tipo Anycast, más exactamente con la dirección: 192.88.99.112. Asimismo, utilizando el mecanismo de la notación en nibble, esta dirección será: 2002:c058:6301::/128.

Para la recomendación (RFC 6343, 2011) hay dos variantes de 6to4, "Router 6to4" y "Anycast 6to4".

A. ROUTER 6TO4

El modelo asume que el usuario del sitio opera con IPv6 nativo, pero el ISP no provee este servicio. El Router de borde actúa como 6to4, si la dirección IPv4 es pública el sitio hereda automáticamente el prefijo de IPv6 *2002:v4addr::/48*, este prefijo se utilizara para delegar el servicio IPv6 en el sitio del usuario.

Consideraremos dos routers de frontera, con direcciones IPv4 públicas *192.0.2.170* y *192.0.2.187* por lo que se heredara el prefijo IPv6 *2002:c000:02aa::/48* y *2002:c000:02bb::/48*, estos routers pueden intercambiar paquetes IPv6 mediante la encapsulación en IPv4 utilizando el número de protocolo 41, y enviarse uno al otro con sus respectivas direcciones IPv4. De hecho cualquier Router 6to4 conectado a la red IPv4 puede intercambiar paquetes IPv6 de esta manera.

También algunos routers 6to4 se configuran como "Routers Relé", los mismos se comportan como describimos anteriormente; pero además que obtienen conectividad de IPv6 nativo con un prefijo IPv6 normal, estos anuncian una ruta IPv6 de *2002::/16*. Por ejemplo, supongamos que el enrutador 6to4 con una IP *192.0.2.187* *2002:c000:02bb::1* es un enrutador Relay (reenvió), por otro lado un host con la dirección 6to4 *2002:c000:02aa::123* envía un paquete a un destino IPv6 nativo con una IP *2001:db8:123:456::321*. Por otra parte el enrutador 6to4 con una IP *192.0.2.170* tiene una ruta por defecto IPv6 con *2002:c000:02bb::1*. El paquete será entregado al Router relé encapsulado en IPv4. El relé desencapsulará el paquete y lo reenviara a IPv6 nativo para su entrega. Cuando el host remoto responde, el paquete (*fuelle 2001:db8:123:456::321, destino 2002:c000:02aa::123*) encontrara una ruta para *2002::/16* y

por lo tanto se entregara al relé 6to4. Ahora el proceso se invierte y el paquete se encapsula y se remitirá al Router 6to4 en *192.0.2.170* para su entrega final.

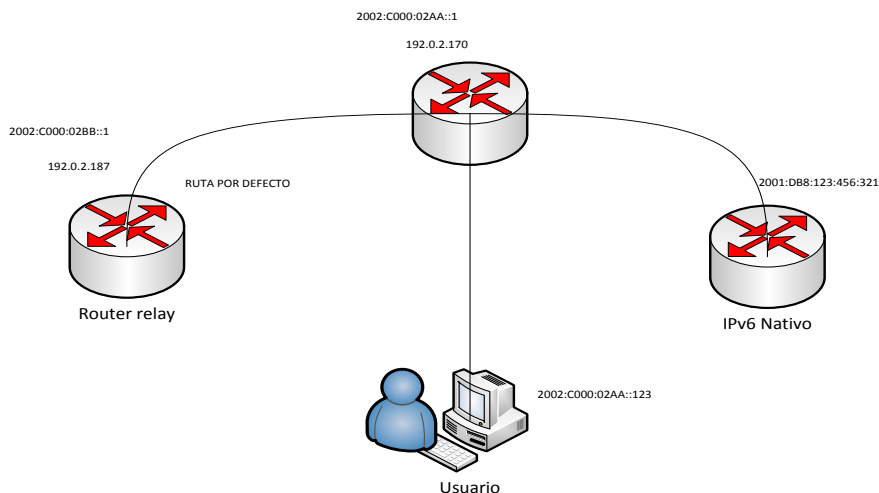


Figura II. 18 Enrutamiento 6to4. Fuente: (Autores)

Hay que tener en cuenta que este proceso no requiere el mismo relé para ser utilizado en ambas direcciones. El paquete de salida ira a cualquier relé de origen y el paquete de vuelta ira a cualquier relé que este anunciando una ruta a *2002::/16*.

B. ANYCAST

En particular, los sitios de 6to4 deben configurar un enrutador Relay para llevar tráfico de salida, que se convierte en un enrutador IPv6 por defecto, excepto para *2002::/16* .Esta solución está disponible para usuarios de pequeñas empresas o home, incluso con un solo Gateway sencillo en lugar de un Router de frontera. Eso se logra mediante la definición de una dirección IPV4 por defecto *192.88.99.1* para el relé 6to4, y por lo tanto *2002:c058:6301::* como dirección del Router IPv6 para un sitio 6to4.

2.2.4.2.2. 6 RD

Es una modificación de 6to4 que permite operar enteramente dentro de la red del ISP y tener más control de la transición, pero tiene un inconveniente requiere cambiar el CPE y el Router que tiene el usuario porque existen muy pocos routers que tienen soporte 6RD, FLIP6LACTF (35).

Además se requiere que toda la infraestructura tenga soporte 6RD, Cisco lo está impulsando muy fuertemente.

6RD ve la red IPv4 como una capa de enlace para IPv6 y soporta túneles automáticos. Un dominio 6RD consiste en routers cliente de borde (CE) y uno o más Relays de borde (RB), RFC 5969 (26).

Los paquetes IPv6 encapsulados por 6RD siguen la topología de ruteo IPv4 dentro de la red del SP (Proveedor de Servicios) entre CE y RB. Los RB son atravesados solo por paquetes IPv6 que están destinados a él o que llegan de fuera del dominio 6rd del SP. Como 6RD es stateless los RB pueden ser alcanzados utilizando comunicación Anycast.

6RD utiliza el mismo mecanismo de encapsulación y base 6to4 y puede ser visto como un súper conjunto de 6to4. A diferencia de 6to4, 6RD se usa solamente en un ambiente donde el SP gestiona el servicio IPv6.

2.2.4.2.3. TEREDO

Se denominó originalmente Shipworm que es un mecanismo de transición que tiene como objetivo proporcionar conectividad IPv6 a aquellos usuarios que estén ubicados detrás de un NAT, es decir, que tengan una dirección IPv4 privada (10.0.0.x, 172.16.x.x, 192.168.x.x), FLIC6LACTF (26).

Teredo está soportado desde Windows XP con SP1 o posterior, así como en Windows 2003. También hay implementaciones de Teredo para Linux.

Intervienen agentes:

- Teredo server
- Teredo relay
- Teredo client

IPv6 envía paquetes como payload (carga útil) en paquetes IPv4. Un problema con estos métodos es que no funcionan cuando el nodo IPv6 está aislado detrás de un dispositivo traductor de direcciones de red (NAT), RFC 4380 (30).

NATs no suelen ser programados para permitir la transmisión de tipos de carga útil arbitrarias, incluso cuando lo son, la dirección local no puede ser utilizada en un esquema de 6to4.

TEREDO SERVICIO: La transmisión de paquetes IPv6 sobre UDP.

TEREDO CLIENTE: Es un nodo que tiene algún tipo de acceso a internet IPv4 y quiere ganar el acceso a la internet IPv6.

TEREDO SERVIDOR: Un nodo que tiene acceso a internet IPv4 a través de una dirección globalmente ruteable y se utiliza como ayuda para proporcionar conectividad IPv6 a clientes teredo.

TEREDO RELAY: Un enrutador IPv6 que puede recibir el tráfico destinado a los clientes teredo y enviarlo mediante el servicio Teredo.

TEREDO BURBUJA: Una burbuja Teredo es un paquete IPv6 mínimo, hecho de una cabecera IPv6 y un payload nulo. Los clientes Teredo y relés pueden enviar burbujas con el fin de crear una asignación en un NAT.

La solución propuesta, transporta paquetes IPv6 como payload en paquetes UDP. Se basa en que TCP y UDP son protocolos garantizados para cruzar la mayoría de los dispositivos NAT.

Enviar paquetes a través de TCP por un túnel sería posible, pero daría mala calidad del servicio, la encapsulación a través de UDP es una mejor opción.

Los dispositivos NAT suelen incorporar algún apoyo para UDP, con el fin de permitir a los usuarios en el dominio de nateo utilizar aplicaciones basadas en UDP.

Teredo está diseñado para proporcionar un "acceso IPV6 de último recurso" para nodos que necesitan conectividad IPV6.

2.2.4.2.4. CARRIER-GRAY NAT

Carrier-gray NAT (CGN) también conocido como NAT444 o large scale NAT; implementar CGN permite retrasar la transición a los ISP's, y esto causa un doble gasto de transición (una vez para añadir CGN y otra para soportar IPv6), RFC 6264 (17).

Es un mecanismo de transición para casos muy concretos, permite tener Dual Stack en la red del usuario lo que se entrega a cada usuario final son las mismas direcciones IPv4. Por ejemplo 192.168.0.10/24. Permite multiplicar muchos usuarios en una LAN pero el inconveniente es que es muy costoso (Cisco vende cajas de CGN en alrededor de un millón de dólares), también exige el reemplazo de los CPE y solo se implementa en los casos en que la red 10.0.0.0 no es suficiente para todos los usuarios que maneja, FLIP6LACTF (26).

Implementar CGN integra múltiples mecanismos de transición pueden simplificar la operación de servicios del usuario final durante el periodo de migración de IPV4 e IPV6 y el periodo de coexistencia. CGN se despliega en el lado de la red de mantenimiento y administración. En el lado del usuario se necesita de nuevos dispositivos (HG) Home Gateway.

Dual-Stack lite (DS_LITE), también llamado DS_LITE es una solución basada en CGN. Pero esto requiere que el ISP actualice su red inmediatamente a IPV6, muchos ISP's dudan en realizar esto como primer paso. Teóricamente, DS_LITE puede ser usado con doble encapsulación (IPV4 en IPV6- IPV6 en IPV4) pero esto es menos probable que sea aceptado por los ISP's.

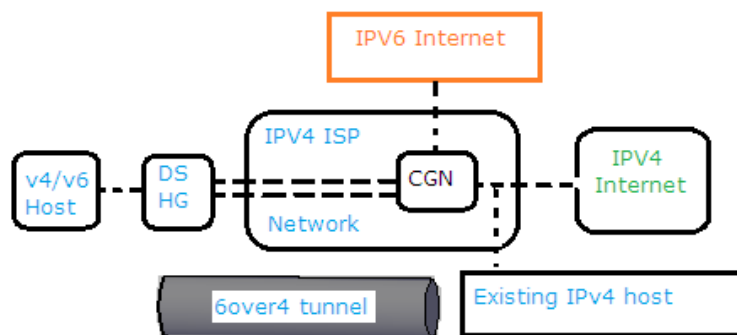


Figura II. 19 Enfoque CGN con la red IPv4 del ISP. Fuente: IETF (RFC 6264, 2011)

Como se muestra en la figura anterior, la red IPv4 del ISP no ha cambiado significativamente. Este enfoque permite acceder a los host IPv4 a internet IPv4 y a los host IPv6 acceder a internet IPv6. Un host Dual-Stack es tratado como un host IPv4 cuando se usa el servicio de acceso IPv4 y como un host de IPv6 cuando se usa el servicio de acceso IPv6. Y para permitir a un host IPv4 acceder a internet IPv6 y a un host IPv6 acceder a internet IPv4, también se puede integrar NAT64 con la CGN.

Dos tipos de dispositivos se necesitan para implementar este enfoque: un Dual-Stack home Gateway (HG) y un Dual-Stack CGN. El HG integra tanto el reenvío de IPv6 e IPv4 y las funciones del túnel 6over4; también puede integrar NAT IPv4. El CGN integra túnel 6over4 y las funciones IPv4-IPv4, así también como enrutamiento IPv6, IPv4.

2.2.4.2.5. TUNNEL BROKER (TB)

Este tipo de túneles permite configurar automáticamente gran cantidad de usuarios. Permite tener una interfaz gráfica (web), que va a permitir que los usuarios se registren y automáticamente tengan una dirección propia de nuestra red. Aunque hay servicios gratuitos de estos túneles no han tenido éxito, FLIP6LACTF (26).

El usuario solicita al TB la creación de un túnel y este le asigna una dirección IPv6 y le proporciona instrucciones para crear el túnel en el lado del usuario.

Existe una lista de TB disponibles para conectarnos al internet IPv6

TSP (Tunnel Setup Protocol) es un caso especial de TB que no está basado en una interfaz web sino en una aplicación que se instala en el cliente y se conecta con un servidor, pero básicamente es el mismo concepto.

La idea de Túnel Broker es un enfoque alternativo basado en servidores dedicados, llamados proveedores de túneles para gestionar peticiones de túnel que vienen de los usuarios. Es un enfoque para estimular el crecimiento de IPv6 y para proveer fácil acceso al servicio IPv6 en las redes de los proveedores, RFC 3053 (33).

El TB encaja bien para los pequeños sitios, host aislados de IPv6, especialmente a través de internet IPv4, que desean conectarse fácilmente a una red IPv6.

Además, los TB permite a los ISP tener un control total de acceso para los usuarios, para hacer cumplir sus propias políticas sobre utilización de los recursos de red.

El modelo de TB se basa en un conjunto de elementos funcionales representados a continuación en la figura II.20.

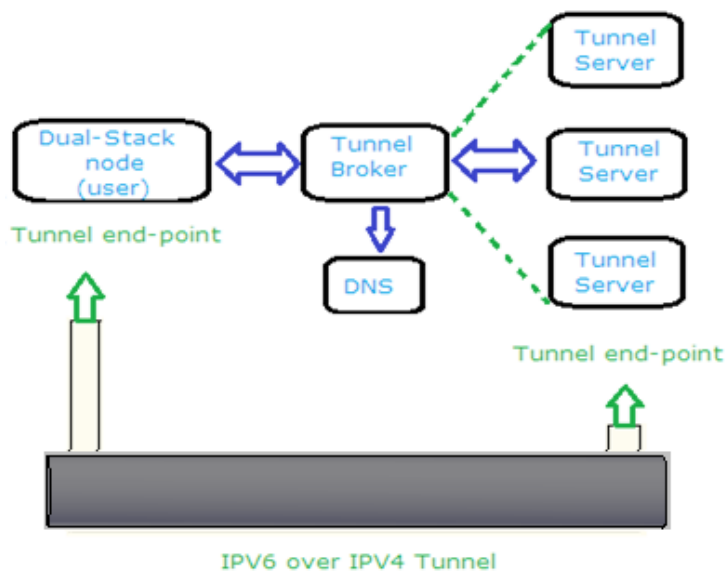


Figura II. 20 Modelo del Túnel Broker. Fuente: IETF (RFC 3053, 2001)

A continuación se describe los campos involucrados en la figura:

TÚNEL BROKER

Túnel Broker es el lugar donde el usuario se conecta se registra y activa el túnel. El TB gestiona la creación del túnel, por razones de escalabilidad el TB puede compartir la carga de red del lado de los end-points entre varios servidores de túnel. Envía órdenes de configuración para el servidor de túneles correspondiente cada vez que un túnel tiene que ser creado, modificado o eliminado. El TB también puede registrar la dirección IPV6 de usuario y el nombre en el DNS.

Un TB puede ser direccionado a IPV4. También puede ser direccionado a IPV6, pero esto no es obligatorio. Las comunicaciones entre el Broker y el servidor pueden tener lugar tanto con IPV4 o IPV6.

TÚNEL SERVER

Un túnel server es un Router Dual-Stack conectado al internet. Tras la recepción de una orden de configuración que viene desde el TB, que se crea, modifica o elimina el servidor de cada túnel. También puede mantener estadísticas de uso para cada túnel activo.

USANDO UN TÚNEL BROKER

El cliente del servicio TB es un nodo Dual-Stack (host o router) conectado a internet con IPV4. Al acceder al TB el cliente debe proporcionar su identidad y credenciales para la autenticación, autorización y opcionalmente puede llevarse a cabo un registro por ejemplo basándose en la existencia de un RADIUS AAA. Esto significa que el cliente y el TB tienen que compartir una pre-configuración o establecer asociación de seguridad automática que se usa para prevenir el uso no autorizado del servicio. El TB puede ser visto como un control de acceso al servidor, para interconectar a usuarios a IPV4 e IPV6.

- Una vez autorizado el cliente para acceder al servicio, el usuario debería proporcionar la siguiente información.

- Dirección IPV4 del lado del túnel.
- Un nombre que se utilizara para el registro en el DNS mundial, la dirección IPV6 asignada al cliente en el lado del túnel.
- La función del cliente(host independiente o router)

Si el host del cliente es un enrutador IPV6 que proporcionara conectividad a varios host IPV6, el cliente deberá pedir al proveedor la cantidad de direcciones requeridas. Esto permite al TB asignar al cliente un prefijo IPV6 que se adapte a sus necesidades en lugar de una sola dirección IPV6.

El TB gestiona las solicitudes de los clientes de la siguiente manera.

- Se designa un servidor de túnel
- Elige el prefijo IPV6 que se asignara al cliente entre 0-128 siendo los valores más comunes /48 prefijo de sitio /64 prefijo de subred /128 host.
- Se fija un tiempo de vida para el túnel.
- Se registra automáticamente en el DNS las direcciones IPV6 globales asignadas al túnel en el cliente.
- Configura el servidor de túnel

2.2.4.2.6. SOFTWIRES

Mecanismo de transición "universal" basado en la creación de túneles es decir IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4

Las propiedades que se describen a continuación son las más relevantes de este mecanismo:

- Permite atravesar NATs en las redes de acceso
- Posibilidad de túneles seguros
- Baja sobrecarga en el transporte de paquetes IPv6 en los túneles
- Fácil inclusión en dispositivos portátiles con escasos recursos hardware.

- Posibilitará la provisión de conectividad IPv6 en dispositivos como routers ADSL, teléfonos móviles, PDAs, etc. cuando no exista conectividad IPv6 nativa en el acceso.
- También posibilita la provisión de conectividad IPv4 en dispositivos que solo tienen conectividad IPv6 nativa.

Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4

Existen dos entidades:

- Softwires Initiator (SI): agente encargado de solicitar el túnel
- Softwires Concentrator (SC): agente encargado de crear el túnel
- El SC está instalado en la red del ISP (DSLAM, Router de agregación u otro dispositivo)

El SI está instalado en la red del usuario CPE típicamente.

El SC proporciona conectividad IPv6 al SI, y el SI hace de enrutador IPv6 para el resto de la red de usuario

Se usa delegación de prefijo IPv6 entre el SC y el SI para proporcionar un prefijo (típicamente /48) a la red del usuario (DHCPv6 PD).

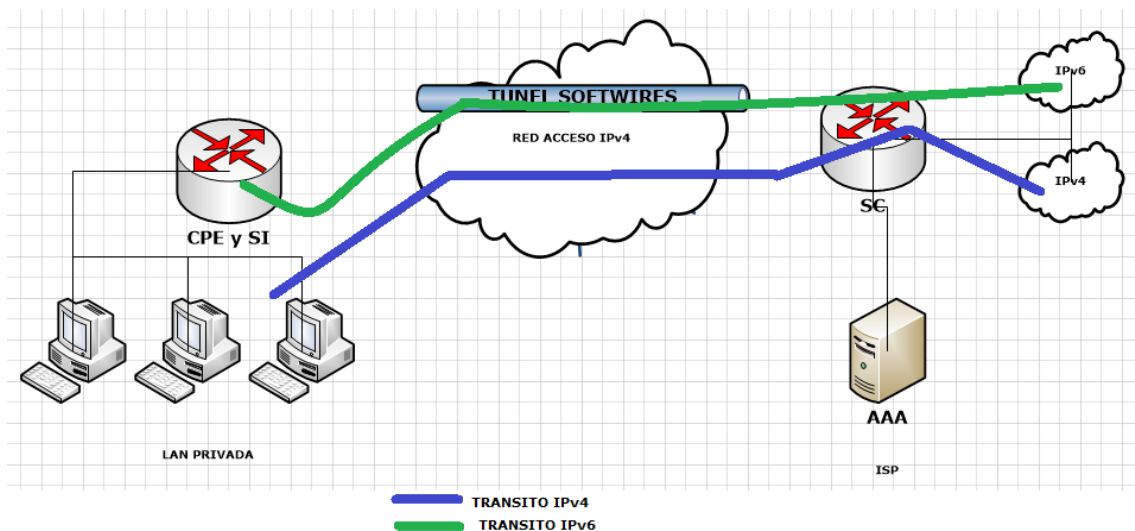


Figura II. 21 Túnel Softwire. Fuente: Herramientas de transición (ConsulIntel & 6Deploy, 2008)

2.2.4.2.7. 6OVER4

Los túneles 6over4 también son conocidos como túnel multicast IPv4. Este mecanismo usa la capacidad multicast o de multidifusión de IPV4 como una capa de enlace de datos virtual para transmitir paquetes IPv6 entre nodos DualStack, Milltec S.A (12).

Por defecto los nodos 6over4 son configurados con direcciones Link local o enlace local FE80 más una dirección IPV4. Por ejemplo si se tiene la dirección 192.168.3.2 en la interfaz quedara así FE80::C0A8:0302, lo que se realizo es parecido al mecanismo de 6to4.

192 ----> C0

168 ----> A8

03 ----> 03

02 ----> 02

Por otro lado las comunicaciones que se realizan entre una infraestructura IPv6 multicast y una infraestructura IPV4 multicast se realizan mediante una traducción de direcciones IPV6 multicas a IPV4 multicast de la siguiente forma.

239.192. (Penúltimo byte dir IPv6). (Último byte dir IPv6)

FF02::1: FF28: 9C5A

9C ----> 156

5A ----> 90

Se mapea a 239.192.156.90 en formato IPv4.

Este método permite que los host aislados con IPV6, situados en un lugar físico que no disponen de este servicio, puedan ser plenamente funcionales en un dominio IPV6 que soporte multicast IPV4, RFC 2529 (31).

Los host conectados con este método no requieren compatibilidad con las direcciones IPV4 o túneles configurados. De este modo IPV6 gana considerablemente independencia de los enlaces adyacentes y puede pasar sobre muchos saltos de subredes IPV4.

El mecanismo se conoce formalmente como "IPV6 over IPV4", "6over4" o informalmente como "virtual ethernet".

UNIDAD MÁXIMA DE TRANSFERENCIA MTU

Por defecto el tamaño del MTU para los paquetes de IPV6 en un dominio IPV4 es **1480** octetos (1 octeto es igual a 8 bits). Este tamaño puede ser variado por un Router Advertisement que contiene una opción específica de MTU, o una configuración manual de cada nodo. Hay que tener en cuenta que si el tamaño del MTU de IPV6 es demasiado grande para algunas subredes IPV4, entonces se producirá una fragmentación IPV4.

Paquetes IPV6 se transmiten en paquetes IPV4 con el protocolo 41 de IPV4. El paquete IPV4 contiene la cabecera IPV6 seguida inmediatamente por la carga útil.

El tiempo de vida de un paquete debería ser fijado a un valor bajo, para evitar accidentalmente fugas de paquetes desde los dominios IPV4. Este parámetro debe ser configurable y su valor por defecto de 8.

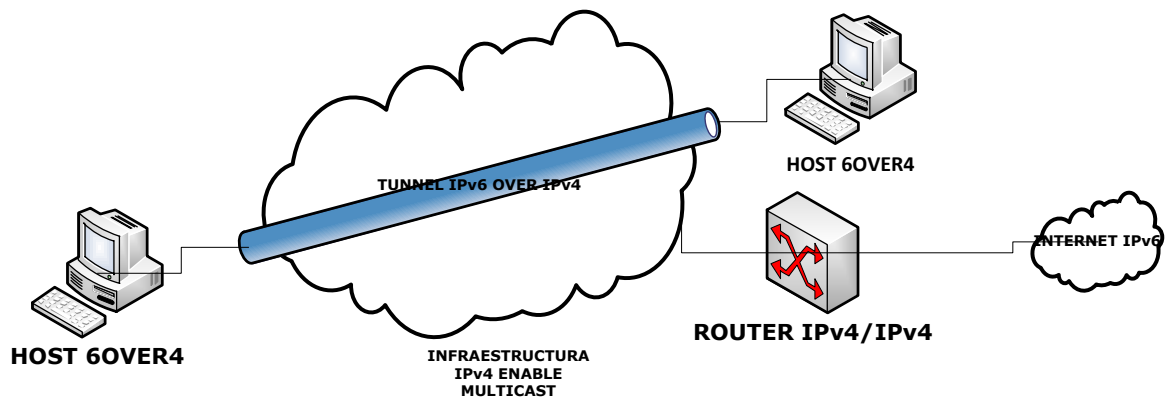


Figura II. 22 Configuración 6over4.Fuente: (Autores)

2.2.4.2.8. ISATAP

Es un mecanismo de transición creado para transmitir paquetes IPV6 entre nodos DualStack. Automatiza la creación de túneles desde los nodos hacia los routers y entre nodos dentro de un mismo sitio, Milltec (12).

Es similar a 6over4 pero este mecanismo no usa una infraestructura multicast. La dirección IPv4 del host será incluida en los últimos 32 bits del identificador de interface como parte de su dirección IPV6.

Cualquier huésped que desee participar en ISATAP en una red IPv4 puede configurar una interfaz de red IPv6 virtual.

Link-Local o prefijo de ISATAP + 5EFE+ dirección IPV4

5EFE reservados por IANA para ISATAP.

Ej. De dirección IPV4

192 ----> **C0**
168 ----> **A8**
03 ----> **03**
02 ----> **02**

FE80:0000:0000:0000:0000:5EFE:C0A8:0302

FE80:: 5EFE: C0A8:0302

El protocolo de direccionamiento de túnel automático del lado de la intranet (ISATAP, Intra-side Automatic Tunnel Addressing Protocol) conecta nodos Dual-Stack sobre redes IPV4. ISATAP ve la red IPv4 como una capa de enlace para IPv6, RFC 5214 (23).

ISATAP habilita túneles automáticamente sea utilizando direcciones privadas o públicas en, host-a-router, router-a-host, host-a-host.

IDENTIFICADORES DE INTERFAZ ISATAP

Se construyen modificando el formato EUI-64 concatenando los 24 bits de IANA OUI (00-00-5F), los 8-bits hexadecimales 0xFE y los 32-bits de la dirección IPV4.

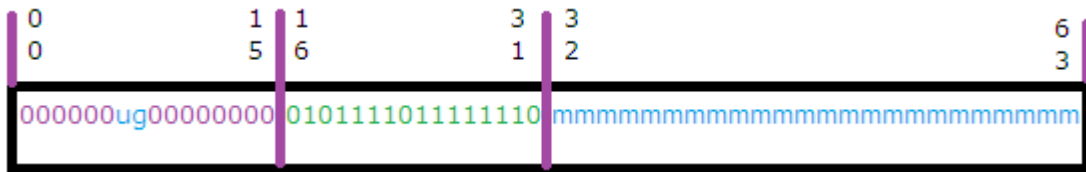


Figura II. 23 Configuración 6over4. Fuente:IETF (RFC 5214,, 2008)

Cuando la dirección IPV4 es identificada como global Unique, el bit "u" (universal/local) se pone a 1, de lo contrario, el bit "u" se establece a 0. "g" es el bit de grupo individual, y "m" representa los bits (32bits) de la dirección IPV4.

2.2.4.3. TÉCNICAS DE TRADUCCIÓN

2.2.4.3.1. NAT64

NAT64 es un mecanismo que permite a hosts IPv6 comunicarse con servidores IPv4. El servidor NAT64 dispone de al menos una dirección IPv4 y un segmento de red IPv6 de 32-bits (por ejemplo 64:ff9b::/96, véase RFC 6052, RFC 6146), RFC 6146-1 (27).

El cliente IPv6 construye la dirección IPv6 destino utilizando el rango anterior de 96 bits más los 32 bits de la dirección IPv4 con la que desea comunicarse, enviando los paquetes a la dirección resultante.

El servidor NAT64 crea entonces un mapeo de NAT entre la dirección IPv6 y la dirección IPv4, permitiendo la comunicación.

Una dirección IPV6 se traduce a su correspondiente dirección IPV4 y viceversa, en los casos donde se usa un algoritmo de mapeo (asignación). Este documento se reserva un "prefijo conocido, Well-Know Prefix" para uso en un algoritmo de mapeo. El valor de este prefijo es **64:ff9b::/96**. Convertir direcciones IPV4 a IPV6 y viceversa siguen el mismo formato, RFC 6052 (32).

Las direcciones IPv6 a IPv4 se componen de un prefijo de longitud variable, la dirección IPv4 incrustada y la longitud variable del sufijo.

PL=Prefix Lenght

PL	0	32	40	48	56	64	72	80	88	96	104
32	Prefix	v4 (32)		u	Suffix						
40	Prefix	v4 (24)		u	(8)	Suffix					
48	Prefix	v4(16)		u	(16)	Suffix					
56	Prefix	(8)		u	v4(24)	Suffix					
64	Prefix	u		v4(32)	Suffix						
96	Prefix	v4 (32)									

Figura II. 24 Longitud del prefijo. Fuente:IETF (RFC 6052, 2010)

En estas direcciones, el prefijo será "Well-Know prefix" o un "Network-Specific Prefix" unique para desplegar la traducción en la organización. El prefijo puede tener solamente una de las

siguientes longitudes: 32, 40, 48, 56, 64 o 96. El prefijo "well-Know" tiene una longitud de 96 bits de largo, y puede solamente ser usado en una sola forma como se muestra en la tabla.

Los bits 64 a 71 de las direcciones son reservadas para compatibilidad con el formato de identificador de host en la arquitectura de direccionamiento de IPV6. Estos bits deben ser puestos a cero. Cuando se usa un prefijo /96 los administradores deben asegurarse que los bits del 64-71 se ponen a cero. Una manera más fácil de conseguir esto es construyendo el prefijo de red específico /96 y escogiendo un /64 entonces añadiendo 4 octetos y poniéndoles a cero.

El prefijo de las direcciones IPV4 se codifican de la siguiente manera, primero el bit más significativo. Dependiendo de la longitud del prefijo, el 4 octeto de la dirección puede ser separado por el octeto reservado "u" cuyos 8 bits deben ser puestos a cero.

- Cuando el prefijo es **32 bits** de longitud, la dirección IPV4 es codificada en la posición **32-63**.
- Cuando el prefijo es **40 bits** de longitud, 24 bits de la dirección IPV4 son codificadas en las posiciones **40 -63**, con los 8 bits restantes en la posición **72-79**.
- Cuando el prefijo es **48 bits** de longitud, 16 bits de la dirección IPV4 son codificadas en las posiciones **48 -63**, con los 16 bits restantes en la posición **72-87**.
- Cuando el prefijo es **56 bits** de longitud, 8 bits de la dirección IPV4 son codificadas en las posiciones **56 - 63**, con los 8 bits restantes en la posición **72-95**.
- Cuando el prefijo es **64 bits** de longitud, la dirección IPV4 es codificada en la posición **72-103**.
- Cuando el prefijo es **96 bits** de longitud, la dirección IPV4 es codificada en la posición **96-127**.

No hay bits restantes, y por lo tanto no hay sufijo, si el prefijo es /96 de longitud. En los otros casos, los bits restantes de la dirección constituyen el sufijo. Estos bits están reservados para futuras ampliaciones y deben ser puestos a cero. Los traductores que reciben direcciones IPV4 incrustadas en las direcciones IPV6 en estos bits no son cero, deben ser ignoradas.

ALGORITMO DE TRADUCCIÓN DE DIRECCIONES

- Concatenar el prefijo, los 32 bits de la dirección IPV4, y el sufijo si es necesario para obtener una dirección de 128-bits.
- Si la longitud del prefijo es menor que los 96 bits, se inserta el octeto nulo "u" en la posición apropiada (**bits 64-71**), causando que el octeto menos significativo sea excluido.

Las direcciones IPV4 son extraídas de las direcciones IPV6 de acuerdo al siguiente formato.

- Si el prefijo es **/96**, se extrae los últimos **32 bits** de la dirección IPV6.
- Para las otras longitudes de prefijo, se remueve el octeto "u" para obtener una secuencia de **120 bits** (cambiando las posiciones de los bits **72-127, 64-119**) entonces se extrae los **32 bits** siguientes del prefijo.

Network-Specific Prefix	IPv4 address	IPV4-embedded IPv6 address
2001:db8::/32	192.0.2.33	2001:db8:c000:221::
2001:db8:100::/40	192.0.2.33	2001:db8:1c0:2:21::
2001:db8:122::/48	192.0.2.33	2001:db8:122:c000:2:2100::
2001:db8:122:300::/56	192.0.2.33	2001:db8:122:3c0:0:221::
2001:db8:122:344::/64	192.0.2.33	2001:db8:122:344:c0:2:2100::
2001:db8:122:344::/96	192.0.2.33	2001:db8:122:344::192.0.2.33

Figura II. 25 Representación de direcciones IPv4 incrustadas en direcciones IPv6 usando el prefijo Network-Specific. Fuente: IETF (RFC 6052, 2010)

Well-Know Prefix	IPv4 address	IPv4-Embedded IPv6 address
64:ff9b::/96	192.0.2.33	64:ff9b::192.0.2.33

Figura II. 26 Representación de direcciones IPv4 incrustadas en direcciones IPv6 usando el prefijo Well-Know. Fuente: IETF (RFC 6052, 2010).

El prefijo Well-Know no debe ser usado para representar direcciones que no sean públicas.
También no debe ser usado para construir traducciones de IPv4 a IPv6.

2.2.5. RESUMEN DE TÉCNICAS EN TUNELES

Tabla II. II Resumen técnica de túneles. Fuente (Autores)

	6IN4	TEREDO	6TO4	6RD	ISATAP	T.BROKER	SOFTWARE
PROTOCOLO	41	UDP/puerto 3544	41	41	41	41	UDP
MODO DE CONEXIÓN	Manual	Automático	Automático	Automático	Automático	Automático	Asistido por el usuario final
ATRAVIESA NAT	No	Si	Si	No		Si	Si
SOPORTE EN SO	Linux/Unix, Mac, Windows	Linux, Mac OS, Solaris, BSD, es nativo de Windows.	Linux, Apple, Windows.	Cisco	Windows.	Linux Windows.	Linux, Mac Windows.
PREFIJO	Asignado por un RIR	2001:000::/32	2002::/16	Asignado por un RIR	Asignado por un RIR	Asignado por un RIR	Asignado por un RIR
NECESITA UNA DIRECCIÓN PÚBLICA/PRIVADA.	Si/no	Si/no	Si/no	Si/no	Si/Si	Si/no	Si/no
PROCESAMIENTO DE HARDWARE	Medio	Bajo	Medio	Alto	Alto	Alto	Bajo
CONECTIVIDAD DIRECTA	Solo entre hosts 6IN4	Solo entre hosts TEREDO	Solo entre hosts 6TO4	Solo entre hosts 6RD	No	No	No

2.2.5.1. DESCRIPCIÓN DE CRITERIO

PROCOLO

La mayoría de túneles utiliza el protocolo 41(IPV6) a excepción de Teredo y Softwire que utiliza el protocolo 17(UDP), lo que primero se realiza es encapsular los paquetes IPV6 sobre UDP y luego sobre IPv4, esto garantiza la calidad de servicio aunque se puede realizar con TCP pero al realizar esto la calidad del servicio disminuiría.

MODO DE CONEXIÓN

La mayoría de túneles realizan la conexión automáticamente es decir las direcciones IPv6 de los extremos de los túneles se determina a través de las direcciones IPv4 de los host, a excepción de 6in4 que hay que determinar la longitud del prefijo en forma manual (rfc 4213). Para los softwires el modo de conexión se la realiza asistido por el usuario ya que se tiene que configurar el CPE.

ATRAVIESA NAT

Esta es la propiedad que permite conexión ipv6 detrás de todos los dispositivos NAT.

Tunnel Broker atraviesa dispositivos NAT, incluyendo configuraciones de NAT anidados. Teredo ofrece NAT transversal pero no funciona si se presenta un NAT simétrico. Softwires muestra mayor facilidades en a travesar diferentes variantes de NATs

6rd y 6in4 no atraviesan Nat, intercambian información solo host que están dentro de los mismos túneles.

SOPORTE EN SO

Describe la propiedad de los sistemas operativos para vincularse con el nuevo protocolo.

Aquellos SO que estén bajo un kernel Linux aceptan ipv6 en todas sus distribuciones, por otro lado los SO más populares ya integran este nuevo protocolo o tienen actualizaciones al alcance del usuario para versiones de SO pasadas.

PREFIJO

Ciertas direcciones IPv6 han sido reservadas y asignadas para uso exclusivo de túneles

NECESITA UNA DIRECCIÓN IPV4 PÚBLICA/PRIVADA.

6to4 necesita una dirección IPV4 pública para a partir de esta calcular la dirección 6to4 del Router.

El objetivo de Teredo es conectar a usuarios que estén ubicados detrás de un NAT, para cumplir esto es necesario tener una dirección IPv4 privada, más para crear el Teredo server se necesita una IPV4 pública.

PROCESAMIENTO DE HARDWARE

La creación de túneles en la red aumenta la fragmentación por lo tanto los equipos requieren mayor proceso para atender el establecimiento de los mismos, dependiendo de la topología de la red se requerirá un full mesh de túneles.

Este tema es crucial en un ISP en donde la disponibilidad del servicio debe ser garantizada, por lo que si se opta por elegir un túnel se debe considerar aquel que presente baja carga en procesamiento.

CONECTIVIDAD DIRECTA

La conectividad directa se logra cuando un host no necesita pasar por un servidor o un relay para conectarse con el otro extremo del túnel. 6RD, Teredo y 6to4 ofrece esta característica, pero sólo funciona entre sí.

2.3.HOME OFFICE

Cuando hablamos de Home Office en IPv6, nos referimos a la implementación de la red de una oficina pequeña u oficina en casa de forma tal que cuente con la capacidad de operar con la nueva versión del protocolo IP.

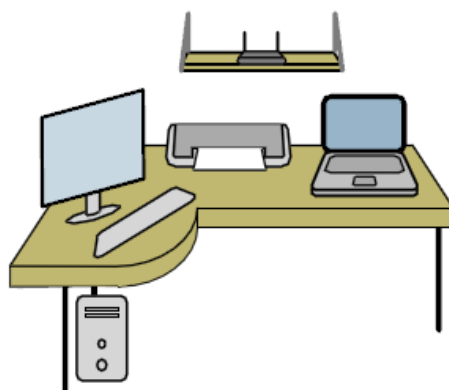


Figura II. 27 SOHO (Small office home office). Fuente: IPv6 para todos (Palet, y otros, 2009)

2.3.1. CONSTRUYENDO UN SOHO CON IPv6

Antes es importante tener claro las diferentes partes que lo componen una SOHO. Una vez que éstas estén identificadas, podremos ver cuáles de ellas será necesario configurar para que funcionen con IPv6. A partir de ahí, será apropiado ver cómo hacerlo.

Las etapas que debemos cumplir serán:

1. Identificar las partes del SOHO
2. Determinar cuáles de ellas requieren configuración para trabajar con IPv6
3. Configurar el SOHO con IPv6

2.2.1.1. IDENTIFICANDO LAS PARTES DE UN SOHO

Este es el primer paso a la hora de pensar en la construcción de la red de un SOHO. Para llevar a cabo tal identificación, sugerimos hacerlo sobre tres aspectos bien delimitados, Pallet (9):

- Identificación de equipos
- Identificación de sistemas operativos
- Identificación de aplicaciones

2.3.1.1.1. IDENTIFICACIÓN DE EQUIPOS

Podemos distinguir entre:

DISPOSITIVOS DE NETWORKING: Deberemos identificar aquellos que contribuyen a la comunicación de la red, en este conjunto podríamos incluir por ejemplo: el switch donde conectamos las terminales o computadoras, el router que el proveedor de Internet nos dejó instalado al contratar el servicio, el equipo que nos provee la conexión inalámbrica, entre otros.

DISPOSITIVOS TERMINALES: En este grupo encontramos aquellos dispositivos con los que interactuamos directamente, como por ejemplo: las computadoras de escritorio, las computadoras portátiles o laptops, tablets, Smartphone teléfonos IP, servidores de aplicaciones, entre otros.

En otra categoría podríamos identificar a las impresoras de red, que si bien no representan una interfaz directa con el usuario, tampoco es un dispositivo de networking, pero sin embargo vamos a querer su servicio dentro de la red y probablemente queramos tenerla en cuenta a la hora de trabajar con IPv6.

2.3.1.1.2. IDENTIFICACIÓN DE SISTEMAS OPERATIVOS

Deberemos identificar los sistemas operativos con los cuales trabajaremos, para ello tendremos en cuenta los sistemas operativos que se ejecutan en aquellos dispositivos terminales que aportan servicios de red, como por ejemplo el servicio de e-mail.

Además sistemas operativos de computadoras y laptops son aquellos que se ejecutan en los dispositivos terminales con los que trabajamos en forma directa. Los más usados en estos casos pueden ser Windows, Linux y MAC OS.

2.3.1.1.3. IDENTIFICACIÓN DE APLICACIONES

Finalizando con la identificación de componentes de la red del SOHO, en este punto distinguimos:

APLICACIONES EN SERVIDORES: Llamamos así a aquellas que proveen servicios en forma centralizada para los distintos dispositivos de la red, como por ejemplo: servicio de DNS, e-mail, páginas web, entre otras.

APLICACIONES EN TERMINALES: Se trata de las aplicaciones que utilizamos para trabajar por ejemplo, nuestra laptop o computadora de escritorio, incluso una tablet.

Entre las más conocidas están: editores de texto, planillas de cálculo, clientes de e-mail, navegador de páginas web, clientes de mensajería instantánea, clientes de servicio multimedia, aplicaciones hechas a medida, etc.

2.3.2. IDENTIFICACIÓN DE LOS COMPONENTES QUE REQUIEREN CONFIGURACIÓN.

En una red medianamente nueva, o sea, con equipos de networking cuya fecha de fabricación data de unos 3 o 4 años atrás, no deberíamos tener que hacer más que actualizar los sistemas operativos si estos no soportaran IPv6, Palet (9).

Una buena práctica sería listar uno a uno los equipos de networking y buscar en la documentación de cada uno su compatibilidad con IPv6. Probablemente, y tal como dijimos anteriormente, nos encontremos con que debemos actualizar alguna versión de sistema operativo o instalar algún firmware para lograr el soporte IPv6.

Por ejemplo, para los routers Cisco, encontramos su soporte a partir de la versión de IOS 12.3T, en el caso de los Juniper todas las versiones de JunOS están soportando IPv6.

Otro dato interesante son los equipos de conexión inalámbrica en los cuales la configuración del equipamiento para qué soporte el protocolo IPv6 dependerá de la marca y modelo del router.

A modo de ejemplo, los routers inalámbricos D-link, así como en Mikrotik tenemos las actualizaciones para IPv6.

En cuanto a los sistemas operativos, la mayoría de las distribuciones de Linux, desde hace varios años, ya vienen con el Stack de IPv6 cargado, así como las versiones de Unix. Respecto a los sistemas operativos MacOS, el soporte IPv6 está dado por defecto desde el año 2003 con las versiones de "Panther". En cuanto a los sistemas Windows XP y Windows Server 2003, estos tienen la posibilidad de cargar de forma muy simple la pila de IPv6. En cambio, en las versiones de Windows Vista, Windows 7 y Windows 8 esta característica está habilitada por defecto.

Debemos tener en cuenta la recomendación de mantener las dos versiones del protocolo IP ejecutándose al mismo tiempo, o sea, lo que suele llamarse "mecanismos de doble pila" o "Dual Stack".

2.3.3. CONFIGURANDO LOS COMPONENTES SOHO CON IPv6

Finalmente, con los dispositivos identificados, las versiones de software actualizadas para que soporten la nueva versión del protocolo IP y las modificaciones que hayan sido necesarias en las aplicaciones, estamos preparados para la etapa de la configuración.

Para ello, dividiremos la tarea en dos partes claramente separadas:

- Configuración de la red interna de nuestro SOHO (LAN)
- Configuración de la conexión con el exterior (Internet)

La figura II.28 muestra el límite entre estas dos áreas:

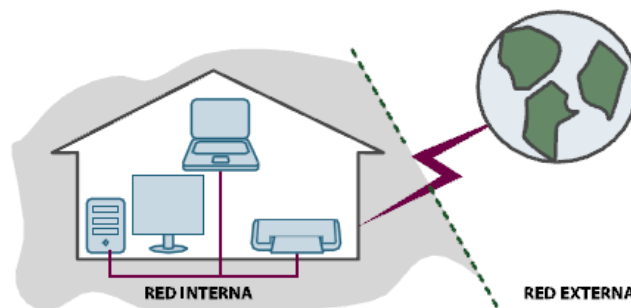


Figura II. 28 Punto de Demarcación. Fuente: IPv6 para todos (Palet, y otros, 2009)

Antes de comenzar con la descripción de estas dos tareas, trataremos el tema de cómo obtener las direcciones IPv6 con las que trabajaremos. Existen varias alternativas, algunas de ellas podrían ser:

- Disponer de direcciones propias, solicitadas al RIR correspondiente según la región donde nos encontremos.
- Que nuestro proveedor de Internet nos asigne un bloque de direcciones.
- Utilizar direcciones 6to4 (en este caso necesitaremos al menos una dirección IPv4 pública para hacerlo funcionar)
- Utilizar Túnel Brokers, de modo tal de establecer túneles automáticos con algún sitio capaz de proveer conectividad IPv6.

2.2.3.1. CONFIGURACIÓN DE LA RED INTERNA

Para que en una red pueda llevar a cabo la autoconfiguración de interfaces con direcciones IPv6, será necesario que los dispositivos que deseen configurarlas soliciten los datos para hacerlo y además que algún otro dispositivo se encargue de anunciar dichos datos.

Estas solicitudes y anuncios forman parte del protocolo Neighbor Discovery, el cual a través de un conjunto de mensajes ICMPv6, se constituye en la base para que pueda llevarse a cabo el proceso de autoconfiguración.

En forma simplificada, los mensajes ICMPv6 que solicitan los datos se denominan "NS" (Neighbor Solicitation) y "RS" (Router Solicitation), y las respuestas vienen dadas por otros mensajes ICMPv6 los llamados "NA" (Neighbor Advertisement) y "RA" (Router Advertisement).

Hecha esta introducción veamos cómo podemos realizar la autoconfiguración en la red del SOHO dependiendo de la topología de la misma.

Tomemos como ejemplo la red de la figura II.29:

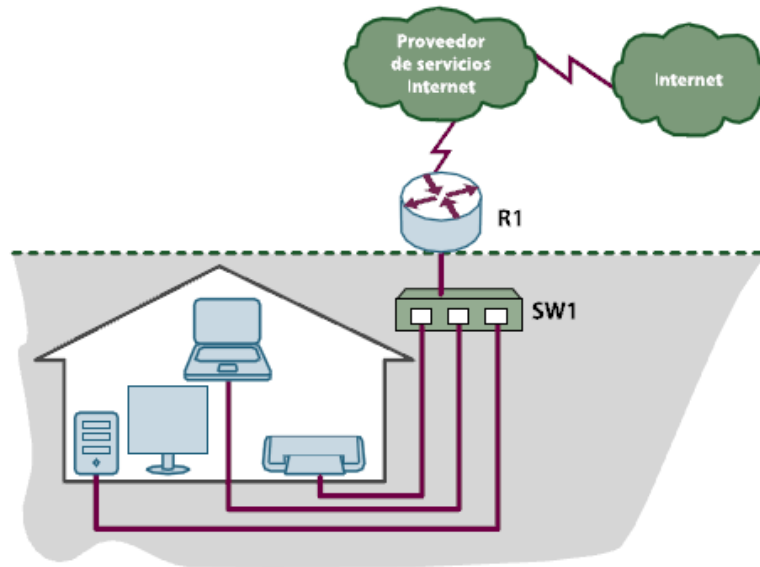


Figura II. 29 Red con enlace dedicado. Fuente: IPv6 para todos (Palet, y otros, 2009)

Como vemos, la red del SOHO posee un enlace a Internet “dedicado”, o sea, que el proveedor deja a disposición del cliente una conexión para que sea utilizada sólo por éste. En estos casos usualmente se dispone de un equipo router a donde llega el enlace de Internet (ejemplo R1).

Una de las interfaces del router está conectada a la red interna del SOHO, a donde también conectan el resto de los dispositivos de la red. Todos lo hacen a través de un switch, al cual llamamos para nuestro ejemplo SW1.

En este caso, cuando un dispositivo (laptop, computadora de escritorio, etc) se conecta a la red, envía un mensaje NS (multicast) para que puedan verlo todos los nodos de la red y generalmente un mensaje RS. Al recibir este último, el router R1 le envía como respuesta un mensaje RA conteniendo el prefijo IPv6 que el dispositivo debe utilizar para realizar el mecanismo de autoconfiguración.

Esta secuencia de mensajes se ve esquematizada en las Figuras que se describe a continuación:

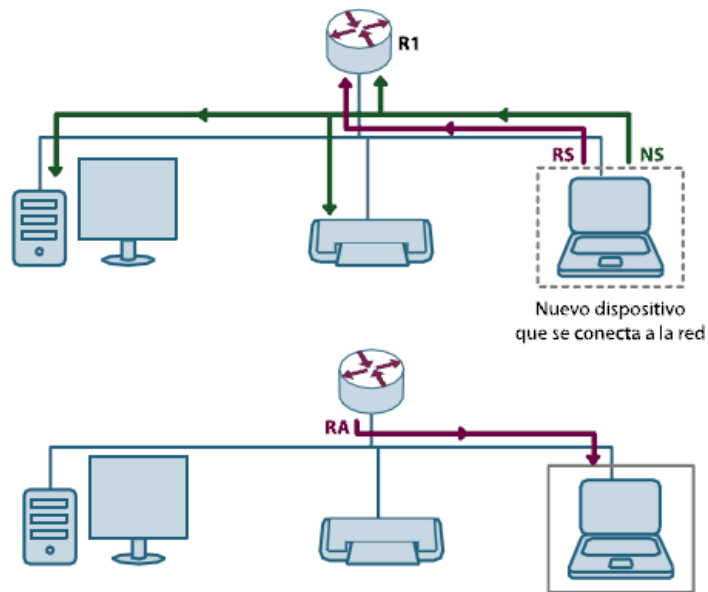


Figura II. 30 Red con enlace dedicado. Fuente: IPv6 para todos (Palet, y otros, 2009)

Obtenido el prefijo, el dispositivo está en condiciones de configurarse una dirección IPv6 basándose en el prefijo anunciado por el router y su propia MAC Address (a través del método EUI-64).

La figura II.31 es un modelo de la obtención de direcciones IPv6 en una red interna, luego de que se realice el proceso de autoconfiguración.

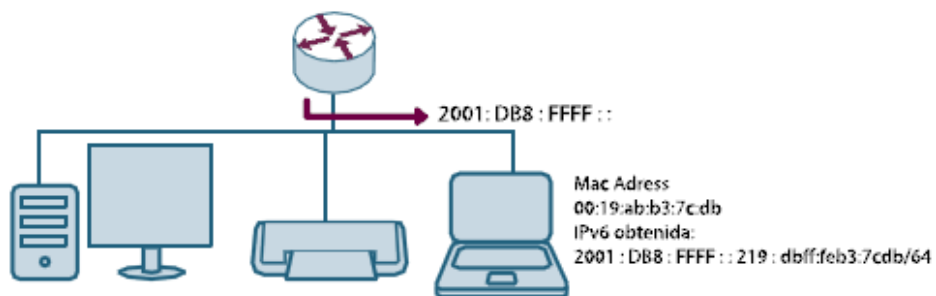


Figura II. 31 Autoconfiguración. Fuente: IPv6 para todos (Palet, y otros, 2009)

Supongamos ahora que no tenemos acceso al router que el proveedor de servicios de Internet dejó en el SOHO para nuestra conexión o, simplemente no existe tal equipo. Por lo tanto, debemos ver quién será el que enviará los mensajes RA.

Una alternativa podría ser una computadora conectada a la red interna, de forma tal que cumpla con la función de anunciar los RA y que con esto pueda llevar adelante la autoconfiguración. Hablamos por ejemplo de, un servidor con sistema operativo Linux corriendo el daemon radvd. Otro método disponible sería usar un servidor de DHCPv6

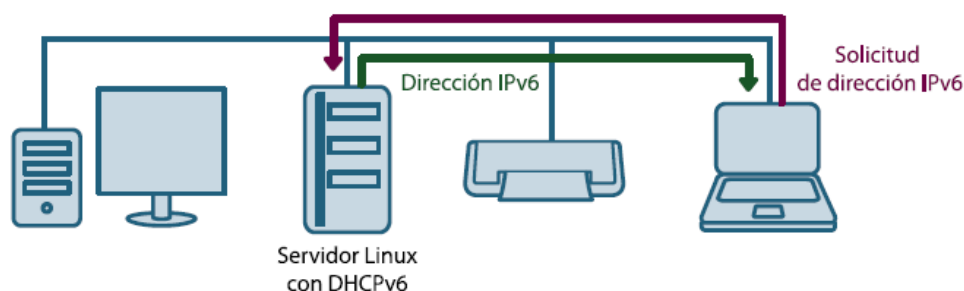


Figura II. 32 Servidor para la autoconfiguración. Fuente: IPv6 para todos (Palet, y otros, 2009)

La diferencia entre utilizar el daemon o un servidor DHCPv6 radica en el mayor o menor grado al que queremos llegar con la autoconfiguración, ya que un servidor de DHCPv6 no solo lo podremos utilizar para anunciar los prefijos de la red sino además para comunicar otros datos como por ejemplo direcciones de los servidores de DNS, entre otros.

En el caso de radvd solo nos permite anunciar los prefijos IPv6 para que las interfaces se autoconfiguren.

2.2.3.2. CONFIGURACIÓN DE LA CONEXIÓN CON EL EXTERIOR (INTERNET)

En esta sección veremos qué variantes hay a la hora de configurar una conexión IPv6 con el exterior de nuestra red.

Tal como se trató anteriormente existe la posibilidad de que la red del SOHO tenga un enlace dedicado y que para ello el proveedor de servicios de Internet haya dispuesto un equipo router que lo conecta con el exterior.

Ahora bien, podemos considerar dos posibilidades:

- A.** Que el proveedor nos facilite, además del servicio de la conexión a través de IPv4, una conexión a Internet a través de IPv6.
- B.** Que el proveedor de servicios de Internet no pueda brindarnos una conexión a través de IPv6.

Si nuestro caso es el **A**, es muy posible que el proveedor ya esté anunciando a Internet su propio prefijo IPv6 y que, si da el servicio a los clientes, también les ofrezca un prefijo de su rango. Con esta situación, si el proveedor anuncia su prefijo, con seguridad también está anunciando el nuestro ya que es un subconjunto de su propio bloque de direcciones.

Tal asignación y anuncio de prefijos se esquematiza en la siguiente figura:

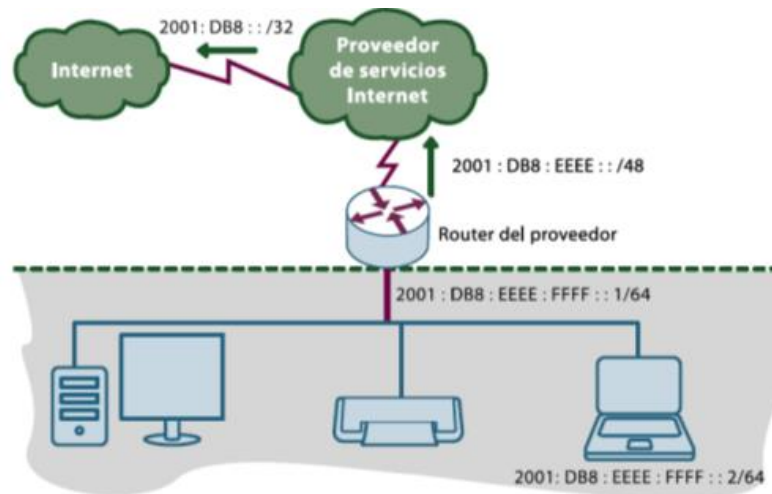


Figura II. 33 Asignación de Prefijos Caso A. Fuente: IPv6 para todos (Palet, y otros, 2009)

Cuando se da esta situación, nada más tenemos que hablar con nuestro proveedor para ver de qué forma prefiere implementar esto (a través de una sesión BGP con la red del SOHO, a través de rutas estáticas hacia nuestro router, etc), pero en todo caso será solamente una cuestión de acuerdos.

Ahora, si nuestro caso es el **B**, vamos a tener que encontrar la forma de atravesar la red IPv4 del proveedor para llegar a otra que pueda interpretar mis paquetes IPv6. Para ello debemos

apelar a algún mecanismo de túneles analizados en la sección 1.2.4 que más se adapte a nuestra realidad.

CAPÍTULO III

METODOLOGÍAS DE MIGRACIÓN A IPv6

La implementación de IPv6 debe realizarse sistemáticamente pues un proceso tan complejo no se lo puede cumplir en poco tiempo, por lo que planificar la transición permitirá que los procesos se cumpla eficazmente en el largo plazo.

Es por eso que la comunidad involucrada con el desarrollo del internet y las telecomunicaciones ha puesto a consideración las mejores prácticas para el despliegue de IPv6 en infraestructura y plataformas.

Organizaciones se han pronunciado con sus recomendaciones, RFCs y metodologías generales de migración tanto para empresas, proveedores de servicio de internet y SOHO.

A continuación se describen las metodologías de despliegue del nuevo protocolo de interés para las personas responsables de la planificación y/o operación de un Backbone IP que actualmente brinda solo servicios IPv4. Este es el caso típico de proveedores de servicios de Internet en

diferentes modalidades (accesos dedicados, proveedores de banda ancha, proveedores regionales o locales.)

Las metodologías que se analizarán son las siguientes:

- Estrategias para la coexistencia y Adopción de IPv6 en el Ecuador.
- Lógica planificación IPv6.
- Escenarios de análisis para la introducción de IPv6 en la red de un ISP.
- ISP's IPv6 en 3 pasos.

Además se extenderá las consideraciones finales para el despliegue para posteriormente diseñar un modelo sistemático de migración que se ajuste a las necesidades del ISP Fastnet.

3.1. ESTRATEGIAS PARA LA COEXISTENCIA Y ADOPCIÓN DE IPV6 EN ECUADOR (IETF IPV6.EC)

La transición a IPv6 dentro del territorio ecuatoriano se está iniciando, por lo que ha creado estrategias para fomentar el despliegue en las empresas públicas y privadas, generando además una metodología de transición de referencia que se analizará en los párrafos siguientes, MINTEL (33).

Cabe mencionar también que se ha realizado un estudio de la situación actual de los proveedores de internet que operan en el Ecuador, que sirve de referencia en lo posterior en esta investigación para el análisis de implementación.

Por otra parte la asociación ecuatoriana de proveedores de valor agregado e Internet (AEPROVI) en año 2009 creó la Fuerza de Trabajo de IPv6 de Ecuador (IPv6TF-EC) con los siguientes objetivos:

1. Ser fuente de información relacionada con el Protocolo de Internet versión 6 (IPv6).
2. Coordinar los esfuerzos de los diferentes actores del Internet ecuatoriano para una eficaz y pronta adopción del IPv6.
3. Fomentar el uso de IPv6.

4. Establecer permanente comunicación e identificar oportunidades de colaboración con los Grupos de Trabajo de otros países y regiones.

Dentro de Task Force Ecuador desde el 2010 se puede encontrar información muy selecta y asesoría en proyectos que se estén ejecutando con IPv6.

3.1.1. ESTRATEGIAS

Dentro del contexto de un Ecuador digital se encuentra el programa nacional de coexistencia y transición IPv4-Ipv6 como un programa de gestión eficiente de recursos y calidad para banda ancha, por lo que El MINTEL formula las siguientes estrategias.

- Fomentar la Adopción de Entidades Estatales iniciando por el Ente de Regulación y Ente Rector de Telecomunicaciones y TIC.
- Integración y cooperación del sector público, sector privado, academia y sociedad civil.
- Propender a la actualización de infraestructura y soporte IPv6.
- Estimular la implementación IPv6 en sector privado para contactarse con las plataformas del gobierno serán ipv4/Ipv6 posteriormente solo IPv6.
- Sensibilización, difusión, capacitación y formación de IPv6, en las que se dispondrá laboratorios de desarrollo.
- Impulso y financiamiento de proyectos tecnológicos con soporte IPv6.
- Adopción de IPv6 en redes de investigación y educación.
- Implementación de plataformas y contenidos para acceso a IPv6.

Es así como se estimula la introducción del nuevo protocolo en los servicios de telecomunicaciones del Ecuador.

3.1.2. METODOLOGÍA POR EL MINISTERIO DE TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN

Para la adopción del nuevo protocolo en las redes del Ecuador se tiene definido lo siguiente, MINTEL (33):

1. Establecimiento de metas, hitos y horizontes para la implementación de planes de transición con tiempos definidos.
2. Generación de marcos referenciales de adquisición (HW, SW, Recursos, Aplicaciones, etc.) y planes de direccionamiento para el soporte adecuado de IPv6.
3. Impulso para la generación de contenidos, aplicaciones y servicios con soporte sobre IPv6.
4. Flujo y tráfico normal de IPv6 coexistente con IPv4 sin incremento de costes y transparente al usuario
5. Transición a IPv6 puro.

En la figura III.1 se presenta el proceso de cumplimiento de la metodología de coexistencia y transición en donde se exhibe las etapas consecutivas:

- Infraestructura
- Servicios
- Aplicaciones
- Usuarios



Figura III. 1 Metodología de coexistencia y transición en el Ecuador. Fuente: IPv6 en Ecuador (MINTEL, 2012)

3.2.LACNIC- PLANIFICACIÓN IPv6

LACNIC nos muestra como planificar la implementación de IPv6 en las siguientes etapas:



Figura III. 2 Planificación LACNIC. Fuente: (Autores)

3.2.1. PRE-PROYECTO

Esta etapa consiste en un estudio inicial, cubriendo lo esencial en el delineamiento del proyecto.

El pre-proyecto se detalla en lo siguiente:

- Informarse
- Relevamiento del Impacto
- Primera experiencia
- Conseguir apoyo interno

3.2.1.1. INFORMARSE

Es el primer paso hacia el entendimiento del nuevo protocolo, que consiste en ponerse al corriente de los aspectos teóricos, características y mejoras que tiene la nueva tecnología.

En la tabla III.I se detalla recursos que ayudarán a la comprensión del protocolo IPv6.

Tabla III. I Recursos disponibles de investigación para el estudio de IPv6 Planificando IPV6 (LACNIC, 2012)

	INFORMARSE
	Fuentes de información: <ul style="list-style-type: none">• Libros

	<ul style="list-style-type: none">• Manuales• Material de vendedores• How to• Tutoriales• Presentaciones• Cursos• RFC's
	<p>Libros:</p> <ul style="list-style-type: none">• IPv6 Essentials -Silvia Hagen. ISBN: 0596100582.• Deploying IPv6 Networks -Ciprian Popoviciu -ISBN: 1587052105.• Running IPv6 -Iljitsch van Beijnum -ISBN: 1590595270.• IPv6 in Practice -Benedikt Stockebrand -ISBN: 3540245243.• Understanding IPv6 (Microsoft) -Joseph Davies -ISBN: 0735624461.• Global IPv6 Strategies: From Business Analysis to Operational Planning (Network Business) -Patrick Grossetete -ISBN: 1587053438.
	<p>How to:</p> <p>Algunos ejemplos:</p> <ul style="list-style-type: none">• http://tldp.org/HOWTO/Linux+IPv6-HOWTO/• http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html.• http://wiki.openwrt.org/IPv6_howto• http://technet.microsoft.com/en-us/network/bb530961.aspx• http://www.microsoft.com/technet/network/ipv6/ipv6faq.msp
	<p>Material de Vendedores:</p> <p>Sirve por dos factores:</p> <ul style="list-style-type: none">• Muestran cuáles equipos ya soportan IPv6 o actualizaciones de software necesarias.• Instruyen sobre configuraciones a realizar.

	Listas de Correos: <ul style="list-style-type: none">• LACTF:www.lac.IPv6tf.org• http://lists.cluenet.de/pipermail/IPv6-ops/
	Reuniones / Eventos: <ul style="list-style-type: none">• Reunión anual de LACNIC.• FLIP-6.• Global IPv6 Summit.• IPv6 Summit Nacionales/Regionales.• Google IPv6 Summit in YouTube.

3.2.1.2. RELEVAMIENTO DEL IMPACTO

En esta etapa ya se conoce lo suficiente sobre IPv6 y es el momento de considerar el impacto que se tendrá, las alternativas que se generan, costos involucrados y las nuevas oportunidades que se abren con IPv6.

El impacto hace referencia en que punto de la red de un ISP se puede presentar problemas, como una mención, según en el estudio realizado por Silva (14) un punto crítico en los ISP es resolver la falta de soporte del nuevo protocolo en los CPE instalados en los clientes, además que un porcentaje muy elevado de los quipos adquiridos se los hizo sin pensar en el nuevo protocolo por lo que no tienen soporte.

En cuanto a las alternativas para la interconexión hacia IPv6 se describen en la sección 2.2.4 en los mecanismos de transición y coexistencia.

Los costos involucrados se dan desde la capacitación del personal, posibles asesorías y sobre todo en compras de equipos y servicios para el tránsito de IPv6, este punto puede ser considerado para hacer mejoras en la infraestructura y potenciar el servicio.

Las oportunidades que se ven en el horizonte, podemos mencionar aquella de anticiparse a los clientes en ofrecer un nuevo servicio y en general ser más competitivo en el mercado de los servicios de telecomunicación.

En la tabla III.II, se detalla los pasos a seguir en el relevamiento del impacto:

Tabla III. II Segunda etapa en el diseño de un pre proyecto IPV6. Fuente: Planificando IPV6 (LACNIC, 2012)

RELEVAMIENTO DEL IMPACTO	
	<p>Determinar Objetivos.</p> <p>La determinación de objetivos ayuda a orientar el relevamiento del impacto.</p> <p>Ejemplo: Para un ISP: Dar servicios de conectividad pública y privada bajo IPV6.</p>
	<p>Inventario</p> <p>Limitarse a los componentes (HW y SW) involucrados en alcanzar el objetivo determinado.</p> <p>Es necesario relevar los sistemas que manipulan paquetes IPV6 (ejemplo: routers, web, mail) como también aquellos que manipulan direcciones IPV6 (bases de datos, análisis de logs).</p>
	<p>Conectividad</p> <ul style="list-style-type: none">• Proveedor de Conectividad: se debe consultar sobre el soporte IPV6 de preferentemente nativo y si existen costos adicionales.• Proveedor de dominios: Consultar sobre soporte IPV6 y si existe costo adicional por registros AAAA.
	<p>Direccionamiento</p> <p>Si utiliza direcciones del proveedor, debe consultar el tamaño de la asignación.</p> <p>Si es usuario final, consultar políticas de LACNIC para ver si califica para asignaciones propias.</p>
	<p>Capacitación</p> <p>Se dan en dos categorías:</p> <ul style="list-style-type: none">• Capacitación sobre IPV6: Aspectos generales de los diferentes protocolos.• Capacitación en los sistemas específicos: Normalmente a través de los proveedores.

3.2.1.3. PRIMERA EXPERIENCIA

En general la primera experiencia consiste en la configuración de un laboratorio para realizar pruebas.

Puede estar conectado o no a la red en operaciones, muchas veces se realizan túneles IPv6 (IPv6 sobre IPv4) pero pueden requerir fragmentación intensiva.

En la tabla III.III se muestra equipos con soporte parcial o total del protocolo IPv6.

Tabla III. III Equipos con soporte Ipv6. Fuente: Planificando IPV6 (LACNIC, 2012)

	PRIMERA EXPERIENCIA
	<p>Equipos disponibles:</p> <ul style="list-style-type: none">• Router CPE, ejemplo Cisco 827.• Open-WRT para CPEs.• Linksys-wrt610n: Implementa 6to4,• Gogo6 y Hurricane Electric: Proporciona la plataforma para crear Tunnel Broker.• Equipos Startbridge: Crean túneles IPv6 sobre IPv4 y viceversa.• Equipos Mikrotik: Soportan IPv6 en Dual Stack en todos sus modelos, así como túneles 6to4, GRE6.

3.2.1.4. APOYO INTERNO

Al tener elaborado un pre-proyecto IPv6 se lo debe poner en consideración de la parte ejecutiva de la organización para exponer la relación costo beneficio ya que el objetivo es plasmar las ideas en un proyecto final con una implementación en toda la infraestructura.

El apoyo puede ser parcial para una implementación piloto en la red de producción pero igualmente debemos pensar como una implementación definitiva pensado en el futuro de la red.

3.2.2. DISEÑO

Para delinear el diseño de transición vamos a considerar los siguientes planes:

- Direccionamiento

- Enrutamiento
- Servicios
- Capacitación

3.2.1.5. DIRECCIONAMIENTO

Este punto es la oportunidad para realizar mejoras en el esquema de direccionamiento, recordemos que en IPv6 no contamos hosts, sino redes, así como cada LAN necesita un /64, se puede ver que hay desperdicio de ip's pero es considerado parte del diseño.

Como hemos visto en el capítulo II, en la sección 2.2.2, la tabla III.IV toma en consideración aquellos aspectos del direccionamiento basados RFC 2373, además se muestra criterios a tomar en cuenta al realizar un direccionamiento independientemente del ambiente.

Tabla III. IV Plan de direccionamiento. Fuente: Planificando IPv6 (LACNIC, 2012)

DIRECCIONAMIENTO	
	<p>Clases:</p> <ul style="list-style-type: none">• Unicast.• Multicast.• Anycast.
	<p>Unicast:</p> <ul style="list-style-type: none">• Global Unicast.• Link-local.• Unique Local Address (ULA)• Especiales
	<p>Subnetting IPv6:</p> <p>Idéntico que IPv4, pero con más bits.</p> <p>No hay notación de máscara, sino sólo de largo de prefijo: Ejemplo: 2001:db8::/32.</p>
	<p>LAN en IPv6:</p> <ul style="list-style-type: none">• Para redes LAN se utilizan generalmente interfaz ID de 64 bits.• Hardware generalmente pensado para trabajar con IID de 64 bits.• En especial para el interfaz ID se utiliza formato EUI-64, basado en la dirección MAC, permitiendo la autoconfiguración.

	<ul style="list-style-type: none">• No hay dirección de red sino: "Subnet-Router Anycast Address",
	<p>WAN en IPv6:</p> <p>Varias opciones:</p> <ul style="list-style-type: none">• Seguir usando redes /64.• Usar Redes /126. (ídem /30 en IPv4).• Incluso sería posible usar /127, usado hoy para evitar ataques DoS en enlaces P2P sin resolución de vecinos.
	<p>Loopbacks en IPv6:</p> <p>De vuelta hay casos en que usan /64.</p> <p>Podemos usar /128.</p>
	<p>Direcciones de Proveedor:</p> <p>En general política por defecto: un /48 o /56 por cliente.</p> <ul style="list-style-type: none">• /48 son 65536 redes /64.• /56 son 256 redes /64. <p>Direcciones de LACNIC:</p> <ul style="list-style-type: none">• ISP's: mínimo /32 para ISP (65536 x /48).• Existe política de segunda distribución si la misma fue insuficiente.• Usuarios Finales: mínimo /48.
	<p>Direccionamiento:</p> <p>Aquí hay dos espacios de direcciones:</p> <ul style="list-style-type: none">• Direccionamiento de infraestructura.• Direcciones para Clientes. <p>Es necesario relevar la cantidad de puntos de presencia de la red (PoP).</p> <p>Mantener el criterio de mantener al menos un 300% reservado para crecimiento.</p>
	<p>Infraestructura interna:</p> <p>Involucra a WANs, Loops y LANs.</p> <p>Definir qué usar como WANs y Loops.</p> <p>Puede ser conveniente usar un espacio totalmente independiente, no ruteable.</p>

	<p>Gestión de Direcciones IPv6:</p> <p>Software disponible:</p> <p>LIBRES:</p> <ul style="list-style-type: none">• HACI• IPPLAN no soporta IPv6. <p>PAGOS:</p> <ul style="list-style-type: none">• IPcontrol, Men & Mice• Efficient IP, Incognito• VitalQIP, Alcatel/Lucent. <hr/> <p>Herramientas</p> <ul style="list-style-type: none">• Randomly ULA address generator based on MAC addresses: http://www.sixxs.net/tools/grh/ula/• Tool: IPv6calc. (apt-get install IPv6calc).• Tool: sipcalc -r for reverse DNS.• 6to4 Address Calculator: http://www.ip-calc.com/• Subnetting tool: www.IPv6book.ca/allocation.html
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.2.1.6. ENRUTAMIENTO

El ruteo es esencialmente repetir lo que se hace en IPv4, intentando mantener la misma topología de IPv4.

La tabla III. V se muestra las opciones para ruteo disponibles para el protocolo IPv6.

Tabla III. V Plan de Enrutamiento Fuente: Planificando IPV6 (LACNIC, 2012)

ENCAMINAMIENTO	
	<p>Opciones:</p> <p>IGP:</p> <ul style="list-style-type: none">• OSPFv3.• ISIS.• Para Cisco EIGRP. <p>EGP:</p> <ul style="list-style-type: none">• MP-BGP: AF: IPv6,• SAFI: Unicast, Multicast y VPN.
	<p>BGP:</p> <p>Normalmente sesiones separadas para IPv4 e IPv6</p>
	<p>MPLS en la red del proveedor:</p> <ul style="list-style-type: none">• 6PE: Utiliza IPv6 sobre MPLS, reutiliza sesiones BGP existentes con próximo salto IPv4 del PE de salida.• 6VPE: Similar a 6PE pero permite el soporte de L3VPN
	<p>Ruta estática:</p> <p>Al igual que en el enrutamiento en IPv4 las rutas estáticas se configuran de manera similar en los equipos Cisco para IPv6, primero se declara que la ruta es estática, luego se declara la dirección de destino y luego la dirección o interfaz por la que saldrá el paquete.</p>

3.2.1.7. SERVICIOS

Los servicios son el centro de la implementación por lo que es un punto crítico.

En la tabla III.VI, se expone los servicios que encontramos en una red:

Tabla III. VI Servicios presentes en una red. Fuente (autores).

SERVICIOS	
Servicios externos:	Ejemplos: mail, web, Dns, jabber, ftp, VoIP, etc.
Servicios internos:	Ejemplo: servicio de DHCP, web interna, jabber, etc.

3.2.1.8. CAPACITACIÓN

Parte de la inversión del proyecto IPv6 debe ser considerada en la capacitación del personal que brinda servicios de planificación, operación e ingeniería, call center, técnicos de campo entre otros.

No es fácil conseguir ofertas de capacitación una opción es pensar en re-usar experiencias adquiridas.

3.2.3. IMPLEMENTACIÓN

La idea en el plan de implementación es llegar desde el estado actual de la red hacia el objetivo planteado.

Como siempre hay que tener cuidado en que no haya interrupciones y cortes de servicio.

Este es el punto final en la planificación, si se presentan problemas en esta etapa, estos debe ser abordada de modo profundo pues una mala implementación conllevaría a un mal servicio y vulnerabilidades en la infraestructura.

3.3. ESCENARIOS DE ANÁLISIS PARA LA INTRODUCCIÓN DE IPv6 EN LA RED DE UN ISP (RFC 4029)

Este documento no está destinado a cubrir a pequeños ISP's o empresas que proveen servicios de alojamiento o centro de datos. Su orientación es a escenarios en los cuales el ISP puede optar por lo menos de un prefijo de asignación /32 por parte de cualquier RIR.

Los escenarios que se muestran son las más probables que se presentan en un proveedor de internet que está pensando en ofrecer IPv6 a sus clientes de manera eficiente y viable.

Tenga en cuenta que en todos los escenarios excepto el primero, el ISP puede ofrecer a sus clientes un servicio tanto IPv4 como IPv6.

Los escenarios son las siguientes:

- Escenario 1 Lanzamiento
- Escenario 2 Backbone
- Escenario 3 Conexión al cliente
- Escenario 4 Completamente IPv6

Después de situarse en el escenario que más se ajuste a la realidad actual del ISP se presentan un modelo de transición a seguir por dicho RFC.

3.3.1. ESCENARIOS

3.2.1.1. LANZAMIENTO

En la actualidad este es el caso más común de todos los ISP's ya que sus servicios los brindan bajo el protocolo IPv4, entonces a partir de esta etapa empieza a someterse a un proceso de transición hacia el nuevo protocolo.

El paso inmediato entonces es obtener la asignación de un prefijo por parte de un RIR (AFRINIC, APNIC, ARIN, LACNIC, RIPE) normalmente un /32 de IPv6. Además necesitara buscar alternativas para establecer conectividad IPv6 con sus proveedores de nivel superior y vecinos a los que actualmente están conectados.

3.2.1.2. BACKBONE

En este escenario el ISP tiene la posibilidad de que su Backbone soporte IPv6 a través de actualizaciones de tipo software, hardware o una combinación de los dos, pero actualmente solo presenta conectividad con IPv4.

En este punto las conexiones de los clientes no han sido actualizadas al nuevo protocolo por lo que el cpe del cliente crea un túnel (si es que dicho dispositivo soporta el mecanismo) para conectarse a la red IPv6.

3.2.1.3. CONEXIÓN AL CLIENTE

Este escenario consiste en un ISP con un Backbone IPv4 sin la posibilidad de soporte IPv6 pero el cliente requiere esta conectividad, podemos ver que este caso es más complicado que el anterior ya que el Backbone no es compatible con el nuevo protocolo, pero la solución podría ser transportar el tráfico generado por el cliente ya sea por un túnel o una red IPv6 superpuesta separada del Backbone IPv4.

3.2.1.4. COMPLETAMENTE IPv6

Esta etapa consiste en un proveedor con servicio Dual IPv6/IPv4, desde el Backbone hasta cliente. Desde la perspectiva del cliente este escenario ofrece una transición transparente, ya que el servicio no ha sufrido ningún tipo de degradación y tampoco la conexión de red ha cambiado.

3.3.2. TRANSICIÓN

Teniendo en cuenta los diferentes escenarios, a continuación se presenta una metodología de transición en donde la etapa inicial es un servicio solo IPv4, concluyendo con un servicio dual IPv4/IPv6 en toda la red.

Luego del análisis es posible dividir el trabajo en un conjunto de pequeñas acciones, cada cual es en gran parte independiente de las demás, las medidas necesarias que se muestran son:

- Transición en el Backbone
- Transición en la conexión del cliente
- Transición en la red y en los servicios

3.2.2.1. TRANSICIÓN EN EL BACKBONE

En el Backbone la cantidad de equipos presentes es menor que en otras partes de la red, por lo que es conveniente que cualquier parámetro IPv6 a implementar debe ser manualmente.

Las principales configuraciones en este punto son protocolo de enrutamiento, direcciones de interfaz, las direcciones loop-back, listas de control de acceso, etc.

En lo que respecta al enrutamiento es similar a lo que el protocolo IPv4 utiliza como **IGP** tenemos la opción de OSPFv2 o IS-IS, además por general los proveedores de servicios no utilizan RIPv2.

Para el enrutamiento externo o **EGP** tenemos BGP así como las rutas estáticas pueden ser usadas internamente como externamente.

3.2.2.2. TRANSICIÓN EN LA CONEXIÓN DEL CLIENTE

Se puede pensar en este punto como primera opción conectar a los clientes mediante túneles considerando que este puede terminar en el CPE o en alguna otra parte de la infraestructura del cliente (por ejemplo un CPE ipv6 o incluso un host).

Como se ha detallado en el capítulo II sección 2.2.4 (mecanismos de transición) existe varias tecnologías para crear túneles de donde debemos tomar en cuenta que 6to4 e ISATAP son incompatibles con NAT y encapsulación UDP para más detalle de los mecanismos de transición revisar tabla II.II resumen de técnicas de túneles.

3.2.2.3. TRANSICIÓN EN LA RED Y EN LOS SERVICIOS

Las acciones a realizar en este punto son de gestión de configuración y monitoreo, además de soporte ipv6 en los servicios.

A continuación se presenta dicho proceso en la red y en los servicios:

- Configurar la conectividad IPv6 con los proveedores de nivel superior y peers¹².
- Configuración y actualizaciones iniciales de dispositivos de red IPv6.
- Gestión de la red IPv6:
 - Control IPv6
 - Gestión de clientes IPv6
 - Red IPv6 y seguridad operación de servicio

Algunos de estos ítems requerirán disponibilidad IPv6 nativa por ejemplo aquellas funciones de monitoreo que usen ICMPv6 requieren solo transporte IPv6.

En muchas plataformas de gestión la incapacidad para analizar el tráfico por separado de las interfaces que corren en DUAL STACK causan problemas en la gestión sobre todo bajo el protocolo SNMP.

En la tabla III.VI, nombraremos algunas herramientas más usadas en el ambiente de los NOC.

¹² **Peer:** Red aledaña a la cual se conecta otra red

Tabla III. VII Herramientas de monitorización para IPv6. Fuente: (Autores).

	PRTG	MRTG	CACTI	HP OPENVIEW	ARGUS	NAGIOS	SMOKEPING	ATHTEK NETWALK
GRATUITO	V.B si, V.F no	Si	Si	No	Si	Si	Si	V.B,V.F
S.O QUE SOPORTA	Windows /Linux/Mac OS/	Windows /Linux	Windows /Linux	Windows /Linux/Mac OS	Mac OS X, Linux, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, IRIX, Windows (under Cygwin) and OpenWrt	Linux	Windows /Linux/Mac OS/BSD/Solaris	Windows /Linux/Mac OS
NUMERO DE SENSORES	V.B=10 V.F=Sin limite		Ilimitado	Ilimitado	Ilimitado	Ilimitado	Ilimitado	Ilimitado
PROTOCOLOS QUE USA PARA GESTIÓN	SNMP,WMI	SNMP /Scripts creado por el usuario		SNMP/Scripts creado por el usuario	SNMP	SNMP/Scripts creado por el usuario	SNMP	SNMP
TAREAS QUE REALIZA	Sniffing, disponibilidad ,Rendimiento, AB	G.F, Configuración, Incidencias, Rendimiento, Seguridad, AB	Monitoreo del tráfico y consumo de red	M.f.L, P.T, E.P.C, C.E SNMP (traps), R.M de R.S y posee I.A, para, E.M	Aplicaciones TCP + UDP, conectividad IP, OID SNMP, programas, B.D	SMTP, POP3, HTTP, SNMP		Sniffing
ALARMAS	A través de mail, SMS		No	A través de mail	SMS	A través de mail, SMS		A través de mail, SMS

Versión básica = V.B

Versión full=V.F

Gestión de fallos=G.F

Ancho de banda=A.B

Gestión de fallos=P.T

Capturar eventos=C.E

Recolectar métricas=R.M

Rendimiento de sistema= R.S

Envío de Mensajes=E.M

Monitoreo de ficheros de log=M.f.L

Interfaces Abiertas=I.A

Ejecutar programas de control=E.P.C

Bases de Datos=B.D

3.4. IPv6 EN 3 PASOS

La metodología que se presenta a continuación simplifica el proceso de transición en un ISP por lo que se pretende sea de fácil comprensión, teniendo en cuenta un conocimiento previo a la parte teórica del nuevo protocolo.

Este proceso está bajo el desarrollo del Portal de Transición a IPv6 de América Latina y el Caribe, en el que menciona que antes de que el ISP pueda pensar en dar servicio IPv6, será necesario que obtenga direcciones IPv6 del RIR regional, para el caso de América Latina y el Caribe será a través de LACNIC, Portal IPv6 (25).

Puede ser que el ISP sea de tipo sectorial para servicios Home por lo que deberá adquirir conectividad IPv6 a su Upstream provider¹³ para empezar el trabajo de soporte del nuevo protocolo en su red.

Luego de haber obtenido las direcciones IPv6, el ISP podrá pensar en proveer el servicio en tres pasos.

- 1) Publicar las direcciones obtenidas en Internet
- 2) Despliegue en el Backbone del ISP.
- 3) IPv6 en el usuario final.

3.4.1. PUBLICAR LAS DIRECCIONES OBTENIDAS EN INTERNET

Una vez adquirido el prefijo de red ya sea por LACNIC o por el proveedor de nivel superior o carrier es necesario publicar las direcciones obtenidas por lo que las opciones que se muestran a continuación son las más probables que se presentan al anunciar una red IPv6.

Modo nativo.- Es necesario que el Upstream provider tenga IPv6 implementado para anunciar sus direcciones IPv6 y este a su vez distribuya la red adquirida en su infraestructura.

¹³ **Upstream Provider:** Por lo general es un gran ISP que proporciona acceso a Internet a un ISP local. Por lo tanto, la palabra Upstream provider también se refiere a la conexión de datos entre dos proveedores de servicios.

Modo tunelizado.- Deberán contactarse con un proveedor de nivel superior que sea capaz de terminar el túnel y tenga IPv6 nativo.

En la creación de túneles se debe tener en cuenta el soporte que se ofrece pues si se trata de un ISP la disponibilidad del servicio es muy importante.

3.4.2. DESPLIEGUE EN EL BACKBONE DEL ISP

El despliegue en el núcleo de un ISP está caracterizado por si en el transporte utiliza MPLS o no, las alternativas que se muestran son:

1. Si se tiene implementado MPLS la transición es sencilla, ya que solo bastaría implementar DualStack en los equipos de borde (PE) y luego habilitar el protocolo 6PE; de modo que los routers de core no necesitan ser modificados.

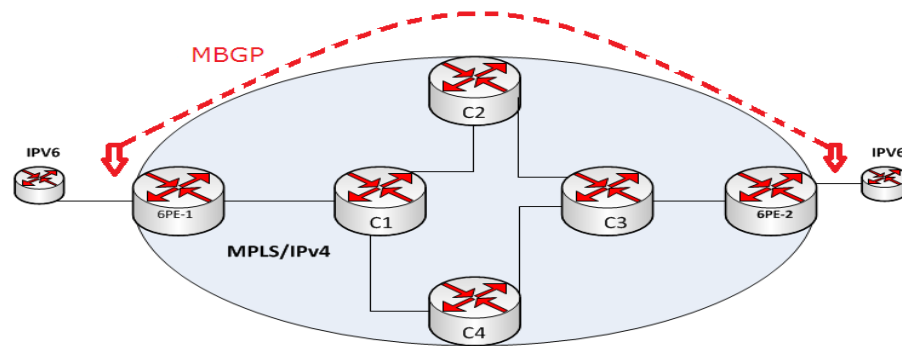


Figura III. 3 IPv6 sobre MPLS. Fuente: Herramientas de transición (ConsulIntel & 6Deploy, 2008)

2. Si el ISP no tiene implementado MPLS en su red, la opción más acertada será crear Dual Stack en todos los routers por los que pasará el tránsito IPv6.

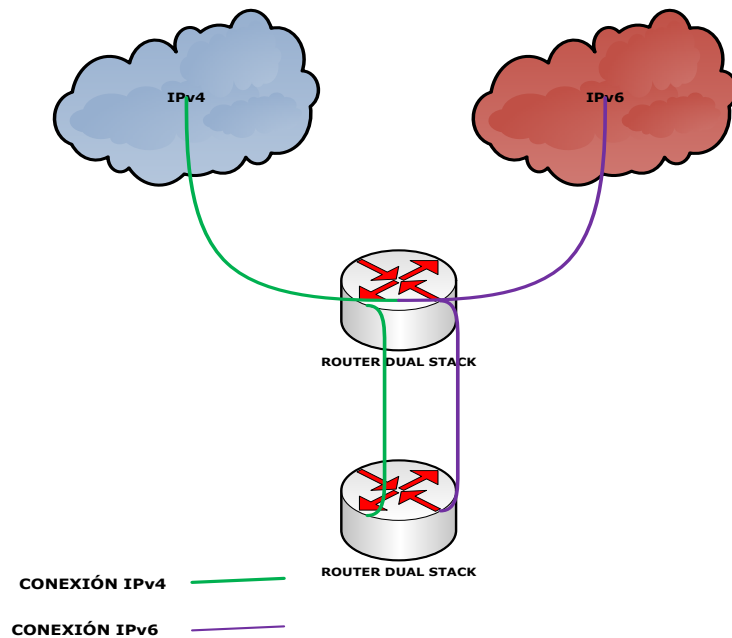


Figura III. 4 IPv6 en Dual Stack. Fuente: : Herramientas de transición (ConsulIntel & 6Deploy, 2008)

3.4.3. IPv6 EN EL USUARIO FINAL

Las opciones que se expone en este punto están destinadas a la implementación que un ISP podría realizar para ofrecer el servicio al usuario final, difiere de la sección expuesta de una red SOHO ya que allí se habla de lo que el cliente podría realizar para conectarse a la internet en versión 6.

A continuación se detallan en orden de preferencia tres alternativas.

1. Dual Stack: Es necesario que el CPE (equipo local del cliente) soporte tanto IPv4 como IPv6 para ser implementado.
2. Túneles manuales: No escala bien es decir no se sabe de antemano cuantos usuarios, servidores se añadirán, solo se justifica en los casos en que se trabaja con pocos clientes.
3. Túneles automáticos: 6to4 (si el cliente dispone de IPv4 pública) y Teredo/Miredo (en los casos en los que el cliente está detrás de un

NAT). En este caso se aconseja que el ISP despliegue Relés 6to4 y Teredo en su red para optimizar el tráfico.

Más allá de las consideraciones técnicas, hay otras cuestiones a tener en cuenta por un ISP, fundamentalmente en los aspectos económicos involucrados en una transición de este tipo.

El impacto que este hecho va a tener en los distintos sectores no va a ser igual: mientras que un usuario doméstico posiblemente obtenga una actualización gratuita del firmware de su router (CPE), que le permita conectar con su ISP con IPv6 habilitado, en las corporaciones más grandes (administraciones públicas, y medianas y grandes empresas) el acceder mediante IPv6 a la nueva Internet, supondrá un esfuerzo bastante más grande. Esfuerzo en horas de trabajo, esfuerzo de formación, y esfuerzo económico en forma de inversión en nuevo equipamiento.

Las siguientes consideraciones económicas son los más relevantes en la implementación de IPv6 en un ISP:

- Capacitación de personal.
- Compra de quipos.
- Costos de implementación del mecanismo de transición que más se ajuste a las necesidades del ISP.
- Posibles asesorías.

3.5.MODELO SISTEMÁTICO DE MIGRACIÓN HACIA EL PROTOCOLO IPv6

Tendiendo como preámbulo las políticas emitidas en torno a IPv6 en las que el MINTEL y la sociedad de la información realizan acciones regulatorias y administrativas para que los ISP's y portadores de telecomunicaciones admitan en sus redes y plataformas el curso normal de IPv6 en coexistencia con IPv4, se presenta una propuesta metodológica de migración para el ISP FASTNET basada en las recomendaciones analizadas en este capítulo.

Previamente se presenta ciertas consideraciones a tomar en cuenta para el despliegue IPv6 en un ISP.

El transporte de IPv6, se da en 2 categorías:

- IPv6 Público (Transporte a Internet)
- IPv6 Privado (Transporte dentro del ISP)

Las principales técnicas de transporte en ISP:

- IPv6 Nativo
- Túneles en IPv4
- Dual Stack
- MPLS

En la tabla III.VIII, se detallan aspectos importantes de las técnicas de migración en las que exponemos las implicaciones que trae cada método.

Tabla III. VIII Técnicas de migración para un ISP. Fuente (autores).

MÉTODO	DESCRIPCIÓN	OBSERVACIÓN
IPv6 NATIVO	Habilitar el forwarding de paquetes IPv6 en todos los routers de la red con lo cual todos los paquetes serían IPv6 nativos.	No todos los equipos que el proveedor disponga en su red podrían soportar IPv6.
TUNELES IPv4	Crear túneles (ej. 6TO4) entre bordes, así los paquetes IPv6 pueden ser encapsulados en IPv4, eliminando la necesidad de habilitar IPv6 en el CORE de la red.	Implica configuración manual de los túneles y overhead en los paquetes. El troubleshooting puede resultar complejo. Dependiendo de la topología del servicio, podría requerir full-mesh de túneles.
DUAL STACK	Ambos protocolos están corriendo en paralelo en toda la red	La gestión y administración implica una para IPv4 y otra para IPv6
IPv6 SOBRE MPLS	Utilizar LSPs MPLS IPv4 entre los routers PE de la red para el transporte de paquetes IPv6. Técnicas principales: <ul style="list-style-type: none">• 6PE (IPv6 Provider Edge).• 6VPE (IPv6 VPN Provider Edge)	Opción más atractiva para los proveedores que ya disponen MPLS en su red; los LSPs existentes y establecidos para el transporte de paquetes IPv4 pueden ser utilizados para IPv6, solución más escalable.

		La mayoría de ISP utilizan MPLS como transporte, MPLS no requiere conocer el payload.
--	--	---------------------------------------------------------------------------------------

Las fases de implementación podrían ser más cortas o más extensas dependiendo de la arquitectura de red, los objetivos de la empresa y el crecimiento de la red.

A continuación se presenta el desarrollo de una propuesta técnica de migración orientada hacia las necesidades del ISP FASTNET.

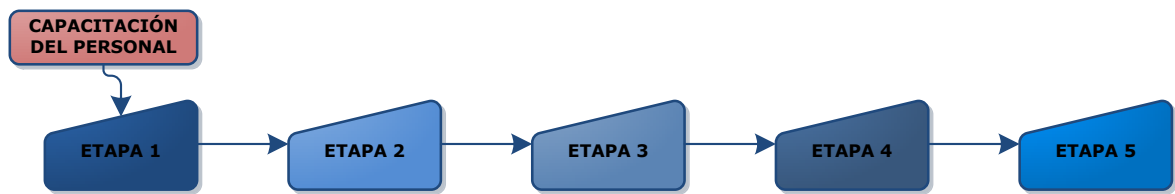


Figura III. 5 Etapas de desarrollo para la migración. Fuente (Autores).

ETAPA 1 - TODO IPv4

Todo el tráfico es IPv4 por lo que es necesario una evaluación de los equipos para ser actualizados o definitivamente cambiados, además con ello nos ubicaremos en qué escenario nos encontramos de acuerdo a la metodología en la sección 3.3.

Se establece el impacto que va a tener en la plataforma el nuevo protocolo y se determina el alcance del proyecto de implementación.

Se debe analizar las propuestas de los proveedores y del mercado para compras de HW y SW con soporte IPv6, además tomar en cuenta posible ayuda de los gobiernos, en el caso ecuatoriano se plantea un marco referencial para adquirir equipos de red con homologación IPv6 , esto nos llevaría a la generación de un propuesta económica para el despliegue.

Finalmente en este punto es necesario que el personal de gestión de la red esté capacitado en IPv6 para garantizar el manejo adecuado de la nueva tecnología y las implementaciones que se aproximan.

ETAPA 2 - TÚNELES IPv6 PARA PRUEBAS Y PARA CLIENTES OBJETIVO

Un túnel IPv6 sobre IPv4 es el primer paso para llegar a los usuarios finales, esto se hace como parte de una prueba por tiempo limitado que luego puede convertirse en un despliegue de IPv6 como una oferta de servicio.

Estos ensayos IPv6 son una parte importante para obtener experiencia en la construcción de redes que operan en IPv6 en el caso de FASTNET se tiene un segmento de red para pruebas conectada al equipo de core simulando la capa de distribución, acceso y cliente.

Se detalla a continuación dicho segmento:

Conexión directa desde el core de Fastnet (RB1100AHX2), en la distribución un router mikrotik con una antena UBNT en puente para irradiar la señal, en el acceso tenemos router SXT 5HnD para escaneo de la señal, y como cpe un router cisco linkys E1200

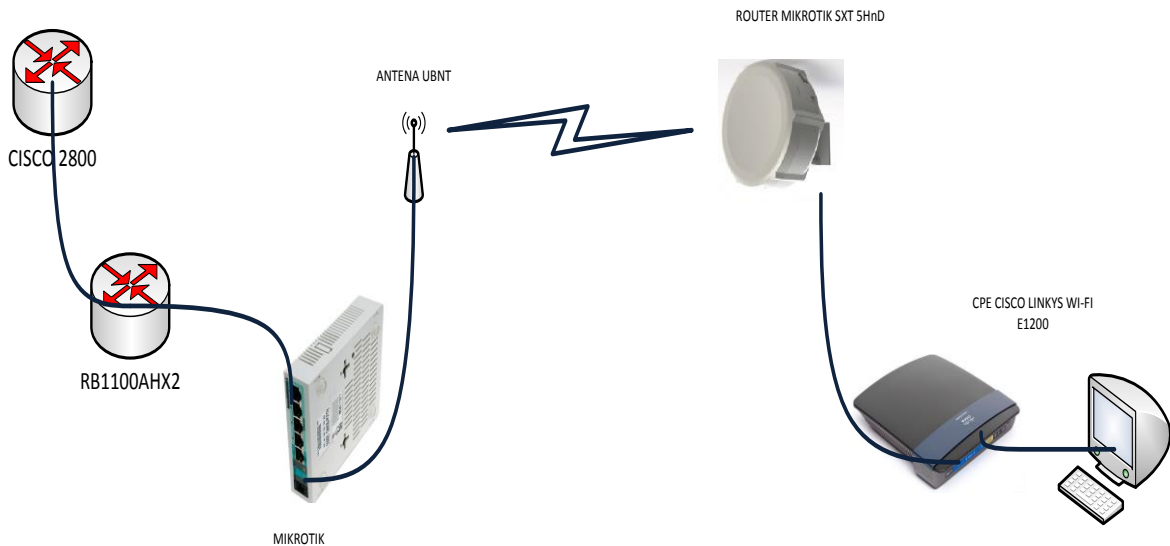


Figura III. 6 Segmento de red de pruebas en el ISP FASTNET. Fuente (autores).

ETAPA 3 - IMPLEMENTACIÓN DEL NÚCLEO DUAL STACK

Es la instancia con mayor aceptación al ser una solución inminente y accesible pero el inconveniente de mantener doble pila sobre una infraestructura es similar a tener dos redes

diferentes con la implicación de doble trabajo en cuestiones de planificación, soporte y troubleshooting.

Esta tecnología se mantendrá por un largo periodo ya que la transición debe ser gradual, en sus inicios el porcentaje de tráfico en IPv6 será pequeño en comparación con el IPv4 por lo que estos protocolo continuaran en convivencia.

La estrategia de migración en doble pila que se propone, es la transición desde el núcleo hacia la periferia.

Por lo que se ha considerado lo siguiente:

- Dual Stack sobre los routers de core
- Luego dual Stack en los equipos de distribución
- Después Dual Stack en los servidores y firewalls
- Finalmente Dual Stack en los routers de acceso

Se realiza un plan de direccionamiento y conmutación con el nuevo protocolo además los servicios serán duales, mientras el operador reduce significativamente el uso de IPv4 y obtiene una red que está listo para el futuro.

Para la elaboración del plan de direccionamiento se debe tener en cuenta las diversas subredes existentes dispuestas a desplegar IPv6 a medio o largo plazo, el objetivo es tratar de garantizar que no se requerirá modificar el plan de direccionamiento en el futuro, cuando se necesite IPv6 en la red de forma masiva.

Finalmente se planteara una opción de gestión de la red con soporte ipv6 o ipv4/ipv6.

ETAPA 4 - PROPORCIONAR CONECTIVIDAD IPv6 A LOS CLIENTES EXISTENTES

Se asigna direcciones a los dispositivos de la red dentro de la infraestructura, así como a los clientes.

Si los cpe de los cliente no soportan el nuevo protocolo en primera instancia debemos tratar de actualizar su firmware, caso contrario cambiarlos pensando en crear una red exclusivamente IPv6.

Los túneles no son una opción escalable, por su alto consumo de recursos de red, por lo que se trata de reducir al máximo la utilización de los mismos.

ETAPA 5 - EXPANDIR IPv6 A TRAVÉS DE LA RED

En LACNIC se estima que las direcciones ipv4 públicas se terminaran el **19-04-2015** a partir de este momento cada vez más redes serán IPv6 a medida que más clientes (dispositivos) se agreguen o se actualizan.

Esta es la etapa final de implementación en donde se tiene soporte IPv6 en todos los puntos de presencia de la red del ISP para lo cual las interfaces que corren en DUAL STACK progresivamente se apagarán aquellas en IPv4.

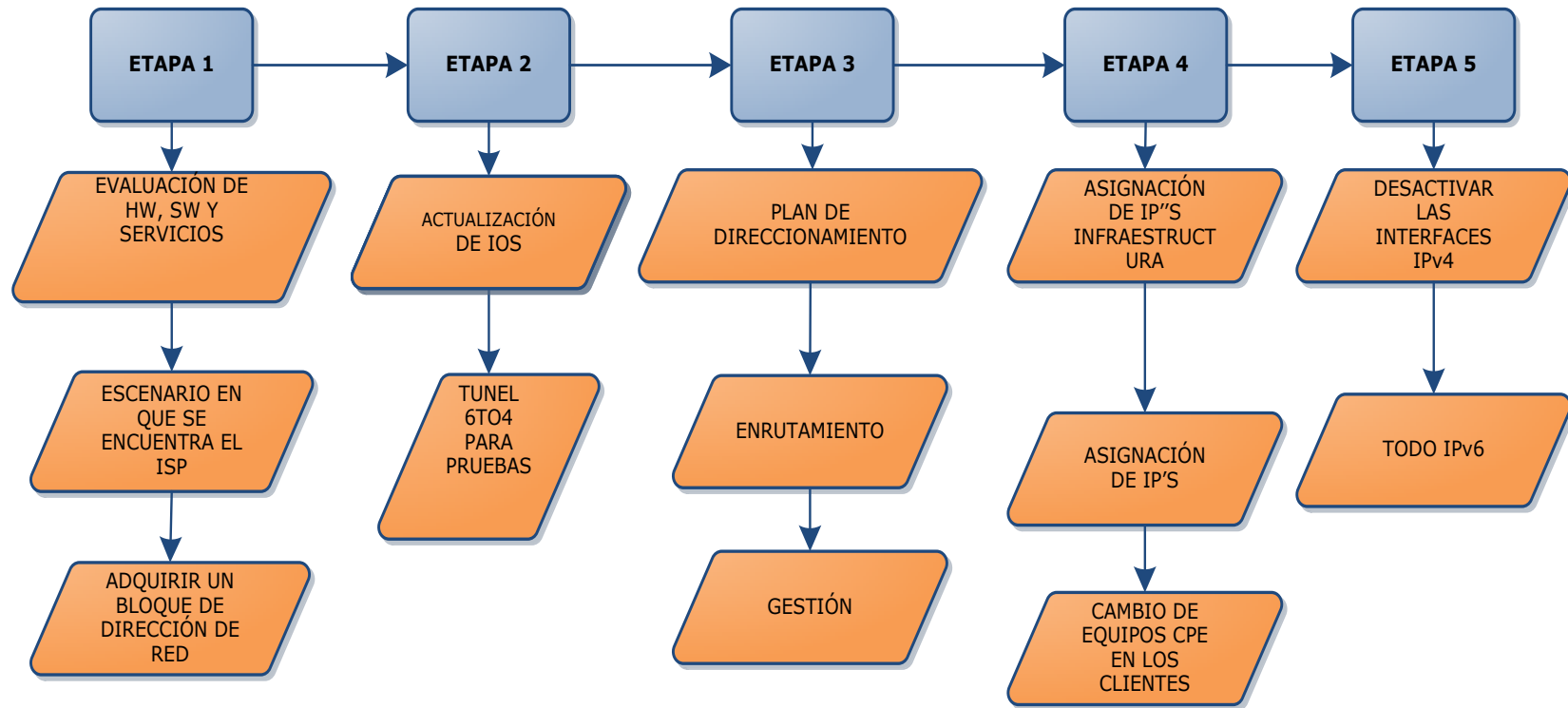


Figura III. 7 Modelo sistemático de transición para el ISP FASTNET

CAPÍTULO IV

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA PROVEEDORA DE INTERNET FASTNET CIA. LTDA.

En este capítulo describiremos el estado actual de los equipos y la red con lo cual definiremos el alcance del proyecto dependiendo del tamaño del ISP, adicionalmente nos permitirá revisar el soporte de los diferentes equipos y software, para luego advertir si es necesario adquirir otros equipos, con lo que finalmente este análisis nos ayudará en lo posterior en la creación de un presupuesto de implementación y en donde empezar la transición.

Fastnet es un proveedor de servicios de internet con una cobertura principal en toda la provincia de Chimborazo, usando tecnología inalámbrica para el acceso del cliente.

Utiliza varias tecnologías en su red como cisco, mikrotik, 3com, D-Link y Ubiquiti networks.

A continuación se detalla los aspectos necesarios para conocer el estado actual de la empresa proveedora de internet podemos observar los siguientes aspectos:

- IPv6 en Mikrotik
- Arquitectura
- Enlace principal
- Estructura de la red de core
- Estructura de la red de distribución
- Estructura de la red de acceso
- Servicios
- Centro de operaciones de la red

4.1.IPv6 EN MIKROTIK

En la tabla IV.I, presentamos las características que la tecnología mikrotik mantiene en cuanto al soporte del protocolo ipv6:

Tabla IV. I Soporte IPv6 por parte de Mikrotik. Fuente (autores).

Soporte IPv6	
DHCPv6	Servidor DHCP para delegación de prefijo de red
DHCPv6 cliente	
Delegación de prefijo IPv6 a través de interfaces PPP.	
Direccionamiento estático y enrutamiento estático.	
Radvd	Para configuración automática de direcciones
Enrutamiento dinámico: BGP +, OSPFv3 y protocolos RIPng;	
Firewall	Filter, mangle, listas de direcciones, tabla de conexión, queue (control de ancho de banda)
DNS	
Túneles 6in4	Creación de una interfaz para túnel
Túnel broker	Túnel bróker a través de Hurricane electric

EoIPv6, ip/ipv6 sobre ipv6 (IPIPv6)	
IPSEC	
VRRPv3;	
GRE6	
Servicios Adicionales	
SSH, Telnet, FTP, Win box	
Ping	
Trace route	
web proxy	
sniffer	
bandwidth test	

4.2.ARQUITECTURA

Se describe el modelo de red de Fastnet, presentando aquellos detalles permitido por la parte de la empresa.

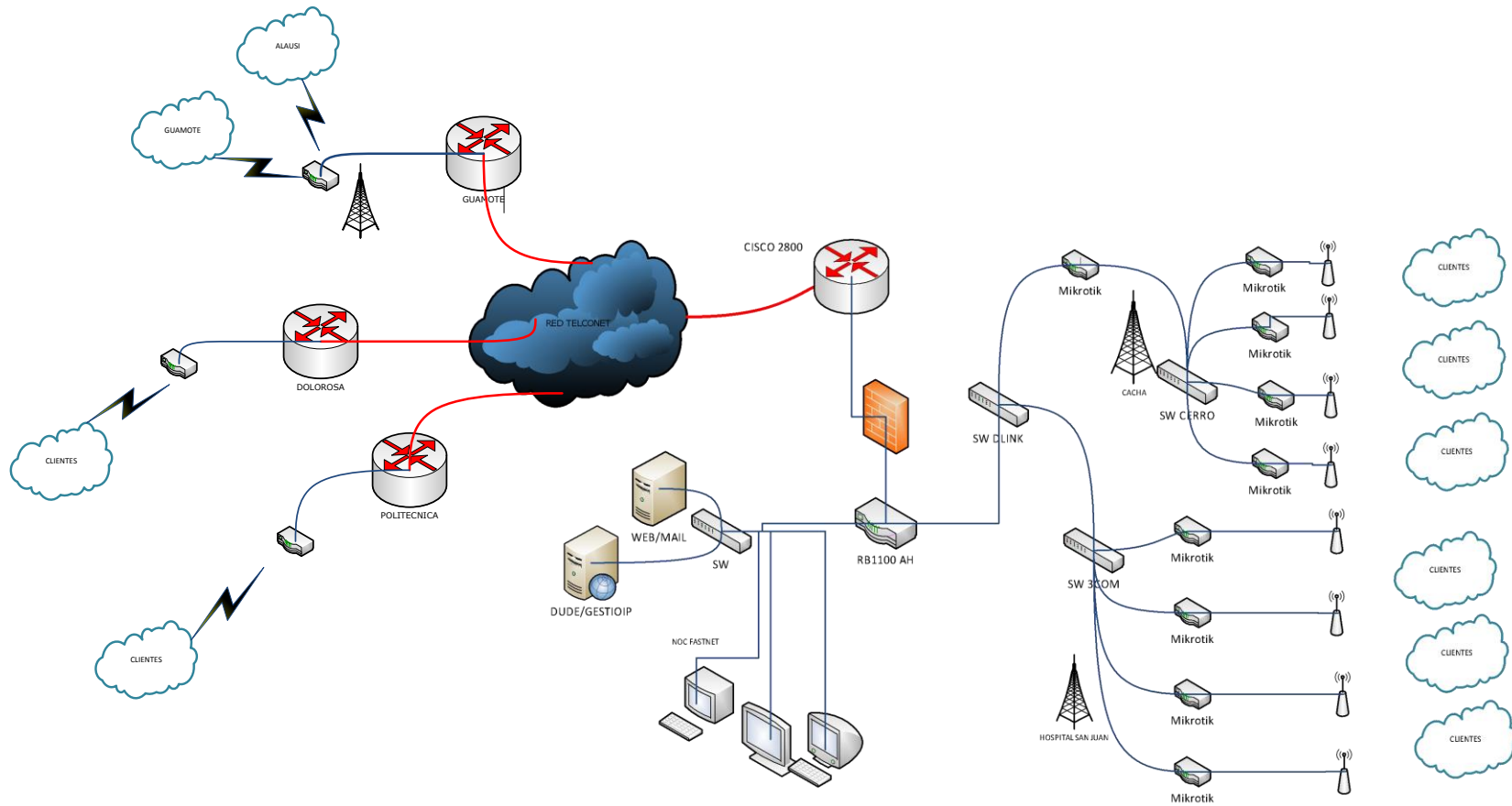


Figura IV. 1 Arquitectura de la red Fastnet. Fuente: (Autores)

4.3.ENLACE PRINCIPAL

Fastnet utiliza la Metro Ethernet del Carrier Telconet basada en fibra óptica y MPLS para transporte del tráfico de los clientes hacia el internet.

Posee un enlace simétrico de fibra óptica Nodo principal Chimborazo-Quito-USA aproximadamente de 71 Mbps de velocidad en Downstream y Upstream.

4.4.ESTRUCTURA DE LA RED DE CORE

La red troncal de Fastnet está conformada por routers Cisco serie 2800 como enlaces hacia el Carrier Telconet y por lo general un router Mikrotik, exclusivamente para la conmutación entre hacia el internet. En la figura IV. 2 se muestra la red de core con más detalle:

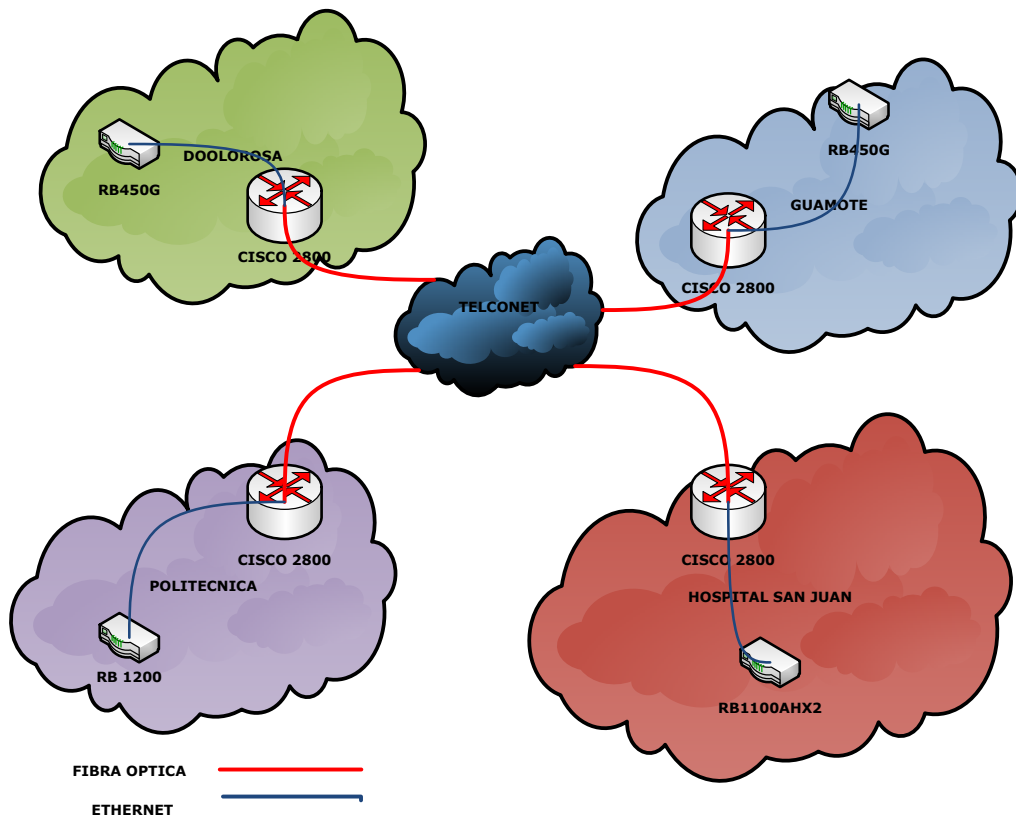


Figura IV. 2 Red de Core

El nodo del Hospital San Juan posee un router mikrotik RB1100AHX2. En la figura IV. 3 se observa las conexiones, pues este es un nodo principal con la mayor cantidad de usuarios.

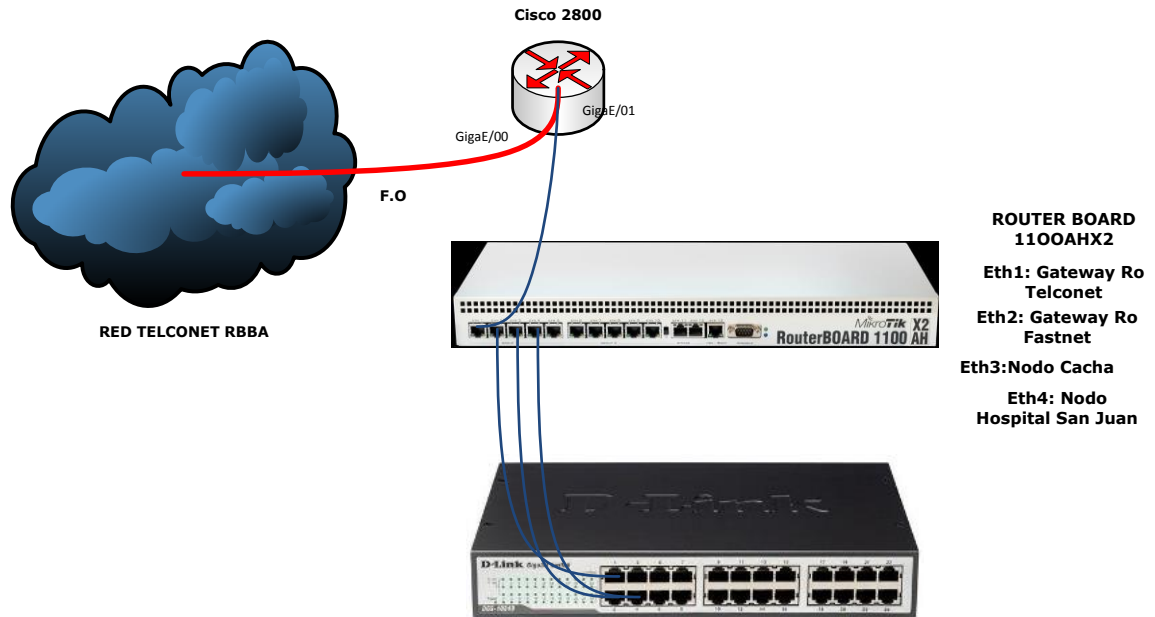


Figura IV. 3 Núcleo de la red. Fuente: (Autores)

En los nodos Dolorosa, Politécnica y Guamote es similar la conexión ya que un router cisco de la serie 2800 por parte de Telconet se conecta con un Mikrotik de Fastnet.

En la tabla IV.II se detalla el soporte del protocolo IPv6 en el core:

Tabla IV. II Soporte de equipos en el núcleo. Fuente (Autores).

EQUIPO	MODELO	SOPORTE IPV6	DUAL STACK
ROUTER	RB1100AHX2	SI	SI
ROUTER	CISCO 2800	SI	SI
SWITCH CAPA 3	D-LINK	--	--
SWITCH CAPA 3	3-COM	--	--
ROUTER	RB450G	SI	SI
ROUTER	RB1200	SI	SI

4.5. ESTRUCTURA DE LA RED DE DISTRIBUCIÓN

La tecnología utilizada para los enlaces es aquella que maneja los Sistemas MDBA utilizando las frecuencias 2,4 GHz y 5,8 GHz.

Los nodos de cobertura principal son:

- Terraza del hospital San Juan
- Cerro Cacha
- Politécnica
- Dolorosa
- Guamote

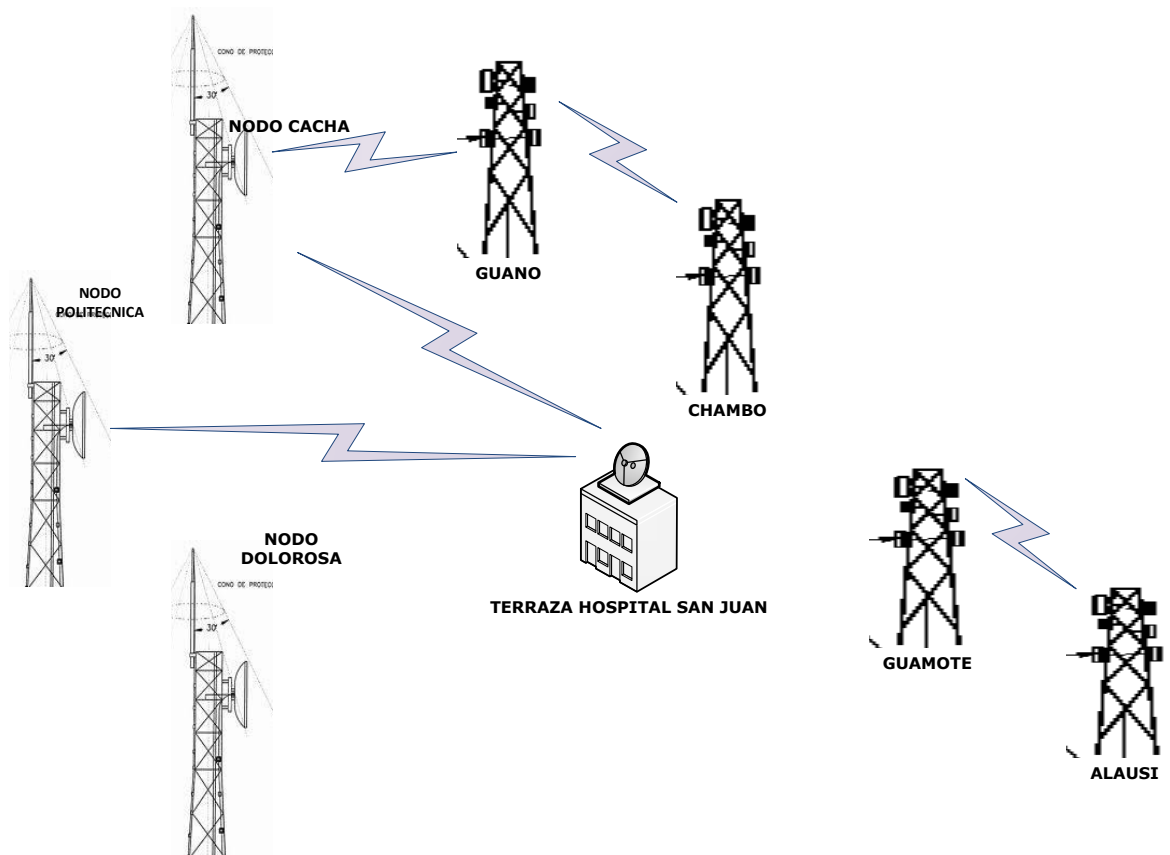


Figura IV. 4 Cobertura de Fastnet. Fuente: (Autores)

Como se puede observar en la figura IV.4, los nodos CACHA, HOSPITAL SAN JUAN y GUAMOTE generan otros nodos secundarios para expandir la cobertura por la provincia de Chimborazo cubriendo Riobamba, Guano, Chambo, Guamote y Alausí.

Sobre estos nodos se realiza la gestión de los usuarios es decir registro de mac's de equipos de acceso, asignación de ip's, control de ancho de banda, cola de espera (queue), nateo.

ANTENAS UBNT

Estos equipos están en modo puente pues la función de las antenas es la de irradiar la señal y generar las cobertura.

En la tabla IV.III, se mencionan las antenas usadas para la recepción y transmisión así como el soporte del protocolo IPv6:

Tabla IV. III Antenas UBNT en la red de distribución. Fuente (Autores).

MODELO	MODO DE OPERACIÓN	SOPORTE IPv6
ROCKET M	BRIDGE	NO
AIRGRID M (AIRMAX)	BRIDGE	NO
NANOBRIDGE M	BRIDGE	NO
ROCKET DISH	BRIDGE	NO

RUTEADORES MIKROTIK

Estos equipos generan la señal para ser irradiada en las antenas, adicionalmente aquí se realizan la gestión de los clientes, es decir configuración, control de desempeño, gestión de fallas y gestión de seguridad.

Tabla IV. IV Ruteadores presentes en la red de distribución . Fuente (Autores).

MODELO	SOPORTE IPv6	DUAL STACK
RB450G	SI	SI

RB1200	SI	SI
RB1100	SI	SI
RB411AH	SI	SI
RB751G-2HnD	SI	SI
RB1200	SI	SI
RB433AH	SI	SI
RB751G-2HnD	SI	SI

4.6. ESTRUCTURA DE LA RED DE ACCESO

La tecnología WI-FI es utilizada para acceder al servicio del ISP, tecnologías como Mikrotik SXT5HPnD y NanoStation son las opciones presentes en este punto de la red.

En la figura se puede observar el acceso del cliente a la infraestructura de ISP.

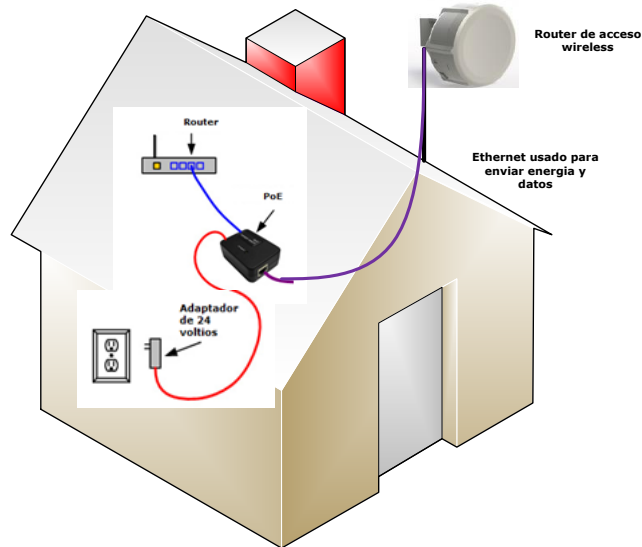


Figura IV. 5 Estructura de acceso en el cliente para acceder al ISP. Fuente: (Autores).

La red de acceso está formado por los equipos que se detallan en la tabla IV.V:

Tabla IV. V Equipos de acceso y soporte IPv6. Fuente (Autores).

MODELO	SOPORTE IPv6	DUAL STACK
MIKROTIK SXT5HPND	SI	SI
NANOSTATION M	NO	NO
AIRGRID M	NO	NO

En lo que respecta al número de usuarios presentes en la red de FASTNET, las estadísticas de la SUPERTEL nos muestran:

Tabla IV. VI Cantidad de cuentas en Fastnet. Fuente(<http://supertel.gob.ec>).

PERMISIO NARIO	COBERTU RA	ACTUALI ZADO	CUENTAS CONMUTA DAS	CUENTA S DEDICA DAS	CUENTA S TOTALES	USUARIO S CONMUT ADOS	USUARI OS DEDICA DOS	USUA RIOS TOTAL ES
FASTNET CIA. LTDA.	CHIMBOR AZO	30-JUN-13	0	184	184	0	1.126	1.126

Finalmente en lo que concierne a los router o equipos finales de cliente (CPE) podemos encontrarnos con los siguientes:

Tabla IV. VII Equipos CPE presentes en los usuarios. Fuente (Autor).

MODELO	SOPORTE IPv6
TP-LINK WR741ND	NO
QPCOM	NO
D-LINK	NO
CISCO LINKSYS E1200	SI

4.7.SERVICIOS

Fastnet tiene habilitado los servicios de WEB y MAIL, los cuales están configurados en un servidor con el S.O Centos.

Estos servicios están corriendo bajo el protocolo IPv4, el servidor web está basado en Apache y el servicio de mail en Postfix.

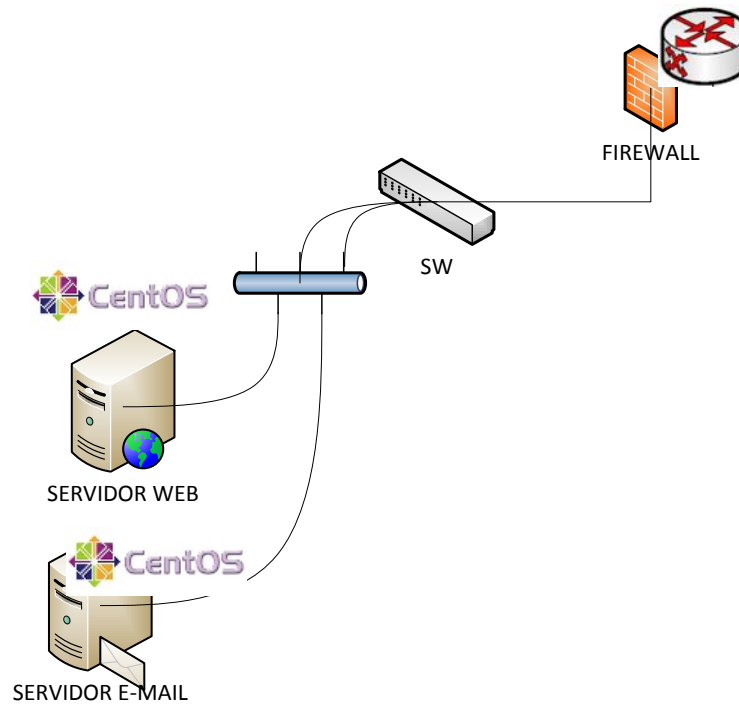


Figura IV. 6 Servicios alojados en Fastnet. Fuente (Autores).

Fastnet no tiene implementado un DNS en su infraestructura. Lo resuelve mediante los DNS del Carrier Telconet.

Tabla IV. VIII Dns FASTNET. Fuente (Autores)

DNS
200.93.216.2
200.93.216.5

En la tabla IV.IX, se puntualiza el soporte de los servidores en la DMZ de Fastnet:

Tabla IV. IX Soporte IPv6 en los servidores. Fuente (autores).

EQUIPO	SOPORTE IPv6	DUAL STACK
SERVIDOR WEB	SI	SI
SERVIDOR EMAIL	SI	SI

4.8. CENTRO DE OPERACIONES DE LA RED (NOC)

En el centro de operaciones se cumplen las siguientes actividades:

- Administración de la red,
- Gestión de fallos, gestión de configuración, gestión contable, gestión de rendimiento, gestión de seguridad y red
- Monitoreo de todos los host conectados a la infraestructura de Fastnet.

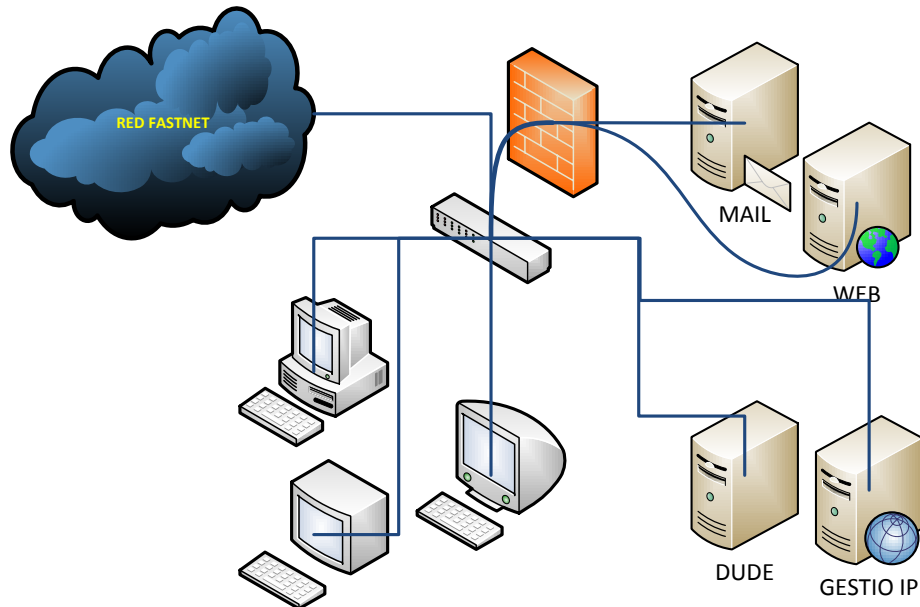


Figura IV. 7 Centro de Operaciones de Fastnet. Fuente (El autor).

En la plataforma DUDE se realiza la administración de los equipos Mikrotik, su entorno gráfico facilita el trabajo sobre toda la red, además posee una serie de herramientas para realizar diferentes acciones como: test de ancho de banda o conexión remota, ping, etc. Ver Figura IV. 8

CARACTERÍSTICAS FUNCIONALES:

- Dude puede detectar automáticamente una red local, y dibujar un esquema preliminar que después se podrá modificar, ajustar y guardar.
- Permite añadir objetos manualmente, personalizar los iconos y textos identificativos de cada elemento o dispositivo de la red, así como conectar nodos.
- Presenta herramientas básicas como test de ancho de banda o conexión remota, ping, traceroute, arp, logs e historiales, y avisos de cualquier evento que se produzca en la red, adicionalmente soporta SNMP.

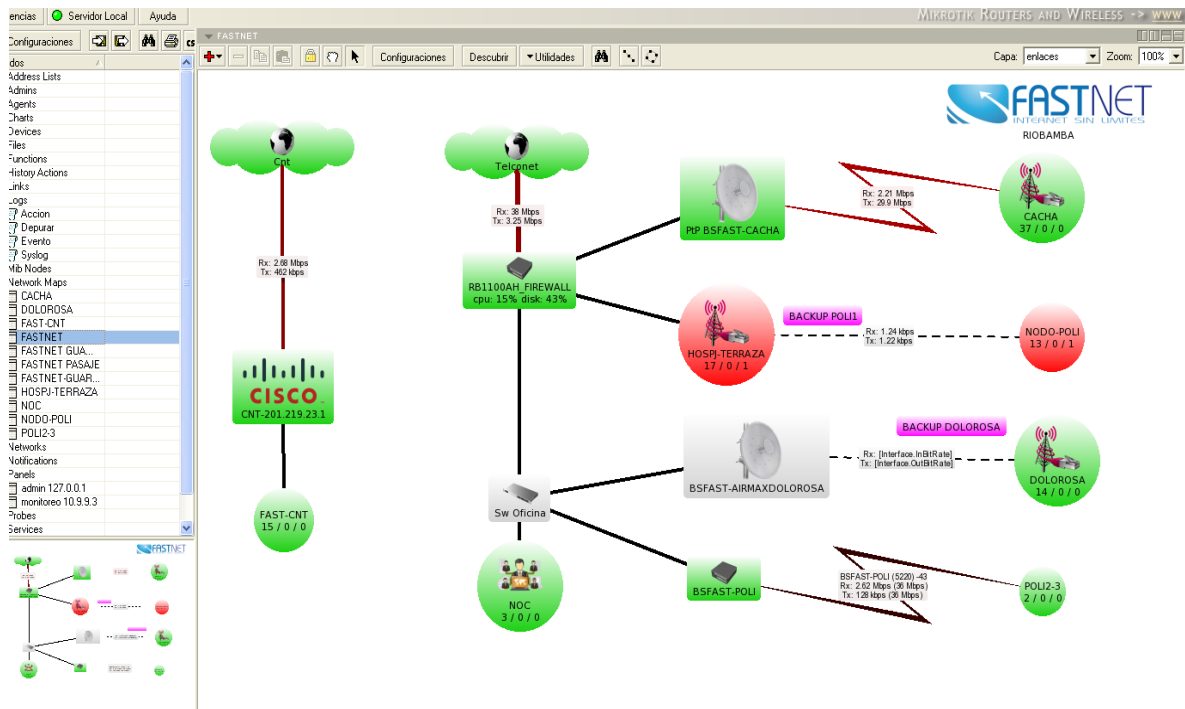


Figura IV. 8 Administración por DUDE (mikrotik.). Fuente: Noc Fastnet Cia. Ltda.

GestioIP es una herramienta para el registro de los clientes en el que se detalla dirección domiciliaria, Dirección IP asignada, nodo o equipo al cual se conecta cada usuario.

Tabla IV. X Soporte IPv6 en el Software. Fuente (autores).

HERRAMIENTA	SOPORTE IPv6
DUDE	PARCIAL
GESTIOIP	SI

CAPÍTULO V

APLICACIÓN/ PROCESO DE MIGRACIÓN

Las recomendaciones analizadas en la presente investigación permiten emitir criterios para realizar un proceso de migración hacia el nuevo protocolo de internet, lo cual consideramos que los aspectos económicos y técnicos son los que determinan el cumplimiento de los objetivos planteados para el despliegue.

En lo económico se requiere una inversión inicial para emprender el proyecto, ya sea para compras de equipos, capacitación del personal. Como veremos en el desarrollo técnico del proceso de migración, el pilar inicial es la capacitación del personal encargado de administrar la red del ISP, para continuar con el desarrollo técnico en donde el mecanismo DUAL STACK es el más apto considerando que la convivencia entre protocolos se dará por un periodo indeterminado. Cabe tomar en cuenta que esta técnica de transición es similar a tener dos redes en paralelo por lo que se necesitara el doble de recursos de procesamiento y generara más overhead¹⁴ en toda la red, pero se ha considerado como el modelo más adecuado según el

¹⁴ **Overhead**: Es el desperdicio de ancho de banda, causado por la información adicional (de control, de secuencia, etc.) que debe viajar además de los datos, en los paquetes de un medio de comunicación. El overhead afecta al Throughput (cantidad de datos por unidad de tiempo que se entregan, mediante de un medio físico o lógico, en un nodo de la red), de una conexión.

análisis del estado actual de la implantación de IPv6 en el Ecuador en el que se dice: “Los operadores señalan que este mecanismo permite que la implementación de IPv6 se lo realice de forma paulatina, consiguiendo que sus clientes se adapten de a poco con el nuevo protocolo” Silva(16) .

5.1. ETAPA 1 TODO IPv4

5.1.1. EVALUACIÓN DE EQUIPOS

La evaluación de los equipos se realizó tomando como parámetro el protocolo que admite, en este caso la cuantificación de valoración fue IPv6.

A continuación presentamos los resultados obtenidos del capítulo III análisis de la situación actual de la empresa proveedora de internet FASTNET Cia. Ltda.

CORE

La cantidad de equipos presentes en esta parte de la red es menor que en otros puntos, podemos ver en la figura V.1, que el soporte de ipv6 se da en 100%, en todos los equipos tanto cisco como mikrotik y el mecanismo DUAL STACK puede ser implementado, los SWITCH no soportan IPv6 pero no intervienen en configuraciones del nuevo protocolo.

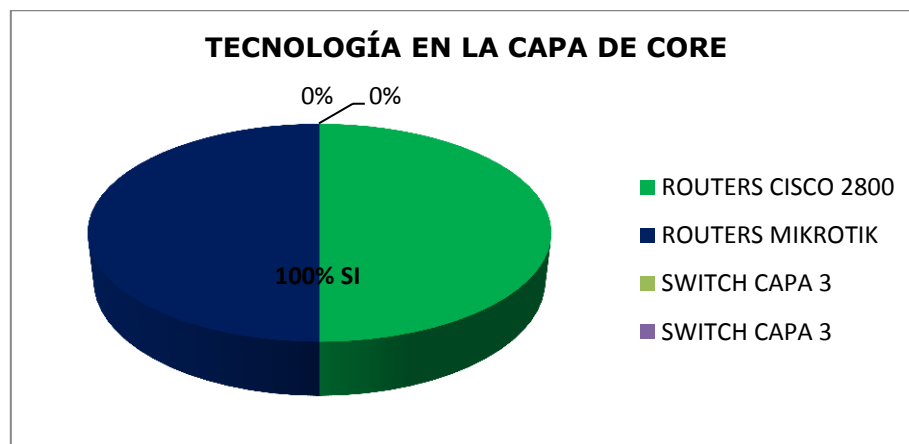


Figura V. 1 Presencia del protocolo IPv6 en los equipos de la capa de acceso. Fuente: (autores).

DISTRIBUCIÓN

En este sitio la presencia de equipos de tipo mikrotik es casi total, por lo que las actualizaciones IPv6 se pueden dar sin ningún inconveniente.

En la figura V.2 el 35% de las antenas UBNT no soportan IPv6 en su IOS pero éstas se encuentran en modo bridge (puente) por lo que no eliminan los paquetes IPv6.

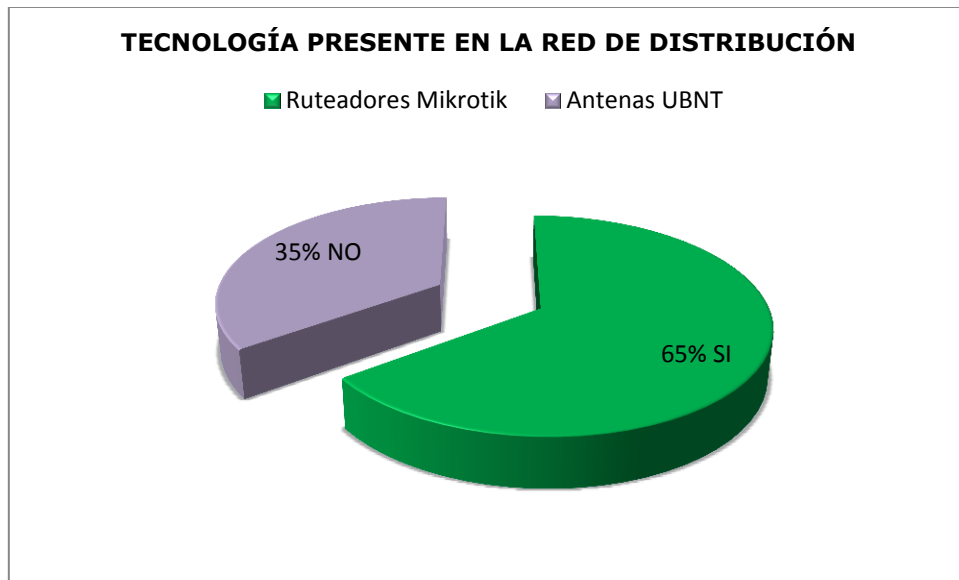


Figura V. 2 Porcentaje de equipos en la capa de distribución Fuente: (autores).

ACCESO

En la figura V.3 se muestra a los ruteadores de acceso mikrotik con soporte IPv6 en un 30%, un porcentaje menor con referencia de aquellos equipos que no soportan IPv6 pues el 50% y 20% de equipos UBNT no admiten el nuevo protocolo.

En esta situación se tiene como primera opción el cambio de la antena o como segunda opción la creación de un túnel terminando en la pc del cliente o en un CPE con soporte de tunelización.

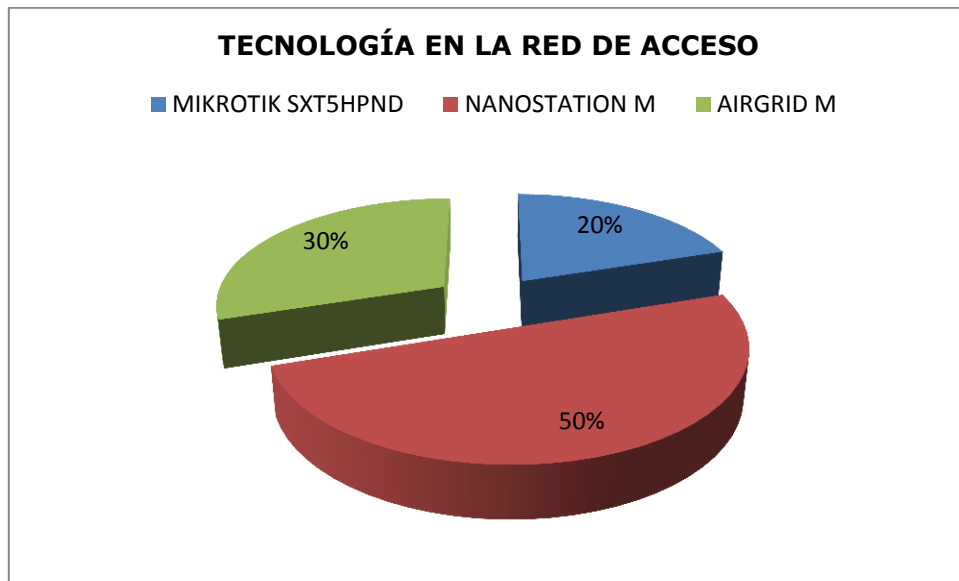


Figura V. 3 Porcentaje de equipos en la capa de acceso. Fuente: (autores).

CLIENTES

La presencia mayoritaria de CPE sin ningún tipo de actualización IPv6 es una de las cuestiones a resolver en los clientes, pero también a favor tenemos que el ISP entrega CPE que ya tiene IPv6 como parte de su SO.

En la figura V.4 se expone los porcentajes de presencia de los CPE, como vemos la tendencia es un valor minoritario de equipos CISCO LINKSYS E1200 con soporte IPv6, tan solo en un 10%.

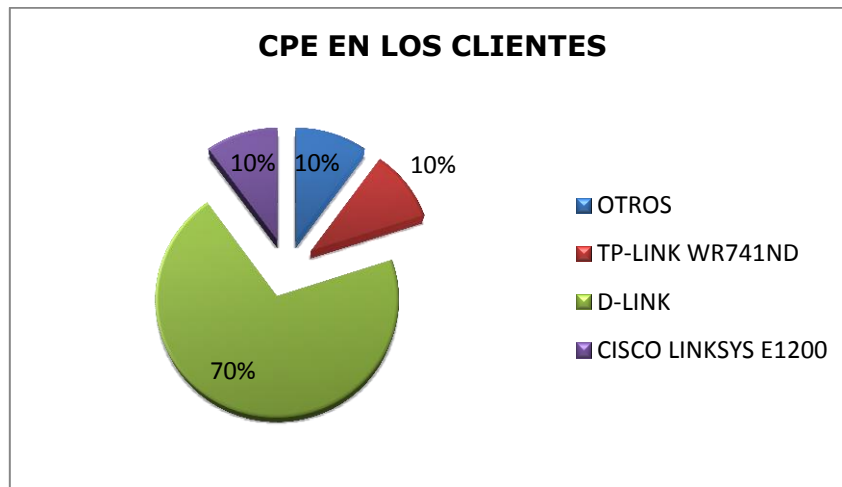


Figura V. 4 Porcentaje de equipos presentes en los clientes. Fuente: Autor

Cabe mencionar que los equipos en los clientes son propiedad del usuario y han estado por mucho tiempo antes que se pensara en el nuevo protocolo.

SERVICIOS

De acuerdo al capítulo III sección 4.7 los servicios como web y mail pueden ser cambiados para un soporte dual, ya que tanto en hardware y software no existe limitante.

GESTIÓN

La herramienta de registro de direcciones (GESTIOIP) es de código abierto por lo que tiene soporte completo para IPv6 en sus datos.

En lo que consiste a la herramienta de gestión DUDE el soporte es parcial, pues el ingreso a los equipos se los puede realizar por IPv4 para realizar configuraciones de tipo IPv6, pero si necesitáramos agregar dispositivos con IPv6 nativo este no lo se podría hacer directamente.

5.1.2. ESCENARIO EN CUAL SE ENCUENTRA EL ISP FASTNET

De acuerdo al análisis del capítulo III, sección 5.1.2, la situación de la empresa FASTNET nos ubica en el escenario en que el ISP puede soportar IPv6 en el Backbone mediante la actualización de firmware pero los CPE en su mayoría no admite el nuevo protocolo.

En general aquellos equipos mikrotik que tiene como sistema operativo cualquier versión de **RouterOS** pueden ser actualizados mediante la activación del paquete IPv6.

La capa de acceso muestra la necesidad de cambio de varios equipos para el tránsito de ipv6 o a su vez buscar una solución de túnel con un dispositivo de red dentro del cliente esta última solo si no hay otra opción.

Los equipos presentes en los clientes (CPE) la mayoría no soportan el protocolo IPv6 a excepción de los equipos cisco que se los ha empezado a utilizar.

5.1.3. ALCANCE DEL PROYECTO DE IMPLEMENTACIÓN

El proveedor de internet FASTNET lleva usando el protocolo IPv4 alrededor de 10 años y actualmente el 100% de sus servicios y clientes operan bajo dicho protocolo, como se ha expuesto en el transcurso de esta investigación, lo óptimo siempre será implantar IPv6 nativo, pero un proceso de transición siempre tiene que ser gradual en el tiempo por lo que hablar de un cambio total en las circunstancias de conectividad del Ecuador sería aislarnos, ya que solamente podríamos visitar determinados dominios y acceder a pocos servicios en la red, sobre todo en la región del RIR LACNIC.

Por lo que un punto de conveniencia es implementar **DUAL STACK** con posibles túneles en donde la situación lo amerite, pero reduciendo al máximo este mecanismo.

5.1.4. CAMBIO DE TECNOLOGÍA

Se observa que la capa de acceso es la que presenta menor soporte por lo que sería necesario el cambio de equipos en este punto de la red.

La cantidad total de equipos son aproximadamente 1.126 de los cuales el 70% necesitan ser cambiados es decir 788 routers de acceso.

En cuestión de CPE's el 90% no soportan IPv6, entonces se tendría que cambiar 1.013 equipos en los usuarios, pero este cambio dependerá de la demanda del cliente.

5.1.5. CAPACITACIÓN DEL PERSONAL

La formación de los recursos humanos es probablemente la mayor inversión en los procesos de activación de una tecnología como IPv6. La mayoría de los técnicos y profesionales en tecnologías de la Información al interior de la organización no estudiaron ni experimentaron con IPv6 durante su formación, por lo que deberán actualizar y nivelar sus conocimientos para asumir con competencias el desafío de la organización.

PROPUESTAS DE CAPACITACIÓN EN SERVIDORES IPv6

Ecuainux brinda capacitación orientado a instalación y uso de ipv6 en servidores Linux.

Hemos tomado la información de la página oficial de dicha empresa:

<http://www.ecuainux.com/cursos/para-administradores/curso-ipv6>.

CÓMO SE DICTARÁ EL CURSO:

El curso se dictará de forma virtual y consta de 12 fáciles capítulos en forma de video que les permitirá aprender rápidamente cómo realizar la configuración de IPv6 en los diversos servicios y se le dará una tutoría en forma de videoconferencia y foros de discusión para aclarar cualquier duda que pueda tener el estudiante. El estudiante contará con máquinas a la cuales se podrá conectar remotamente (por ssh) para preparar y verificar los contenidos que se dictarán en el curso. Por tanto no es necesario que tenga de infraestructura IPv6 ya establecida en su red sino que puede realizarlo en nuestra red IPv6 en lo que espera que su proveedor de internet le asigne una red de IPv6 para su uso.

Al momento todos los estudiantes que han cursado este módulo de IPv6 resaltan la facilidad de aprendizaje a través de video tutoriales y con los servidores de Linux que les brindamos para realizar las pruebas.

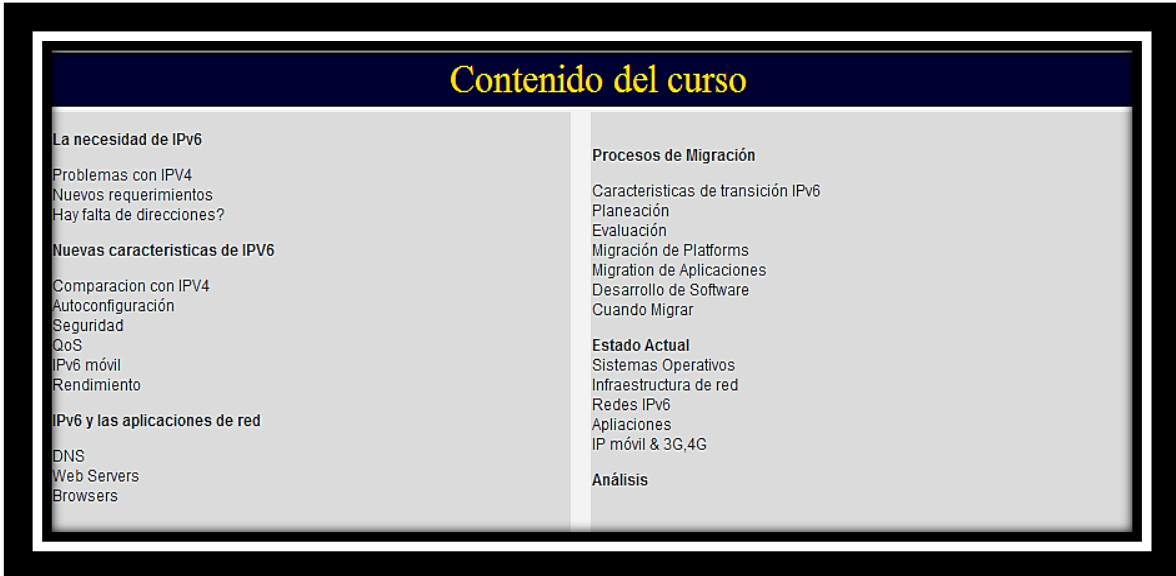
Costo: El costo es de 199USD+IVA por estudiante..

Estudiantes por módulo: 6.

PROPUESTA DE CAPACITACIÓN DE EQUIPOS CON IPv6

NetSoSe presenta capacitación para administradores de red, así como procesos de migración.

En la Figura V.5 se muestra detalles de la capacitación que hemos considerado favorable para el personal de FASTNET.



El diagrama muestra el contenido del curso de IPv6, dividido en dos columnas. El título principal es 'Contenido del curso'. La columna izquierda lista temas como 'La necesidad de IPv6', 'Problemas con IPV4', 'Nuevas características de IPV6', 'Comparación con IPV4', 'IPv6 y las aplicaciones de red'. La columna derecha lista temas como 'Procesos de Migración', 'Estado Actual', y 'Análisis'.

Contenido del curso	
La necesidad de IPv6	Procesos de Migración
Problemas con IPV4	Características de transición IPv6
Nuevos requerimientos	Planeación
Hay falta de direcciones?	Evaluación
Nuevas características de IPV6	Migración de Platforms
Comparación con IPV4	Migration de Aplicaciones
Autoconfiguración	Desarrollo de Software
Seguridad	Cuando Migrar
QoS	Estado Actual
IPv6 móvil	Sistemas Operativos
Rendimiento	Infraestructura de red
IPv6 y las aplicaciones de red	Redes IPv6
DNS	Aplicaciones
Web Servers	IP móvil & 3G,4G
Browsers	Análisis

Figura V. 6 Propuesta de capacitación por NetSose. Fuente:
<http://www.netsose.com/ipv6administradores.html>.

5.1.6. COSTOS DE IMPLEMENTACIÓN

La descripción de costos que se realiza a continuación es pensando en efectuar DUAL STACK en la red.

Al contar con equipos mikrotik que soportan el protocolo IPv6 en las capas de core y distribución, la inversión sustancial está en la capa de acceso y CPE´s.

En la tabla V.I se recomienda la compra de 788 equipos RouterBoard Sxt 5HPnD.

Tabla V. I Cantidad de routers para cambio. Fuente (autores)

Número de equipos	Equipo	Precio (\$)	Total (\$)
788	Sxt 5HPnD	60	47.280

En cuanto a los CPE para los usuarios, en el mercado ecuatoriano encontramos una limitada propuesta en cuanto a marcas y modelos, pero hemos considerado aquellos que se adapten a nuestras necesidades, es decir que posea una interfaz WAN y al menos una interfaz LAN y soporte IPv6 en modo Dual Stack.

En la Tabla V.II se muestra diferentes modelos, precios y costo que tendría al cambiar por cada modelo de CPE.

Tabla V. II CPE's Modelo/Precio. Fuente (autores)

Número de equipos	Equipo (Modelo)	Precio (\$)	Total (\$)
1.013	TP-LINK TL-WDR3500	50	50.650
1.013	TP-LINK TL-WDR3600	65	65.845
1.013	TP-LINK TL-WDR4300	70	70.910
1.013	CISCO LINKYS E1200	40	40.520

CAPACITACIÓN

Los costos de capacitación por las empresas que proponen capacitación se detallan en la Tabla V.III.

Tabla V. III Costos de Capacitación. Fuente (autores)

Capacitación	Valor	Técnicos	Total
Ecuainux	199+iva	5	1114,4
NetSoSe	180+iva	5	1038

COSTO DE INVERSIÓN INICIAL

En la tabla V. IV se expone el costo de inversión inicial para la implementación de DUAL STACK, tomando en cuenta la capacitación del personal propuesta por NetSose, el cambio de la capa de acceso y equipos terminales de los clientes (CPE´s), además considerando el modelo de CPE TP-LINK TL-WDR3500.

Tabla V. IV Costo inversión inicial

CONCEPTO	\$
CAPACITACIÓN	1.038
ROUTERS DE ACCESO	47.280
CPE´s	50.650
TOTAL	98.968

5.2. ETAPA 2 TÚNELES IPv6 PARA PRUEBAS Y PARA CLIENTES OBJETIVO.

5.2.1. ACTUALIZACIÓN

Echa la evaluación de los equipos en esta etapa el primer paso es actualizar los IOS para que presenten las opciones IPv6.

CORE

En esta capa el proceso es simple ya que los equipos requieren actualizar su IOS para que nuevas características se inicien, en el caso de equipo de mikrotik RB1100AHX2 se observa todas las propiedades bajo el protocolo IPv6 que se exponen en el capítulo IV sección 4.1 IPv6 en MIKROTIK.

DISTRIBUCIÓN

En este punto la actualización se lo realiza en todos los equipos mikrotik, que son alrededor de 35 equipos para la distribución, además aquí se cumple funciones de control de ancho de banda, y ruteo.

En la figura V.6 se muestra la actualización de un equipo RB751G-2HnD. En estos equipos la versión más reciente es v6.0

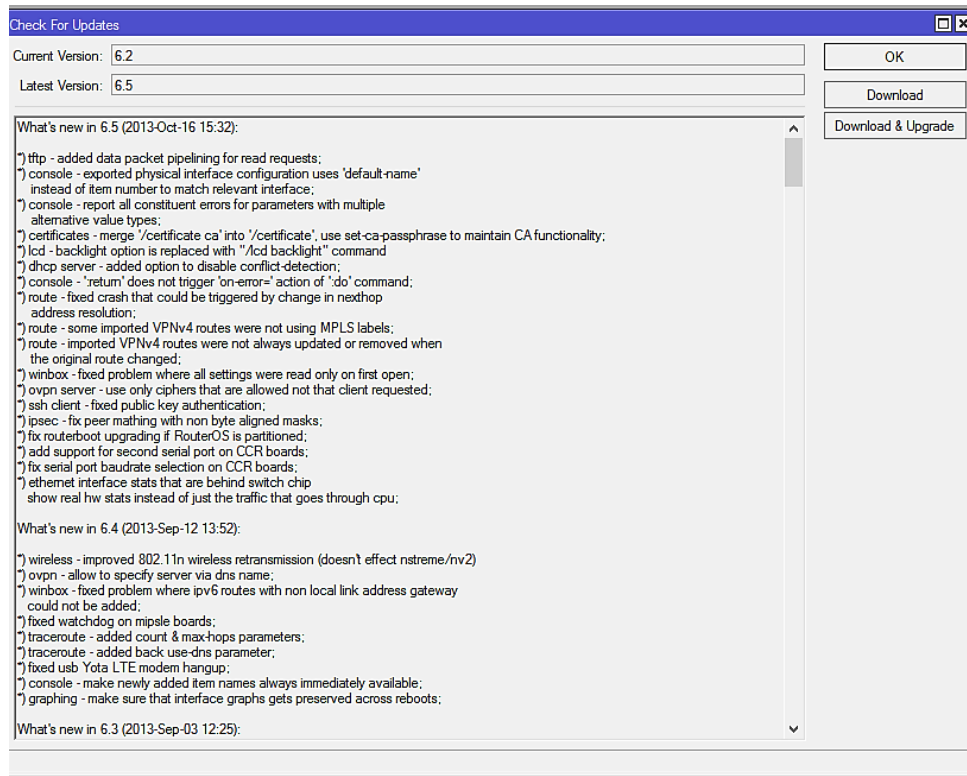


Figura V. 7 Actualización de Router de distribución. Fuente: (Autores).

A continuación se muestra las características IPv6 del equipo.

- Figura V.8 Dual Stack
- Figura V.9 Opciones de ruteo
- Figura V.10 Opciones de Tunelización

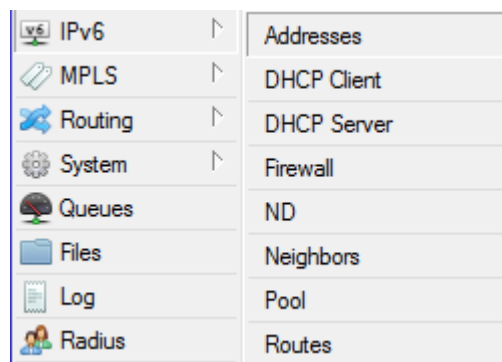


Figura V. 8 Dual Stack en el Equipo. Fuente (autores)

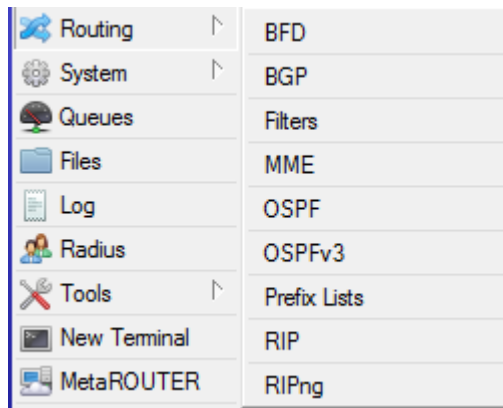


Figura V. 9 opciones de ruteo. Fuente (autores)

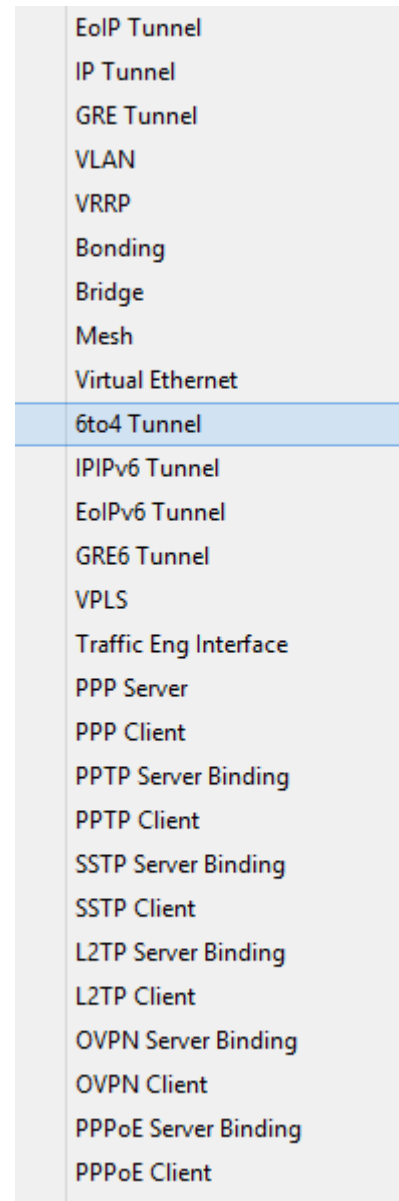


Figura V. 10 Características IPv6 para túneles.

Acceso

En el acceso como ya sabemos, tenemos los siguientes equipos:

1. MikroTik SXT 5HPnD
2. Ubiquiti NanoStation5
3. AIRGRID

1. MikroTik SXT 5HPnD (CPE):

En la figura V.11 se observa el ingreso al router vía Winbox¹⁵.

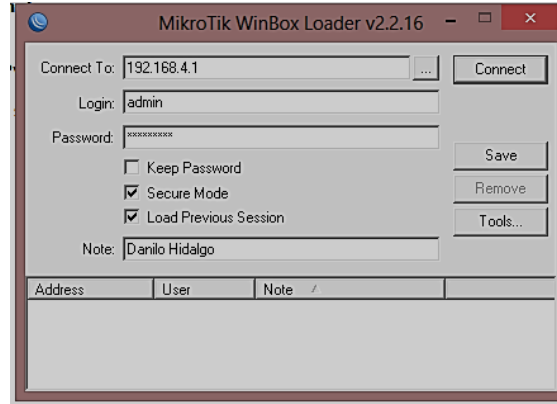


Figura V. 11 Ingreso vía Winbox. Fuente: (Autores)

La figura V.12, expone la actualización de los routers de acceso a su última versión en este caso la versión 5.26

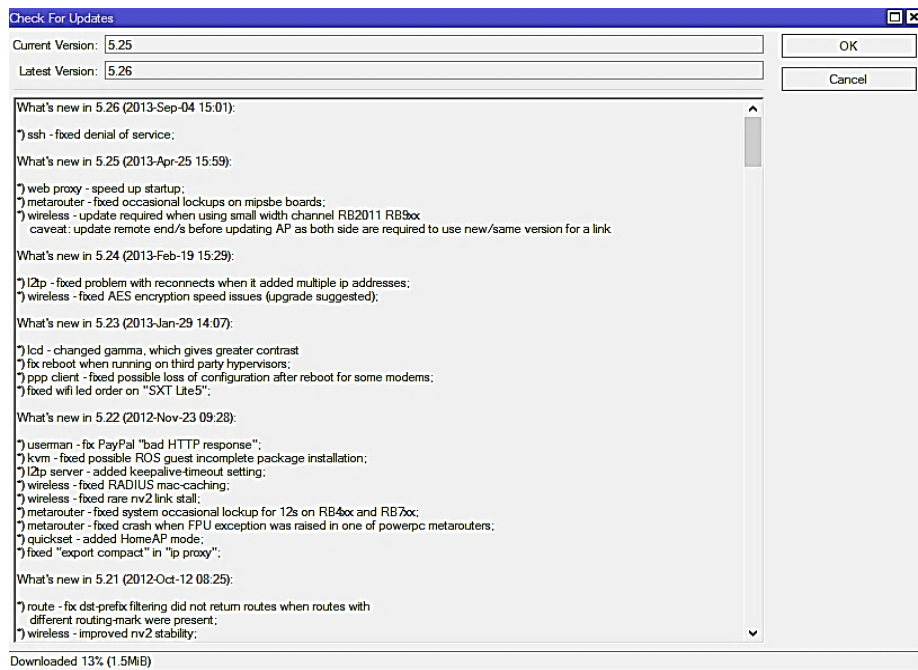
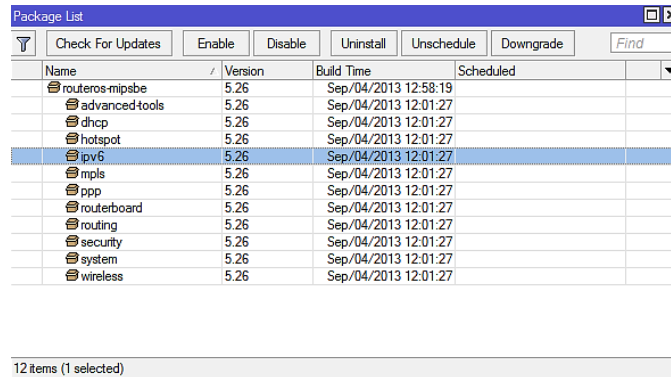


Figura V. 12 Actualización de Router de acceso Fuente: (Autores)

¹⁵ **Winbox:** es una herramienta de tipo cliente-servidor. Incluye una tecnología para realizar conexiones basadas en el sistema operativo RouterOS. Este software permite a sus usuarios realizar conexiones vía FTP, telnet y SSH.

Como vemos en la figura V.13 mediante la actualización se encuentra activo el paquete IPv6.

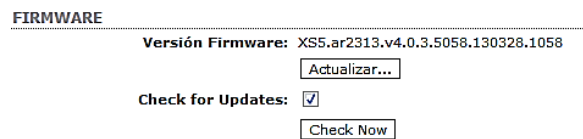


Name	Version	Build Time	Scheduled
routers-mipsbe	5.26	Sep/04/2013 12:58:19	
advanced-tools	5.26	Sep/04/2013 12:01:27	
dhcp	5.26	Sep/04/2013 12:01:27	
hotspot	5.26	Sep/04/2013 12:01:27	
ipv6	5.26	Sep/04/2013 12:01:27	
mpls	5.26	Sep/04/2013 12:01:27	
ppp	5.26	Sep/04/2013 12:01:27	
routerboard	5.26	Sep/04/2013 12:01:27	
routing	5.26	Sep/04/2013 12:01:27	
security	5.26	Sep/04/2013 12:01:27	
system	5.26	Sep/04/2013 12:01:27	
wireless	5.26	Sep/04/2013 12:01:27	

Figura V. 13 Presencia del Paquete IPv6 en router Mikrotik. Fuente (Autores).

2. Ubiquiti "NanoStation5" y AirGrid no soportan el protocolo IPv6

En la figura V.14 se muestra la actualización del Firmware de un equipo UBNT y la figura V.15 expone la incompatibilidad de IPv6.



FIRMWARE

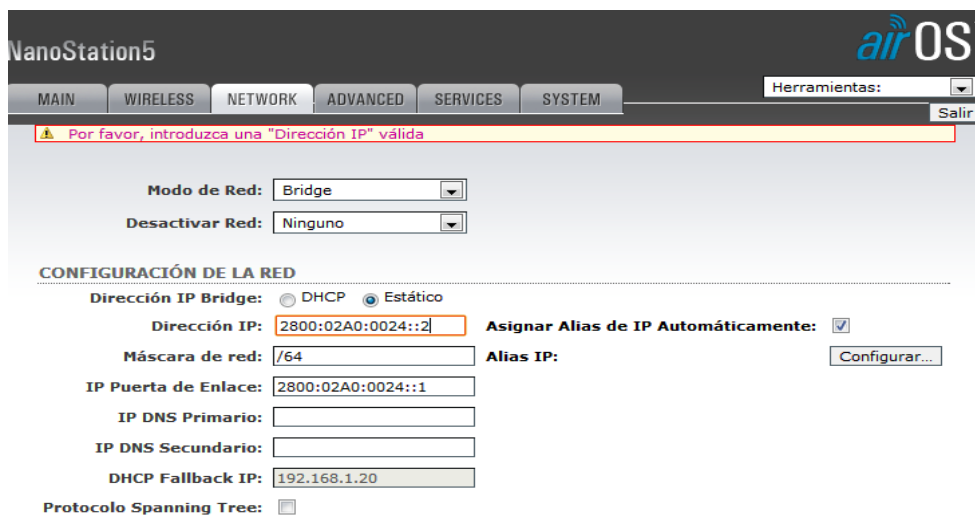
Versión Firmware: XS5.ar2313.v4.0.3.5058.130328.1058

Actualizar...

Check for Updates:

Check Now

Figura V. 14 Actualización de Firmware. Fuente (autores).



NanoStation5 **airOS**

MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM Herramientas: Salir

⚠ Por favor, introduzca una "Dirección IP" válida

Modo de Red: Bridge

Desactivar Red: Ninguno

CONFIGURACIÓN DE LA RED

Dirección IP Bridge: DHCP Estático

Dirección IP: 2800:02A0:0024::2 Asignar Alias de IP Automáticamente:

Máscara de red: /64 Alias IP: Configurar...

IP Puerta de Enlace: 2800:02A0:0024::1

IP DNS Primario:

IP DNS Secundario:

DHCP Fallback IP: 192.168.1.20

Protocolo Spanning Tree:

Figura V. 15 Incompatibilidad IPv6 con Ubiquiti. Fuente (Autores)

CPE's

A continuación se presenta la configuración de un equipo TP-LINK TL-WDR3500, en el que podemos ver en la figura V.16 el soporte ipv6 está en modo Dual Stack.

The screenshot shows the configuration page for a TP-LINK N600 Wireless Dual Band Router (Model No. TL-WDR3500). The left sidebar contains a navigation menu with options like Status, Quick Setup, Network, Dual Band Selection, Wireless 2.4GHz, Wireless 5GHz, Guest Network, DHCP, USB Settings, NAT, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6 Support, IPv6 Status, IPv6 Setup, and System Tools. The main content area is divided into two sections: WAN Setup and LAN Setup. In the WAN Setup section, 'Enable IPv6' is checked, 'WAN Connection Type' is set to 'Static IPv6', 'IPv6 Address' is '2800:2a0:2400:c::2/64', 'Default Gateway' is '2800:2a0:2400:c::1/64', 'MTU Size' is 1500, 'Primary DNS' is '2001:4860:4860:8888', and 'Secondary DNS' is '2001:4860:4860:8844'. The LAN Setup section shows 'IPv6 Address Assign Type' set to 'DHCPv6 Server', 'IPv6 Address Prefix' as '2800:2a0:2400:fa::/64', and 'Release Time' as 86400 seconds. A 'Save' button is at the bottom. On the right, there is an 'IPv6 WAN Help' section with instructions on enabling IPv6 and choosing a WAN connection type, listing options like DHCPv6, Static IPv6, PPPoEIPv6, and Tunnel 6to4.

Figura V. 16 Configuración de CPE TP-LINK TL-WDR3500. Fuente (autores).

5.2.2. TUNELIZACIÓN

5.2.2.1. EN EL CORE

Las pruebas con túneles en equipo de borde fue la primera experiencia para conectarnos a IPv6, bajo este concepto se configuro 6to4 en el router de core mikrotik RB1100AHX2.

Requisitos necesarios previos son aquellos expuesto en el capítulo II sección 2.2.5.1 :

IPv4 pública: 186.3.9.1

IPv6 global: 2002:ba03:901:0001::1

En la figura V.17, calculamos la dirección ip 6to4 a partir de IPv4 pública.

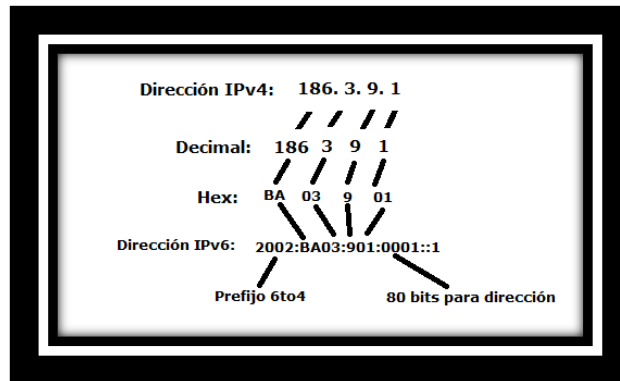


Figura V. 17 Ip 6to4 pública. Fuente(Autores).

1. La Figura V.18 muestra cómo crear una interface 6to4

```
/interface 6to4 add mtu=1280 name=Ipng_Tunnel local-address=186.3.9.1 remote-address=192.88.99.1 disabled=no
```

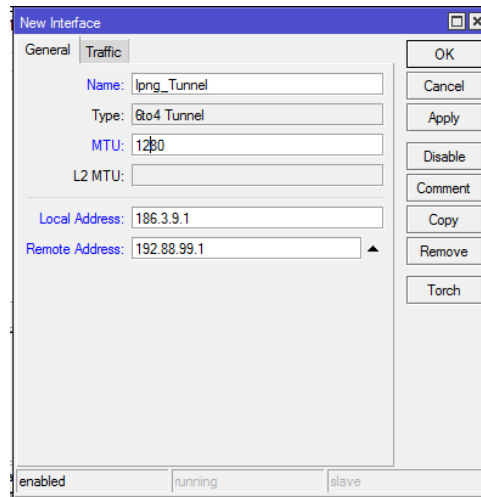


Figura V. 18 Pseudo interface para 6to4. Fuente (Autores).

2. En la figura V.19 se muestra como Agregar una dirección IPv6 a la interface túnel

```
/ipv6 address add address=2002:ba03:901:1::1/3 interface=Ipng_Tunnel
```

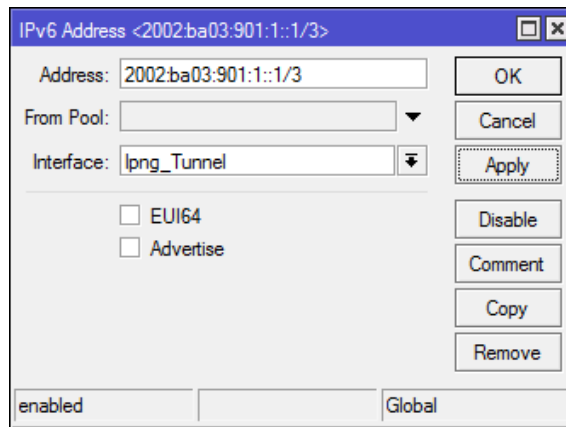



Figura V. 19 Configuración de IPv6 en la interfaz túnel. Fuente (autores).

3. Adicionamos una ruta por defecto hacia el internet IPv6 a través de la interface túnel como se indica en la figura V.20

```
ipv6 route add dst-address=2000::/3 gateway=Ipng_Tunnel
```

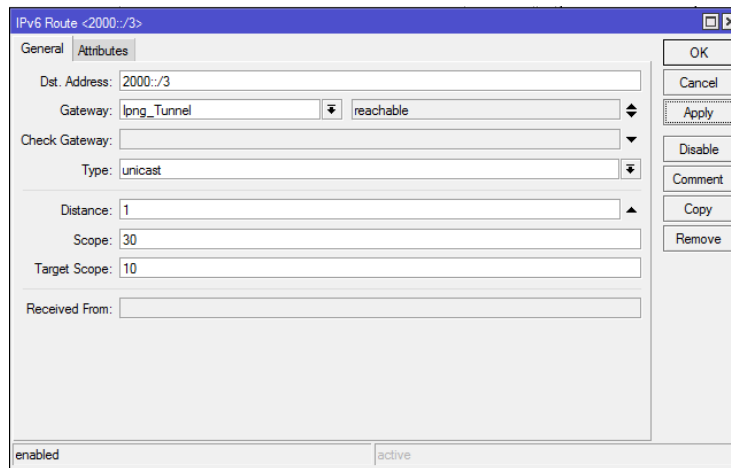


Figura V. 20 Configuración de ruta IPv6. Fuente (autores)

4. Pruebas de ping y traceroute se exponen en la figura V.21

Ping 2001:4860:4860::8888 DNS Google

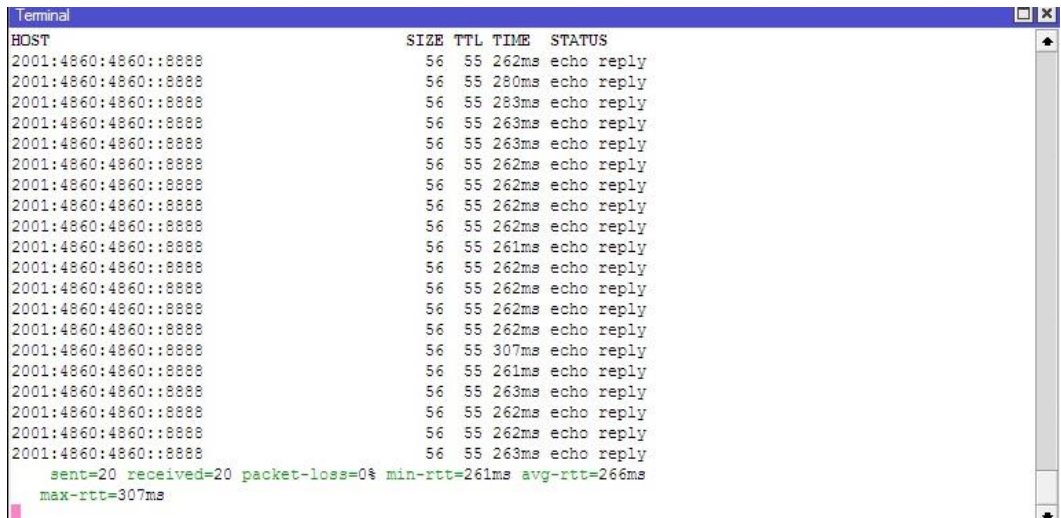


Figura V. 21 Respuesta de DNS de Google. Fuente (autores).

En la figura V.22 se muestra el tráfico en la interfaz túnel del router de core, como vemos es de tan solo unos kbps.

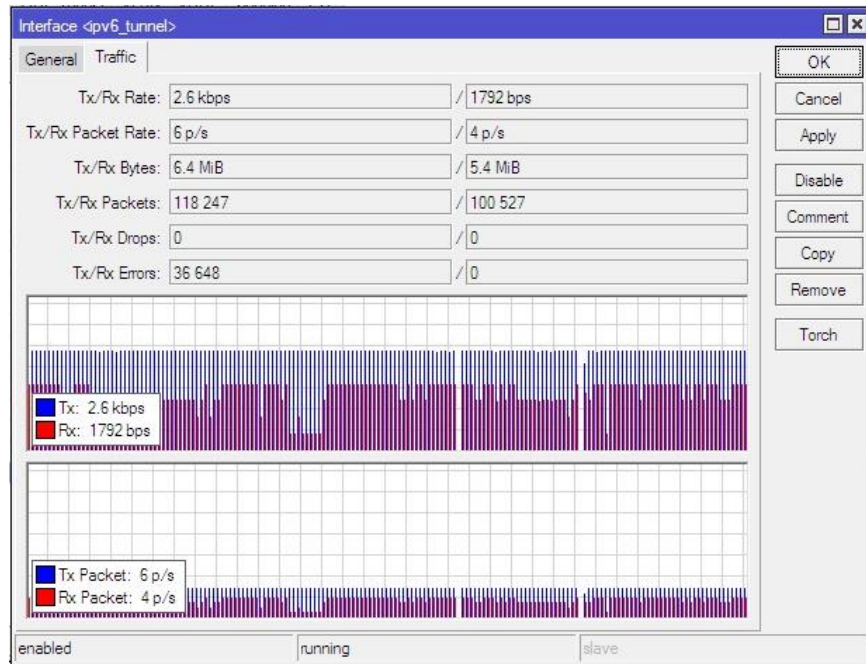


Figura V. 22 Tráfico IPv6 generado. Fuente (autores).

5.2.2.2. EN LOS CLIENTES

En este punto tenemos la opción de implementar túneles 6to4 con aquellos clientes que posean una dirección IPv4 pública y tunnel broker con aquellos clientes que no dispongan de dicha ip pública.

6to4

Este mecanismo puede proveer conectividad a toda una red o a una máquina en particular, pero en ambos casos se necesita una dirección IPv4 pública, adicionalmente se requiere de un CPE Dual Stack.

TUNNEL BROKER

Este mecanismo es independiente de la infraestructura ya que utiliza recursos de sitios dedicados que brindan la apertura del túnel de manera gratuita.

Mencionemos algunos:

- Gogo6
- Hurricane Electric

5.2.3. PRUEBAS INICIALES EN LA RED

Se implementó un segmento de red IPv6 en forma nativa desde el Backbone hasta el cliente.

En la figura V.23 se muestra detalles de la estructura de la red de pruebas, en donde la salida hacia el internet es por un túnel 6to4 y rutas estáticas en todas las capas.

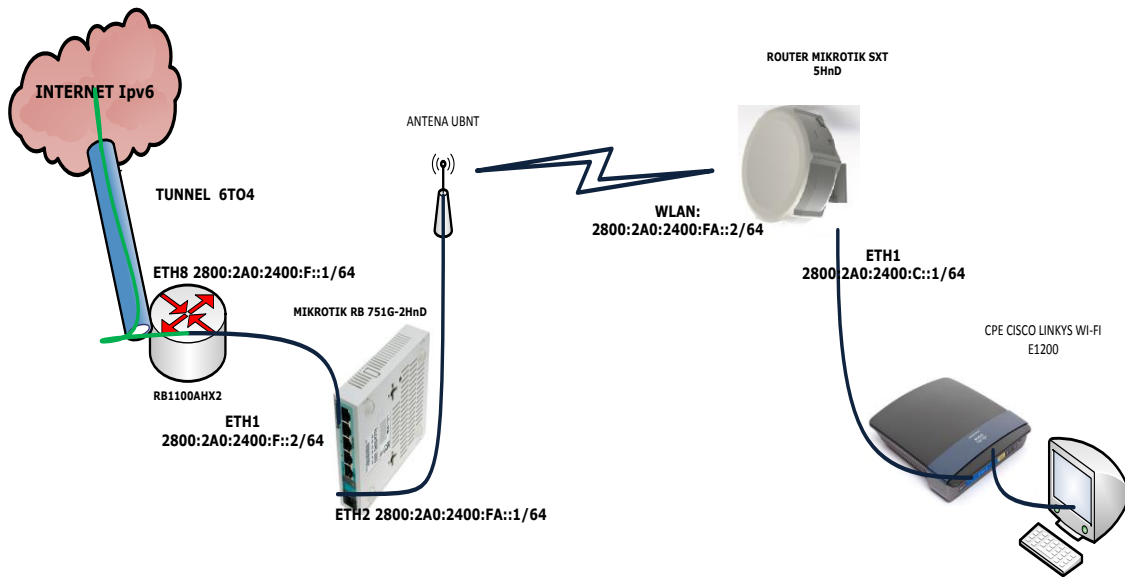


Figura V. 23 Estructura de la red de pruebas. Fuente (autores).

CONFIGURACIÓN EL CORE

Se utilizó el túnel 6to4 configurado en la sección 5.2.2.1 para la salida al internet IPv6. Adicionalmente se implementó las siguientes rutas estáticas.

```
ipv6 route add dst-address=2800:2a0:fa::/64 gateway=2800:2a0:f::2  
ipv6 route add dst-address=2800:2a0:c::/64 gateway=2800:2a0:f::2
```

CONFIGURACIÓN RB751G-2HnD

En la tabla V.V se muestra las IP's configuradas en el equipo de distribución

Tabla V. V IP's en el equipo de distribución. Fuente (autores).

DIRECCION IPv6	INTERFACE
2800:2A0:2400:F::2/64	ETH1
2800:2A0:2400:FA::1/64	ETH2

En la Figura V.24 se muestra las configuraciones hechas en el distribuidor

IPv6 Address List					
G	::: ENLACE HACIA EL RB1100AHX2				
	Address: 2800:2a0:2400:f::2/64	Interface: ether1-gateway	EUI64:		no
	Advertise: no				
G	::: GATEWAY EN DISTRIBUCION				
	Address: 2800:2a0:2400:fa::1/64	Interface: ether2-master-local	EUI64:		no
	Advertise: no				
DL	Address: fe80::20c:42ff:febc:a222/64	Interface: ether1-gateway	EUI64:		no
	Advertise: no				
DL	Address: fe80::20c:42ff:febc:a223/64	Interface: bridge-local	EUI64:		no
	Advertise: no				

Figura V. 24 Configuración de IP's en el Distribuidor. Fuente (Autores).

Se configuró rutas estáticas para alcanzar el internet y al cliente.

```
ipv6 route add dst-address=::/0 gateway=2800:2a0:f::1  
ipv6 route add dst-address=2800:2a0:c::/64 gateway=2800:2a0:fa::2
```

CONFIGURACIÓN ANTENA UBT NANOSTATION

La antena de irradiación contiene la señal con nombre "ipv6", está en modo puente para que funcione como transmisor.

ESTADO			
SSID Estación Base:	ipv6		
Calidad AirMax:	- %		
Frecuencia:	5765 MHz		
Antena:	Horizontal		
Seguridad:	Ninguno		
Tiempo en funcionamiento:	00:01:15		
Cable LAN:	ON		
LAN MAC:	00:27:22:91:F1:FB		
MAC WLAN:	00:27:22:90:F1:FB		
Información Adicional:	- - -		
Capacidad AirMax:	- %		
Canal:	153		
Ruido Base:	-89 dBm		
Time out:	30		
Fecha:	2013-03-28 11:02:08		
Nombre del Host:	UBNT		
LAN Dirección IP:	192.168.1.20		
Dirección IP WLAN:	192.168.1.20		
<input type="button" value="Actualizar"/>			
LAN ESTADÍSTICAS			
	Bytes	Paquetes	Errores
Recibido:	99075	530	0
Transmitidos:	44313	175	0
ESTADÍSTICAS WLAN			
	Bytes	Paquetes	Errores
Recibido:	12980	211	0
Transmitidos:	87931	481	0

Figura V. 25 Configuración de la antena de irradiación. Fuente (Autores).

En la figura V.26 se muestra la configuración de los parámetros de transmisión de la antena, como podemos ver a esta antena se pueden adherir clientes ya que está en modo de AP.

CONFIGURACION INALÁMBRICA BÁSICA

Modo Inalámbrico: [f21](#) Punto de Acceso

SSID: Esconder SSID

Código País:

Modo IEEE 802.11:

Anchura del espectro de canal: [f21](#) Vel. máx. de datos: 54Mbps

Cambio de canal: [f21](#)

Canal:

Potencia de salida: dBm Autolimitar PIRE según dominio regulatorio

Velocidad de datos, Mbps: Auto

Activar DFS: [f21](#)

Figura V. 26 Configuración antena en modo AP. Fuente (autores)

CONFIGURACIÓN DE ROUTER MIKROTIK SXT 5HND (ACCESO)

En la Tabla V.VI están presentes las direcciones ip's configuradas en el equipo

Tabla V. VI Direcciones Ipv6 en el router de Acceso. Fuente (Autores).

DIRECCION IPv6	INTERFACE
2800:2A0:2400:FA::2/64	WLAN
2800:2A0:2400:C::1/64	ETH1

Como se muestra en la Figura V.27, se configuró una dirección estática por defecto para alcanzar todos los destinos.

IPv6 Route

General Attributes

Dest. Address:

Gateway: unreachable

Check Gateway:

Type:

Distance:

Scope:

Target Scope:

Received From:

enabled active static

OK Cancel Apply Disable Comment Copy Remove

Figura V. 27 Ruta estática por defecto en router de acceso.

5.3. ETAPA 3 IMPLEMENTACIÓN DEL NÚCLEO DUAL STACK

5.3.1. ADQUISICIÓN DE UN PREFIJO DE RED IPv6

La adquisición de un prefijo nos indica que este debe estar distribuido en la infraestructura del Carrier, es decir con salida hacia el internet, podemos observar en la Figura V.28 las estadísticas del internet de Hurricane electric, que la red asignada a Fastnet se encuentra creada:

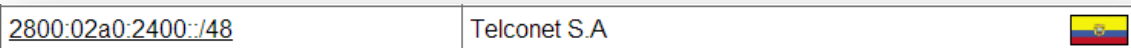


Figura V. 28 Red asignada a Fastnet. Fuente: http://bgp.he.net/AS27947#_prefixes6

En Hurricane Electric, se puede encontrar estadísticas de asignación de recursos de red y sistemas autónomos ipv4 e ipv6 de todo el mundo.

En el caso de Telconet podemos observar en la Figura V.29 la propagación de las rutas IPv6.

AS27947 IPv6 Route Propagation

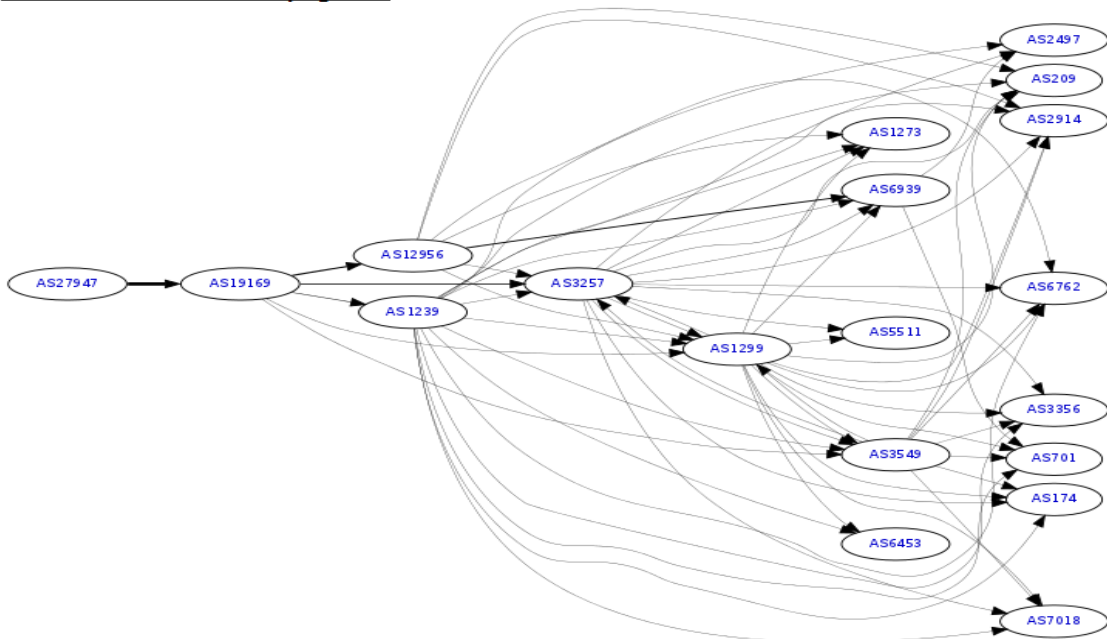


Figura V. 29 Propagación de rutas IPv6 en Telconet. Fuente: http://bgp.he.net/AS27947#_graph6

El Carrier Telconet provee IPv6 sobre MPLS utilizando el modelo 6VPE para el transporte con sus router de borde en DUAL STACK.

Tenemos la dirección IPv6 asignada **2800:02A0:2400:0000:0000:0000:0000 /48** con lo cual tenemos **65.536** redes disponibles con **18'446744'073709'551616** de direcciones IP asignables por cada subred.

En la tabla V.VII se puntualiza la dirección Unicast Globales IPv6, además se detalla los tres campos: el prefijo global de enrutamiento, el identificador de subred y el identificador de interfaz.

Tabla V. VII Dirección IPv6 Unicast Global. Fuente (Autores).

Base	Prefijo de enrutamiento	ID de Subred	Id de interfaz (Dispositivo)
Hexadecimal	2800:2A0:2400	0000	0000:0000:0000:0000
Número de bits	48 bits	16 bits	64 bits

5.3.2. PLAN DE CONMUTACIÓN

La conmutación en el ISP se maneja bajo rutas estáticas en todos los niveles de la estructura de la red, por lo que se mantendrá el mismo esquema en IPv6. Las configuraciones de direcciones estáticas en un router mikrotik son de fácil implementación, todos los conceptos Ipv4 se mantienen.

5.3.3. CONECTIVIDAD CON EL PROVEEDOR DE NIVEL SUPERIOR

La conectividad se dará entre el router core Fastnet y el router Telconet, el proceso se inicia con las configuración de direcciones IPv6 y rutas estáticas en los equipos.

En la Figura V.31 se expone los detalles de la conexión:

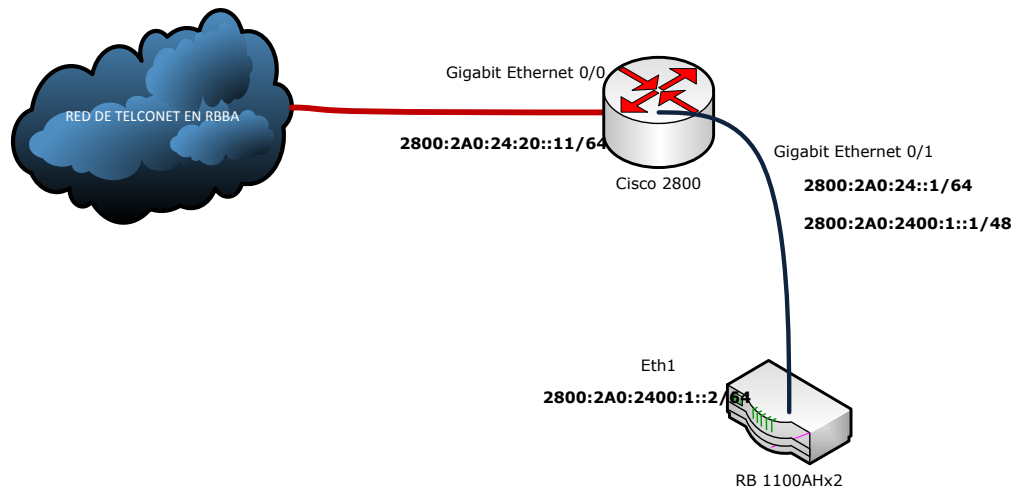


Figura V. 30 Conectividad con el proveedor de nivel superior. Fuente (autores).

Direcciones IP's configuradas en el router Telconet:

Tabla V. VIII Asignación de direcciones en el Router Telconet. Fuente (Autores).

Dirección IPv6	Interface	
2800:2A0:24:20::11/64	Gigabit Ethernet 0/0	WAN
2800:2A0:24::1/64	Gigabit Ethernet 0/1	LAN
2800:2A0:2400:1::1/64		

Configuración en el router cisco Telconet

```
interface GigabitEthernet0/0
description TO TELCONET
ip address 201.218.45.49 255.255.255.128
no ip redirects
no ip proxy-arp
load-interval 30
duplex auto
speed auto
ipv6 address 2800:2A0:24:20::11/64
no cdp enable
!
interface GigabitEthernet0/1
description TO LAN
ip address 10.10.10.1 255.255.255.252
ip access-group 170 in
no ip redirects
no ip proxy-arp
load-interval 30
duplex auto
speed auto
ipv6 address 2800:2A0:24::1/64
```

```
ipv6 address 2800:2A0:2400:1::1/64

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 201.218.45.1
ip route 186.3.9.0 255.255.255.0 10.10.10.2
ip route 186.5.67.0 255.255.255.224 10.10.10.2
ip route 201.218.45.224 255.255.255.224 10.10.10.2
ipv6 route 2800:2A0:2400::/48 2800:2A0:2400:1::2
ipv6 route ::/0 2800:2A0:24:20::1
!
```

Dirección ip configurada en el router principal de FASTNET

Tabla V. IX Direcciones IPv6 en el router core Fastnet. Fuente (autores)

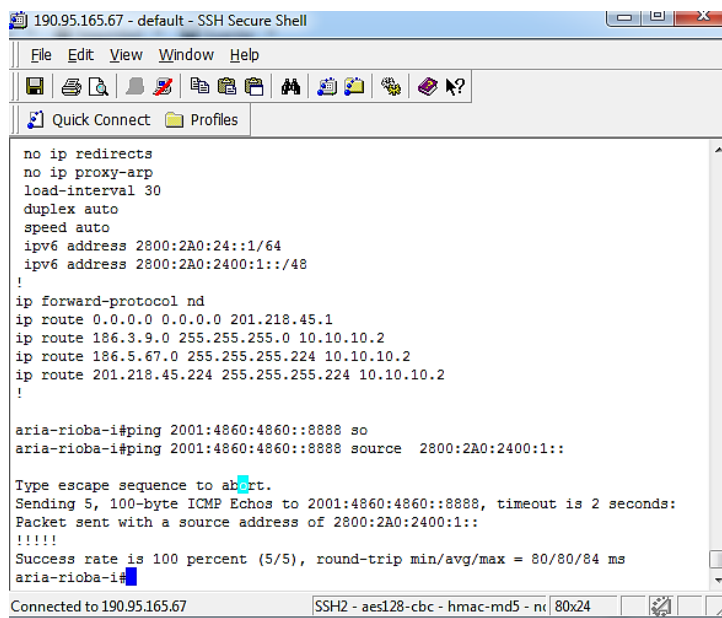
Dirección IPv6	Interface
2800:2A0:2400:1::2/64	Eth1

Ruta estática por defecto para la salida desde el router FASTNET

::/0 vía 2800:2A0:1::1

PRUEBAS DE CONECTIVIDAD

En la Figura V.32 se muestra al Router Cisco Telconet realizando una prueba ICMPv6 con source 2800:2A0:2400:1:: destination 2001:4860:4860::8888 (DNS de Google).



```
190.95.165.67 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
no ip redirects
no ip proxy-arp
load-interval 30
duplex auto
speed auto
ipv6 address 2800:2A0:24:1/64
ipv6 address 2800:2A0:2400:1::/48
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 201.218.45.1
ip route 186.3.9.0 255.255.255.0 10.10.10.2
ip route 186.5.67.0 255.255.255.224 10.10.10.2
ip route 201.218.45.224 255.255.255.224 10.10.10.2
!
aria-rioba-i#ping 2001:4860:4860::8888 so
aria-rioba-i#ping 2001:4860:4860::8888 source 2800:2A0:2400:1::

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
Packet sent with a source address of 2800:2A0:2400:1::
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/80/84 ms
aria-rioba-i#
```

Figura V. 31 Ping a DNS IPv6 Google desde el router Telconet

Traza hacia el mundo desde el router Telconet

```
aria-rioba-i#traceroute ipv6 2001:4860:4860::8888
```

```
Type escape sequence to abort.
```

```
Tracing the route to google-public-dns-a.google.com (2001:4860:4860::8888)
```

```
 1 2800:2A0:24:20::1 0 msec 0 msec 0 msec
 2 ::FFFF:10.201.24.253 12 msec 12 msec 12 msec
 3 ::FFFF:10.201.111.145 12 msec 12 msec 12 msec
 4 2800:2A0:11:30::1 12 msec 12 msec 12 msec
 5 2800:2A0:11:30::3 16 msec 16 msec 16 msec
 6 2800:2A0:11:11:1::1A 12 msec 12 msec 12 msec
 7 So4-1-2-0-gramiana4-ip6.red.telefonica-wholesale.net (2001:1498:1:235::1) 68 msec 64
msec 68 msec
 8 * * *
 9 2001:1498:1:2F3::2 128 msec 128 msec 132 msec
10 2001:4860::1:0:245C 68 msec 68 msec
   2001:4860::1:0:245B 64 msec
11 2001:4860::8:0:2F03 80 msec
   2001:4860::8:0:52BB 80 msec 80 msec
12 2001:4860::2:0:A7 100 msec 80 msec 84 msec
13 * * *
14 *
   google-public-dns-a.google.com (2001:4860:4860::8888) 76 msec 80 msec
aria-rioba-i#t.
```

5.3.4. PLAN DE DIRECCIONAMIENTO

Ahora tenemos que determinar que parte de los 16 bits del espacio de direcciones disponibles se requiere para el plan de direccionamiento seleccionado, esto dependerá de cuantos grupos de usuarios y localidades o sitios disponga la red.

La asignación de 65.536 posibles subredes Ipv6 de prefijo /64 puede parecer a primera vista excesiva, sin embargo existe varias razones para ello:

El despliegue futuro de redes NGN facilitara la implementación de servicios nuevos como VoIP, IPTv cuya distribución puede requerir el uso de redes /64 específicas para cada usuario final.

Así como la llegada de nuevos servicios basados en la domótica, el advenimiento del internet de las cosas requerirá un espacio de direcciones propio y separado del resto de tráfico en la red del usuario.

En la tabla V.X calculamos la cantidad de subredes que necesitaremos

Sitios de presencia de la red

- Fastnet
- Cacha
- Hospj
- Politécnica
- Dolorosa
- Noc
- Usos futuros

Tipos de redes

- Infraestructura (Enlaces)
- Clientes
- Servicios

Tabla V. X Cálculo de Subredes IPv6. Fuente (autores).

Conexión al Carrier	Numero de subredes
Telconet	1
Nodo	Numero de subredes
Cacha	64
Hospital San Juan	64
Politécnica	64
Dolorosa	16
Otros	Numero de subredes
Noc y Servicios	2
Usos Futuros	45
Total subredes	256

5.3.4.1. DIRECCIONAMIENTO NIVEL 1

Aproximadamente se calcula 256 subredes con los que 8 bits de la parte del ID de Subred serán suficientes, además recordemos que en IPv6 se cuenta las redes y no hosts.

$$2^8 = 256$$

2800	2A0	2400	1111 1111 0000 0000	0000 0000 0000 0000	0000 0000 0000 0000
16	16	16	8	8	16
			/56		

Distancia entre los múltiplos: El incremento lo calculamos con el número de bits restantes a partir del último que utilizamos en este caso son 8 bits es decir 10000000 en binario (agregamos un 1 a los 8 bits), o 100 en hexadecimal

Entonces tendríamos las direcciones de nivel 1 para la infraestructura:

- 2800:2a0:2400::/48

1	2800:2a0:2400::/56	64	2800:2a0:2400:3f00::/56
2	2800:2a0:2400:100::/56	65	2800:2a0:2400:4000::/56
3	2800:2a0:2400:200::/56	66	2800:2a0:2400:4100::/56
4	2800:2a0:2400:300::/56	67	2800:2a0:2400:4200::/56
5	2800:2a0:2400:400::/56	68	2800:2a0:2400:4300::/56
6	2800:2a0:2400:500::/56	69	2800:2a0:2400:4400::/56
7	2800:2a0:2400:600::/56	70	2800:2a0:2400:4500::/56
8	2800:2a0:2400:700::/56	71	2800:2a0:2400:4600::/56
9	2800:2a0:2400:800::/56	72	2800:2a0:2400:4700::/56
10	2800:2a0:2400:900::/56	73	2800:2a0:2400:4800::/56
11	2800:2a0:2400:a00::/56	74	2800:2a0:2400:4900::/56
12	2800:2a0:2400:b00::/56	75	2800:2a0:2400:4a00::/56
13	2800:2a0:2400:c00::/56	76	2800:2a0:2400:4b00::/56
14	2800:2a0:2400:d00::/56	77	2800:2a0:2400:4c00::/56
15	2800:2a0:2400:e00::/56	78	2800:2a0:2400:4d00::/56
16	2800:2a0:2400:f00::/56	79	2800:2a0:2400:4e00::/56
17	2800:2a0:2400:1000::/56	80	2800:2a0:2400:4f00::/56
18	2800:2a0:2400:1100::/56	81	2800:2a0:2400:5000::/56
19	2800:2a0:2400:1200::/56	82	2800:2a0:2400:5100::/56
20	2800:2a0:2400:1300::/56	83	2800:2a0:2400:5200::/56
21	2800:2a0:2400:1400::/56	84	2800:2a0:2400:5300::/56
22	2800:2a0:2400:1500::/56	85	2800:2a0:2400:5400::/56
23	2800:2a0:2400:1600::/56	86	2800:2a0:2400:5500::/56
24	2800:2a0:2400:1700::/56	87	2800:2a0:2400:5600::/56
25	2800:2a0:2400:1800::/56	88	2800:2a0:2400:5700::/56
26	2800:2a0:2400:1900::/56	89	2800:2a0:2400:5800::/56
27	2800:2a0:2400:1a00::/56	90	2800:2a0:2400:5900::/56
28	2800:2a0:2400:1b00::/56	91	2800:2a0:2400:5a00::/56
29	2800:2a0:2400:1c00::/56	92	2800:2a0:2400:5b00::/56
30	2800:2a0:2400:1d00::/56	93	2800:2a0:2400:5c00::/56
31	2800:2a0:2400:1e00::/56	94	2800:2a0:2400:5d00::/56
32	2800:2a0:2400:1f00::/56	95	2800:2a0:2400:5e00::/56
33	2800:2a0:2400:2000::/56	96	2800:2a0:2400:5f00::/56
34	2800:2a0:2400:2100::/56	97	2800:2a0:2400:6000::/56
35	2800:2a0:2400:2200::/56	98	2800:2a0:2400:6100::/56
36	2800:2a0:2400:2300::/56	99	2800:2a0:2400:6200::/56
37	2800:2a0:2400:2400::/56	100	2800:2a0:2400:6300::/56
38	2800:2a0:2400:2500::/56	101	2800:2a0:2400:6400::/56
39	2800:2a0:2400:2600::/56	102	2800:2a0:2400:6500::/56
40	2800:2a0:2400:2700::/56	103	2800:2a0:2400:6600::/56
41	2800:2a0:2400:2800::/56	104	2800:2a0:2400:6700::/56
42	2800:2a0:2400:2900::/56	105	2800:2a0:2400:6800::/56
43	2800:2a0:2400:2a00::/56	106	2800:2a0:2400:6900::/56
44	2800:2a0:2400:2b00::/56	107	2800:2a0:2400:6a00::/56
45	2800:2a0:2400:2c00::/56	108	2800:2a0:2400:6b00::/56
46	2800:2a0:2400:2d00::/56	109	2800:2a0:2400:6c00::/56
47	2800:2a0:2400:2e00::/56	110	2800:2a0:2400:6d00::/56
48	2800:2a0:2400:2f00::/56	111	2800:2a0:2400:6e00::/56
49	2800:2a0:2400:3000::/56	112	2800:2a0:2400:6f00::/56
50	2800:2a0:2400:3100::/56	113	2800:2a0:2400:7000::/56
51	2800:2a0:2400:3200::/56	114	2800:2a0:2400:7100::/56
52	2800:2a0:2400:3300::/56	115	2800:2a0:2400:7200::/56
53	2800:2a0:2400:3400::/56	116	2800:2a0:2400:7300::/56
54	2800:2a0:2400:3500::/56	117	2800:2a0:2400:7400::/56
55	2800:2a0:2400:3600::/56	118	2800:2a0:2400:7500::/56
56	2800:2a0:2400:3700::/56	119	2800:2a0:2400:7600::/56
57	2800:2a0:2400:3800::/56	120	2800:2a0:2400:7700::/56
58	2800:2a0:2400:3900::/56	121	2800:2a0:2400:7800::/56
59	2800:2a0:2400:3a00::/56	122	2800:2a0:2400:7900::/56
60	2800:2a0:2400:3b00::/56	123	2800:2a0:2400:7a00::/56
61	2800:2a0:2400:3c00::/56	124	2800:2a0:2400:7b00::/56
62	2800:2a0:2400:3d00::/56	125	2800:2a0:2400:7c00::/56
63	2800:2a0:2400:3e00::/56	126	2800:2a0:2400:7d00::/56

En la Tabla V.XI se asigna los números de direcciones de nivel 1 para ser usadas en cada punto de la red.

Tabla V. XI Números de direcciones IPv6's asignado para uso en la infraestructura. Fuente (autores)

Red	Numero de asignación
Telconet	1
Usos Futuros	2 -16 y 211-240
Hospital San Juan	17-80
Cacha	81-144
Politécnica	145-208
Noc y Servicios	209-210
Dolorosa	241-256

5.3.4.2. DIRECCIONAMIENTO NIVEL 2

El objetivo de este direccionamiento es asignar una ip visible en todo el internet a cada usuario del proveedor de internet por lo que se plantea un direccionamiento para el futuro.

A cada dirección de la red podemos subnetearla a un prefijo /64 con los 8 bits restantes.

/56 id de subred asignada a los nodos

/64 id de subred asignada a los clientes

$$64 - 56 = 8bits$$

$$2^8 = 256 \text{ subredes por direccion de cada nodo}$$

Es decir que por cada dirección de red del grupo asignada a los nodos principales Cacha, Hospital San Juan, Dolorosa y Politécnica se dividen en 256 subredes.

Por ejemplo elijamos la primera red del nodo Hospital San Juan:

- 2800:2a0:2400:1000::/56

1 2800:2a0:2400:1000::/64

2 2800:2a0:2400:1001::/64

```
3          2800:2a0:2400:1002::/64
4          2800:2a0:2400:1003::/64
5          2800:2a0:2400:1004::/64
6          2800:2a0:2400:1005::/64
7          2800:2a0:2400:1006::/64
8          2800:2a0:2400:1007::/64
9          2800:2a0:2400:1008::/64
10         2800:2a0:2400:1009::/64
11         2800:2a0:2400:100a::/64
12         2800:2a0:2400:100b::/64
13         2800:2a0:2400:100c::/64
14         2800:2a0:2400:100d::/64
15         2800:2a0:2400:100e::/64
16         2800:2a0:2400:100f::/64
..         ...      ..      ..      ..
..         ...      ..      ..      ..
256        2800:2a0:2400:10ff::/64
```

5.3.5. SERVICIOS

Se verificara que los servicios como DNS, mail, Web, soporten IPv6. Algunos de los servicios mencionados anteriormente están activados bajo Linux-S.O Centos.

5.3.5.1. ACTIVAR IPv6 EN CENTOS

En el archivo modprobe.conf comentamos un par de líneas y activamos otras, como sigue a continuación en la Figura V.33.

Comentamos las siguientes líneas

```
#alias net-pf-10 off
#alias IPv6 off
```


Figura V. 32 /etc/modprobe.conf. Fuente: (Autores).

Luego cambiamos el 1 por el 0 en la línea

```
options IPv6 disable=0
```

Figura V. 33 /etc/modprobe.conf. Fuente: (Autores).

Bajo sysconfig/network cambiamos la línea

```
NETWORKING_IPV6=no por  
NETWORKING_IPV6=yes
```

Figura V. 34 /etc/sysconfig/network. Fuente (Autores).

En el archivo sysconfig/network-scripts/ifcfg-eth0 cambiamos por las líneas que detallamos a continuación.

```
DEVICE=eth0  
BOOTPROTO=none  
HWADDR=08:00:27:9A:DB:91  
ONBOOT=yes  
DHCP_HOSTNAME=none  
IPV6INIT=yes
```

Figura V. 35 /etc/sysconfig/network-scripts/ifcfg-eth0. Fuente: (Autores).

Reiniciamos el servicio

```
service network restart
```

Figura V. 36 Línea de comandos para reiniciar el Sistema. Fuente (Autores)

5.3.5.2. SERVIDOR MAIL

Fastnet tiene habilitado el servicio de mail, por lo que es necesario actualizar para que soporte el nuevo protocolo. Ahora bien el servidor de mail está configurado para el protocolo IPV4, solamente basta habilitar para que escuche peticiones IPV6; esto lo hacemos verificando que estén habilitadas las siguientes líneas del archivo de Postfix.

Ingresamos al main.cf y verificamos que los siguientes parámetros estén activos.

```
mydomain = DOMINIO_DE_FASTNET
myhostname = mail.$mydomain
myorigin = $mydomain
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mynetworks_style = subnet
mynetworks = 127.0.0.0/8
home_mailbox = Maildir/
```

Figura V. 37 /etc/Postfix/main.cf. Fuente (Autores).

Reiniciamos el servicio

```
service postfix restart
```

Figura V. 38 Línea de comando para reiniciar el servicio Postfix. Fuente(Autores).

Y por último y lo más importante al archivo "dovecot.conf" le habilitamos para que escuche IPV6 y así el servidor estará listo para recibir este tipo de peticiones en lo referente al nuevo protocolo.

```
Listen= [::]
```

Figura V. 39 /etc/dovecot.conf. Fuente: (Autores).

Luego reiniciamos el servicio

```
Service dovecot restart
```

Figura V. 40 Línea de comandos para reiniciar el servicio Dovecot. Fuente (Autores).

Fastnet posee una interfaz gráfica basada en web para el envío y recepción de correo electrónico, el cual es "Squirrelmail", este tipo de software basado en web soporta el nuevo protocolo, así que no se tiene que realizar ninguna modificación.

Con esto estamos listos para enviar y recibir correos electrónicos en DualStack.

5.3.5.3. SERVIDOR WEB

Para promocionar los planes de servicio de internet, así como información general de la empresa Fastnet cuenta con el servicio web.

Para que reciba peticiones IPv6 solo basta modificar un par de líneas en el archivo "httpd.conf".

Habilitamos el puerto 80 para recibir peticiones IPv6

```
Listen [DIR_IPV6_SERVER]:80  
  
Listen [::1]:80
```

Figura V. 41 /etc/httpd/conf/httpd.conf. Fuente: (Autores).

Y al final del mismo archivo agregamos

```
NameVirtualHost [DIR_IPV6_SERVER]:80[  
  
    <VirtualHost [DIR_IPV6_SERVER]:80>  
  
        DocumentRoot "/var/www/folder_IPv6/"  
  
        ServerName fastnet.net.ec  
  
        <Directory "/var/www/folder_IPv6/">  
  
            allow from all
```

Figura V. 42 /etc/httpd/conf/httpd.conf. Fuente: (Autores).

Luego reiniciamos el servicio

```
service httpd restart
```

Figura V. 43 Línea de comandos para reiniciar el servicio httpd. Fuente (Autores).

Con esta configuración el servidor está listo para resolver peticiones web tanto en IPV4 como en IPV6.

5.3.6. HERRAMIENTA DE MONITOREO

En el NOC de Fastnet se usa la herramienta "The Dude" para gestión y monitoreo, pero hasta la fecha de esta publicación no existe actualización para IPv6 en la plataforma DUDE.

Mediante DUDE la gestión de configuración no se ve afectada pero el monitoreo se pierde por lo que se recomienda la herramienta Nagios, para monitorear la red de Fastnet por los siguientes motivos.

- Soporta el nuevo protocolo IPv6.
- Los reportes se presentan como gráficas estadísticas.
- Customización de paneles.

- Se puede monitorear servidores, BD, puertos, switches, routers.
- Reportes programados
- Podemos crear nuestros propios Plugins para utilizarlos con Nagios, solo basta con tener conocimientos básicos de Python, C, C# o Perl.

Para lo cual necesitaríamos activar SNMP en los equipos remotos,

En la sección anexos se muestra la instalación, de Nagios, compiladores y configuración de Plugins.

5.4.ETAPA 4 PROPORCIONAR CONECTIVIDAD IPv6 A LOS NODOS Y CLIENTES EXISTENTES.

Una vez creado el plan de direccionamiento de las redes IPv6, podemos continuar con la asignación en los equipos de la red.

Para ello tenemos tres métodos:

- Configuración automática de direcciones sin estado (SLAAC)
- Protocolo de configuración dinámica de host para IPv6 (DHCPv6)
- Configurar direcciones IPv6 estáticas

La configuración automática a través SLAAC o DHCPv6 será la opción para la mayoría de los clientes porque esto hace que la gestión sea más fácil. Si se aplica correctamente, incluso podría aumentar la privacidad de los usuarios.

La configuración estática se dará para equipos como routers, switches, firewalls, servidores y enlaces.

5.4.1. DIRECCIONES IPv6 ESTÁTICAS

A continuación se realiza la asignación de direcciones ipv6 a los nodos, como se indicó la asignación debe ser de manera estática, seleccionando las direcciones de red del plan de direccionamiento

5.4.1.1. ROUTER DE CORE

En la tabla V.XII se asigna direcciones IPv6 a la interfaces del router Mikrotik RB1100AHX2:

TELCONET

1 2800:2a0:2400::/56

PRUEBAS

2 2800:2a0:2400:100::/56

HOSP. SAN JUAN

17 2800:2a0:2400:1000::/56

CACHA

81 2800:2a0:2400:5000::/56

SERVICIOS, NOC

210 2800:2a0:2400:d000::/56

Para la asignación tomamos cualquiera de las 256 subredes que contiene cada ip con un prefijo /64.

Por ejemplo tomaremos la segunda dirección para asignar a la interfaz que se conecta al router Telconet

- 2800:2a0:2400::/56

1 2800:2a0:2400::/64

2 2800:2a0:2400:1::/64

3 2800:2a0:2400:2::/64

4 2800:2a0:2400:3::/64

5 2800:2a0:2400:4::/64

6 2800:2a0:2400:5::/64

7 2800:2a0:2400:6::/64

8 2800:2a0:2400:7::/64

9 2800:2a0:2400:8::/64

10 2800:2a0:2400:9::/64

11 2800:2a0:2400:a::/64

12 2800:2a0:2400:b::/64

```

13          2800:2a0:2400:c::/64
14          2800:2a0:2400:d::/64
15          2800:2a0:2400:e::/64
16          2800:2a0:2400:f::/64
..          ..      ..      ..      ..
256         2800:2a0:2400:ff::/64
    
```

Tabla V. XII Direcciones IPv6 Router Core Hospital San Juan. Fuente (Autores)

HOST	INTERFACE	DIR IPV6 (GATEWAYS)	DESCRIPCION	PREFIJO
MIKROTIC- RB1100AHX2	ETH1	2800:2A0 :2400:1::1	CONEXIÓN TELCONET	/64
	ETH2	2800:2A0 :2400:D000::1	CONEXIÓN FASTNET	/64
	ETH3	2800:2A0 :2400:5000::1	CONEXIÓN CACHA	/64
	ETH4	2800:2A0 :2400:1000::1	CONEXIÓN HOSPITAL SAN JUAN	/64
	ETH5	Libre	-----	-----
	ETH6	Libre	-----	-----
	ETH8	2800:2A0 :2400:100::1	CONEXIÓN PARA PRUEBAS	
	ETH9	Libre	-----	-----

5.4.1.2. SERVICIOS

En la Tabla V.XIII se observa la asignación de direcciones para los servidores, físicamente se posee dos equipos por lo que el servidor web y mail están en un mismo servidor.

Tabla V. XIII Direcciones IPv6 en los servidores. Fuente (Autores).

HOST	DIR_IPV6	PREFIJO
SERVIDOR WEB	2800:2A0 :2400:D000::2	/64
SERVIDOR MAIL	2800:2A0 :2400: D000::2	/64
GESTIOIP Y DUDE	2800:2A0 :2400: D000::3	/64

A continuación se muestra la asignación de direcciones IPv6 a los equipos de cada nodo, como notación aquellas marcadas con rojo representan las direcciones para enlace y las restantes se identifican como direcciones de Gateway para enlazar clientes a la infraestructura:

5.4.1.3. NODO TERRAZA HOSPITAL SAN JUAN

DIRECCIÓN DE RED NIVEL 1

2800:2a0:2400:1000::/56

DIRECCIÓN GATEWAY

2800:2a0:2400:1000::1/64

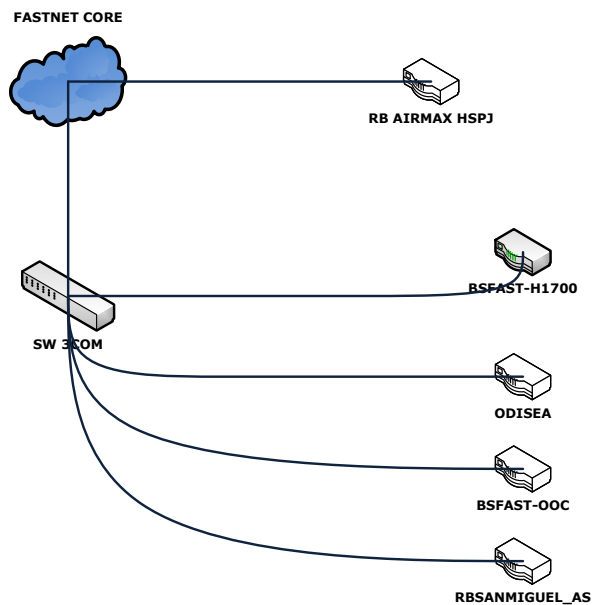


Figura V. 44 Equipos en el nodo Hospital San Juan. Fuente (autores).

Tabla V. XIV Asignación de direcciones. Fuente (Autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
RB AIRMAX HSPJ	2800:2A0 :2400:1001::/64	2800:2A0 :2400:1001::1/64
	2800:2A0 :2400:1002::/64	2800:2A0 :2400:1002::1/64
	2800:2A0 :2400:1003::/64	2800:2A0 :2400:1003::1/64
	2800:2A0 :2400:1004::/64	2800:2A0 :2400:1004::1/64
	2800:2A0 :2400:1005::/64	2800:2A0 :2400:1005::1/64
BSFAST H1700	2800:2A0 :2400:1006::/64	2800:2A0 :2400:1006::1/64
	2800:2A0 :2400:1007::/64	2800:2A0 :2400:1007::1/64
ODISEA	2800:2A0 :2400:1008::/64	2800:2A0 :2400:1008::1/64
	2800:2A0 :2400:1009::/64	2800:2A0 :2400:1009::1/64
BSFAST-OOC	2800:2A0 :2400:100A::/64	2800:2A0 :2400:100A::1/64
	2800:2A0 :2400:100B::/64	2800:2A0 :2400:100B::1/64
	2800:2A0 :2400:100C::/64	2800:2A0 :2400:100C::1/64
	2800:2A0 :2400:100D::/64	2800:2A0 :2400:100D::1/64
	2800:2A0 :2400:100E::/64	2800:2A0 :2400:100E::1/64
RBSAN MIGUEL_AS	2800:2A0 :2400:100F::/64	2800:2A0 :2400:100F::1/64
	2800:2A0 :2400:1010::/64	2800:2A0 :2400:1010::1/64
	2800:2A0 :2400:1011::/64	2800:2A0 :2400:1011::1/64

5.4.1.4. NODO CACHA

DIRECCION DE RED NIVEL 1

2800:2a0:2400:5000::/56

2800:2a0:2400:6000::/56

2800:2a0:2400:7000::/56

DIRECCION GATEWAY

2800:2a0:2400:5000::1/64

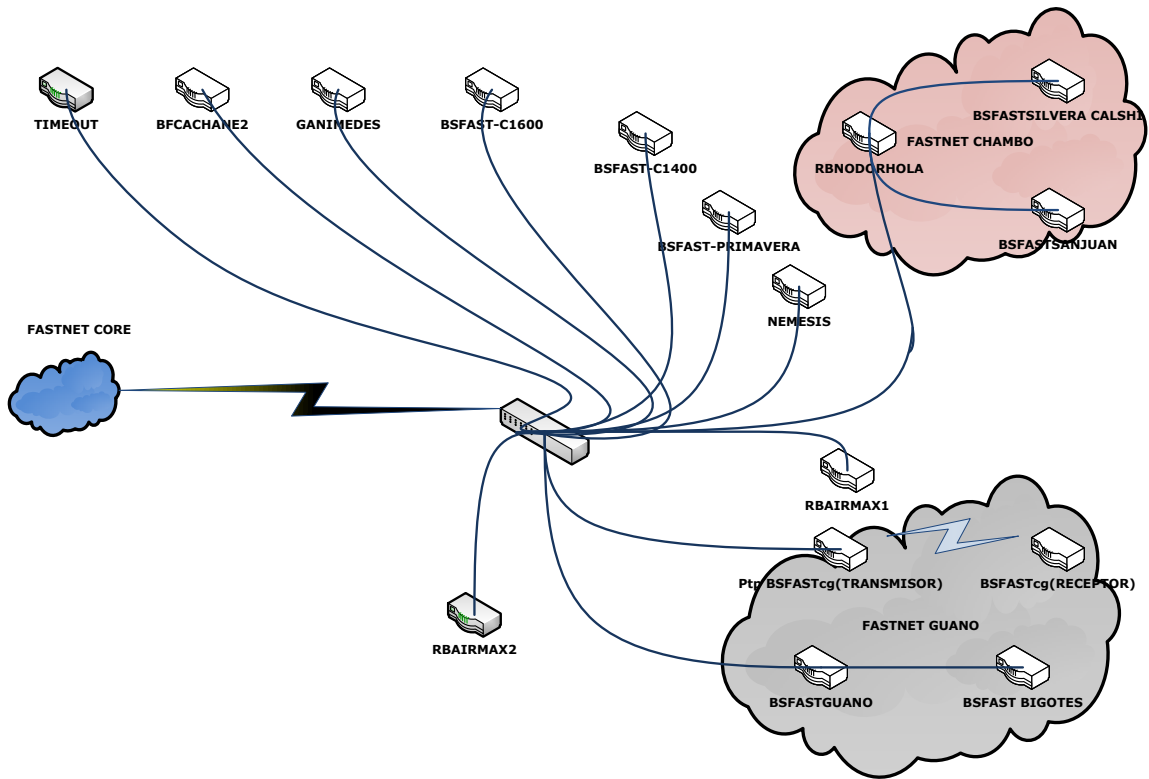


Figura V. 45 Equipos en el nodo Cacha. Fuente (autores).

En la tabla V.XV se muestra la asignación de direcciones en el nodo, recordemos que Cacha genera nodos secundarios orientado hacia los cantones Guano, Chambo.

Tabla V. XV Asignación de direcciones nodo Cacha. Fuente (autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
TIMEOUT	2800:2A0 :2400:5001::/64	2800:2A0 :2400:5001::1/64
	2800:2A0 :2400:5002::/64	2800:2A0 :2400:5002::2/64
BFCACHANE2	2800:2A0 :2400:5003::/64	2800:2A0 :2400:5003::1/64
	2800:2A0 :2400:5004::/64	2800:2A0 :2400:5004::1/64
GANIMEDES	2800:2A0 :2400:5005::/64	2800:2A0 :2400:5005::1/64

	2800:2A0 :2400:5006::/64	2800:2A0 :2400:5006::1/64
BSFAST-C1600	2800:2A0 :2400:5007::/64	2800:2A0 :2400:5007::1/64
	2800:2A0 :2400:5008::/64	2800:2A0 :2400:5008::1/64
BSFAST-C1400	2800:2A0 :2400:5009::/64	2800:2A0 :2400:5009::1/64
	2800:2A0 :2400:500A::/64	2800:2A0 :2400:500A::1/64
BSFAST-PRIMAVERA	2800:2A0 :2400:500B::/64	2800:2A0 :2400:500B::1/64
	2800:2A0 :2400:500C::/64	2800:2A0 :2400:500C::1/64
NEMESIS	2800:2A0 :2400:500D::/64	2800:2A0 :2400:500D::1/64
	2800:2A0 :2400:500E::/64	2800:2A0 :2400:500E::1/64
RBAIRMAX1	2800:2A0 :2400:500F::/64	2800:2A0 :2400:500F::1/64
	2800:2A0 :2400:500F::/64	2800:2A0 :2400:500F::1/64
	2800:2A0 :2400:5010::/64	2800:2A0 :2400:5010::1/64
	2800:2A0 :2400:5011::/64	2800:2A0 :2400:5011::1/64
	2800:2A0 :2400:5012::/64	2800:2A0 :2400:5012::1/64
RBAIRMAX2	2800:2A0 :2400:5013::/64	2800:2A0 :2400:5013::1/64
	2800:2A0 :2400:5014::/64	2800:2A0 :2400:5014::1/64
	2800:2A0 :2400:5015::/64	2800:2A0 :2400:5015::1/64
	2800:2A0 :2400:5016::/64	2800:2A0 :2400:5016::1/64

GUANO

Tabla V. XVI Asignación de direcciones en el nodo Guano. Fuente (autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
Ptp BSFASTcg(TRANSMISOR)	2800:2a0:2400:6000::/64	2800:2a0:2400:6000::1/64
	2800:2a0:2400:6001::/64	2800:2a0:2400:6001::1/64
BSFASTcg(RECEPTOR)	2800:2a0:2400:6000::/64	2800:2a0:2400:6000::2/64
	2800:2a0:2400:6002::/64	2800:2a0:2400:6002::1/64
BSFASTGUANO	2800:2a0:2400:6003::/64	2800:2a0:2400:6003::1/64
	2800:2a0:2400:6004::/64	2800:2a0:2400:6004::1/64
BSFAST BIGOTES	2800:2a0:2400:6004::/64	2800:2a0:2400:6004::2/64

CHAMBO

Tabla V. XVII Asignación de direcciones en el nodo Chambo. Fuente (autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
RBNODORHOLA	2800:2a0:2400:7000::/64	2800:2a0:2400:7000::1/64
	2800:2a0:2400:7001::/64	2800:2a0:2400:7001::1/64
	2800:2a0:2400:7002::/64	2800:2a0:2400:7002::1/64
	2800:2a0:2400:7003::/64	2800:2a0:2400:7003::1/64
	2800:2a0:2400:7004::/64	2800:2a0:2400:7004::1/64
	2800:2a0:2400:7005::/64	2800:2a0:2400:7005::1/64
	2800:2a0:2400:7006::/64	2800:2a0:2400:7006::1/64
	2800:2a0:2400:7007::/64	2800:2a0:2400:7007::1/64

	2800:2a0:2400:7008::/64	2800:2a0:2400:7008::1/64
BSFASTSILVERA CALSHI	2800:2a0:2400:7004::/64	2800:2a0:2400:7004::2/64
	2800:2a0:2400:7009::/64	2800:2a0:2400:7009::1/64
BSFASTSANJUAN	2800:2a0:2400:700A::/64	2800:2a0:2400:700A::1/64

5.4.1.5. GUAMOTE

DIRECCION DE RED NIVEL 1

2800:2a0:2400:8000::/56

DIRECCION GATEWAY

En este caso la salida se lo realiza directamente por el CPE del Carrier Telconet. En la Figura V.47 se observa los detalles de la conectividad que se presenta en el nodo Guamote.

ROUTER CISCO TELCONET

Tabla V. XVIII Direcciones IPv6 en Router Telconet. Fuente (autores)

Dirección IPv6	Interface	
2800:2A0:2400:2::1/64	Gigabit Ethernet 0/1	LAN

5.4.1.6. NODO DOLOROSA

DIRECCIÓN DE RED NIVEL 1

2800:2a0:2400:f000::/56

DIRECCIÓN GATEWAY

En este caso la salida se lo realiza directamente por el CPE del Carrier Telconet

ROUTER CISCO TELCONET

Tabla V. XX Direcciones IPv6 en Router Telconet. Fuente (autores)

Dirección IPv6	Interface	
2800:2A0:2400:3::1/64	Gigabit Ethernet 0/1	LAN

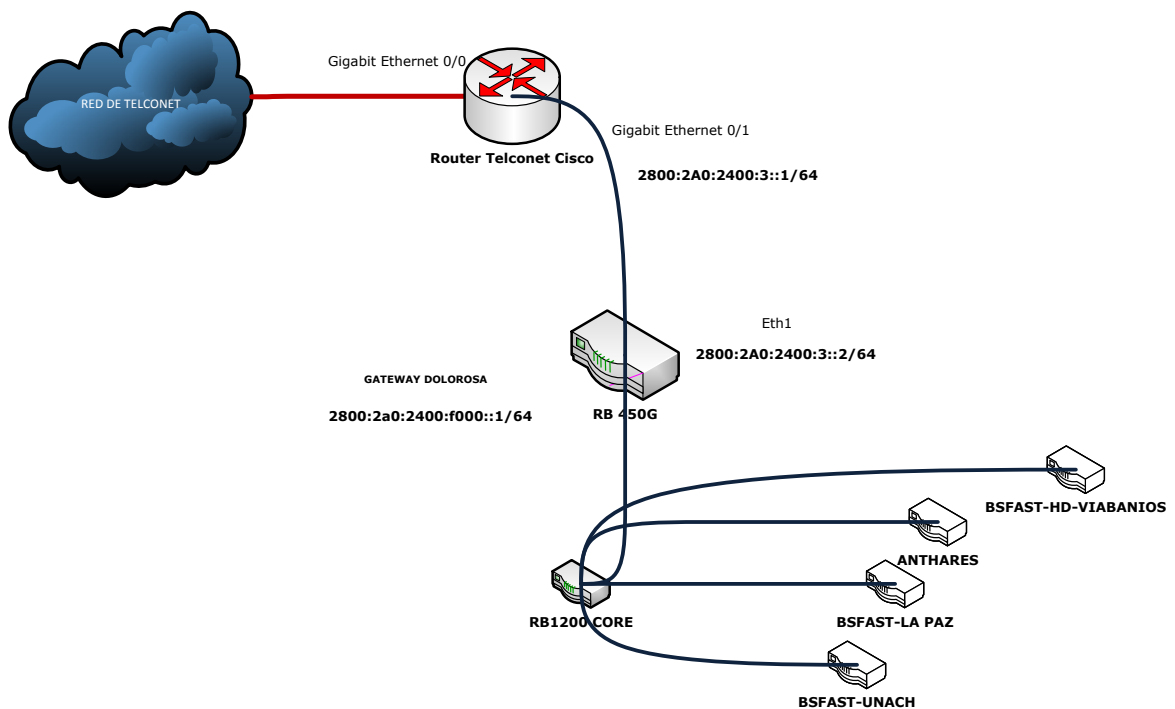


Figura V. 47 Equipos en el nodo Dolorosa. Fuente (autores).

Tabla V. XXI Asignación de direcciones en el Nodo Dolorosa. Fuente (autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
RB 450G	2800:2A0:2400:3::/64	2800:2A0:2400:3::2/64
	2800:2a0:2400:f000::/64	2800:2a0:2400:f000::1/64
RB 1200 CORE	2800:2a0:2400:f000::/64	2800:2a0:2400:f000::2/64
	2800:2a0:2400:f001::/64	
	2800:2a0:2400:f002::/64	
	2800:2a0:2400:f003::/64	
	2800:2a0:2400:f004::/64	
	2800:2a0:2400:f005::/64	
	2800:2a0:2400:f006::/64	
	2800:2a0:2400:f007::/64	
	2800:2a0:2400:f008::/64	
	2800:2a0:2400:f009::/64	
BSFAST-LA PAZ	2800:2a0:2400:f006::/64	2800:2a0:2400:f006::2/64
BSFAST-UNACH	2800:2a0:2400:f007::/64	2800:2a0:2400:f007::2/64
ANTHARES	2800:2a0:2400:f004::/64	2800:2a0:2400:f004::2/64
BSFAST-HD- VIABANIOS	2800:2a0:2400:f003::/64	2800:2a0:2400:f003::2/64

5.4.1.7. NODO POLITÉCNICA

DIRECCION DE RED NIVEL 1

2800:2a0:2400:9000::/56

DIRECCIÓN GATEWAY

En este caso la salida se lo realiza directamente por el CPE del Carrier Telconet. En la Figura V.49 se observa con más detalle la conectividad del nodo.

ROUTER CISCO TELCONET

Tabla V. XXII Direcciones IPv6 en Router Telconet. Fuente (autores)

Dirección IPv6	Interface	
2800:2A0:2400:4::1/64	Gigabit Ethernet 0/1	LAN

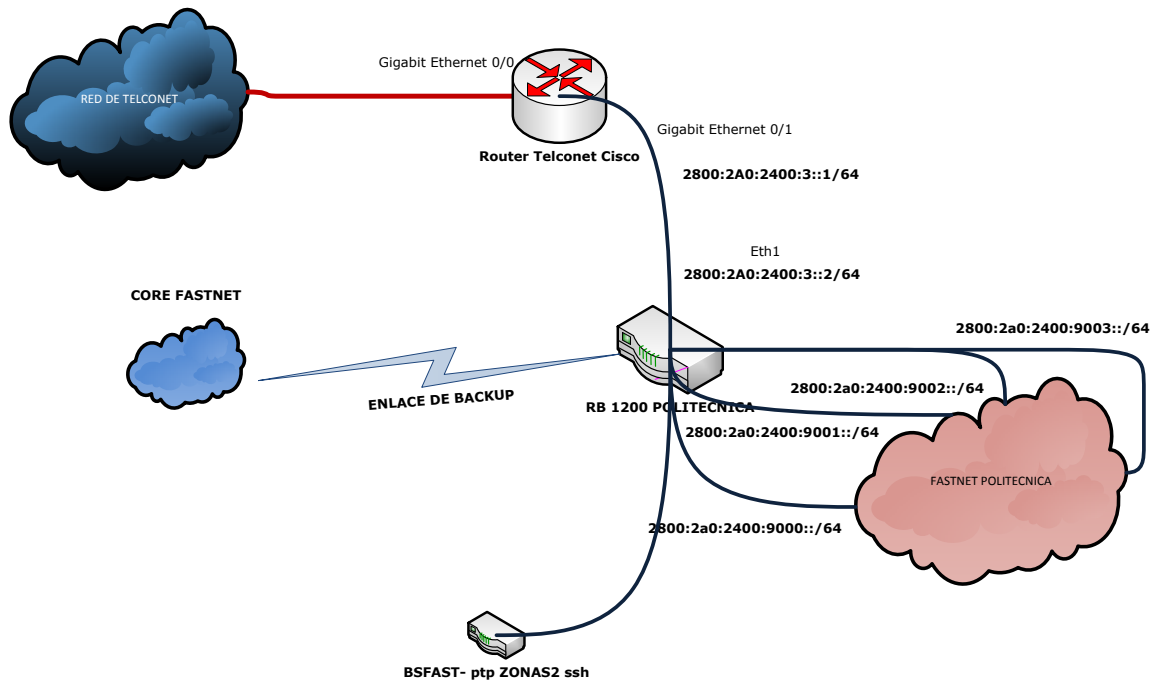


Figura V. 48 Equipos en el nodo Politécnica. Fuente (autores)

Tabla V. XXIII Asignación de direcciones del Nodo Politécnica Fuente (autores)

EQUIPO	DIRECCION	DIRECCION HOST IPv6
RB 1200 POLITECNICA	2800:2A0 :2400:4::/64	2800:2A0 :2400:4::2/64
	2800:2A0 :2400:9000::/64	2800:2A0 :2400:9000::1/64
	2800:2A0 :2400:9001::/64	2800:2A0 :2400:9001::1/64
	2800:2A0 :2400:9002::/64	2800:2A0 :2400:9002::1/64
	2800:2A0 :2400:9003::/64	2800:2A0 :2400:9003::1/64
	2800:2A0 :2400:9004::/64	2800:2A0 :2400:9004::1/64
	2800:2A0 :2400:9005::/64	2800:2A0 :2400:9005::1/64
BSFAST- ptp ZONAS2 ssh	2800:2A0 :2400:9005::/64	2800:2A0 :2400:9005::2/64

5.5. ETAPA 5 EXPANDIR IPv6 A TRAVÉS DE LA RED

Los mecanismos de transición se crearon para una convivencia de protocolos ip, por lo que la transición a IPv6 nativo dependerá de las tendencias del internet pues convertir la infraestructura en solo ipv6, en este momento seria incomunicarnos por lo que la etapa que se propone es a largo plazo, en donde las interfaces que corren en dual Stack pueden ser desactivadas progresivamente de acuerdo a las necesidades, políticas nacionales regionales y mundiales.

Según se investigó en el Ecuador la migración tomaría 5 años a partir del 2012 pero eso no significa que IPv4 desaparecerá, pero la implementación en dual Stack debe estar realizada hasta la capa de acceso del ISP FASTNET.

COMPROBACIÓN DE LA HIPÓTESIS

Por la naturaleza del tema objeto de estudio, la investigación se la considera como una investigación de tipo exploratoria. Lo que se pretende con este trabajo de investigación es realizar el análisis de las metodologías de migración a IPv6 que permita elaborar un modelo sistemático a una migración acorde a los requerimientos del ISP de la empresa Fastnet Cía. Ltda. de la ciudad de Riobamba, estudio que no ha sido realizado por ninguna empresa pública o privada para realizar dicha migración de una tecnología como la IPv6 en lugar de la IPv4 en la ciudad, razón por la cual se realizó este trabajo.

Los estudios exploratorios nos sirven para aumentar el grado de familiaridad con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular de la vida real, investigar problemas de comportamiento o cambios que se consideren cruciales en determinadas áreas, identificar conceptos o variables promisorias, establecen prioridades para investigaciones posteriores o sugerir afirmaciones (postulados) verificables, *Hernández y otros(1)*.

De los resultados obtenidos de la investigación, se puede determinar dos métodos hipotéticos:

El método hipotético inductivo, que no es más que ascender lógicamente a través del conocimiento científico, desde la observación de los fenómenos o hechos de la realidad a la ley universal que los contiene, *Hernández y otros(1)*. Según este método, se admite que cada conjunto de hechos de la misma naturaleza está regido por una Ley Universal. El objetivo científico es enunciar esa Ley Universal partiendo de la observación de los hechos, y el método hipotético-deductivo es el procedimiento o camino que siguió para la comprobación de la hipótesis, para la cual se siguieron varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno, y verificación o comprobación de la verdad de los enunciados deducidos comparándolos con la experiencia. Este método combina la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación).

Como método de verificación, la observación sistemática consiste en recoger datos de un comportamiento que para el caso es el uso de la tecnología IPv4 y que parámetros físicos y tecnológicos se requieren para realizar la migración a una nueva versión como es el IPV6, impactos y consecuencias tanto para la empresa proveedora de servicio de Internet como el servicio de calidad a los usuarios del mismo.

Se descarta la presencia de una hipótesis nula por la característica misma de la investigación, por lo que queda demostrada y comprobada la hipótesis planteada en este trabajo de investigación

CONCLUSIONES

1. Todas las metodologías de transición que se analizaron fueron de valiosa importancia, para emitir un criterio técnico de acuerdo a las necesidades del ISP, pues planificar hoy garantizará reducir el impacto del nuevo protocolo en la infraestructura.
2. De la investigación podemos ubicar al ISP, en el escenario que puede soportar IPv6 utilizando el mecanismo Dual Stack en un 100% en la capa de core, servicios email y web, 65% en la capa de distribución, 30% en la capa de acceso y 10% en los equipos terminales (CPE).
3. Un factor determinante en la elección del mecanismo de transición fue la coexistencia que deben tener los protocolos IPv4 e IPv6, esto se analizó y el mecanismo Dual Stack se ajusta a la situación del ISP pues el Carrier que proporciona la salida al internet cuenta con este mecanismo implementado.
4. De acuerdo a las políticas de asignación y distribución de direcciones por parte de IANA, el RIR LACNIC posee un prefijo /12, en la escala jerárquica Telconet es un ISP que le corresponde /32 y Fastnet al ser un usuario corporativo se le asignó un /48 con lo que nos permite tener 65.536 subred con 2^{64} direcciones para hosts.
5. Al crear un modelo sistemático garantizamos que en la futura implementación de la metodología se avance en forma rápida y eficiente con los procesos planificados.
6. Al desarrollar la propuesta técnica, evidenciamos que todos los routers de tipo Mikrotik tanto en la capa de core como de distribución soportan el protocolo IPv6 a través de actualizaciones de Firmware, pero es necesario cambiar los equipos de acceso y terminales de los clientes (CPEs).

7. Actualmente IPv6 no puede ser nativo en la red del ISP, ya que sería aislar la red del mundo, además considerando el requerimiento de la SENATEL, señala a los ISP y portadores nacionales que deberán admitir el curso normal del tráfico de IPv6 en coexistencia con IPv4.
8. Al iniciar con el desarrollo de la propuesta se evidencia la necesidad de una inversión inicial de \$98.968 en capacitación, compra de hardware y software, en el caso de Fastnet el análisis económico permitió determinar los costos generados en la transición, que será un valor distribuido en el tiempo reduciendo así la percepción de dicha inversión.
9. Se adquirió del carrier Telconet un prefijo /48, ya que se tenía la necesidad de crear diferentes subredes para los nodos del ISP.
10. Al realizar el subneting, se tiene dos niveles de redes, de primer nivel /56 para ser usadas en cada punto de la red y un prefijo /64 para que cada cliente sea visible en el internet.

RECOMENDACIONES

1. Se recomienda a la empresa Fastnet estar pendiente de la metodología de transición por parte del MINTEL, ya que se espera se cumplan los lineamientos ahí propuestos.
2. Se recomienda el establecimiento del mecanismo DUAL STACK en los equipos de FASTNET, ya que permitirá en el futuro desactivar IPv4 en las interfaces duales, de acuerdo al avance que tenga en las redes el nuevo protocolo.
3. Se recomienda el uso de las direcciones IPv6 con un prefijo de /64 para asignaciones en la parte de host ya que si se rompe el /64, desaparecen muchas de las ventajas de IPv6 como autoconfiguración, privacidad, CGAs (Cryptographically Generated Addresses). Así que no es conveniente, y más bien al contrario es incorrecto, hacer Subnetting por debajo del /64.
4. Se recomienda el uso de subredes / 64 incluso para enlaces punto a punto.
5. Se recomienda a la empresa FASTNET que en el futuro, todas las nuevas adquisiciones en hardware y software que realice tendrán que ser compatible con IPv6.
6. Para mejorar significativamente la presencia de IPv6 en la red, se recomienda cambiar los equipos en la red acceso y los CPE de clientes, estos últimos deben promoverse en los futuros usuarios del servicio.
7. Promover el uso de software libre con soporte IPv6 abarata costos de implementación.
8. En los servidores, actualizar el S.O Centos es de vital importancia al momento de realizar las configuraciones para los servicios que correrán bajo el mismo, con ello se tendrá un mejor desempeño del S.O.

9. Al desarrollar el proceso de migración, evidenciamos que el recurso humano debe estar completamente capacitado para realizar implementaciones, esto permite avanzar en forma segura y eficiente en los procesos.
10. Se recomienda un plan de seguridad para el protocolo IPv6 en la red, mikrotik presenta un Firewall para IPv6.
11. Adicionalmente es necesario crear VLANS en los switch capa 3 que se hallan en la infraestructura, para disminuir el dominio de broadcast, mejorar la seguridad y la administración de la red, entre otras características propias que se dan al configurar este método.
12. Finalmente se recomienda a la comunidad universitaria realice estudios sobre herramientas de monitoreo y gestión sobre una red IPv6, este último generaría gran interés a empresas proveedoras de internet.

RESUMEN

Se investigó las metodologías de migración de IPv4 hacia IPv6, aplicada en una propuesta de migración para el Proveedor de Servicios de Internet (ISP) FASTNET CIA LTDA, para la cobertura en la provincia de Chimborazo.

El presente estudio empleó el método analítico que permite descomponer las partes del nuevo protocolo para ser analizadas, también se usó la síntesis para relacionar las mejores prácticas de procesos de convivencia/migración hacia el protocolo IPv6 en infraestructuras orientadas a brindar servicios de telecomunicaciones que se adapte a las necesidades de ISP, además se utilizó técnicas de revisión bibliográfica para desarrollar planes de direccionamiento, conectividad, y conmutación de la red.

Se usó la infraestructura de Fastnet, que cuenta con una combinación de tecnologías como CISCO, MIKROTIK, UBIQUITI, servidores en Centos, DUDE y GESTIOIP (software de gestión de redes y usuarios respectivamente).

De la investigación podemos ubicar al ISP, en el escenario que puede soportar IPv6 utilizando el mecanismo Dual Stack en un 100% en la capa de core, servicios email y web, 65% en la capa de distribución, 30% en la capa de acceso, 10% en los equipos terminales (CPE).

Las metodologías analizadas permitió crear un proceso sistemático de convivencia de protocolos, que concluye como necesidad que el mecanismo Dual Stack sea el más adecuado porque permitirá en el largo plazo que la transición sea gradual, y se ajuste a los requerimientos de las políticas nacionales y regionales en la adopción de IPv6.

Se recomienda al ISP FASTNET cambiar los equipos en la capa de acceso y equipos terminales para mejorar la presencia del nuevo protocolo. Finalmente este punto puede ser el inicio de un nuevo servicio para sus usuarios, ya que actualmente en el Ecuador solo grandes Carriers de Telecomunicaciones brindan IPv6.

SUMMARY

Methodologies for migration from IPv4 to IPv6 were investigated; it was applied in a proposed migration to the Internet Service Provider (ISP) FASTNET CIA LTDA, for coverage in the province of Chimborazo.

This study used the analytical method to decompose the parts of new protocol to be analyzed; synthesis was also used to relate the process best practices for coexistence/migration to IPv6 protocol in infrastructure aimed at providing telecommunications service suit ISP needs, further literature review techniques were used to develop plans addressing, connectivity, and network communication.

We used FASTNET infrastructure, with a combination of technologies such as CISCO MIKROTIK, UBIQUITI, CENTOS servers, DUDE and GESTIOIP (network management software and users respectively).

From the research we can locate the ISP, in the scenario that can support IPv6 by using Dual Stack mechanism by 100% in the core layer, email and web services, 65% in the distribution layer, 30% in the access layer, 10% in the terminal equipment (CPE).

The methodologies discussed made possible to establish a systemic process of coexistence of protocols, which concludes as a need that Dual Stack mechanism is most appropriate because in the long run will allow the transition to be gradual, and conforms to the requirements of national and regional policies in the adoption of IPv6.

It is recommended to FASTNET ISP to change the equipment in the acces layer and terminal equipment to enhance the presence of the new protocol. Finally, this point maybe the start of a new service for its users, as currently in Ecuador only major Telecommunications Carriers provided IPv6.

GLOSARIO

6in4: Es un mecanismo de transición que encapsula IPv6 dentro de IPv4 por medio del protocolo 41.

6over4: Es un mecanismo de transición que permite conectividad IPv6 utilizando una infraestructura IPv4 multicast.

6PE: Es un mecanismo de transición de IPv6 en infraestructuras MPLS.

6rd: Es un mecanismo de transición que se basa en 6to4; es un súper conjunto de 6to4.

6to4: Es un mecanismo de transición que permite conectividad automática IPv6, cliente a cliente a través de una infraestructura IPv4. Utiliza la dirección IPv4 pública para construir un prefijo global IPv6(/48).

Anycast: Dirección IPv6 que identifica a múltiples interfaces y la entrega del paquete se lo realiza a una sola interfaz generalmente la más cercana.

CGN: También conocido como DS-Lite o Carrier Grade NAT.

Datagrama: Es la estructura interna de un paquete de datos.

DHCPv6: Protocolo de configuración con estado "stateful", proporciona direcciones IPv6, e información de los DNS.

DMZ: Es una red local que se ubica entre la red interna y una red externa, generalmente el Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada.

EUI-64: Dirección del nivel de enlace de 64 bits.

Link-local address: Dirección IPv6 que es asignada a una interfaz y solo es válida para comunicarse en ese enlace.

Metro Ethernet: Es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN .

Multicast: Dirección que identifica a un grupo de interfaces.

Nibble: Es el conjunto de cuatro dígitos binarios o medio octeto.

Nodo: Cualquier dispositivo que tiene una dirección ip asignada.

RouterOS: Sistema Operativo Mikrotik.

Softwires: Es un mecanismo de transición basado en L2TP.

TCP: Se ubica en la capa de red del modelo OSI, asegura la llegada de paquetes a su destino.

Túnel: Mecanismo de transición que permite atravesar redes IPv4 con tráfico IPv6, o bien redes IPv6 con tráfico IPv4, mediante el encapsulado de un protocolo en el otro.

Tunnel Broker: Es un mecanismo de transición que permite automatizar el uso de túneles.

UDP: Se ubica en la capa de transporte del modelo TCP/IP. No proporciona detección de errores. No es orientado a la conexión.

Unicast: Dirección IPv6 que identifica a una solo interfaz y permite la conectividad punto a punto.

Firmware: Lenguaje máquina, grabado en una memoria de lectura/escritura, que controla la lógica de un circuito electrónico.

ANEXOS

ANEXO 1

INSTALACIÓN DE NAGIOS 4.0.0 BAJO CENTOS.

Antes de instalar Nagios necesitamos varios compiladores adicionales para el perfecto funcionamiento de esta valiosa herramienta de monitorización.

Entonces iniciamos instalando dichos requerimientos; gcc, gd y otros adicionales.

```
[root@servercentos etc]# yum install -y gcc gd gd-devel net-snmp-utils net-snmp  
openssl openssl-devel
```

INSTALACIÓN DE COMPILADORES, PARA NAGIOS.

Es de vital importancia crear usuarios para Nagios y agregarlos a un grupo.

Creamos el grupo nagcmd

```
[root@servercentos etc]# /usr/sbin/groupadd nagcmd
```

Creación de usuarios para administrar Nagios

```
[root@servercentos etc]# /usr/sbin/useradd -m nagiosadmin
```

Ahora agregamos al usuario "nagiosadmin" y a apache al grupo nagcmd.

```
[root@servercentos ~]# usermod -a -G nagcmd nagiosadmin  
[root@servercentos ~]# usermod -a -G nagcmd apache
```

Descomprimos NAGIOS.

```
[root@servercentos Desktop]# tar xzvf nagios-4.0.0.tar.gz
```

Ejecutamos el script de configuración, pasándole el grupo que creamos anteriormente.

```
[root@servercentos etc]# ./configure -with-command-group=nagcmd
```

Compilamos el programa principal y asignamos los respectivos permisos al directorio donde están los comandos externos.

```
[root@servercentos nagios]# make all
```

Instalamos los binarios.

```
[root@servercentos nagios]# make install
```

Instalamos los script para el inicio automático bajo /etc/rc.d/init.d

```
[root@servercentos nagios]# make install-init
```

Instalamos los comandos externos.

```
[root@servercentos nagios]# make install-commandmode
```

Todos los archivos de "ejemplo" de configuración han sido instalados en el directorio /usr/local/nagios/et, en este path se pueden revisar los mismos.

Instalamos la interfaz web

```
[root@servercentos nagios]# make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
*** Nagios/Apache conf file installed ***
```

INSTALACIÓN DE PLUGINS PARA NAGIOS

Descomprimos los plugins.

```
[root@servercentos Desktop]# tar xzvf nagios-plugins-1.5.tar.gz
```

Compilamos los plugins

```
[root@servercentos nagios-plugins-1.5]# ./configure --with-nagios-user=adminnagios --with-nagios-group=admins
```

Construimos e instalamos.

```
[root@servercentos nagios-plugins-1.5]# make
```

```
[root@servercentos nagios-plugins-1.5]# make install
```

Configuramos para que Nagios arranque al iniciar el servidor

```
[root@servercentos nagios-plugins-1.5]# chkconfig --add nagios
[root@servercentos nagios-plugins-1.5]# chkconfig nagios on
```

Cambiamos la configuración de alertas, para poder recibir en nuestro mail.

```
#####
#####
#
# CONTACTS
#
#####
#####

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-contact'
# template which is defined elsewhere.

define contact{
    contact_name      nagiosadmin           ; Short name of user
    use                generic-contact       ; Inherit default values from gen
eric-contact template (defined above)
    alias              Nagios Admin         ; Full name of user
    email              rodrigoigm@gmail.com ; <<***** CHANGE THIS TO YOUR EMA
IL ADDRESS *****
}
}
```

Verificamos los archivos de configuración de Nagios. Aquí vemos si existen errores.


```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

```
Running pre-flight check on configuration data...

Checking objects...
  Checked 8 services.
  Checked 1 hosts.
  Checked 1 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 1 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
[root@servercentos nagios]#
```

Si todo estuvo bien, iniciamos Nagios.

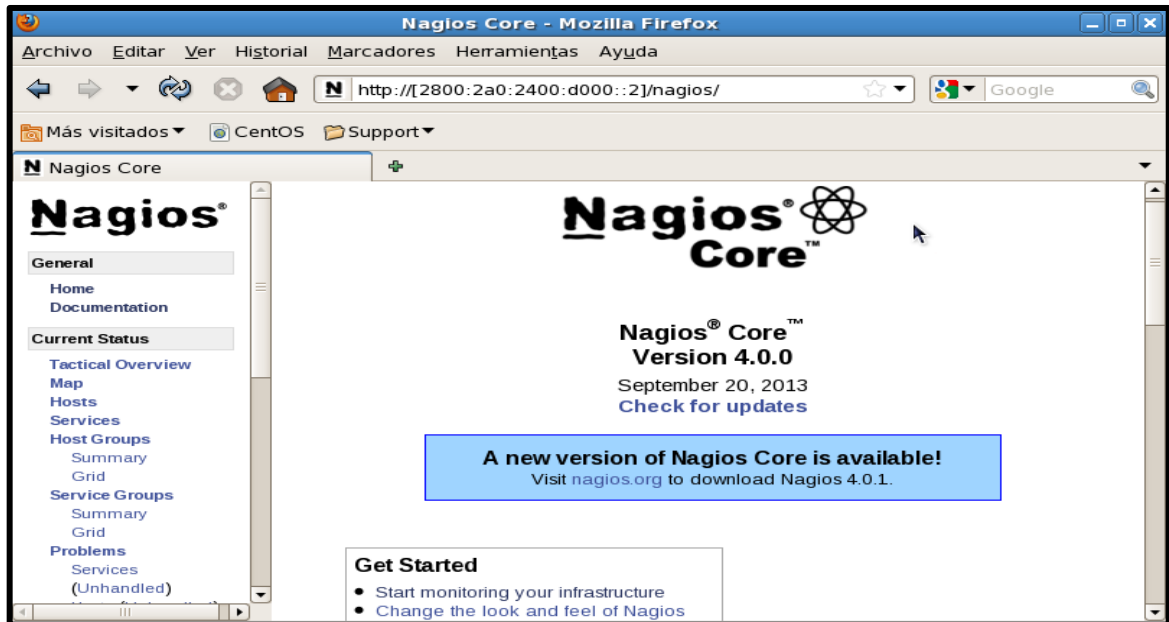
```
[root@servercentos nagios]# service nagios start
nagios está parado
Iniciando nagios: [ OK ]
[root@servercentos nagios]#
```

Instalado todo arrancamos Nagios desde una interfaz web digitando en la barra del browser.

La dirección IPv6 del servidor seguido de un "/nagios".



Y nos muestra la pantalla de Nagios.



Hasta ahora hemos visto la instalación de Nagios, tal como está no soporta el protocolo IPv6, para dicho cometido necesitamos instalar los plugins "Nagios Plugin 1.5".

DESCARGAMOS LOS PLUGINS

```
wget https://www.nagios-plugins.org/download/nagios-plugins-1.5.tar.gz
```

Descomprimos

```
tar zxvf nagios-plugins-1.5.tar.gz
```

Ingresamos al directorio

```
cd /tmp/nagios-plugins-1.5
```

Entonces instalamos

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

```
make
```

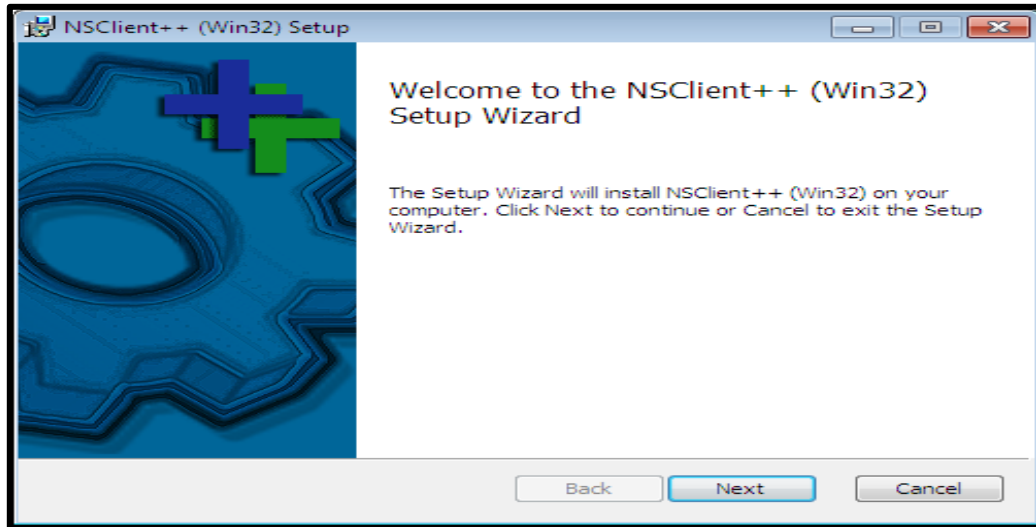
```
make install
```

MONITOREAR HOST CON S.O WINDOWS MEDIANTE NAGIOS.

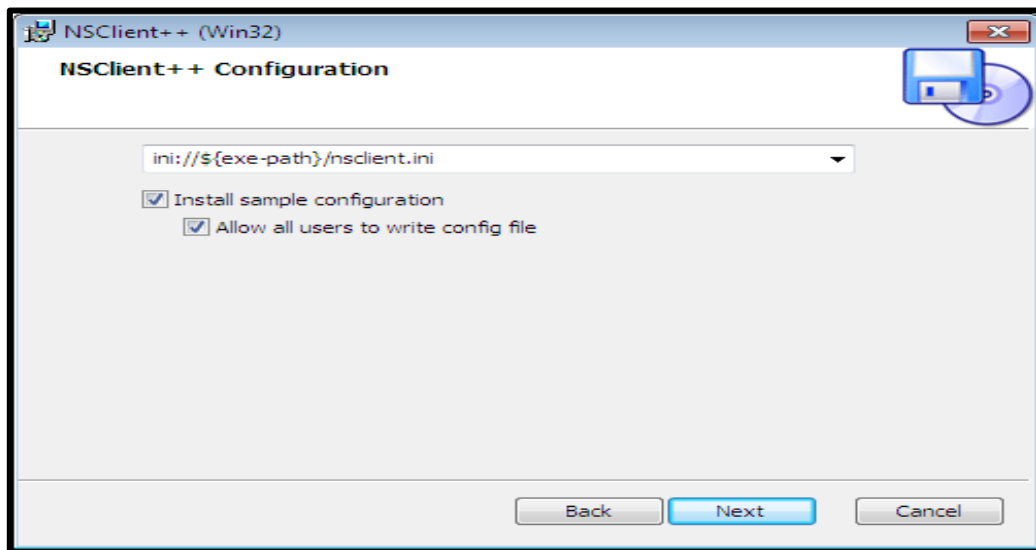
Para realizar este apartado se necesita instalar un agente, el mismo que actúa como un proxy entre el plugin de Nagios quien se encarga del monitoreo de host bajo Windows. Sin instalar dicho agente en Windows, Nagios no podrá monitorear servicios privados o atributos de Windows.

En el host con el S.O Windows necesitamos instalar el agente NSClient++ o NC_NET para poder comunicarse con el servidor que tiene Nagios, y a la vez el servidor Nagios debe tener instalado el plugin check_nt.

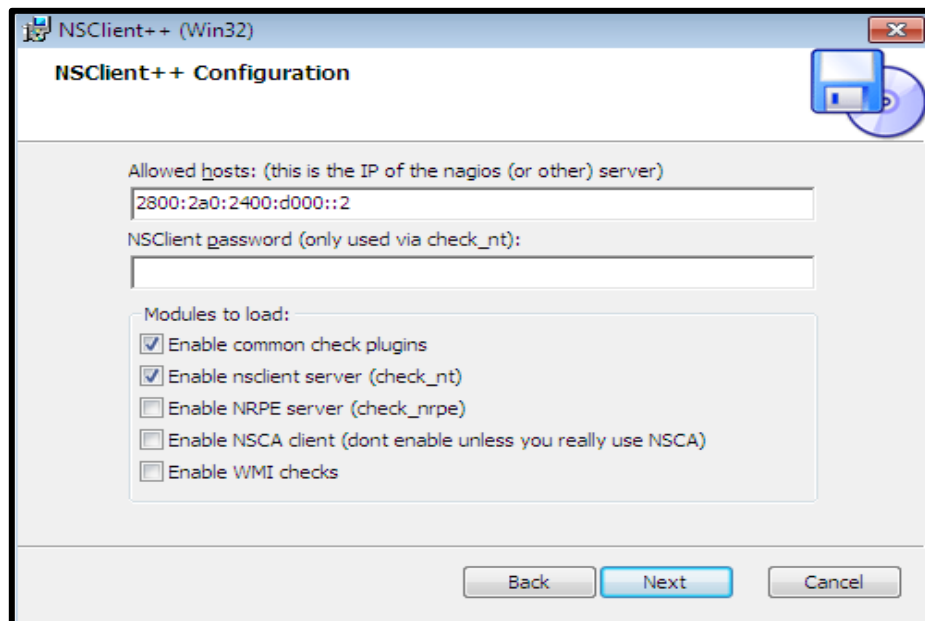
Bajo Windows instalamos NSClient++ 32bits o 64 bits .msi ver.0.4.1.102



La siguiente pantalla nos muestra la instalación de archivos de configuración y permisos de escritura.



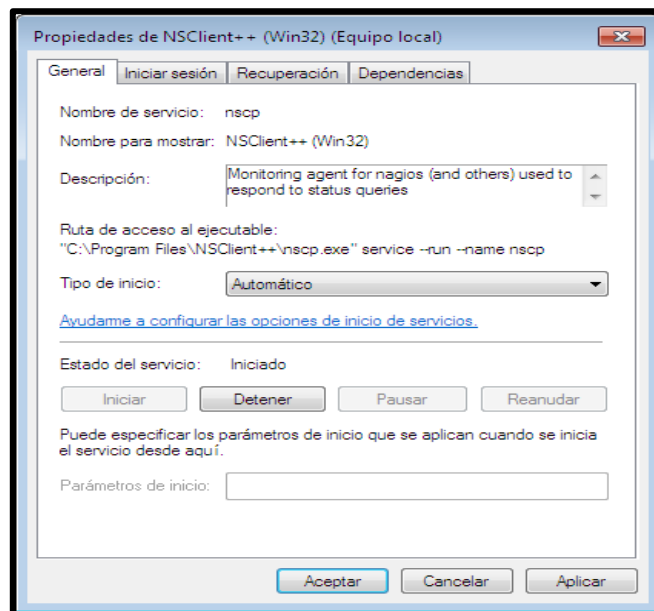
A continuación tenemos que ingresar la dirección IPv6 del servidor nagios.



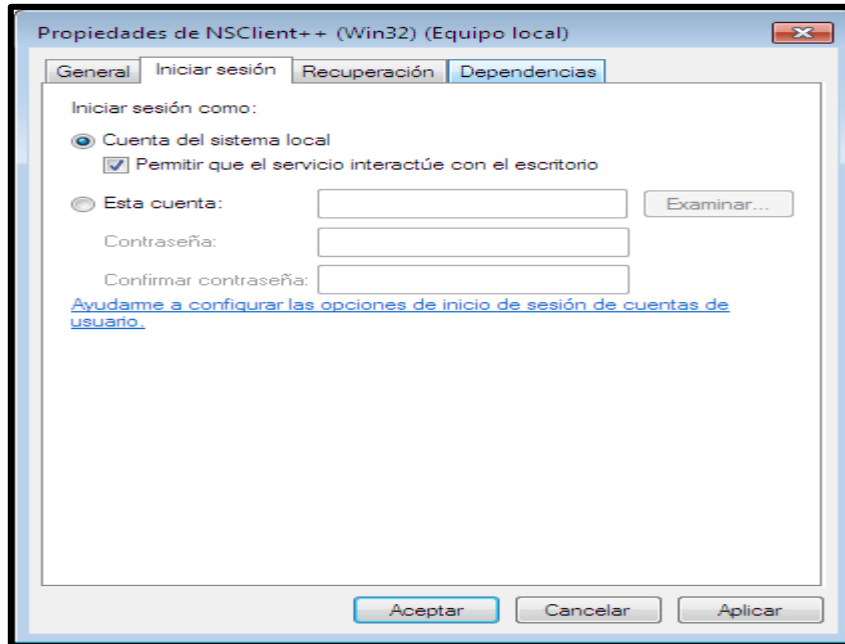
El servicio de NSClient server y NRPE server, nos permitirá recopilar la información del equipo.

Luego verificamos que el servicio este iniciado.

En la consola de ejecutar escribimos "services.msc" entonces seleccionamos NSClient++ (win32), en la pestaña "General" y luego en tipo de inicio automático, como se muestra en la figura a continuación.



También en la misma ventana pero en la pestaña " Iniciar sesión", seleccionamos permitir que el servicio interactúe con el escritorio.



SUPERVISANDO CON NAGIOS S.O WINDOWS.

Ahora monitorearemos una PC con win7, para esto necesitamos el nombre de la PC, que en este caso será "ad-PC".

El siguiente path "/usr/local/nagios/etc /nagios.cfg" habilitamos la línea quitando el signo numeral, como se muestra a continuación,

```
vi /usr/local/nagios/etc /nagios.cfg
```

```
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
```

Bajo Nagios para poder monitorear un host con Windows tenemos que modificar varios parámetros como se muestra a continuación.

Cambiamos el nombre y dirección del Pc en la sección host, para Windows.

```
# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
    use                windows-server ; Inherit default values from a template
    host_name          ad-PC ; The name we're giving to this host
    alias               ad-PC ; A longer name associated with the host
    address             2800:2a0:2400:d000::20 ; IP address of the host
}
```

Modificamos solamente el nombre del Pc, en la parte de servicios.

```
# Create a service for monitoring the version of NSClient++ that is installed
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name           ad-PC
    service_description NSClient++ Version
    check_command       check_nt!CLIENTVERSION
}
```

Modificamos la parte de servicios adicionales, con el nombre del Pc.

```
# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name           ad-PC
    service_description Uptime
    check_command       check_nt!UPTIME
}
```

Servicio para monitorear la carga del CPU.

```
# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          ad-PC
    service_description CPU Load
    check_command      check_nt!CPULOAD!-l 5,80,90
}
```

Servicio para monitorear memoria en uso.

```
# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          ad-PC
    service_description Memory Usage
    check_command      check_nt!MEMUSE!-w 80 -c 90
}
```

Servicio para monitorear espacio en disco.

```
# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          ad-PC
    service_description C:\ Drive Space
    check_command      check_nt!USEDISKSPACE!-l c -w 80 -c 90
}
```

Servicio para monitorear Explorer.exe


```
# Create a service for monitoring the Explorer.exe process
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          ad-PC
    service_description Explorer
    check_command      check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}

```

Lo que acabamos de hacer es permitir a Nagios que pueda visualizar definiciones adicionales de objetos.

REINICIAMOS EL SERVICIO DE NAGIOS.

Service Nagios restart

Después de esto NAGIOS nos detecta la pc.

Host Status Details For All Host Groups

Limit Results:

Host	Status	Last Check	Duration	Status Information
ad-PC	UP	10-10-2013 04:24:28	0d 0h 5m 20s	(No output on stdout) stderr:
localhost	UP	10-10-2013 04:25:21	0d 10h 6m 31s	(No output on stdout) stderr:

Results 1 - 2 of 2 Matching Hosts

Así, si una interfaz de red cae, NAGIOS detectara.

Host Status Details For All Host Groups

Limit Results:

Host	Status	Last Check	Duration	Status Information
ad-PC	DOWN	10-10-2013 04:33:27	0d 0h 0m 29s	(No output on stdout) stderr:
localhost	UP	10-10-2013 04:30:21	0d 10h 12m 41s	(No output on stdout) stderr:

Results 1 - 2 of 2 Matching Hosts

SUPERVISANDO CON NAGIOS S.O LINUX

Creamos el usuario "nagios" y el grupo "nagios".

```
Adduser nagios
```

```
Adduser nagios nagios
```

Instalamos los plugins

```
tar zxvf nagios-plugins-1.5.tar.gz
```

ingresamos al directorio

```
cd /tmp/nagios-plugins-1.5
```

entonces instalamos

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

```
make
```

```
make install
```

Luego instalamos xinetd

```
Yum -y install xinetd
```

Configuraremos NRPE para entornos Linux. Entonces iniciamos en el host remoto.

Descomprimos el archivo de NRPE- 2.15.tar.gz

```
tar xzf nrpe-2.15.tar.gz
```

Cambiamos de directorio

```
cd nrpe-2.15
```

Compilamos

```
./configure
```

make all

make install-plugin

make install-daemon

make install-daemon-config

Ahora tenemos que instalar dicho demonio "NRPE" como un servicio de xinetd.

make install-xinetd

Tenemos que editar el archivo /etc/xinetd.d/nrpe y agregamos la direccion IPV6 del servidor Nagios en la siguiente directiva.

```
Only_from= 2800:2^0:2400:d000::30
```

También tenemos que agregar la siguiente entrada para el demonio NRPE en el archivo

/etc/services

```
nrpe 5666/tcp #NRPE
```

Procedemos a reiniciar el servicio.

```
Service xinetd restart
```

Verificamos si el demonio esta ejecutándose bajo xinetd.

```
netstat -a | grep nrpe
```

Si todo va bien debemos observar lo siguiente

```
tcp 0 0 *:nrpe *: * LISTEN
```

Podemos editar las definiciones de los comandos ingresando a /usr/local/nagios/etc/nrpe.cfg

INSTALAR NRP EN EL SERVIDOR DE NAGIOS

Instalamos el archivo NRP en el servidor para esto seguimos los mismos pasos que en el apartado anterior.

Comprobamos la comunicación con el demonio NRPE, nos aseguramos que el plugin check_nrpe puede hablar con el demonio NRPE en el host remoto.

Para esto digitamos

```
IPv6 host remoto: 2800:2a0:2400:d000::30
```

```
/usr/local/nagios/libexec/check_nrpe -H 2800:2a0:2400:d000::30
```

Si se muestra un mensaje con la versión de NRPE todo va bien, caso contrario revise el firewall, iptables, etc.

Para utilizar check_nrpe, tenemos que definir comandos en uno de los archivos de configuración de Nagios.

```
vi /usr/local/nagios/etc/commands.cfg
```

```
define command{  
    command_name check_nrpe  
    command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$  
}
```

Luego de esto agregamos los servicios a ser monitoreados.

Comprobamos los archivos de configuración en el servidor Nagios.

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Si todo va bien reiniciamos Nagios.

```
service nagios restart
```

CAPÍTULO VI

BIBLIOGRAFÍA

1. HERNÁNDEZ, R. Y OTROS., Metodologías de Investigación., 4ta. edición., México D.F-México., McGranw-Hill., pp. 121-155.

2. BOCCIA, O. Y OTROS., Las telecomunicaciones de Banda Ancha en la Región Américas., Asunción-Paraguay., UIT., 2006., Pp. 4-67.

http://www.itu.int/ITU-D/finance/Work%20on%20Financing/Telecom_Banda_Ancha_Latinoamerica-sp.pdf

3. CUBA., LACNIC., Manual de Políticas., La Habana-Cuba., 2012., Pp. 26.

4. DÍAZ, M. Y OTROS., Despegando con movilidad IPv6 (MIPv6)., Guayaquil-Ecuador., ConsulIntel., 2007., Pp.1-5.

http://www.ist-enable.eu/open/enable_pu_paper_consulintel_despegando_con_MIPv6_AUI_v1_5.pdf

5. ECUADOR., MINISTERIO DE TELECOMUNICACIONES., Acuerdo N° 007-2012., Quito-Ecuador., 2012., Pp. 2-3.

6. ECUADOR., MINISTERIO DE TELECOMUNICACIONES., Acuerdo N° 039-2012., Quito-Ecuador., 2012., Pp. 1-3

7. GAGLIANO, R., Planificando IPv6., Quito-Ecuador., Lacnic., 2009., Pp.2-86.

<http://lacnic.net/documentos/lacnicxii/presentaciones/Planificacion.pdf>

8. PALET, J. Y OTROS., IPv6 para todos., Buenos Aires-Argentina., DCV Anahí Maroñas., 2012., Pp.43-48.

<http://www.ipv6tf.org/pdf/ipv6paratodos.pdf>

9. PALET, J., Introducción a IPv6., Panamá-Panamá., ConsulIntel., 2001., Pp.67.

http://long.ccaba.upc.es/long/050Dissemination_Activities/jordi_palet_tutorialipv6introduccion.pdf

10. SUPERTEL., IPv6 en el Ecuador., Revista institucional Vol.1, N° 14., Don Bosco., 2012., Pp. 9-10.

11. SUPERTEL., El ABC de la banda ancha: Condiciones de operación beneficios situación actual protocolo de internet., Revista institucional Vol.1, N° 17., Don Bosco., 2012., Pp. 5-8

12. NÚÑEZ, D., Estudio para la migración de IPV4 a IPV6 para la empresa proveedora de internet MILLTEC S.A., Facultad de Ingeniería Eléctrica y Electrónica., Escuela de Ingeniería Electrónica y Redes de Información., Escuela Politécnica Nacional., Quito-Ecuador., **TESIS.**, 2009., Pp. 59-63.

13. RAMÍREZ, D., Investigar y desarrollar una guía metodológica de los mecanismos de transición y coexistencia ipv4-ipv6 en el área de sistemas de la facultad de ingeniería de la universidad nacional de Chimborazo., Facultad de Ingeniería., Escuela de Sistemas y

Computación., Universidad Nacional del Chimborazo., Riobamba-Ecuador., **TESIS.**, 2010; Pp. 24.

- 14. SILVA, L.,** Estudio y análisis del estado actual de la implantación de ipv6 en los proveedores de servicios de internet a nivel nacional., Facultad de Ingeniería Eléctrica y Electrónica., Ingeniería Electrónica y Redes de Información., Escuela Politécnica Nacional., Quito-Ecuador., **TESIS.**, 2009., Pp.22-23-66-128.

15. ACUERDOS DEL MINISTERIO DE TELECOMUNICACIONES.

http://www.ipv6tf.ec/site/index.php?option=com_remository&Itemid=61&func=fileinfo&id=4

2013-08-02

<http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/10/Acuerdo-No.-039-2012.pdf>

2013-08-02

16. ASIGNACIÓN DE DIRECCIONES IPv6

<http://lacnic.net/documentos/politicas/manual-politicas-sp-1.10.pdf>

2012-08-13

17. CARRIER GRADE NAT

<http://tools.ietf.org/html/rfc6264>

2013-06-17

18. DIRECCIONES IPV6 RESERVADAS

<http://www.freebsd.org>

2013-04-23

19. FRECUENCIA DE MODULACIÓN DIGITAL DE BANDA ANCHA

<http://www.conatel.gob.ec>

2013-04-03

20. HERRAMIENTAS DE TRANSICIÓN

<http://www.cu.ipv6tf.org/talleripv6-2008/5.pdf>

2013-06-15

21. HERRAMIENTAS DE MONITOREO IPV6

[http://www.qosient.com/argus/Analisis de las herramientas](http://www.qosient.com/argus/Analisis%20de%20las%20herramientas)

2013-05-04

<http://oss.oetiker.ch/smokeping>

2013-05-04

<http://www.nagios.org/>

2013-05-04

<http://www.athtek.com/index.html>

2013-05-04

<http://www.protocolsoftware.com/hp-openview-downloads.php>

2013-05-04

<http://www.es.paessler.com/>

2013-05-04

<http://www.mrtg.com/>

2013-05-04

<http://www.cacti.net>

2013-05-04

22. IMPLEMENTACIÓN 6TO4

<http://tools.ietf.org/html/rfc6343>

2013-07-12

23. ISATAP

<http://tools.ietf.org/html/rfc5214>

2013-05-19

24. MANUAL IPv6

<http://lacnic.net/sp/politicas/manual5.html>

2012-08-13

25. MIGRACIÓN IPv6

<http://portalipv6.lacnic.net/es/ipv6/ipv6-en/isps>

2012-01-17

26. MECANISMOS DE TRANSICIÓN

<http://www.youtube.com/watch?v=E1g2O2N-LX8>

2013-04-20

27. NAT64

<http://tools.ietf.org/html/rfc6146-1>

2013-03-14

28. RECOMENDACIONES IPV6 EN 3GPP

<http://www.ietf.org/rfc/rfc3314.txt>

2013-07-12

29. TUTORIAL IPv6

<http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf>

2013-06-12

30. TEREDO

<http://www.ietf.org/rfc/rfc4380.txt>

2013-05-18

31. TRANSICIÓN IPv6 CON TUNELIZACIÓN

<http://www.ietf.org/rfc/rfc2529.txt>

2013-06-25

32. TRADUCCIÓN DE DIRECCIONES

<http://tools.ietf.org/html/rfc6052>

2013-06-31

33. TRANSICIÓN IPv6 EN ECUADOR

http://www.ecu.ipv6tf.org/index.php?option=com_phocadownload&view=category&id=6:ipv6-en-ecuador-2012-06-06&Itemid=88

2013-06-30

34. TUNNEL BROKER

<http://tools.ietf.org/html/rfc3053>

2013-05-17

35. 6RD

<http://tools.ietf.org/html/rfc5969>

2013-05-25

36. 6OVER4

<http://flylib.com/books/en/2.223.1.103/1/>

2013-05-12