PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES.

ESTUDIO PARA LA ELABORACIÓN DEL PLAN DE MIGRACIÓN A IPV6 Y LA COEXISTENCIA CON IPV4 EN LA RED DE LA UNIVERSIDAD INTERNACIONAL DEL ECUADOR

VILLEGAS CHILIQUINGA WILLIAM EDUARDO

Trabajo previo a la obtención del título de:
MAGISTER EN REDES DE COMUNICACIONES

Quito, noviembre de 2014

Dedicatoria.

Me gustaría dedicar este trabajo a toda mi familia.

En especial a mis padres, por su comprensión y ayuda en momentos malos y menos malos. Me han enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Me han dado todo lo que soy como persona, mis valores, mis principios mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Por su paciencia, por empeño, por su fuerza, por su amor. A ellos las personas que directamente han sufrido las consecuencias del trabajo realizado. Realmente ellos me llenan por dentro para conseguir un equilibrio que me permita dar el máximo de mí. Nunca les podre estar suficientemente agradecido.

Muchas gracias por todo.

Agradecimientos.

No es sencillo pensar en las palabras adecuadas para poder definir la relación entre el autor de una tesis y su director. Resulta más fácil adentrarse en los recónditos pasajes de una literatura creada para navegar en el recuerdo, donde coexiste la razón y la emoción.

"tanto para iniciar, como para concluir una singladura es preciso contar con una tripulación preparada, disciplinada y entregada a su pasión por la investigación, y abierta a los que la buscan, como ellos, la esencia del conocimiento. Y, por supuesto, al mando, alguien presto a escuchar, con el convencimiento de que la ilusión de interlocutor merece una atención especial y dispuesto, sobre todo ser paciente".

En mi pequeño viaje particular he tenido la gran suerte de navegar siguiendo las indicaciones de quien representa, bajo mi punto de vista, ese modelo ideal de director de tesis, debido a su gran capacidad de trabajo, su dedicación plena, su atención continuada, su afable y sosegado, su incansable disposición y su inestimable ayuda en la elaboración y revisión de este trabajo.

Ing. Carlos Egas Msc. GRACIAS por haberme permitido formar parte de una gran experiencia, como es la realización de esta tesis de Maestría de redes de comunicaciones.

Contenido

Dedicatoria. II
Agradecimientos III
Introducción. 1
CAPITULO 1. Aspectos fundamentales. 3
1.1. Antecedentes. 3
1.2. Estado actual de la red de datos de la Universidad internacional del Ecuador. 4
1.3. Justificación. 4
1.4. Objetivos. 6
1.4.1. Objetivo General: 6
1.4.2. Objetivos Específicos: 6
1.5. Hipótesis. 6
1.6. Metodología de investigación. 7
1.6.1. Alcance: 7
1.6.2. Paradigma: 7
1.6.3. Método: 7
1.6.4. Diseño de la Investigación: 7
CAPITULO 2. Marco teórico. 8
2.1. Historia de IPV4 e IPV6 8
2.1.1. Protocolo IP. 8
2.1.2. Protocolo IPV4 8
2.1.3. Las características de Ipv4 son: 9
2.1.4. Formato de IPv4 11
2.1.5. Funcionamiento de IPv4 en la red 12
2.1.6. Tipos de direccionamiento de una IPV4 12
2.1.6.1. Dirección de red 12
2.1.6.2. Dirección de broadcast 13
2.1.6.3. Direcciones de host. 13
2.1.7. Tipos de comunicación (Unicast, Broadcast, multicast) 13
2.1.7.1. Tráfico unicast 14
2.1.7.2. Transmisión de broadcast 14
limitado 15
2.1.7.3. Transmisión de multicast. 15
2.1.8. Rangos de Dirección IPV4 reservadas 16
2.1.9. Direcciones experimentales 16

2.1.10. Direcciones multicast 16
2.1.11. Direcciones Públicas y Privadas 17
2.1.11.1. Los bloques de direcciones privadas son: 17
2.1.12. Anfitrión local (Localhost) 18
2.1.13. Referencia de sub-redes de IPv4. 19
2.1.13.1. Marcará de Subred 19
2.1.13.2. Direcciones IPV4 especiales 22
2.1.14. Planificación de direcciones de RED 23
2.1.14.1. Evitar duplicación de direcciones 23
2.1.14.2. Proveer y controlar el acceso 23
2.1.14.3. Monitorear seguridad y rendimiento 24
2.1.15. Direccionamiento estático o dinámico para dispositivos finales. 24
2.1.15.1. Asignaciones. 24
2.2. Protocolo IPV6 26
2.2.1. Descripción del Protocolo IPV6 26
2.2.2. Características principales de IPV6: 28
2.2.3. Jerarquía de direcciones – Agregación de prefijos de red 30
2.2.4. Modos de configuración de IPv6 30
2.2.5. Renumeración. 31
2.2.6. Multicasting 31
2.2.7. Encabezado eficiente 32
2.2.8. Etiqueta de flujo 32
2.2.9. Extensiones de encabezado 33
2.2.10. Movilidad 33
2.2.11. Seguridad 34
2.2.12. Cabecera de IPV6 35
2.2.13. Resolución de nombres de IPV6. 41
2.3. Principales Protocolos de IPV6 42
2.3.1. Protocolo ICMPV6. 42
2.3.2. Protocolo MLD (“Descubrimiento de escucha de multidifusión”). 43
2.3.3. Protocolo ND (“Descubrimiento de Vecinos”). 45
2.3.4. Protocolos de Enrutamiento. 48
2.3.4.1. Consideraciones de Enrutamiento 49
2.3.4.1.1. Plano de control de IPv6 49
2.3.4.1.2. Plano de datos de IPv6 51

2.3.4.2. Protocolo RIPng. 52
2.3.4.3. Protocolo OSPFV3 E IPV6. 54
2.3.4.3.1. Configuración de OSPF para IPv6 55
2.3.4.4. Protocolo BGP-4 ("Border Gateway Protocol"). 55
2.3.5. Direccionamiento de IPV6. 58
2.3.5.1. Tipos de direcciones IPv6 58
2.3.5.1.1. Direcciones Unicast. 59
2.3.5.1.2. Direcciones anycast (RFC2526) 61
2.3.5.1.3. Direcciones multicast (RFC2375) 63
2.3.6. Representación de direcciones IPv6 66
2.3.7. Prefijos de direcciones. 68
2.3.8. Enrutamiento de IPV6. 68
2.3.9. Tabla de enrutamiento IPv6 69
2.4. Ventajas y desventajas de IPv6. 71
2.4.1. Ventajas: 71
2.4.2. Desventajas: 72
2.5. Mecanismos de Transición de Ipv4 a Ipv6. 72
2.5.1. Doble Pila 73
2.5.2. Tipo Túnel 74
2.5.2.1. Túneles configurados o manuales. [RFC3904] 76
2.5.2.2. Túneles automáticos. 78
2.5.2.3. Túnel 6TO4 78
2.5.2.4. Túnel 6OVER4 81
2.5.2.5. Túneles ISATAP 83
2.5.3. Protocolo de Separación Localizador/Identificador (LISP). 86
Capítulo 3 Levantamiento de la información de la red de la Universidad Internacional del Ecuador. 88
3.1. Identificación de la RED de la UIDE. 88
3.1.1. Tráfico de red. 92
3.1.2. Distribución del cableado 96
3.1.2.1. Cableado horizontal. 97
3.1.2.1.1. Cable UTP 98
3.1.2.2. Cableado Vertical 99
3.2. Levantamiento y obtención del Diagrama Lógico. 101
3.2.1. Diseño de la topología de red. 101

3.2.2. Diseño de Vlans 104
3.2.2.1. Reglas de conectividad de VLANS 105
3.2.3. Distribuciones de direcciones IP. 106
3.2.4. Elaboración de tablas de enrutamiento. 108
3.2.5. Servicios. 108
3.3. Levantamiento del Diagrama Físico. 110
3.3.1. Características de los Equipos de Red. 112
CAPITULO 4. Diseño del plan de migración a IPV6 y la coexistencia con IPV4 de la red de datos de la Universidad Internacional del Ecuador. 121
4.1. Metodología de la migración 121
4.2. Conexión a internet. 122
4.3. Protocolos de Enrutamiento para el plan de migración. 124
4.3.1. Configuración del protocolo OSPF en Ipv6 128
4.3.2. Configuración del protocolo RIP en IPv6 130
4.3.3. Configuración de las rutas estáticas en ipv6 132
4.4. Escenarios de transición a IPV6. 132
4.4.1. Primer escenario 132
4.4.1.1. Configuración del primer escenario 133
4.4.2. Segundo Escenario. 134
4.4.2.1. Configuración del segundo escenario 135
Comandos de configuración del segundo escenario. 136
4.5. Diseño del diagrama lógico 137
4.5.1. Diseño de la topología de red IPv6. 137
4.5.2. Diseño de Vlan en IPV6 137
4.5.2.1. Configuración de Vlans en IPV6 137
4.5.3. Reglas de conectividad entre Vlans en IPV6 139
4.5.4. Direccionamiento Ipv6 en la red de datos en la Sede Matriz de la UIDE 139
4.5.4.1. Distribución de direcciones IPV6 para las Vlans 142
4.5.5. Servicios sobre IPv6 143
4.6. Diseño del diagrama Físico. 144
4.6.1. Evaluación del diagrama físico. 144
4.7 Consideraciones para el Plan de implementación 146
4.7.1 Consideraciones. 146
4.7.2. Perspectiva general de la metodología. 147
4.7.3. Fase 2: Modelo de Negocios/organización. 151

4.7.4. Fase 3: Modelo de tecnologías de la Información. 155
4.7.5. Fase 4: Modelo de la planeación. 156
4.7.5.1. Escenarios de migración 156
4.7.5.2. Prioridades de la Implementación. 157
4.7.5.2.1. Seguridad. 158
4.7.6. Plan de implementación de IPV6 162
4.7.7 Costos de la implementación. 168
4.7.7.1 Hardware. 169
4.7.7.2 Software. 170
4.7.7.3 Recurso Humano. 171
4.7.7.4 Capacitación. 171
4.7.7.5. Costo Final. 172
4.7.8. Impacto de la implementación de IPV6 172
4.7.9. Riesgos del proyecto. 173
4.7.10. Riesgos de no implementar IPv6. 174
Conclusiones. 175
Recomendaciones. 178
Bibliografía. 179
Glosario de palabras 181
Anexos 184
Anexo A 184
Características de los dispositivos. 184
Switch 3750. 184
Switch 2960-X. 186
Switch 3560. 188
Switch 2960-s 190
Switch 2960 192
Anexo B 194
Características de las RFC 194
Características de las RFC 791 194
Características de RFC 3024 198
Características de las RFC 3531 201
Anexo C. 203
Topología vista de Cisco network 203
Anexo C. 205

Cronograma de actividades para la migración 205

Tabla de Figuras.

Figura 1 IP independencia de los medios Fuente: internet 10
Figura 2 Formato de direcciones IPv4. Fuente: Internet..... 11
Figura 3. Bloques de direcciones IPv4 e Ipv6. Fuente: http://www.elmundo.es/imasd/ipv6/queesipv6.html..... 30
Figura 4 Cabecera de IPV4. Fuente: Internet..... 35
Figura 5 Cabecera de IPV6. Fuente: http://www.ramonmillan.com/tutoriales/ipv6_parte1.php 38
Figura 6 Formato General de Paquete ICMPV6. Fuente: Internet..... 43
Figura 7 Protocolo ND. Fuente: http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html..... 46
Figura 8 Servicios mejorados de enrutamiento en IPV6. Fuente: http://www.franciscosepulveda.eu..... 48
Figura 9 Arquitectura Doble Pila Fuente: internet..... 74
Figura 10 Mecanismo de túneles de IPV6 Fuente:http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-47/index.html..... 75
Figura 11 Nivel lógico y físico en el uso de Túneles. Fuente: http://www.rau.edu.uy/ipv6/queesipv6.htm#12..... 76
Figura 12 Túnel configurado Fuente: http://ipv4to6.blogspot.com/p/tunelizacion-ipv6.html77
Figura 13 Túnel entre dos Ubicaciones. Fuente: http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-50/index.html..... 79
Figura 14 Entorno 6over4 Fuente: http://repositorio.utn.edu.ec/bitstream/123456789/619/3/CAPITULO3.pdf..... 82
Figura 15. Funcionamiento de ISATAP. Fuente: http://www.franciscosepulveda.eu/2011/12/08/tecnologias-de-transicion-a-ipv6-isatap-12/ 84
Figura 16 Topología de la UIDE. Fuente: Autor 89
Figura 17 Interfaz de TracePlus. Fuente: Datos de la UIDE..... 95
Figura 18 Estrella extendida. Fuente: http://topologias4conalep.blogspot.com/p/topologia-en-estrella-y-estrella.html 102
Figura 19 Diagrama Físico. Fuente: El Autor..... 111
Figura 20 Esquema del mecanismo de transicion Dual Stack. Fuente: http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-1/ 122
Figura 21 Configuración de IPv6 y ospf en Router 2911 en packet tracer. Fuente: El autor 130
Figura 22 Configuración del Protocolo RIP en un Router. Fuente: el Autor..... 131
Figura 23 Configuración de rutas estáticas. Fuente: http://repositorio.cedia.org.ec/bitstream/123456789/44/2/cedia%20ipv6%20curso.pdf. 132
Figura 24 Esquema primer escenario. Fuente. El Autor. 133
Figura 25 Configuración de equipos para el escenario 1. Fuente: El Autor 135
Figura 26 Esquema segundo escenario. Fuente: El Autor. 136
Figura 27 Vlan´s en packet tracer. Fuente: El autor..... 138
Figura 28 Distribución de una dirección IPV6. Fuente: El Autor..... 140
Figura 29 Versión de Switch 3750. Fuente: Datos de la UIDE. 185
Figura 30 Versión de IOS de switch cisco 2960-X. Fuente: Datos de la UIDE. 186
Figura 31 Versión de IOS de switch cisco 2960-X. Fuente: Datos de la UIDE. 187
Figura 32 Versión de IOS de switch cisco 3560 Fuente: Datos de la UIDE..... 188

Figura 33 Versión de IOS de switch cisco 3560 Fuente: Datos de la UIDE..... 189
Figura 34 Versión de IOS de switch cisco 2960-S Fuente: Datos de la UIDE. 190
Figura 35 Versión de IOS de switch cisco 2960-S Fuente: Datos de la UIDE. 191
Figura 36 Versión de IOS de switch cisco 2960 Fuente: Datos de la UIDE..... 192
Figura 37 Versión de IOS de switch cisco 2960 Fuente: Datos de la UIDE..... 193

Índice de tablas.

Tabla 1: Bloque de dirreciones reservadas Fuente:http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4..... 18
Tabla 2: Referencia de sub-redes de IP versión 4. Fuente: http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4 22
Tabla 3 Tabla de Ips multidifusión reservadas Fuente:http://msdn.microsoft.com/es-es/library/cc776494%28v=ws.10%29.aspx 44
Tabla 4. Significados de bits. Fuente: Internet..... 64
Tabla 5.IPv6 ISATAP Formato de la dirección Fuente: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html 85
Tabla 6 Servidores y servicios que estos brindan a la UIDE. Fuente: Del Autor 91
Tabla 7 Edificios de la matriz de la UIDE. Fuente: Autor..... 97
Tabla 8 Distribución de bastidores y tipo rack de la UIDE. Fuente: El autor..... 98
Tabla 9 Características de cable categoría 6A. Fuente: http://www.ds3comunicaciones.com/AMP/1859218-X_.pdf..... 99
Tabla 10. Vlans de la UIDE. Fuente Autor..... 104
Tabla 11. Access list. Fuente: Autor. 105
Tabla 12 Tipo de direcciones IP. Fuente: el Autor 106
Tabla 13 Proyección de crecimiento de la red de la UIDE. Fuente. Datos de la UIDE..... 107
Tabla 14. Direcciones IP. En cada VLAN. Fuente: Autor. 107
Tabla 15 Tabla de enrutamiento en Firewall. Fuente: Datos de la UIDE 108
Tabla 16 Características de Chasis IBM. Fuente: Datos de la UIDE. 112
Tabla 17 Características de los servidores. Fuente: Datos de la UIDE..... 112
Tabla 18 Aplicaciones de los servidores. Fuente: Datos de la UIDE 113
Tabla 19 Características de CPU del Área administrativa y laboratorios. Fuente: datos de la UIDE..... 113
Tabla 20 Características del Equipo Firewall ASA 5540. Fuente: Datos de la UIDE..... 114
Tabla 21 Caracteristicas de Router cisco 7604. Fuente: http://www.hardware.com/us/products/cisco/7604-RSP720C-P 115
Tabla 22 características del Switch Core. Fuente: http://www.andovercg.com/datasheets/cisco-faq_c3750_Public1.pdf 116
Tabla 23 Caracteristicas de Switch 2960. Fuente: http://www.electronisys.cl/index.php?route=product/product&product_id=485 117
Tabla 24 Características de teléfono IP Yealink T20P. Fuente: Datos de la UIDE..... 118
Tabla 25 Caracteristicas de Telefono IP Yealink T21P. Fuente: http://www.yealink.com/sp/product_info.aspx?ProductsCateID=650&CateId=622&BaseInfoCateId=650&Cate_Id=650&parentcateid=622..... 119
Tabla 26 Características de teléfono IP Yealink T28P. Fuente: http://www.yealink.com/sp/product_info.aspx?ProductsCateID=650&CateId=622&BaseInfoCateId=650&Cate_Id=650&parentcateid=622..... 120
Tabla 27. Universidades que soportan IPv6. Fuente: http://www.telconet.net/servicios/internet2 124
Tabla 28 Comando de configuración de Router con datos de IPV6 y de ospf 129
Tabla 29 Configuración del protocolo RIP en IPv6 en router 2911. Fuente: El autor..... 131
Tabla 30. Configuración de Firewall primer escenario. Fuente: el Autor..... 134

Tabla 31 Configuración de equipos para el segundo escenario. Fuente: El autor 136
Tabla 32 Configuración de Vlan´s. Fuente: El Autor. 138
Tabla 33 Configuración de las interfaces para vlan´s Fuente: El Autor 139
Tabla 34 Direcciones IPv6 Disponibles. Fuente:
http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6..... 142
Tabla 35 Distribución de IP´s en cada dependencia. Fuente: El Autor..... 143
Tabla 36 Distribución de vlan - Gateway. Fuente: El Autor..... 143
Tabla 37 Detalle de Equipos. Fuente: Datos de la UIDE..... 145
Tabla 38 Sistemas Operativos de los servidores. Fuente: Datos de la UIDE..... 146
Tabla 39 Sistema Operativo en PC´s de la UIDE. Fuente: Datos de la UIDE..... 146
Tabla 40 Tabla de equipos de la UIDE. Fuente: El Autor 170
Tabla 41 Paquete de horas de soporte. Fuente: Shekinan 171
Tabla 42 Costos de capacitaciones. Fuente: Shekinan..... 171
Tabla 43 Valores totales a invertir. Fuente: El Autor. 172

Introducción.

La realidad sobre IPv4 al momento se basa en la disponibilidad de direcciones IP, desde hace ya varios años la 1IANA (organismo encargado de la asignación de direcciones IP) ha manifestado que IPV4 está llegando a su límite, como consecuencia quien necesite una nueva conexión a internet recibirá una IP tipo IPV6, esto significa que la red de cada empresa debe prepararse para asumir este protocolo.

Este trabajo presenta la elaboración del diseño y el plan de migración a IPV6 en la red de datos de la Universidad Internacional del Ecuador, tratará la coexistencia de ipv4 con ipv6. El fin principal es evolucionar de mano de los últimos mecanismos de transición de tal manera se permita aprovechar los beneficios de IPV6.

Ipv4 está definido en el RFC 791, este protocolo es utilizado para gestionar el tráfico de datos en la red

El trabajo consta de un INVENTARIO de los equipos que actualmente componen la parte activa de la red de la Universidad Internacional de Ecuador, la misma que a lo largo de este perfil de trabajo se la llamará por las siglas de su nombre “UIDE”, con el inventario al cual se hace mención se desea saber los equipos que deben ser cambiados o a su vez actualizados de tal manera soporten el protocolo sin presentar fallas a corto o largo plazo, además es muy importante la REVISIÓN de manera exhaustiva la red

[1] Internet Assigned Numbers Authority

que se dispone, y por este medio conocer el estado de los servicios y aplicaciones que se maneja en la UIDE y si están en la capacidad de ser actualizadas para soportar la coexistencia entre IPV4 e IPV6.

En este trabajo además consta del diseño de un cronograma dentro del cual se va a desarrollar cada una de las etapas sin perder la eficiencia en la red y sin que esto genere problemas para los usuarios, también trata un aspecto muy importante como son los costes que conlleva un diseño que abarca la coexistencia entre IPv4 que es el protocolo actual de la UIDE a IPv6.

La primera parte de este anteproyecto de tesis de maestría en comunicaciones, presenta los conceptos relacionados con el tema, para luego pasar a describir la justificación del porque realizarlo.

Una tercera parte, señala, los objetivos, un índice tentativo y finalmente propone un cronograma de desarrollo de la investigación. Es importante señalar que la bibliografía de este documento está sólidamente sustentada.

CAPITULO 1. Aspectos fundamentales.

1.1. Antecedentes.

En la actualidad la Universidad Internacional del Ecuador cuenta con una red basada en IPV4 la misma que está vigente desde el 2004, sobre esta red transitan varios servicios como son telefonía IP, cámaras IP, internet, aplicaciones operacionales de la UIDE.

El crecimiento exponencial de usuarios de internet y la cantidad de dispositivos móviles que utilizan el protocolo TCP/IP ha llevado a la necesidad de mejorar las condiciones del diseño de la red.

En los últimos años se ha venido actualizando los equipos de la parte activa de red por modelos que soportan en gran medida el protocolo IPV6 mismo que al momento no es utilizado tomando en cuenta que la UIDE también posee un enlace dedicado a este protocolo.

Las seguridades que ofrece al momento la red están quedando obsoletos por lo que es necesario llevar a cabo un plan de acción con fin de conocer las características y ventajas que brindan nuevos protocolos en temas de seguridad para tomarlos en cuenta en el diseño de la red que finalmente tendrá coexistencia con la red actual.

Por otro lado la IANA [2]tras su anuncio en febrero del 2011 del agotamiento de IPv4 y la entrega de los últimos cinco bloques /8 disponibles a los [3]RIRs ha despertado un

[2] Internet Assigned Numbers Authority
[3] Registro Regional de Internet

gran interés a nivel mundial por la migración paulatina al protocolo sucesor de IPv4, IPV6 por la suma de estos factores es vital para la Universidad Internacional del Ecuador iniciar los procesos de análisis y posterior implementación de IPV6 con la coexistencia de IPV4 a fin de hacer uso de las características y ventajas que ofrece el protocolo.

1.2. Estado actual de la red de datos de la Universidad internacional del Ecuador.

La Universidad internacional del Ecuador está formada por la matriz que se encuentra en Quito Av. Simón Bolívar, dos sedes, una ubicada en la ciudad de Loja y otra en la ciudad de Guayaquil, un centro de Apoyo ubicado en Quito sector Eloy Alfaro y otro ubicado en el sector Gran Colombia además de dos clínicas odontológicas para prácticas.

La red de la Universidad Internacional del Ecuador se encuentra formado por varias redes LAN una en cada establecimiento, la interconexión entre estas redes se realiza a través de los diferentes Routers que están ubicados en sus centros de Distribución principal de cableado “MDF” y por gestión del ISP “Telconet”.

Para el estudio y elaboración del plan de migración a IPV6 y la coexistencia con IPV4 de la red de la Universidad Internacional del Ecuador teniendo en cuenta la topología de red, distribución del cableado y los equipos activos se tomara en cuenta a la matriz.

1.3. Justificación.

La red de datos de la UIDE está en funcionamiento desde el 2004, a lo largo de este tiempo la red se ha extendido de manera considerable por lo cual es necesario

realizar un diseño que acoja los servicios que actualmente se encuentran en producción con nuevos requerimientos en aspectos de coexistencia con Ipv4 – Ipv6, políticas de seguridad, movilidad, dimensionamiento de la capacidad de expansión de la red.

Al momento la red de datos de la Universidad maneja varias Vlan lo que ha permitido sobre llevar el tema de agotamiento de IP's sin embargo la integración de nuevas aplicaciones y el aumento tanto de personal administrativo, académico y estudiantil ha creado la necesidad de adoptar nuevas tecnologías que permitan una efectiva distribución de IP's y aumento en su número sin descuidar temas como la seguridad y coexistencia con lo que al momento es parte de la red de la UIDE.

La Universidad internacional del Ecuador busca aprovechar al máximo los enlaces que dispone por ser parte de CEDIA, organismo que siempre ha venido buscando mejoras en la eficiencia de los servicios y en la parte técnica, dentro de la cual está la eficiencia de la redes, canal usado para la investigación que es un tema muy importante en la actualidad para una institución educativa y más con la UIDE que es parte de la red avanzada de Ecuador, es necesario para todo este proceso que se ha mencionado, un estudio que abarque todos los aspectos técnicos, teóricos y financieros que conlleva a una ejecución del proyecto de tal manera sea invisible para el usuario.

El avance tecnológico brinda la posibilidad de realizar un proceso de coexistencia entre protocolos (Ipv4 – Ipv6), esto permitirá a la UIDE aprovechar las ventajas que ofrece IPV6 que es de hecho uno de los objetivos principales para la UIDE que busca la calidad y ser una institución dedicada a la investigación. Con el diseño de la red de datos planteado se puede desarrollar nuevas aplicaciones que lo manejen, tal como el

control de sistemas electrónicos que sean capaces de conectarse a internet y sean gobernados desde estás instancias.

1.4. Objetivos.

1.4.1. Objetivo General:

Desarrollar un estudio para la elaboración del plan de migración a Ipv6 y la coexistencia con Ipv4 en la red de la Universidad Internacional del Ecuador.

1.4.2. Objetivos Específicos:

1. Describir el estado del arte respecto al protocolo IPV4 e IPV6.
2. Determinar el mecanismo a utilizar en la transición del protocolo IPV4 a IPV6.
3. Analizar el estado actual de las aplicaciones y su capacidad para soportar los nuevos requerimientos informáticos de la UIDE.
4. Identificar las políticas de seguridad necesarias en la red de la Universidad Internacional del Ecuador.
5. Realizar la configuración básica de los equipos y la simulación de la red de datos donde coexistan los protocolos Ipv4 e Ipv6.

1.5. Hipótesis.

El estudio propuesto tiene en cuenta los mecanismos de transición para la coexistencia de los protocolos IPV4 e IPV6 lo cual permitirá el aprovechamiento de los canales dedicados que dispone la UIDE con ello se mejorara la calidad de la trasmisión.

1.6. Metodología de investigación.

1.6.1. Alcance:

El presente trabajo es de carácter Exploratorio y Explicativo, pues se explorara los protocolos de internet IPv4 e IPv6 a través del estado del arte que originan el fenómeno en cuestión, con lo cual se emita una explicación del mismo.

1.6.2. Paradigma:

Empírico-Analítico con enfoque cuantitativo.

1.6.3. Método:

Ex post facto, puesto que se pretende evidenciar las posibles relaciones de causa efecto entre las técnicas o mecanismos de transición para interconexión y coexistencia de IPV4 a IPV6.

1.6.4. Diseño de la Investigación:

No experimental Transversal.- Puesto que no se manipularán deliberadamente las variables de estudio, se procederá a la observación directa de los protocolos de internet tal y como se da en su contexto natural, y posteriormente su análisis respectivo.

CAPITULO 2. Marco teórico.

2.1. Historia de IPV4 e IPV6

2.1.1. Protocolo IP.

[4]"Internet Protocol, según el MODELO OSI es un protocolo de comunicación de datos perteneciente a la Capa de Red, su funcionalidad radica en el uso bidireccional de comunicación para llevar datos a través de redes físicas enlazadas usando un protocolo no orientado a conexión".

2.1.2. Protocolo IPV4

[5]"Ipv4 (internet protocol versión 4) es el protocolo de nivel de red usado en internet. Junto con otros protocolos auxiliares es responsable de transferir la información del usuario por la red. El protocolo está definido en el [6]RFC 791. Fue creado en los años 1973 – 1974 por Vint Cert y Robert Kahn".

[7]"Ipv4 es la versión 4 del protocolo de internet (IP, Internet Protocol) constituye la primera versión de IP que es implementada de forma extensa, es un protocolo de nivel de red orientado hacia datos que es usado para la comunicación entre redes a través de interrupciones de paquetes. No es orientado a conexión y no confiable. En caso de haber errores, se espera que el nodo involucrado descarte el paquete. Debido a que un paquete debe transitar por varios nodos, siguiendo un camino que

[4] http://10conceptos.com/concepto-de-ipv6/
[5] http://www-2.dc.uba.ar/materias/tc/downloads/apuntes/ipv4.pdf
[6] PROTOCOLO INTERNET
[7] http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html

no es necesariamente el mismo que el usado por otros paquetes, los datos enviados pueden llegar en desorden. Ipv4 no corrige el orden de los paquetes".

[8]"Ipv4 es un protocolo no confiable esto no significa que funcione inadecuadamente, se refiere a que no es un protocolo capaz de administrar ni recuperar paquetes no entregados o corruptos. De la confiabilidad se encarga la capa de Transporte, lo que hace de IP un protocolo más flexible a los distintos tipos de comunicación, al poder prescindir de esta tarea en la capa de Red".

2.1.3. Las características de Ipv4 son:

- Es un protocolo de servicio de datagramas no fiable (mejor esfuerzo).
- No proporciona garantía en la entrega de datos.
- No proporciona garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

"Otra de las características del protocolo es que IP es independiente de los medios físicos, es decir, un paquete IP puede ser enviado eléctricamente por cable, como por señales ópticas por fibra o señales de radio como se puede observar en la figura 1."

[8] http://ciclodeinformatica.blogspot.com/2013/04/protocolo-ipv4-caracteristicas-y.html

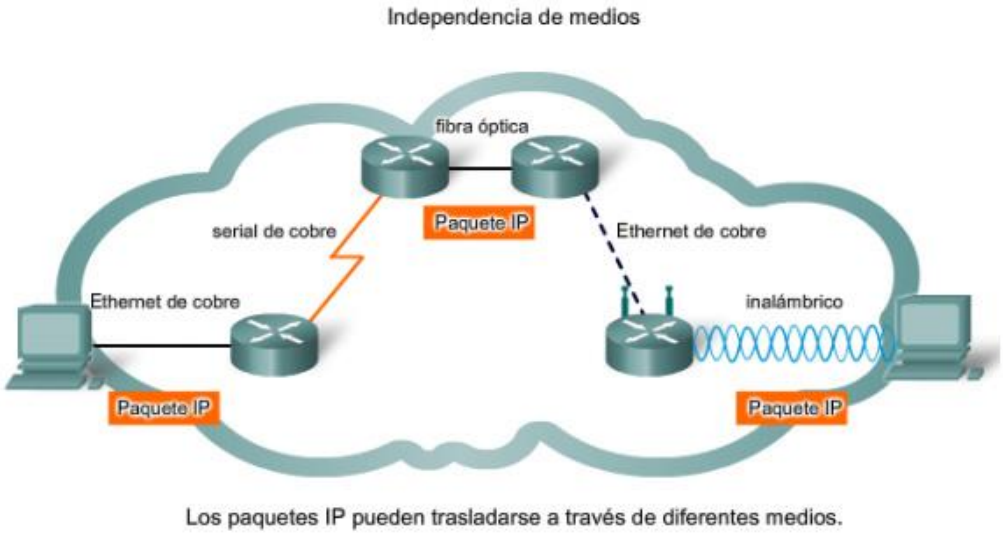


Figura 1 IP independencia de los medios Fuente: internet

"Los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, a través de TCP o UDP.

El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra".

[9]"IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4, 294, 967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión (Multicast), etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto lo que ha impulsado la creación de IPv6 como reemplazo eventual dentro de algunos años para IPv4".

[9] http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html

2.1.4. Formato de IPv4

[10]"En una red TCP/IP a cada computadora se le asigna una dirección lógica de 32-bits que se divide en dos partes: el número de red y el número de computadora. Los 32 bits son divididos en 4 grupos de 8 bits, separados por puntos, y son representados en formato decimal.

Cada bit en el octeto tiene un peso binario. El valor mínimo para un octeto es 0 y el valor máximo es 255. La figura 2 muestra el formato básico de una dirección IP con sus 32 bits agrupados en 4 octetos.

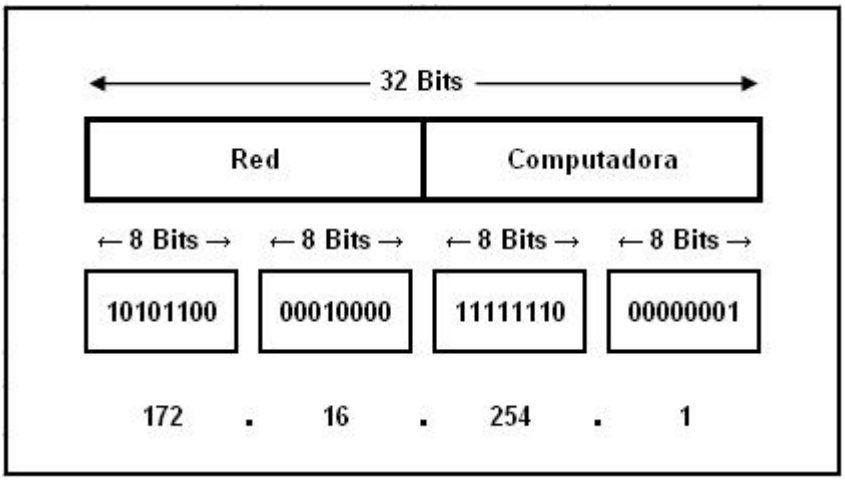


Figura 2 Formato de direcciones IPv4. Fuente: Internet

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada

[10] http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4

paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa tres.

2.1.5. Funcionamiento de IPv4 en la red.

[11]Porciones de red y de host

"En cada dirección IPv4, alguna porción de los bits de orden superior representa la dirección de red. En la capa tres una red se define como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones".

2.1.6. Tipos de direccionamiento de una IPV4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- Dirección de red: la dirección en la que se hace referencia a la red.
- Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.
- Direcciones host: las direcciones asignadas a los dispositivos finales de la red.

2.1.6.1. Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Es la manera más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán

[11] http://los9mm.over-blog.es/article-29399073.html

los mismos bits de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

2.1.6.2. Dirección de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos uno.

2.1.6.3. Direcciones de host.

Cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

2.1.7. Tipos de comunicación (Unicast, Broadcast, multicast)

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

- Unicast: el proceso por el cual se envía un paquete de un host a un host individual.
- Broadcast: el proceso por el cual se envía un paquete de un host a todos los hosts de la red.

- Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

2.1.7.1. Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork[12].

2.1.7.2. Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección

[12] unión de redes diferentes a cualquier nivel

- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento.

2.1.7.2.1. [13]Broadcast dirigido: Se envía un broadcast dirigido a todos los hosts en una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local.

2.1.7.2.2. Broadcast limitado: El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino 255.255.255.255. Los routers no envían estos broadcasts. Los paquetes dirigidos a la dirección de broadcast limitada sólo aparecerán en la red local.

2.1.7.3. Transmisión de multicast.

La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts.

Algunos ejemplos de transmisión de multicast son:

- Distribución de audio y video
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento.
- Distribución de software

[13] http://los9mm.over-blog.es/article-29399073.html

- Suministro de noticias

2.1.8. Rangos de Dirección IPV4 reservadas

Expresado en formato decimal punteado, el rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255.

2.1.9. Direcciones experimentales

Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 experimentales de 240.0.0.0 a 255.255.255.254. En la actualidad, no es posible utilizarlas en redes IPv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

2.1.10. Direcciones multicast

El rango de direcciones IPv4 multicast de 224.0.0.0 a 239.255.255.255. Además, el rango de direcciones multicast se subdivide en diferentes tipos de direcciones:

- Direcciones de enlace locales reservadas
- Direcciones agrupadas globalmente.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones reservadas de enlace local. Estas direcciones se utilizarán con grupos multicast en una red local.

Las direcciones de alcance global son de 224.0.1.0 a 238.255.255.255. Se las puede usar para transmitir datos en Internet mediante multicast.

2.1.11. Direcciones Públicas y Privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. A estas direcciones se las denomina direcciones privadas.

2.1.11.1. Los bloques de direcciones privadas son:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas. Por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones en la tabla 1 se puede observar a detalle los bloques de direcciones privadas.

Bloque de direcciones CIDR	**Descripción**	**Referencia**
0.0.0.0/8	Red actual (solo válido como dirección de origen)	RFC 1700
10.0.0.0/8	**Red Privada**	RFC 1918
14.0.0.0/8	Red de datos públicos	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Anfitrión local (localhost)	RFC 1700
128.0.0.0/16	Reservado	

169.254.0.0/16	**Red Privada** (Zeroconf)	RFC 3927
172.16.0.0/12	**Red Privada**	RFC 1918
191.255.0.0/16		
192.0.0.0/24		
192.0.2.0/24	Red de pruebas	RFC 3330
192.88.99.0/24	Retransmisión desde **IPv6** hacia **IPv4**	RFC 3068
192.168.0.0/16	**Red Privada**	RFC 1918
198.18.0.0/15	Pruebas de desempeño de red	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multidifusión (Multicast, antes red Clase D)	RFC 3171
240.0.0.0/4	Reservado (Antes red Clase E)	RFC 1700
255.255.255.255	Difusiones (Broadcast)	

Tabla 1: Bloque de dirreciones reservadas

Fuente:http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4.

2.1.12. Anfitrión local (Localhost)

[14]Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255 o 127.0.0.0/8 en la notación CIDR[15], está reservado para la comunicación del anfitrión local (localhost). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

[14] http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4
[15] enrutamiento entre dominios sin clases

2.1.13. Referencia de sub-redes de IPv4.

Algunos segmentos del espacio de direcciones de IP, disponibles para la versión 4, se especifican y asignan a través de documentos RFC (Request For Comments o Solicitud De Comentarios), que son conjuntos de notas técnicas y de organización que se elaboran desde 1969 donde se describen los estándares o recomendaciones de Internet, antes ARPANET. Ejemplos de esto son los usos del Retorno del sistema (loopback, RFC 1643), las redes privadas (RFC 1918) y Zeroconf (RFC 3927) que no están bajo el control de los RIR (Regional Internet Registries o Registros Regionales de Internet).

[16]La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Cuando se usa un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles.

2.1.13.1. Marcará de Subred

La máscara de sub-red es utilizada para separar los bits de un identificador de una red a partir de los bits del identificador del anfitrión. Se escribe

[16] http://los9mm.over-blog.es/article-29399073.html

utilizando el mismo tipo de notación para escribir direcciones IP. La máscara de subred se expresa con el mismo formato decimal punteado que la dirección IPv4. La máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección. La máscara de subred se configura en un host junto con la dirección IPv4 para definir la porción de red de esa dirección. Si la máscara de subred de un octeto está representada por 255, entonces todos los bits equivalentes de ese octeto de la dirección son bits de red.

Existen varios métodos para calcular la cantidad de subredes así como la cantidad de host por ejemplo:

- Fórmula para calcular subredes

  Fórmula para calcular la cantidad de subredes:

  2^n donde n = la cantidad de bits que se tomaron prestados

  En este ejemplo, el cálculo es así:

  2^1 = 2 subredes

La cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula 2^n - 2 donde n = la cantidad de bits para hosts.

CIDR	Máscara de sub-red	Anfitriones	Nombre de la clase	Uso típico
/8	255.0.0.0	16777216	Clase A	Bloque más grande definido por la IANA
/9	255.128.0.0	8388608		
/10	255.192.0.0	4194304		
/11	255.224.0.0	2097152		
/12	255.240.0.0	1048576		
/13	255.248.0.0	524288		
/14	255.252.0.0	262144		
/15	255.254.0.0	131072		
/16	255.255.0.0	65536	Clase B	
/17	255.255.128.0	32768		ISP / negocios grandes
/18	255.255.192.0	16384		ISP / negocios grandes
/19	255.255.224.0	8192		ISP / negocios grandes
/20	255.255.240.0	4096		ISP pequeños / negocios grandes
/21	255.255.248.0	2048		ISP pequeños / negocios grandes
/22	255.255.252.0	1024		
/23	255.255.254.0	512		
/24	255.255.255.0	256	Clase C	LAN grande

/25	255.255.255.128	128		LAN grande
/26	255.255.255.192	64		LAN pequeña
/27	255.255.255.224	32		LAN pequeña
/28	255.255.255.240	16		LAN pequeña
/29	255.255.255.248	8		
/30	255.255.255.252	4		Redes de unión (enlaces punto a punto)
/31	255.255.255.254	2		Red no utilizable, sugerida para enlaces punto a punto (RFC 3021)
/32	255.255.255.255	1		Ruta del anfitrión

Tabla 2: Referencia de sub-redes de IP versión 4. Fuente:
http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4

2.1.13.2. [17]Direcciones IPV4 especiales

Direcciones de red y de broadcast

No es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son la dirección de red y la dirección de broadcast, respectivamente.

[17] http://los9mm.over-blog.es/article-29399073.html

Ruta predeterminada

Se representa la ruta predeterminada IPv4 como 0.0.0.0. La ruta predeterminada se usa como ruta "comodín" cuando no se dispone de una ruta más específica.

2.1.14. Planificación de direcciones de RED

Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

2.1.14.1. Evitar duplicación de direcciones: Cada host en una interwork debe tener una dirección única Sin la planificación y documentación adecuada de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

2.1.14.2. Proveer y controlar el acceso: Algunos hosts ofrecen recursos tanto para la red interna como para la red externa. El acceso a estos recursos puede ser controlado por la dirección de la Capa tres. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos.

2.1.14.3. Monitorear seguridad y rendimiento: Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red.

2.1.15. Direccionamiento estático o dinámico para dispositivos finales.

En las redes de datos, la mayor población de host incluyendo dispositivos finales como PC, teléfonos, etc. Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

Las direcciones IP pueden asignarse de manera estática o dinámica.

2.1.15.1. Asignaciones.

[18]Desde 1993 rige el esquema CIDR (Classless Inter-Domain Routing o Encaminamiento Inter Dominios sin Clases) cuya principal ventaja es permitir la subdivisión de redes y permite a las entidades sub-asignar direcciones IP, como haría un ISP con un cliente.

El principio fundamental del encaminamiento (routing) es que la dirección codifica información acerca de localización de un dispositivo dentro de una red. Esto implica que una dirección asignada a una parte de una red no funcionará en otra parte de la red. Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el CIDR y hasta 1998 fue supervisada por la IANA (Internet Assigned Numbers

[18] http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4

Authority o Agencia de Asignación de Números Internet) y sus RIR (Regional Internet Registries o Registros Regionales de Internet). Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la ICANN (Internet Corporation for Assigned Names and Numbers o Corporación de Internet para los Nombres y Números Asignados). Cada RIR mantiene una base de datos WHOIS disponible al público y que permite hacer búsquedas que proveen información acerca de las asignaciones de direcciones IP. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas las cuales se utilizan para localizar direcciones IP geográficamente.

- **Asignación estática de direcciones**

  Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto.

  Las direcciones estáticas tienen ventajas contra las direcciones dinámicas ya que estas resultan útiles para impresoras, servidores y otros dispositivos que son accesibles para los clientes de la red.

- **Asignación dinámica de direcciones**

  Los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el Protocolo de configuración dinámica de host (DHCP).

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el gateway por defecto y otra información de configuración. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada. Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo.

- **Direcciones para servidores y periféricos**

Los servidores y periféricos son un punto de concentración para el tráfico de red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red debe poder identificar rápidamente estos dispositivos.

2.2. Protocolo IPV6

2.2.1. Descripción del Protocolo IPV6

[19]IPv6 (también conocido como IPng o "IP de nueva generación") es la nueva versión del conocido protocolo de red IP, también llamado IPv4. IPv6 se puede instalar

[19] https://www.freebsd.org/doc/es/books/handbook/network-ipv6.html

como una actualización de software en las máquinas y es capaz de trabajar con el actual protocolo en coexistencia.

IPv6 nace del rápido consumo de las direcciones de IPV4 y dada la expansión del internet se encuentran los siguientes inconvenientes:

- El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force o Grupo de Trabajo de Ingeniería de Internet), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones. Actualmente no se trata del principal problema debido al uso generalizado del espacio de direccionamiento privado (10.0.0.0/8, 192.168.0.0/24, etc.) junto con NAT.
- El número de entradas de las tablas de rutas comienza a ser imposible de manejar. Esto es un problema prioritario.

IPv6 trata de resolver estos problemas y algunos más de la siguiente forma:

- IPv6 posee un espacio de direccionamiento de 128 bits. Esto significa que existen aproximadamente 6.67 * 10^27 direcciones IPv6 por metro cuadrado disponibles para todo el planeta.
- Los "routers" sólo almacenan direcciones de red agregadas así que se reduce el número de entradas para cada tabla de rutas a un promedio de 8192.

2.2.2. [20]Características principales de IPV6:

1. "Mayor espacio de direccionamiento (RFC 2373 o draft de 16/09/2002).

   Las direcciones pasan de los 32 a 128 bits, o sea de 2^32 direcciones (4.294.967.296) a 2^128 direcciones (3.402823669 e38).

   - Esto hace que desaparezcan los problemas de direccionamiento del protocolo IPv4 actual.
   - Que no sean necesarias técnicas como el NAT para proporcionar conectividad a todos los ordenadores/dispositivos de nuestra red.

   Por tanto, todos los dispositivos actuales o futuros (ordenadores, PDAs, teléfonos, GPRS o UMTS, neveras, lavadoras, etc.) podrán tener conectividad completa a Internet.

2. Seguridad (RFC 2401 y RFC 2411).

   Uno de los grandes problemas de Internet es su falta de seguridad en su diseño base. Este es el motivo por el que han tenido que desarrollarse, el SSH o SSL, protocolos a nivel de aplicación que añaden una capa de seguridad a las conexiones que pasan a través suyo.

   IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

[20] http://www.elmundo.es/imasd/ipv6/queesipv6.html

3. Autoconfiguración (RFC 2462, en español)

   En el actual en IPv4 se han desarrollado protocolos a nivel de aplicación que permitan a los ordenadores conectados a una red asignarles los datos de conectividad de manera automática. Ejemplos son el DHCP o BootP.

   IPv6 incluye esta funcionalidad en el protocolo base, la propia pila intenta auto-configurarse y descubrir el camino de conexión a Internet (router discovery).

4. Movilidad (RFC 3024).

   Con la movilidad (o roaming) ocurre lo mismo que en los puntos anteriores, una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita acceder directamente al internet.

5. Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
6. La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado.
7. La difusión ARP es reemplazada por el uso de multicast en el link local.
8. El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
9. Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6".

2.2.3. [21]Jerarquía de direcciones – Agregación de prefijos de red

Un espacio mayor de direcciones de IPv6 permite mayores distribuciones de direcciones a las organizaciones y a los proveedores de servicios de Internet (ISPs). Al tener una gran disponibilidad de direcciones se posibilita el uso de un solo prefijo grande para toda la red de una organización, por ende, el ISP puede sumar las rutas (agregar) de todos los prefijos de sus clientes en un solo prefijo y anunciarlo al Internet IPv6, la figura 3 marca los bloques de una dirección Ipv4 e Ipv6.

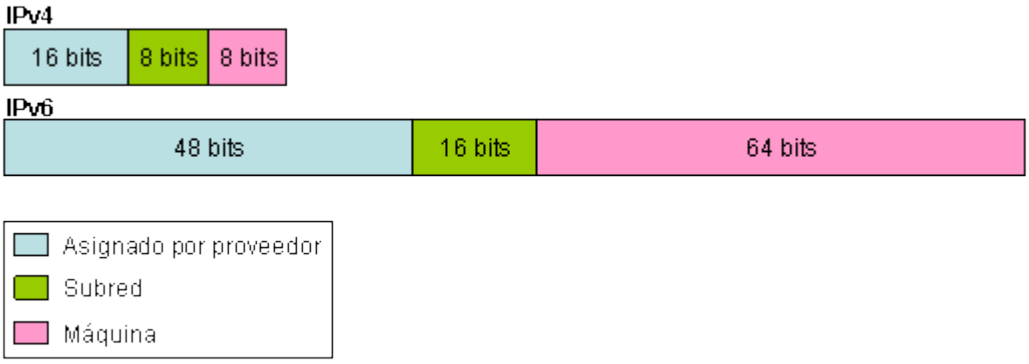


Figura 3. Bloques de direcciones IPv4 e Ipv6. Fuente: http://www.elmundo.es/imasd/ipv6/queesipv6.html

Cuando un usuario final cambia su proveedor de IPv6, el cual le proveía de direccionamiento IPv4, entonces también debe cambiar su prefijo de IPv6 para preservar su agregación global. Al mismo tiempo, el cambiar de proveedor implica una renumeración de la red.

2.2.4. Modos de configuración de IPv6

Autoconfiguración. Definida en el RFC 2462 y también es conocida como Configuración Automática de Dirección Sin Estado IPv6. Esta funcionalidad permite que un ruteador IPv6 envíe, a través del enlace local la información de red a las

[21] http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

computadoras y que ellas puedan configurarse correctamente. La información enviada es el prefijo de IPv6 del enlace local y la ruta por defecto del mismo protocolo. Mediante este mecanismo cada computadora y servidor de IPv6 añade su dirección de capa de enlace (dirección MAC) en el formato EUI-64 al prefijo de IPv6 de unicast global único anunciado en la subred.

Configuración mediante servidor. Las computadoras que utilizan IPv6 pueden obtener sus parámetros y direcciones de configuración de un servidor de DHCP versión 6. Este modo es llamado Configuración de Direcciones con Estado IPv6.

2.2.5. Renumeración.

El proceso de renumeración de IPv6 fue diseñado para ser transparente entre los proveedores de IPv6 unicast y los usuarios finales. Esto se logra con el mecanismo de autoconfiguración que permite una renumeración sencilla a las computadoras con sólo enviarles el nuevo prefijo IPv6 unicast para la red. Una desventaja de este mecanismo es la pérdida de las sesiones TCP y UDP que ocurren entre las computadoras y los servidores al momento exacto de la transición. Esto es algo que también ocurre actualmente con IPv4.

2.2.6. [22] Multicasting

La difusión del Protocolo de Resolución de Dirección (Address Resolution Protocol, ARP) de IPv4 afecta la eficiencia de la red. Esta situación no ha sido incluida en IPv6, y en su lugar se utiliza el Multicasting el cual funciona de la siguiente manera:

[22] http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

- Se crea un grupo Multicast, formado por un conjunto de interfaces de red.
- Si se está interesado en que cierta computadora reciba los paquetes de difusión del grupo se agrega una interfaz de red, de esa forma se envía un paquete multicast al grupo X.
- Ese paquete sólo llegará a aquellas computadoras que tengan su interfaz incluida en el grupo multicast X. Con ello se permite tener niveles de eficiencia de red superiores a los presentados en IPv4, lo cual se verá traducido en la disminución de los ciclos de procesamiento de CPU de las computadoras en la red local al no procesar paquetes de difusión que no van dirigidos a ellos y de la misma manera se estará eliminando el problema de las tormentas de paquetes de difusión de IPv4.

2.2.7. Encabezado eficiente

El nuevo encabezado de IPv6 es más sencillo que el de IPv4. Del encabezado de IPv4 se removieron 6 campos: Longitud de encabezado, Identificación, Banderas, Desplazamiento por fragmentación, Suma de verificación de encabezado, Opciones y Relleno. Al pasar de un encabezado de IPv4 con longitud variable a IPv6 con menos campos y longitud fija se obtiene una reducción en los ciclos de CPU de los ruteadores al momento de enviar los paquetes de IPv6.

2.2.8. Etiqueta de flujo

Dentro del encabezado de IPv6 existe un nuevo campo llamado Etiqueta de Flujo, éste es usado por el nodo fuente para solicitar un manejo especial de secuencias específicas de paquetes. La etiqueta está dirigida al procesamiento de la estación

destino, no para los ruteadores, y es de gran utilidad para aplicaciones como videoconferencias y voz sobre protocolo de Internet (VoIP). Asimismo agrupa todas aquellas que requieren un tratamiento especial de Calidad de Servicio (Quality of Service, QoS) en los ruteadores de la trayectoria.

2.2.9. Extensiones de encabezado

La utilización del campo Opciones en el encabezado de IPv4 presenta desventajas a la transmisión de los paquetes y a la eficiencia de la red. En lo que respecta a la variación del tamaño del encabezado es debido a que tiene campos opcionales. En el segundo caso todos los ruteadores que procesan el paquete deben computar el encabezado con su campo de longitud variable lo que introduce retardos y gasto de la capacidad del CPU en ciclos de procesamiento que son innecesarios. Para resolver esto, IPv6 sustituye el campo Opciones al final del encabezado por las Extensiones de Encabezado, formando un encadenamiento de encabezados enlazados por un campo llamado Siguiente Encabezado. Se presenta un campo Siguiente Encabezado dentro de cada Extensión de Encabezado usado por IPv6. Este diseño con extensiones permite una mejor eficiencia en el procesamiento de los paquetes, ya que asegura que los ruteadores y nodos computan los encabezados dirigidos a ellos a lo largo de la trayectoria.

2.2.10. [23]Movilidad

"Debido a que la movilidad es una característica importante y deseable por las compañías proveedoras y los consumidores finales el Protocolo de Internet Móvil

[23] http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

(MobileIP) está disponible tanto en IPv4 como en IPv6. Cabe destacar que en este último la movilidad se construyó dentro del protocolo en lugar de ser una nueva función agregada como en IPv4. Ello implica que cualquier nodo IPv6 puede usar un IP Móvil tanto como lo requiera. IPv6 Móvil utiliza dos Extensiones de Encabezado: un Encabezado de Enrutamiento para el registro y un Encabezado de Destino para entrega del datagrama entre los nodos móviles y sus nodos fijos correspondientes".

2.2.11. Seguridad

El protocolo IPSec estandarizado por el Grupo Especial sobre Ingeniería de Internet provee las funciones de:

- Limitar el acceso a sólo aquellos autorizados.
- Certifica la autenticación de la persona que envía los datos.
- Encripta los datos transmitidos a través de la red.
- Asegura la integridad de los datos.
- Invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos.

Los protocolos que respaldan el funcionamiento de IPSec son: la Autenticación de Encabezado (Autentication Header, AH) y la Carga de Seguridad Encapsulada (Encapsulated Security Payload, ESP). Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que IPSec está presente en todos los nodos de la red.

2.2.12. Cabecera de IPV6

Para un mayor entendimiento de la cabecera de IPV6 se hace una comparación con la de IPv4 de tal manera sea entendible los conceptos que se manejan.

La cabecera de un paquete IPV4 se la puede observar en detalle en la figura 4.

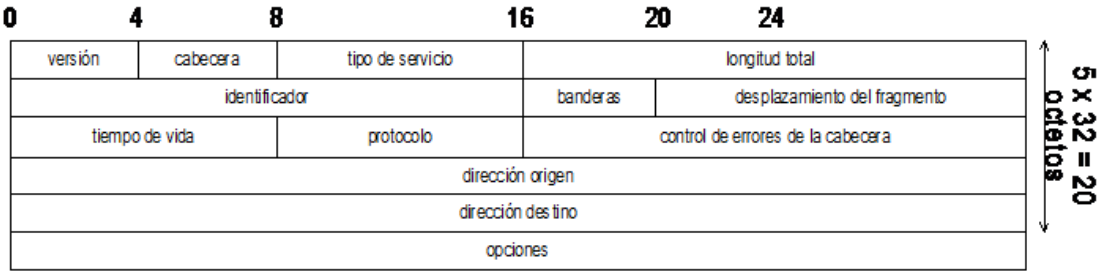


Figura 4 Cabecera de IPV4. Fuente: Internet

[24]"La cabecera de IPv4, tiene una longitud variable mínima de 20 octetos. El bit más significante se numera por 0 a la izquierda, y el menos significante se numera por 31 a la derecha. La forma de transmitir los diferentes bytes, sigue el orden conocido por big endian, es decir, de izquierda a derecha y de arriba abajo según la estructura presentada en la Figura 4. La cabecera consiste en los siguientes campos:

- Versión (4 bits). Es el número de versión de IP, es decir, 4.
- Cabecera (4 bits). Especifica la longitud total de la cabecera en palabras de 32 bits. El valor mínimo y más común es de 5, siendo la longitud de cabecera mínima. Puesto que el campo es de 4 bits, se limita la longitud total de la cabecera a 60 bytes.

[24] http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

- Tipo de servicio (8 bits). Indica la calidad de servicio solicitada por el paquete IP. De los 8 bits, actualmente sólo se utilizan 4, indicando cada uno de ellos: conseguir el retardo mínimo, maximizar caudal, maximizar la fiabilidad, y minimizar el coste monetario. Sólo uno de estos cuatro bits puede estar a 1. Su uso viene descrito en la RFC 1340 y RFC 1349.

- Longitud total (16 bits). Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes.

- Identificador (16 bits). Es un número único asignado por el dispositivo que envía el paquete, con el fin de que el destinatario pueda re ensamblar un paquete fragmentado por los nodos intermedios. La fragmentación es necesaria porque no todas las redes físicas tienen la misma longitud de trama máxima, por lo cual en muchos casos es necesario que los nodos intermedios dividan el datagrama en varios fragmentos. Cada uno de estos fragmentos podrá seguir rutas distintas al resto y, de perderse alguno de los fragmentos, el origen deberá retransmitir el paquete completo.

- Banderas (3 bits). Es un campo para el control de la fragmentación. El primer bit no es utilizado y está siempre puesto a 0. Si el segundo bit es 0, significa que puede haber fragmentación, y si es 1, significa que no puede haber fragmentación. Si el tercer bit es 0, indica que es el último fragmento, y si es 1, indica que aún hay más fragmentos.

- Desplazamiento del fragmento (13 bits). Es utilizado en los paquetes que han sido fragmentados, para posibilitar el re ensamblado total del paquete. Su valor indica el número de bloques de 8 bytes (sin contabilizar los bytes de la

cabecera) que estaban contenidos en los fragmentos previos. En el primer fragmento, o en un único fragmento, este valor es siempre 0. Tiempo de vida (8 bits). Contiene el tiempo máximo que un paquete puede permanecer en una red. Cada dispositivo por el que pasa el paquete decrementa el valor de este campo en el tiempo que tarda en procesar la cabecera IP, siendo 1 el valor mínimo. Si el valor llega a 0, el paquete es descartado. Esto garantiza que los paquetes no viajan a través de una red haciendo bucles, incluso si las tablas de encaminamiento son erróneas.

- Protocolo (8 bits). Indica al protocolo de nivel superior al que IP deberá pasar los datos del paquete. Por ejemplo, UDP es 17 y TCP es 6.
- Control de errores de la cabecera (16 bits). Es un campo para controlar los errores únicamente en la cabecera IP, exceptuando este campo.
- Dirección origen (32 bits). Es la dirección del origen del paquete.
- Dirección destino (32 bits). Es la dirección del destino del paquete.
- Opciones (variable). No son requeridas en todos los paquetes".

[25]"La cabecera de IPv6, descrita principalmente en la RFC 2460, elimina o hace opcionales varios campos de la cabecera de IPv4, consiguiendo una cabecera de tamaño fijo y más simple, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6 como lo muestra la figura 5".

[25] http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

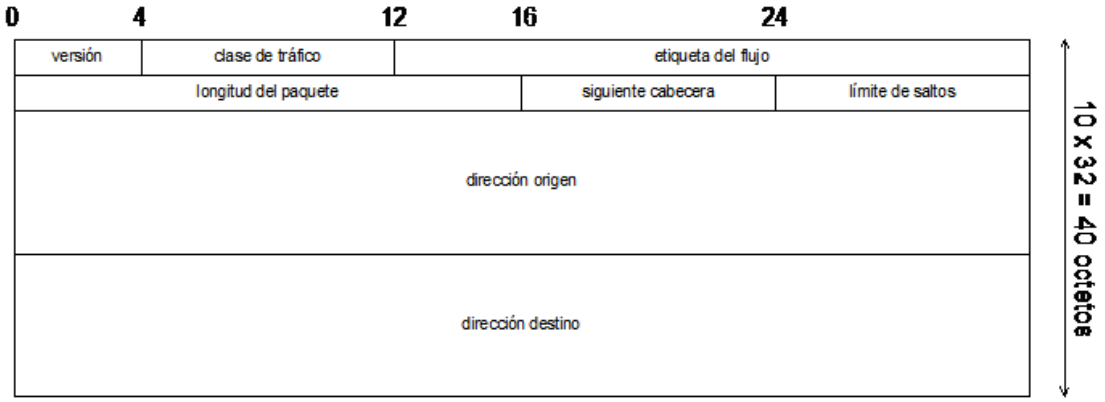


Figura 5 Cabecera de IPV6. Fuente:

http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

La cabecera básica de IPv6, tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

- Versión (4 bits). Es el número de versión de IP, es decir, 6.
- Clase de tráfico (8 bits). El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de la congestión.
- Etiqueta del flujo (20 bits). El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino específico. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20 bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo. La utilización de esta etiqueta, que identifica un camino a lo largo de la red, posibilita encaminar conmutar en vez de encaminar. Su uso viene descrito en la RFC 1809.

- Longitud del paquete (16 bits). Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.
- Siguiente cabecera (8 bits). Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.
- Límite de saltos (8 bits). Es el número de saltos máximo que le quedan al paquete. El límite de saltos es establecido a un valor máximo por el origen y decrementando en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es decrementado y toma el valor 0, el paquete es descartado.
- Dirección origen (128 bits). Es la dirección del origen del paquete.
- Dirección destino (128 bits). Es la dirección del destino del paquete.

[26]"De acuerdo a lo revisado, de los 12 campos de la cabecera de IPv4 se ha pasado a 8 campos en IPv6. El motivo fundamental por el que estos campos (tipo de servicio, indicadores, identificación y control de errores) son eliminados, es la innecesaria redundancia, en IPv4 se está facilitando la misma información de diversas formas, como es el caso del campo de control de errores, pues otros mecanismos de encapsulado de capas inferiores, por ejemplo IEEE 802, ya realizan esta función. El campo de desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que

[26] http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

se produce extremo a extremo. El único campo realmente nuevo en IPv6 es la etiqueta de flujo.

La información opcional a la estrictamente necesaria para encaminar los paquetes de datos, es codificada en cabeceras adicionales que pueden ubicarse entre la cabecera IPv6 y las cabeceras de niveles superiores, como por ejemplo la cabecera TCP/UDP. En la actualidad, hay un pequeño número de cabeceras de extensión (opciones de salto por salto, encaminamiento extendido, fragmentación y reensamblado, opciones del destino, autentificación, y encapsulación) estando cada una identificada por un valor distinto del valor del campo siguiente cabecera. Cada paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el valor del campo siguiente cabecera de la cabecera que la precede. Las cabeceras de extensión deben de ser procesadas en orden, ya que el contenido y semántica de cada una de ellas indican si se debe o no procesar la siguiente cabecera.

De esta forma, las cabeceras de extensión no son examinadas o procesadas por los nodos intermedios, sólo cuando lleguen al nodo que venga identificado por el campo de dirección de destino de la cabecera IPv6. La única excepción es la cabecera de opciones de salto por salto, que lleva información que debe ser procesada y examinada en todos los nodos por los que pasa el paquete, incluyendo los nodos origen y destino. La cabecera de opciones de salto por salto, cuando esté presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia se indica por el valor 0 en el campo de siguiente cabecera de la cabecera IPv6.

Cada cabecera de extensión tiene una longitud múltiplo entero de 8 octetos, con el fin de mantener el alineamiento de 8 octetos en las cabeceras siguientes. La razón de que los distintos campos de la cabecera estén alineados a 64 bits, es que la nueva generación de procesadores, de 64 bits pueden procesar dichos campos de una manera más eficiente".

2.2.13. Resolución de nombres de IPV6.[27]

"La resolución de nombres de host significa asignar correctamente un nombre de host a una dirección IPv6. Un nombre de host es un alias que se asigna a un nodo IPv6 para identificarlo como host IPv6. El nombre de host puede tener un máximo de 255 caracteres y puede incluir caracteres alfabéticos y numéricos, guiones y puntos. Es posible asignar varios nombres al mismo host.

Los programas de Windows Sockets (Winsock) pueden utilizar uno de dos valores para el destino al que desea conectarse: la dirección IPv6 o un nombre de host. Si se especifica la dirección IPv6, no es necesaria la resolución de nombres. Cuando se especifica un nombre de host, este nombre se debe resolver en una dirección IPv6 para que pueda iniciarse la comunicación basada en IPv6 con un recurso.

Los nombres de host pueden adoptar diversas formas. Las dos formas más comunes son sobrenombres y nombres de dominio. Los sobrenombres son alias de direcciones IPv6 que los usuarios pueden asignar y utilizar. Los nombres de dominio son nombres

[27] http://technet.microsoft.com/es-es/library/cc784659(v=ws.10).aspx

estructurados en un espacio de nombres jerárquico llamado Sistema de nombres de dominio (DNS, Domain Name System).

Los nombres de dominio se resuelven enviando consultas de nombres DNS a un servidor DNS configurado, que es un equipo donde se almacenan registros de asignación de nombre de dominio a dirección IPv6 o que tiene registros de otros servidores DNS. El servidor DNS resuelve el nombre de dominio consultado en una dirección IPv6 y devuelve el resultado. El cliente DNS de Windows XP y la familia de servidores de Windows Server 2003 admiten el procesamiento de registros de recursos AAAA (cuádruple A). Todas las consultas y respuestas DNS se envían mediante IPv6 e IPv4. También se admite la devolución de nombres DNS para nombres de dominio completos".

2.3. Principales Protocolos de IPV6.

2.3.1. Protocolo ICMPV6.

IPv6 para informar sobre los errores durante el procesamiento de los paquetes además del diagnóstico de otras funciones en la capa de internet utiliza el protocolo ICMPv6.

[28]"ICMPv6 es utilizado por los nodos IPv6 reportar errores encontrados en procesar paquetes y para realizar otras funciones de Internet-capa, como diagnósticos ("ping" ICMPv6). ICMPv6 es una parte integral de IPv6 y el protocolo de base (todos los

[28] http://tools.ietf.org/html/rfc4443

mensajes y los comportamientos necesarios por esta especificación) debe aplicarse plenamente por todos los nodos IPv6.

Mensajes ICMPv6 se agrupan en dos clases: los mensajes de error y mensajes informativos. Los mensajes de error son identificados por un cero en el bit de orden superior de sus valores de campo de tipo de mensaje. Por lo tanto, mensajes de error tienen tipos de mensaje de 0 a 127; los mensajes informativos tienen tipos de mensajes 128-255".

El formato general de los paquetes ICMPV6 lo podemos observar en la figura 6.

Paquete ICMPv6

Bit offset	0–7	8–15	16–31
0	Type	Code	Checksum
32	Message body		

Figura 6 Formato General de Paquete ICMPV6. Fuente: Internet.

2.3.2. Protocolo MLD ("Descubrimiento de escucha de multidifusión").[29]

"El tráfico de multidifusión se envía a una única dirección, pero se procesa en múltiples hosts. La multidifusión es similar a la suscripción a un boletín. Al igual que sólo los suscriptores reciben el boletín cuando se publica, sólo los equipos host que pertenecen al grupo de multidifusión reciben y procesan el tráfico enviado a la dirección reservada del grupo. El conjunto de hosts que atienden en una dirección de multidifusión específica se denomina grupo de multidifusión".

[29] http://technet.microsoft.com/es-es/library/cc776494(WS.10).aspx

“Las direcciones IPv6 de multidifusión son reservadas y se asignan a partir del prefijo de formato 1111 1111 (0xFF). En la siguiente tabla se incluye una lista parcial de direcciones IPv6 de multidifusión que están reservadas para multidifusión IPv6 y están registradas en la Autoridad de números asignados de Internet (IANA, Internet Assigned Numbers Authority)”.

Dirección IPv6 de multidifusión	Descripción
FF02::1	La dirección para todos los nodos utilizada para llegar a todos los nodos del mismo vínculo.
FF02::2	La dirección para todos los enrutadores utilizada para llegar a todos los enrutadores del mismo vínculo.
FF02::4	La dirección para todos los enrutadores de Protocolo de enrutamiento de multidifusión de vectores de distancia (DVMRP, Distance Vector Multicast Routing Protocol) utilizada para llegar a todos los enrutadores de multidifusión DVMRP del mismo vínculo.
FF02::5	La dirección para todos los enrutadores de Abrir primero la ruta más corta (OSPF, Open Shortest Path First) utilizada para llegar a todos los enrutadores OSPF del mismo vínculo.
FF02::6	La dirección para todos los enrutadores designados OSPF utilizada para llegar a todos los enrutadores designados OSPF del mismo vínculo.
FF02::1:FF*XX:XXXX*	La dirección de nodo solicitado utilizada en el proceso de resolución de direcciones para resolver la dirección IPv6 de un nodo local del vínculo en su dirección de nivel de vínculo. Los últimos 24 bits (*XX:XXXX*) de la dirección de nodo solicitado son los últimos 24 bits de una dirección IPv6 de unidifusión.

Tabla 3 Tabla de Ips multidifusión reservadas Fuente:http://msdn.microsoft.com/es-es/library/cc776494%28v=ws.10%29.aspx

“Cada grupo de multidifusión se identifica mediante una única dirección IPv6 de multidifusión. La dirección IPv6 reservada de cada grupo es compartida por todos los hosts miembros del grupo, que atienden y reciben los mensajes IPv6 enviados a la dirección del grupo.

Las direcciones IPv6 de multidifusión se asignan a un conjunto reservado de direcciones de multidifusión de Control de acceso a los medios (MAC, Media Access Control). La información acerca de la asignación de direcciones IPv6 de multidifusión a direcciones MAC de Ethernet, se encuentra en el documento RFC

2464, "Transmission of IPv6 Packets over Ethernet Networks" (Transmisión de paquetes IPv6 a través de redes Ethernet).

MLD se utiliza para intercambiar información acerca del estado de pertenencia entre los enrutadores IPv6 que admiten la multidifusión y los miembros de grupos de multidifusión en un segmento de red. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia. MLD está definido en el documento RFC 2710, "Multicast Listener Discovery (MLD) for IPv6"".

2.3.3. Protocolo ND ("Descubrimiento de Vecinos").[30]

"En IPv6, el protocolo semejante a ARP en IPv4, es el llamado protocolo de descubrimiento del vecino (ND, Neighbor Discovery). Este protocolo es el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros en su mismo enlace, determina sus direcciones en la capa de enlace, localiza los routers y mantiene la información de conectividad acerca de las rutas a los vecinos activos. La figura 7 muestra el protocolo ND.

[30] http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html

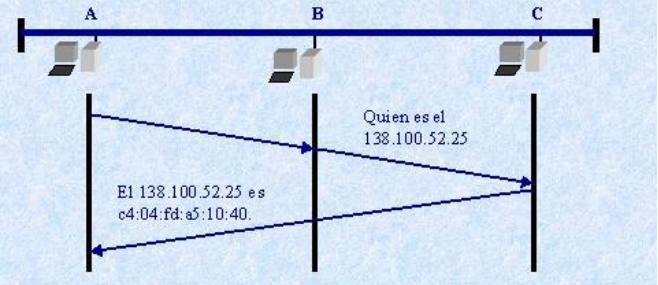


Figura 7 Protocolo ND. Fuente: ***http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html***

El protocolo ND se emplea también para mantener limpios los caches donde se almacena la información relativa al contexto de la red a la que está conectada un servidor o un router, y para detectar cualquier cambio en la misma. Si un router o una ruta falla, el servidor buscará alternativas funcionales.

ND emplea los mensajes ICMPv6 para algunos de sus servicios, este protocolo es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6".

ND define cinco tipos de mensajes ICMPv6:

- Solicitud de router. Generado por una interfaz cuando es activada, para pedir a los routers que se anuncien inmediatamente. Tipo de mensaje ICMPv6 133 código 0.

- Anunciación de router. Generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia a una solicitud de router, a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempo de vida, configuración de

direcciones, límite de salto sugerido, etc. Es importante para permitir la renumeración. Tipo de mensaje ICMPv6 134 código 0.

- Solicitud de vecino. Generado por los nodos para solicitar la dirección en la capa de enlace de la tarjeta de su vecino, o para verificar que el nodo vecino es alcanzable, así como para detectar las direcciones duplicadas. Las solicitudes son multicast cuando el nodo necesita resolver una dirección y unicast cuando el nodo quiere verificar que el vecino es alcanzable. Tipo de mensaje ICMPv6 135 código 0.
- Anunciación de vecino. Generado por los nodos como respuesta a la solicitud de vecino. Tipo de mensaje ICMPv6 136 código 0.
- Redirección. Generado por los routers para informar a los hosts de un mejor salto para llegar a un destino. Tipo de mensaje ICMPv6 137 código 0.

El protocolo de Descubrimiento de vecinos IPv6 corresponde a una combinación de los protocolos IPv4 ARP, descubrimiento de router ICMP, y redirección ICMP

A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto está en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace.

La detección de vecinos inalcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.

2.3.4. Protocolos de Enrutamiento.[31]

"Al igual que el enrutamiento entre dominios sin clase (CIDR, Classless Interdomain Routing) de IPv4, IPv6 utiliza un enrutamiento de concordancia de prefijo más largo. IPv6 utiliza versiones modificadas de la mayoría de los protocolos de enrutamiento comunes para administrar las direcciones IPv6 más largas y las diferentes estructuras de encabezado. Se puede visualizar en la figura 8 los servicios mejorados de enrutamiento en IPV6.

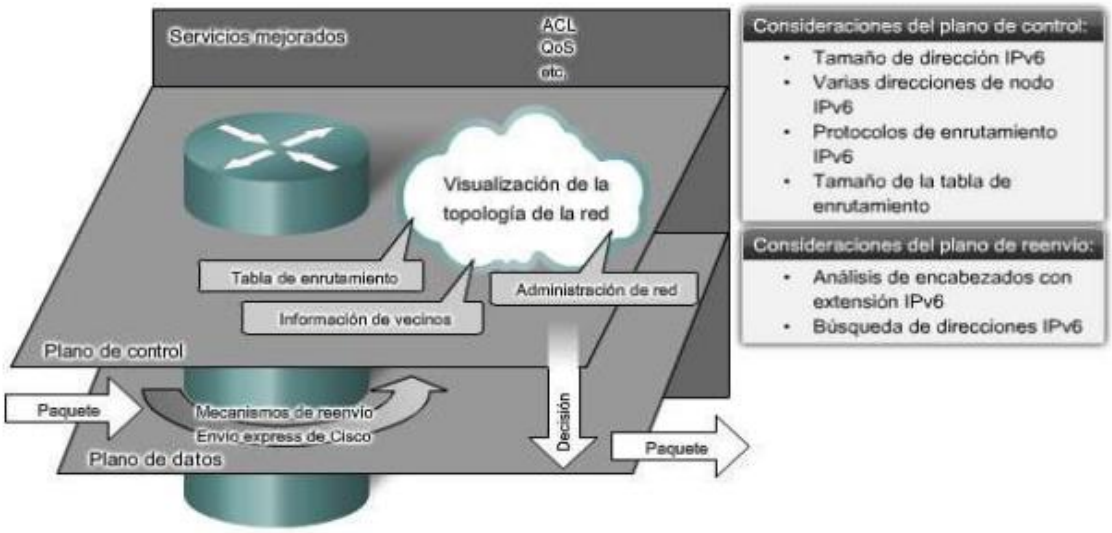


Figura 8 Servicios mejorados de enrutamiento en IPV6. Fuente:
http://www.franciscosepulveda.eu

Los espacios de dirección más grandes permiten asignaciones de direcciones grandes a los ISP y las organizaciones. Un ISP agrupa todos los prefijos de sus clientes en un único prefijo y lo anuncia en Internet IPv6. El mayor espacio de direcciones es suficiente para permitir a las organizaciones definir un único prefijo para toda su red".

[31] http://www.franciscosepulveda.eu

2.3.4.1. Consideraciones de Enrutamiento

Un breve resumen del funcionamiento de un router en una red será útil para mostrar cómo IPv6 afecta el enrutamiento. Conceptualmente, un router tiene tres áreas funcionales:

- El plano de control administra la interacción del router con los demás elementos de la red y proporciona la información necesaria para tomar decisiones y controlar el funcionamiento general del router. Este plano ejecuta procesos, tales como protocolos de enrutamiento y administración de red. Estas funciones en general son complejas.
- El plano de datos administra el reenvío de paquetes de una interfaz física o lógica a otra. Utiliza diferentes mecanismos de conmutación, por ejemplo, la conmutación de procesos y el envío express de Cisco (CEF, Cisco Express Forwarding) en routers con el software IOS de Cisco.
- Los servicios mejorados incluyen funciones avanzadas que se aplican al reenviar datos, por ejemplo, filtrado de paquetes, calidad de servicio (QoS, Quality Of Service), encriptación, traducción y contabilidad.

IPv6 presenta nuevos desafíos específicos para cada una de estas funciones.

2.3.4.1.1. Plano de control de IPv6

Al habilitar IPv6 en un router se inicia el proceso operativo del plano de control específicamente para IPv6. Las características del protocolo definen el

rendimiento de estos procesos y la cantidad de recursos necesarios para operarlos:

- Tamaño de la dirección IPv6: el tamaño de la dirección afecta las funciones de procesamiento de la información de un router. Los sistemas que utilizan una estructura de memoria, bus o CPU de 64 bits pueden transmitir una dirección IPv4 de origen y destino en un único ciclo de procesamiento. Para IPv6, las direcciones de origen y destino requieren dos ciclos cada una, o sea cuatro ciclos, para procesar la información de las direcciones de origen y destino. Como resultado, los routers que utilizan exclusivamente procesamiento de software probablemente tengan un rendimiento más lento que en un entorno IPv4.
- Varias direcciones de nodos IPv6: como los nodos IPv6 pueden usar varias direcciones unicast IPv6, el consumo de memoria caché para la detección de vecinos puede verse afectado.
- Protocolos de enrutamiento IPv6: los protocolos de enrutamiento IPv6 son similares a sus contrapartes IPv4, pero como un prefijo IPv6 es cuatro veces más grande que un prefijo IPv4, las actualizaciones de enrutamiento deben transportar más información.
- Tamaño de la tabla de enrutamiento: el mayor espacio de dirección IPv6 genera redes más grandes y hace que aumente mucho el tamaño de Internet. Esto hace que se necesiten tablas de enrutamiento más grandes y más requisitos de memoria para su funcionamiento.

2.3.4.1.2. Plano de datos de IPv6

El plano de datos reenvía paquetes IP en función de las decisiones tomadas por el plano de control. El motor de reenvío analiza la información relevante del paquete IP y hace una búsqueda para establecer una equivalencia entre la información analizada y las políticas de reenvío definidas por el plano de control. IPv6 afecta el rendimiento de las funciones de análisis y búsqueda:

- Análisis de los encabezados de extensión IPv6: las aplicaciones, incluido IPv6 móvil, con frecuencia utilizan información de la dirección IPv6 en los encabezados de extensión, lo que hace que aumenten de tamaño. Estos campos adicionales requieren procesamiento adicional. Por ejemplo, un router que utiliza ACL para filtrar información de Capa 4 necesita aplicar las ACL tanto a los paquetes que tienen encabezados de extensión como a los que no los tienen. Si la longitud del encabezado de extensión excede la longitud fija del registro de hardware del router, la conmutación por hardware genera un error y los paquetes pueden ser derivados a conmutación por software o descartados. Esto afecta seriamente el rendimiento de reenvío del router.

- Búsqueda de direcciones IPv6: IPv6 realiza una búsqueda en los paquetes que ingresan al router para encontrar la interfaz de salida correcta. En IPv4, el proceso de decisión de reenvío analiza una dirección de destino de 32 bits. En IPv6, la decisión de reenvío puede requerir el análisis de una dirección de destino de 128 bits. La mayoría de los routers actuales realizan búsquedas mediante un circuito integrado de aplicación específica (ASIC,

Application-Specific Integrated Circuit) con una configuración fija que realiza las funciones para las que fue diseñado originalmente: IPv4. Nuevamente, esto puede dar como resultado que los paquetes sean derivados a un procesamiento por software que es más lento o que sean descartados por completo.

2.3.4.2. Protocolo RIPng.

Las rutas de IPv6 usan los mismos protocolos y las mismas técnicas que IPv4. Si bien las direcciones son más largas, los protocolos utilizados en el enrutamiento IPv6 son simplemente extensiones lógicas de los protocolos utilizados en IPv4.

RFC 2080 define el protocolo de información de routing de siguiente generación (RIPng, Routing Information Protocol Next Generation) como un protocolo de enrutamiento simple basado en RIP. RIPng no es ni más ni menos potente que RIP, pero proporciona una manera sencilla de crear una red IPv6 sin necesidad de crear un nuevo protocolo de enrutamiento.

RIPng es un protocolo de enrutamiento vector distancia con un límite de 15 saltos que usa Actualizaciones de envenenamiento en reversa y horizonte dividido para evitar routing loops. Su simplicidad proviene del hecho de que no requiere ningún conocimiento global de la red. Sólo los routers vecinos intercambian mensajes locales.

RIPng incluye las siguientes características:

- Basado en IPv4 RIP versión 2 (RIPv2) y es similar a RIPv2.

- Usa IPv6 para el transporte.
- Incluye el prefijo IPv6 y la dirección IPv6 del siguiente salto.
- Usa el grupo multicast FF02::9 como dirección de destino para las actualizaciones de RIP (similar a la función de broadcast que realiza RIP en IPv4)
- Envía actualizaciones por el puerto UDP 521.
- Es compatible con Cisco IOS Release 12.2(2)T y posteriores

En implementaciones de stack doble, se necesitan RIP y RIPng.

Hay dos pasos básicos para activar IPv6 en un router.

Primero, debe activar el reenvío de tráfico IPv6 en el router y, a continuación, debe configurar cada una de las interfaces que requiere IPv6.

De forma predeterminada, el reenvío de tráfico IPv6 está deshabilitado en los routers Cisco. Para activarlo entre interfaces, debe configurar el comando global ipv6 unicast – routing.

El comando ipv6 address puede configurar una dirección IPv6 global. La dirección link-local se configura automáticamente cuando se asigna una dirección a la interfaz. Debe especificar la dirección IPv6 completa de 128 bits o debe especificar el uso de un prefijo de 64 bits con la opción eui-64.

Al configurar los protocolos de enrutamiento admitidos en IPv6, se debe crear el proceso de enrutamiento, habilitar el proceso de enrutamiento en las interfaces y personalizar el protocolo de enrutamiento para una red en particular.

2.3.4.3. Protocolo OSPFV3 E IPV6.

[32]"Es un protocolo de enrutamiento por estado del enlace el cual fue descrito por primera vez en el RFC 2740. El protocolo OSPFv3 trabaja con direcciones IPv6, distribuyendo por la red solamente el prefijo de estas direcciones. No posee soporte para direcciones IPv4, razón por la cual si se desea tener dentro de la misma red direcciones IPv6 y direcciones IPv4 se deben configurar tanto el protocolo OSPFv2 como su versión 3.

El protocolo OSPFv3 tiene los mismos fundamentos que el protocolo OSPFv2 (Algoritmo SPF, inundaciones, elección del DR, áreas, métricas, temporizadores), pero a pesar de tener ciertas similitudes también poseen diferencias entre las cuales tenemos:

- OSPFv3 trabaja sobre un enlace en vez de hacerlo sobre subred.
- La topología OSPFv2 no soporta el protocolo IPv6.
- OSPFv3 posee un mecanismo de autenticación (RFC 4552).
- OSPFv3 posee múltiples instancias por enlace".

[32] http://entendiendo-redes-ae.blogspot.com/2010/07/aspectos-basicos-de-ospfv3.html

2.3.4.3.1. Configuración de OSPF para IPv6

- Habilitar el protocolo de encaminamiento OSPFv3 para IPv6 en todos los routers usar área 0 para OSPFv3.
- Habilitar CEF switching para IPv6 en los routers CISCO.
- Habilitar el proceso OSPFv3 que haya configurado en el paso 1 en todas las interfaces de su router (excepto las interfaces de loopback). Usar área para OSPFv3.
- Comprobar que las conexiones OSPFv3 se han establecido entre los routers.
- Redistribuir las direcciones de loopback en OSPFv3.
- Comprobar que todos los routers reciben todos los prefijos de las interconexiones y de loopback vía OSPFv3.
- Comprobar que se llega a la dirección de loopback de todos los routers desde su router utilizando el comando ping.

2.3.4.4. Protocolo BGP-4 ("Border Gateway Protocol").

"BGP es un protocolo de enrutamiento diseñada para proporcionar vínculos de enrutamiento sin bucles entre las organizaciones. BGP está diseñado para funcionar en un protocolo de transporte fiable; que utiliza TCP (puerto 179), como el protocolo de transporte como TCP es un protocolo orientado a la conexión. El puerto TCP de destino se le asigna 179, y el puerto local se le asigna un número de puerto aleatorio. El Software de Cisco soporta BGP versión 4 y es esta versión que

ha sido utilizado por los proveedores de servicios de Internet (ISP) para ayudar a construir la Internet. RFC 1771 presentó y discutió un número de nuevas características BGP para permitir el protocolo a escala para el uso de Internet. RFC 2858 introdujo extensiones multiprotocolo BGP para permitir llevar la información de enrutamiento de rutas de multidifusión IP y múltiples familias de direcciones de protocolo de Capa 3, incluyendo IPv4, IPv6 y CLNS.

BGP se utiliza principalmente para conectar una red local a una red externa para obtener acceso a Internet o para conectarse a otras organizaciones. Cuando se conecta a una organización externa, se crean sesiones BGP (eBGP) peering externos. Aunque BGP se conoce como un protocolo de pasarela exterior (EGP), muchas redes dentro de una organización se están volviendo tan complejo que BGP se puede utilizar para simplificar la red interna utilizado dentro de la organización.

BGP utiliza un algoritmo de encaminamiento ruta-vector para el intercambio de información de accesibilidad de la red con otros dispositivos de red de habla BGP. Información de accesibilidad de la red se intercambia entre los interlocutores BGP en las actualizaciones de enrutamiento. Información de accesibilidad de red contiene el número de red, los atributos de ruta específica, y la lista de números de sistema autónomo que una ruta obligada de tránsito para llegar a una red de destino.

Esta lista se encuentra en el atributo AS-path. BGP evita los bucles de enrutamiento al rechazar cualquier actualización de enrutamiento que contiene el número de sistema autónomo local, porque esto indica que la ruta ya ha viajado a través de ese sistema autónomo y por lo tanto se creará un bucle. La ruta-vector algoritmo

de enrutamiento BGP es una combinación de la algoritmo de enrutamiento de vector de distancia y la detección de bucle AS-path.

BGP selecciona una sola ruta, por defecto, como el mejor camino a un destino de acogida o de la red. El mejor algoritmo de selección de ruta analiza ruta atributos para determinar qué ruta se instala como la mejor ruta en la tabla de enrutamiento BGP. Cada camino lleva atributos conocidos obligatorios, conocidos discrecionales y opcionales transitivos que se utilizan en BGP mejor análisis de la ruta. Cisco y su software proporciona la capacidad de influir en la selección de rutas BGP alterando algunos de estos atributos utilizando la interfaz de línea de comandos (CLI.) de selección de ruta BGP también puede ser influenciada a través de la configuración de políticas BGP estándar".

BGP utiliza el algoritmo de selección de la mejor ruta para encontrar un conjunto de rutas igualmente buenas. Estas rutas son las multipaths potenciales. En Cisco IOS versión 12.2 (33) SRD y versiones posteriores, cuando hay más igualmente buenos multipaths disponibles que el número máximo permitido, los caminos más antiguos son seleccionados como multipaths.

BGP se puede utilizar para ayudar a manejar las redes internas complejas mediante una interfaz con protocolos de gateway interior (IGP). BGP interno puede ayudar con problemas tales como la ampliación de las IGPs existentes para satisfacer las demandas de tráfico y mantener la eficiencia de la red.

No hay BGP real para IPv6. El soporte IPv6 se deriva de la capacidad de BGP-4 para el intercambio de información acerca de los protocolos de capa de red distintos

de IPv4. Estas extensiones multiprotocolo de BGP-4 se definen en el RFC 2858, que deja obsoleto el RFC 2283. RFC 2283 se menciona aquí porque es el documento base para el RFC 2545, que define las extensiones de IPv6 para BGP-4.

2.3.5. Direccionamiento de IPV6.

[33]"Los cambios introducidos por IPv6 no sólo son en cantidad de direcciones sino que incluyen nuevos tipos, representaciones y sintaxis".

2.3.5.1. Tipos de direcciones IPv6

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

- Unicast. Se utiliza únicamente para identificar una interfase de un nodo IPv6.
- Multicast. Se utiliza para identificar a un grupo de interfases IPv6.
- Anycast. Se asigna a múltiples interfases (usualmente en múltiples nodos).

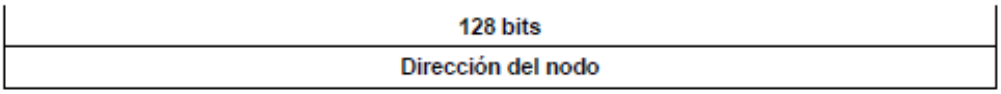
Cada uno de los tres tipos se subdivide en direcciones diseñadas para resolver casos específicos de direccionamiento IP, los cuales a continuación se presentan y describen".

[33] http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

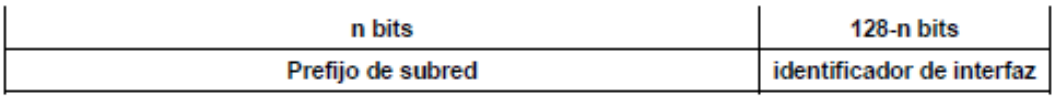
2.3.5.1.1. Direcciones Unicast.[34]

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Hay varias formas de asignación de direcciones unicast.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:



Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que está conectado:



Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El "identificador de interfaz" se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz

[34] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de direcciones unicast de uso local: Local de Enlace (Link-Local) y Local de Sitio (Site-Local).

- Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers. Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Se trata de direcciones FE80::<ID de interfaz>/10.

- Las direcciones locales de sitio permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea "local de sitio" (su ámbito está limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	Identificador de interfaz

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10.

2.3.5.1.2. Direcciones anycast (RFC2526)[35]

"Tal y como se ha indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast.

Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast. Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	0000000000000000000

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del router de la subred", serán enviados a un router de la subred.

[35] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred. La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/local" igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	1111110111 ... 111	ID anycast
	Identificador de interfaz	

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema".

n bits	121-n bits	7 bits
Prefijo de subred	1111111 ... 1111111	ID anycast
	Identificador de interfaz	

2.3.5.1.3. Direcciones multicast (RFC2375)[36]

"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.

Las direcciones multicast tienen el siguiente formato:

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

El bit "T" indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits "ámbito" tienen los siguientes significados expuestos en la tabla 4:

[36] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

Tabla 4. Significados de bits. Fuente: Internet

El "Identificador de Grupo", identifica, el grupo de multicast concreto al que se refiriere, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si se asigna una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

- FF01::101 significa todos los NTS en el mismo nodo que el paquete origen.
- FF02::101 significa todos los NTS en el mismo enlace que el paquete origen.
- FF05::101 significa todos los NTS en el mismo sitio que el paquete origen.
- FF0E::101 significa todos los NTS en Internet.

Las direcciones multicast no-permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de

sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

- FF01:0:0:0:0:0:0:1 – todos los nodos (ámbito local).
- FF02:0:0:0:0:0:0:1 – todos los nodos (ámbito de enlace).
- FF01:0:0:0:0:0:0:2 – todos los routers (ámbito local).
- FF02:0:0:0:0:0:0:2 – todos los routers (ámbito de enlace).
- FF05:0:0:0:0:0:0:2 – todos los routers (ámbito de sitio).

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original.

Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada".

2.3.6. Representación de direcciones IPv6[37]

"Una dirección IPv6 consiste de 128 bits. Como una dirección de 128 bits, se ha diseñado un formato de representación, hexadecimal, que permite una visualización mucho más sencilla, y a la vez una relación con la representación binaria.

1. La representación de las direcciones IPv6 sigue el siguiente esquema:

   x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es necesario escribir los ceros a la izquierda en cada campo. Ejemplo:

   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

   1080:0:0:0:8:800:200C:417A

2. Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits, se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits. Este símbolo solo puede aparecer una vez en la dirección IPV6. Ejemplo:

   Las direcciones:

   - 1080:0:0:0:8:800:200C:417A (una dirección unicast).
   - FF01:0:0:0:0:0:0:101 (una dirección multicast).

[37]http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

- 0:0:0:0:0:0:0:1 (la dirección loopback).
- 0:0:0:0:0:0:0:0 (una dirección no especificada).

Pueden representarse como:

- 1080::8:800:200C:417A (una dirección unicast).
- FF01::101 (una dirección multicast).
- ::1 (la dirección loopback).
- :: (una dirección no especificada).

3. Una forma alternativa y muy conveniente cuando nos hallamos en un entorno mixto IPv4 e Ipv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las cuatro porciones de 8 bits de menor peso (Ipv4). Ejemplo:

    - 0:0:0:0:0:0:13.1.68.3
    - 0:0:0:0:0:FFFF:129.144.52.38

    Pueden representarse como:

    - ::13.1.68.3
    - ::FFFF:129.144.52.38

    Las reglas exactas de representación de las direcciones IPv6 se pueden constan en el RFC5952".

2.3.7. Prefijos de direcciones.[38]

"Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4. Un prefijo de dirección IPv6 se representa con la siguiente notación:

direccion-ipv6/longitud-prefijo, donde:

- direccion-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
- longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

2.3.8. Enrutamiento de IPV6.[39]

"El enrutamiento es el proceso de reenviar paquetes entre segmentos de red conectados. En las redes basadas en IPv6, el enrutamiento es la parte de IPv6 que proporciona capacidades de reenvío entre hosts que se encuentran en segmentos independientes que pertenecen a una red mayor basada en IPv6.

IPv6 es la oficina de correos donde se ordenan y entregan los datos de IPv6. Cada paquete entrante o saliente se denomina paquete IPv6. Un paquete IPv6 contiene la dirección de origen del host que realiza el envío y la dirección de destino del host receptor. A diferencia de las direcciones de nivel de vínculo, las direcciones

[38] http://www.rau.edu.uy/ipv6/queesipv6.htm
[39] http://msdn.microsoft.com/es-es/library/cc758763(v=ws.10).aspx

IPv6 del encabezado IPv6 no suelen cambiar cuando el paquete se transmite por una red IPv6.

El enrutamiento es la función principal de IPv6. Los paquetes IPv6 se intercambian y procesan en cada host mediante IPv6 en el nivel de Internet.

Por encima del nivel IPv6, los servicios de transporte del host de origen pasan los datos en forma de segmentos TCP o mensajes UDP al nivel IPv6. El nivel IPv6 crea los paquetes IPv6 con la información de las direcciones de origen y destino, que se utiliza para enrutar los datos a través de la red. Después, el nivel IPv6 pasa los paquetes al nivel inferior del vínculo, donde los paquetes IPv6 se convierten en tramas para su transmisión a través de los medios específicos de una red física. Este proceso se produce en el orden inverso en el host de destino.

En cada host remitente, los servicios del nivel IPv6 examinan la dirección de destino de cada paquete, comparan esta dirección con una tabla de enrutamiento mantenida localmente y, después, determinan qué acción de reenvío adicional es necesaria. Los enrutadores IPv6 están conectados a dos o más segmentos de red IPv6 habilitados para reenviar paquetes entre ellos".

2.3.9. Tabla de enrutamiento IPv6

Todos los equipos que ejecutan IPv6 determinan cómo deben reenviar los paquetes en función del contenido de la tabla de enrutamiento IPv6.

Las entradas de la tabla de enrutamiento IPv6 constan de los elementos siguientes:

- Un prefijo de dirección.

- La interfaz a través de la cual se envían los paquetes que coinciden con el prefijo de dirección.
- Una dirección de reenvío o salto siguiente.
- Un valor de preferencia que se utiliza para seleccionar entre varias rutas que tengan el mismo prefijo.
- La duración de la ruta.
- La especificación de si la ruta está publicada (anunciada en un Anuncio de enrutamiento).
- La especificación de caducidad de la ruta.
- El tipo de ruta

La tabla de enrutamiento IPv6 se genera automáticamente y está basada en la configuración IPv6 actual del equipo. Al reenviar los paquetes IPv6, el equipo busca en la tabla de enrutamiento la entrada más similar a la dirección IPv6 de destino. La ruta para el prefijo local del vínculo (FE80::/64) no se muestra.

La ruta predeterminada (una ruta con un prefijo de ::/0) se suele utilizar para reenviar un paquete IPv6 a un enrutador predeterminado del vínculo local. Como el enrutador que corresponde al enrutador predeterminado contiene información acerca de los prefijos de red de las demás subredes IPv6 del conjunto de redes IPv6 mayor, reenvía el paquete a otros enrutadores hasta que finalmente se entrega en el destino.

2.4. Ventajas y desventajas de IPv6.

Ipv6 como ofrece una mayor cobertura con respecto al número de direcciones en respuesta a la falta de Ip's del protocolo IPv4, sin embargo esta no es la única ventaja que ofrece.

2.4.1. Ventajas:

- Asignación de Ips desde el cliente: esto quiere decir que dentro de una red IPv6 no es necesario que un dispositivo o servidor DHCP se encargue de generar IPs. Esto también influye en amenorar el trabajo de los router que se encargaban del asignamiento.
- Cifrado e IPsec integrados: IPv6 es un protocolo más seguro ya que de serie trabaja de manera cifrada, si se intercepta una comunicación, la información no podrá ser leída sin antes descrifrarla.
- Mejor rendimiento, fin de los checksum: IPv6 elimina las sumas de verificación ya que dispone de un mecanismo de control de errores propio y no hay necesidad de realizar los tradicionales checksums. Esto implica que la conexión será más rápida y el tiempo de respuesta mucho menor.
- Mejora la calidad de servicio (QoS), ahora llamado "Flow Labeling"
- IPv6 Mejora el proceso de enrutamiento de paquetes.
- Simplificación del formato del "Header", eliminando algunos campos del Header IPv4 o haciéndolos opcionales.
- Capacidad de etiquetas de flujo. Esta capacidad puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de

tráfico particular que requiere manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real.

- IPv6 incluye en su estándar el mecanismo "plug and play", lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración se realiza automáticamente. Esto permite que al conectar una máquina a una red IPv6, se le asigne automáticamente una (ó varias) direcciones IPv6.
- Renumeración y "multihoming". Es posible cambiar el formato de numeración manteniendo la misma dirección IP facilitando así el cambio de proveedor de servicios.

2.4.2. Desventajas:[40]

- "La necesidad de extender un soporte permanente. Necesita una dirección IPv4 o algún tipo de NAT en los routers pasarela. Problemas restantes de arquitectura. Más difíciles de memorizar.
- La mayoría de redes son ipv4 entonces la implementación total de ipv6 sería muy costosa y tardaría mucho tiempo mientras tanto se requieren la implementación de los mecanismos de transición para la interacción de las 2 redes".

2.5. Mecanismos de Transición de Ipv4 a Ipv6.

De acuerdo al documento [RFC4213] la clave para una transición exitosa está en la compatibilidad con la gran base instalada de hosts y routers IPv4. Al mantener la

[40] http://alejandromartinezclase.wordpress.com/ipv6-caracteristicas-ventajas-y-desventajas/

compatibilidad con IPv4 mientras se distribuye IPv6 se mejorará la tarea de migrar el internet hacia IPv6.

Tomando en cuenta la infraestructura de la UIDE es necesario crear un plan donde la coexistencia sea la base para la migración, para esto es vital conocer los diversos mecanismos de transición.

2.5.1. Doble Pila.

En general, el término doble pila se refiere a una duplicación completa de todos los niveles de la pila de protocolos de aplicaciones en la capa de red. Un ejemplo de duplicación completa es un sistema que ejecuta los protocolos OSI y TCP/IP.

En este protocolo los hosts, el servidor y el enrutador en la red pueden manejar una pila de IPv4 y una IPv6 de forma simultánea. Cuando las dos pilas son utilizadas en los nodos conectados a las redes en los cuales ambos protocolos están habilitados simultáneamente, el modo de pila dual provee a los nodos la flexibilidad para establecer sesiones extremo a extremo sobre IPv4 o IPv6.

[41]"El protocolo doble pila es muy sencillo de implementar un requisito es que los hosts y los routers soporten ambas versiones de IP y, por tanto, servicios y aplicaciones tanto IPv4 como IPv6.

El enfoque de doble pila es un mecanismo fundamental para introducir IPv6 en las arquitecturas IPv4 actuales y se prevee que siga siendo muy utilizado en el futuro. Su punto flaco es que obliga a que cada máquina retenga una dirección IPv4, cada vez

[41] http://www.networkworld.es/archive/de-ipv4-a-ipv6-asegurando-la-coexistencia

más escasas. Así, a medida que se difunde IPv6, la técnica de doble pila tendrá que ser aplicada allí donde específicamente ayuda al proceso de transición, por ejemplo en routers y servidores. Un servidor de doble pila puede soportar clientes sólo IPv4 convencionales, nuevos clientes sólo IPv6, y por supuesto clientes de doble pila. Para aquellos casos en que haya insuficientes direcciones IPv4 se ha definido una combinación del modelo de conversión y de doble pila de protocolos, conocido como DSTM (Dual Stack Transition Mechanism). En la figura 9 se observa el mecanismo de doble pila".

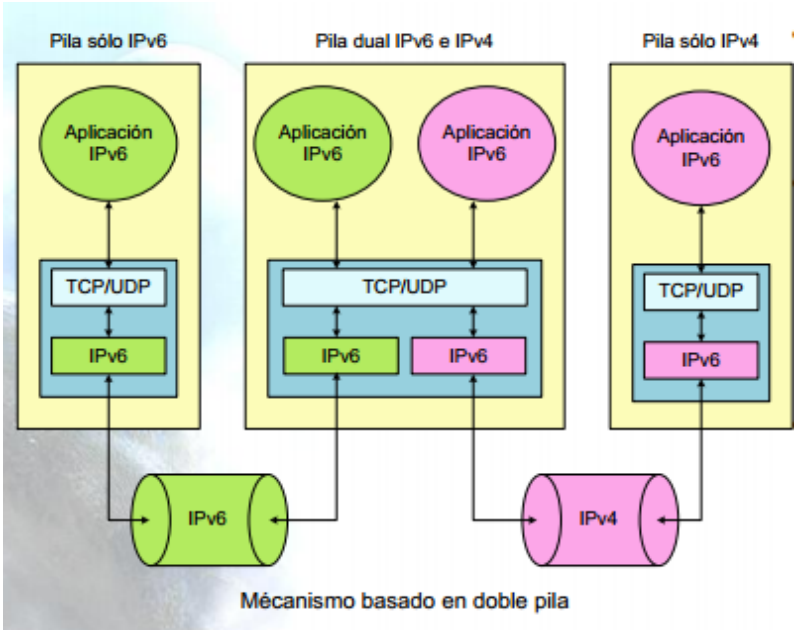


Figura 9 Arquitectura Doble Pila Fuente: internet

2.5.2. Tipo Túnel

[42]"Para minimizar las dependencias en un sitio de IPv4/IPv6 de doble pila, todos los enrutadores de la ruta entre dos nodos IPv6 no necesitan ser compatibles con IPv6.

[42] http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-47/index.html

El mecanismo que admite esta clase de configuración en red se denomina colocación en túneles. Básicamente, los paquetes de IPv6 se colocan en paquetes de IPv4, que luego se enrutan a través de enrutadores de IPv4. La figura 10 ilustra el mecanismo de colocación en túneles mediante enrutadores de IPv4.

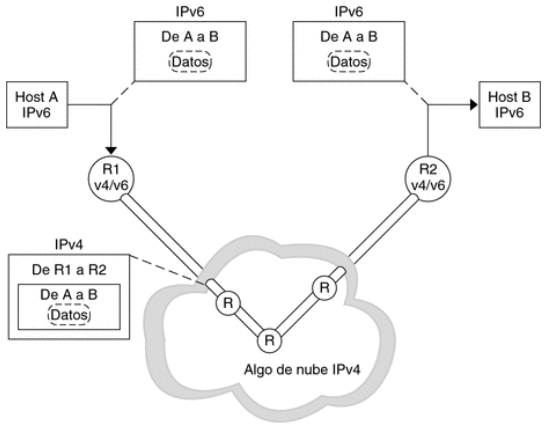


Figura 10 Mecanismo de túneles de IPV6 Fuente:http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-47/index.html

Los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Se pueden utilizar dos tipos de túneles: configurados y automáticos la figura 11 presenta la ilustración de los niveles de los túneles.

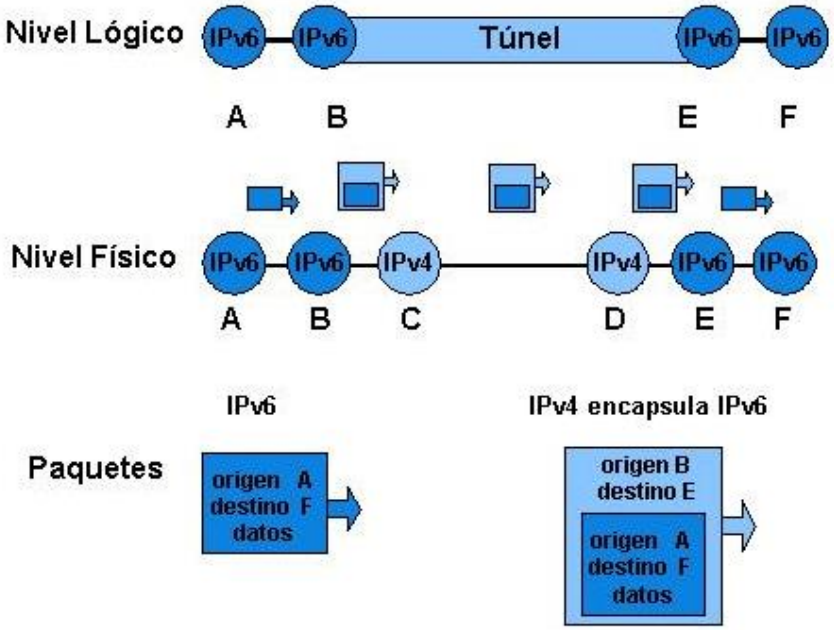


Figura 11 Nivel lógico y físico en el uso de Túneles. Fuente:

http://www.rau.edu.uy/ipv6/queesipv6.htm#12

2.5.2.1. Túneles configurados o manuales. [RFC3904][43]

"Un túnel configurado requiere la configuración manual de los puntos finales del túnel. En un túnel configurado, las direcciones IPv4 de los puntos finales del túnel no derivan de direcciones dentro de las direcciones IPv6 origen y destino o de las direcciones del siguiente salto de la ruta correspondiente.

Típicamente, las configuraciones de túnel entre ruteadores se configuran manualmente. La configuración de la interfaz del túnel consiste en las direcciones IPv4 de los puntos finales del túnel, las cuales deben de ser configuradas manualmente junto con las rutas estáticas que usa la interfaz del túnel. Un router o host se identifica a sí

[43]http://www.tlalpan.uvmnet.edu/oiid/download/T%C3%BAneles%20en%20IPv6%20gesti%C3%B3n%20PO%20TI.pdf

mismo a un servicio de túnel para establecer un servicio configurado con un router de túnel explícitamente definido la figura 12 representa un túnel configurado".

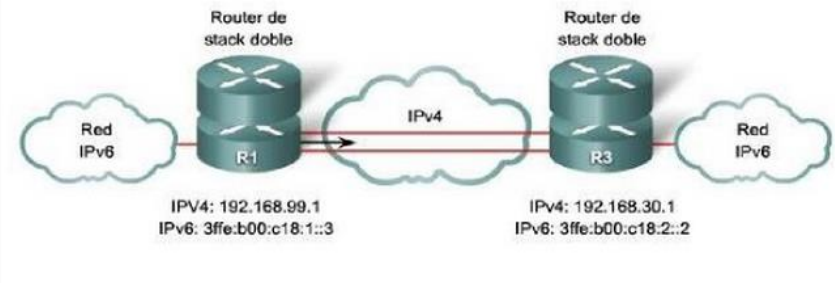


Figura 12 Túnel configurado Fuente: http://ipv4to6.blogspot.com/p/tunelizacion-ipv6.html

[44]"En esencia un túnel configurado en forma manual equivale a un enlace permanente entre dos dominios IPv6 sobre un enlace troncal IPv4. El uso principal es para conexiones estables que requieren comunicación segura periódica entre dos routers de borde, entre un sistema final y un router de borde o para conexión con redes IPv6 remotas. Los routers de borde deben ser de stack doble y la configuración no puede cambiar dinámicamente a medida que cambian las necesidades de la red y de enrutamiento.

Para la administración se configuran una dirección IPv6 estática de manera manual en una interfaz de túnel y se asignan las direcciones IPv4 estáticas configuradas manualmente al origen y al destino del túnel. El host o el router de cada extremo de un túnel configurado debe admitir stacks de protocolos IPv4 e IPv6. Los túneles configurados manualmente pueden establecerse entre dos routers de borde o entre un router de borde y un host".

[44] http://ipv4to6.blogspot.com/p/tunelizacion-ipv6.html

La configuración de los túneles tanto en los routers y host se pueden realizar de varias formas:[45]

1. Router a Router: Cada extremo es un nodo dual y en ellos se configura direcciones IPv6 e IPv4 tanto local como remotas.
2. Host a Router (GRE/IPv6): Los host IPv6/IPv4 pueden pasar paquetes IPv6 por un router IPv6/IPv4 Intermediario que sea alcanzable por la infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete.
3. Host a Host: host con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
4. 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.

2.5.2.2. Túneles automáticos.

Los túneles automáticos, permiten interconectar redes aisladas de IPv6 a través de una infraestructura de IPv4. Los túneles se crean de manera dinámica (punto - multipunto) y se encapsulan dentro de paquetes de Ipv4

2.5.2.3. Túnel 6TO4

[46]"Un túnel 6to4 proporciona conectividad IPv6 a todas las ubicaciones 6to4 en cualquier parte. Asimismo, el túnel ejerce como vínculo con todas las ubicaciones IPv6, incluida Internet IPv6 nativa, siempre que el enrutador se configure para reenviar a un enrutador de repetición. La figura siguiente ilustra la

[45] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf
[46] http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-50/index.html

forma en que un túnel 6to4 proporciona esta clase de conectividad entre sitios 6to4 en la figura 13 muestra dos redes 6to4 independientes, Site A y Site B. Cada ubicación tiene configurado un enrutador con una conexión externa a una red IPv4. Un túnel 6to4 en la red IPv4 proporciona una conexión para vincular ubicaciones 6to4".

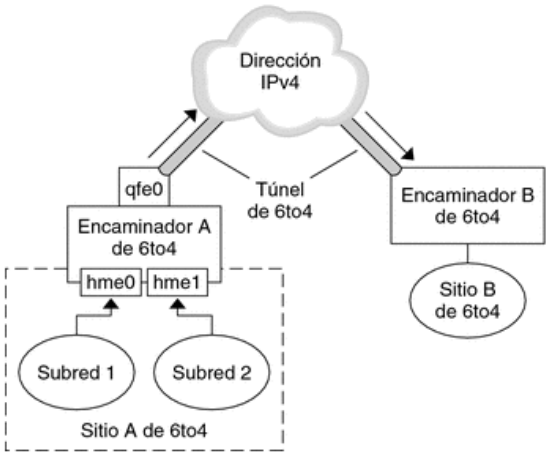


Figura 13 Túnel entre dos Ubicaciones. Fuente: ***http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-50/index.html***

Antes de que una ubicación IPv6 pueda convertirse en 6to4, debe configurar al menos una interfaz de enrutador para que admita 6to4. Esta interfaz debe proporcionar la conexión externa a la red IPv4. La dirección configurada en qfe0 debe ser única globalmente. En la figura 13, la interfaz qfe0 del enrutador de límite de sistema Router A conecta la ubicación Site A con la red IPv4. La interfaz qfe0 ya debe estar configurada con una dirección IPv4 antes de que sea posible configurar qfe0 como una pseudointerfaz 6to4.

En la figura 13, la ubicación 6to4 Site A está compuesta de dos subredes, que están conectadas a las interfaces hme0 y hme1 del enrutador Router A. Todos los hosts IPv6 de ambas subredes de la ubicación Site A se reconfiguran automáticamente con direcciones derivadas 6to4 al recibir el anuncio del enrutador Router A.

[47]"La ubicación Site B es otra ubicación 6to4 aislada. Para recibir correctamente tráfico de la ubicación Site A, se debe configurar un enrutador de límite en la ubicación Site B para admitir 6to4. De no ser así, los paquetes que reciba el enrutador de Site A no se reconocen y se descartan".

[48]6to4 se describe en el documento RFC 3056. Los hosts 6to4 no requieren configuración manual y crean direcciones 6to4 mediante configuración automática estándar. En 6to4 se utiliza el prefijo de dirección global 2002:WWXX:YYZZ::/48, donde WWXX:YYZZ es la representación hexadecimal con dos puntos de una dirección IPv4 pública (w.x.y.z) que está asignada a un sitio o host. WWXX:YYZZ es la parte de Agregador de siguiente nivel (NLA, Next Level Aggregator) de una dirección 6to4.

El servicio 6to4 permite que los sitios y hosts habilitados para IPv6 se comuniquen mediante direcciones IPv6 de unidifusión a través de Internet. Los sitios y hosts IPv6 pueden utilizar su prefijo de dirección 6to4 e Internet para comunicarse sin necesidad de obtener un prefijo de dirección global IPv6 de un proveedor de servicios Internet y conectarse a la red Internet IPv6.

[47] http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-50/index.html
[48] http://msdn.microsoft.com/es-es/library/cc736336%28v=ws.10%29.aspx

2.5.2.4. Túnel 6OVER4

[49]"IPv6 over IPv4, comúnmente se le conoce como "6over4" o "Virtual Ethernet" (se entiende como una capa de enlace virtual), también es denominado túnel de multidifusión o multicast de IPv4, es una técnica de túneles automáticos ya sea de equipo a equipo, de equipo a ruteador o de ruteador a equipo que se describe en el documento RFC 2529. El servicio 6over4 permite la comunicación entre nodos IPv6 e IPv4 mediante IPv6 a través de una infraestructura IPv4. En 6over4 se utiliza la infraestructura IPv4 como vínculo con capacidad de multidifusión. Para que 6over4 funcione correctamente, la infraestructura IPv4 debe estar habilitada para multidifusión IPv4".

[50]"6over4 maneja la infraestructura IPv4 como una liga simple con capacidades multicast, esto significa que el proceso de descubrimiento de vecinos como la resolución de direcciones y descubrimiento de ruteadores, trabaja como si hicieran un enlace físico con capacidades "multicast", para emular un enlace con capacidades "multicast", la infraestructura IPv4 debe de tener habilitado "multicast" para IPv4.

Cuando se habilita 6over4, la capa IPv4 utiliza mensajes IGMP (Internet Group Membership Protocol) para informar a los ruteadores locales IPv4 de su interés en recibir tráfico "multicast" IPv4 el cual es enviado a las direcciones "multicast" IPv4.

[49]http://msdn.microsoft.com/es-es/library/cc736336%28v=ws.10%29.aspx
[50]http://www.tlalpan.uvmnet.edu/oiid/download/T%C3%BAneles%20en%20IPv6%20gesti%C3%B3n%20PO%20TI.pdf

Las direcciones de la capa de enlace 6over4 son los puntos terminales de los túneles. Los equipos y los ruteadores pueden utilizar mensajes de solicitud de ruteador y de aviso de ruteador para el descubrimiento de ruteadores, prefijos y parámetros", El esquema de este método se muestra en la figura 14:

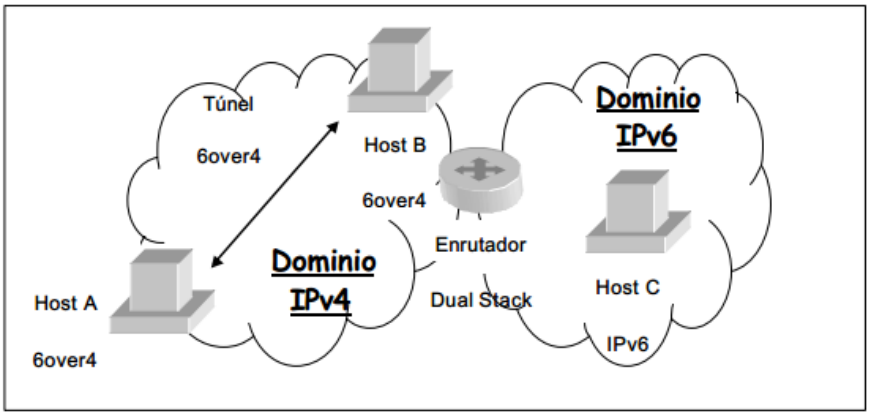


Figura 14 Entorno 6over4 Fuente:
http://repositorio.utn.edu.ec/bitstream/123456789/619/3/CAPITULO3.pdf

[51]"Para el direccionamiento en 6over4 el dominio IPv4 debe ser multicast para que se puedan llevar a cabo algunos mensajes o procesos de descubrimiento de nodos vecinos (Neighbor Discovery)". Para la traducción de direcciones IPv6 multicast a direcciones IPv4 multicast se ha definido el siguiente patrón:

- 239.192.[segundo byte más a la derecha de la dir. IPv6].[último byte de la dir. IPv6]

[52]"A continuación se muestran algunos ejemplos de direcciones IPv6 multicast traducidas a direcciones IPv4 multicast:

[51] http://repositorio.utn.edu.ec/bitstream/123456789/619/3/CAPITULO3.pdf
[52] http://repositorio.utn.edu.ec/bitstream/123456789/619/3/CAPITULO3.pdf

- FF02::1 (dirección multicast de enlace local con alcance a todos los hosts) se cambia por la dirección 239.192.0.1
- FF02::2 (dirección multicast de enlace local con alcance a todos los enrutadores) se cambia por la dirección 239.192.0.2
- FF02::1:FF45:8C54 (dirección multicast de un nodo solicitado) se cambia por la dirección 239.192.140.84

A continuación se muestran algunas direcciones MAC correspondientes a direcciones IPv4 multicast para un adaptador de tipo Ethernet:

- La dirección MAC multicast correspondiente a la dirección 239.192.0.1 es 01-00-5E-40-00-01
- La dirección MAC multicast correspondiente a la dirección 239.192.0.2 es 01-00-5E-40-00-02
- La dirección MAC multicast correspondiente a la dirección 239.192.140.84 es 01-00-5E-40-8C-54”

2.5.2.5. Túneles ISATAP[53]

ISATAP es un mecanismo de tunelización de superposición automática que utiliza la red IPv4 subyacente como una capa de enlace de NBMA (``NoBroadcast MultiAccess networks") para IPv6. ISATAP está diseñado para el transporte de paquetes IPv6 dentro de un sitio donde una infraestructura IPv6 nativa aún no está

[53] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html

disponible, por ejemplo, cuando los hosts IPv6 dispersas se despliegan para la prueba. Túneles ISATAP permiten IPv4 individual o IPv6 hosts de doble pila dentro de un sitio para comunicarse con otras máquinas de la misma conexión virtual, básicamente la creación de una red IPv6 mediante la infraestructura IPv4. En la figura 15 se observa en funcionamiento de ISATAP.

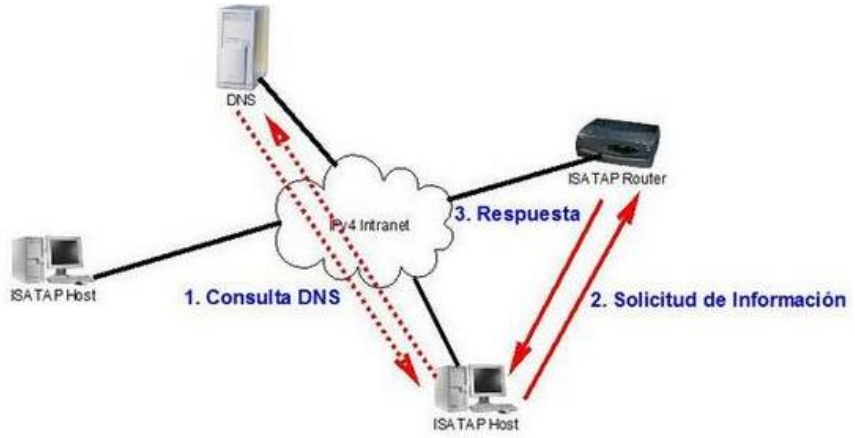


Figura 15. Funcionamiento de ISATAP. Fuente: http://www.franciscosepulveda.eu/2011/12/08/tecnologias-de-transicion-a-ipv6-isatap-12/

El router ISATAP proporciona soporte estándar de configuración de red del router para el sitio ISATAP. Esta característica permite que los clientes se configuran automáticamente como lo harían si estuvieran conectados a un GigabitEthernet o FastEthernet. También se puede configurar para proporcionar conectividad a cabo del sitio. ISATAP utiliza un formato de dirección IPv6 bien definida compuesta por el prefijo IPv6 unicast (/ 64), que puede ser enlace local o global (incluyendo prefijos 6a4), lo que permite el enrutamiento IPv6 a nivel local o en Internet. La dirección IPv4 está codificada en los últimos 32 bits de la dirección IPv6, lo que permite un túnel automático IPv6-in-IPv4.

Aunque el mecanismo de tunelización de ISATAP es similar a otros mecanismos de tunelización automáticas, tales como IPv6 túnel 6a4, ISATAP está diseñado para el transporte de paquetes IPv6 dentro de un sitio, no entre sitios.

ISATAP utiliza direcciones de unidifusión que incluyen un prefijo IPv6 de 64 bits y un identificador de interfaz de 64 bits. El identificador de interfaz se crea en formato modificado EUI-64 en la que los primeros 32 bits contienen el valor 000:5 EFE para indicar que la dirección es una dirección ISATAP IPv6. La tabla cinco describe un formato de dirección ISATAP.

64 Bits	**32 Bits**	**32 Bits**
vincular prefijo unicast IPv6 local o global	0000:5 EFE	Dirección IPv4 del enlace ISATAP

Tabla 5.IPv6 ISATAP Formato de la dirección Fuente:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html

En la tabla cinco, se observa que una dirección ISATAP consiste en un prefijo IPv6 y el identificador de interfaz ISATAP. Este identificador de interfaz incluye la dirección IPv4 del enlace IPv4 subyacente. El siguiente ejemplo muestra lo que una dirección ISATAP real se vería como si el prefijo es 2001: DB8: 1234:5678 :: / 64 y la dirección IPv4 incrustada es 10.173.129.8. En la dirección ISATAP, la dirección IPv4 se expresa en hexadecimal como 0AAD: 8108:

2001: DB8: 1234:5678:0000:5 EFE: 0AAD: 8108

2.5.3. Protocolo de Separación Localizador/Identificador (LISP).

[54]"LISP es una arquitectura de red y un conjunto de protocolos que implementa una nueva semántica de direccionamiento IP".

[55]"LISP es un protocolo de encapsulación originalmente diseñado para reducir el rápido crecimiento del número de rutas en la tabla global de enrutamiento IPv4, es una arquitectura de enrutamiento revolucionaria desarrollado por Cisco y el IETF que implementa un nuevo paradigma para el direccionamiento IP que utiliza la dirección IP para crear dos espacios de nombres: los identificadores de punto final (EIDs), que se asignan a terminar anfitriones, y localizadores de enrutamiento (RLOCs), que se asignan a los dispositivos (principalmente routers y switches) que componen el sistema de enrutamiento global. Usando este enfoque, la arquitectura LISP resuelve las limitaciones actuales y facilita la nueva funcionalidad de una manera interoperable con efecto mínimo a las redes existentes. LISP utiliza un modelo de enrutamiento mapa-y-encapsulado en el que el tráfico destinado a un EID se encapsula y se envía a un RLOC autorizada, en lugar de directamente a la EID de destino, sobre la base de los resultados de una búsqueda en una base de datos de mapeo"[56]. Las funciones LISP como DNS, cuando hay una solicitud de un lugar desconocido, requieren una consulta a un servidor que contenga las tablas de asignación que apuntan los paquetes al destino correcto.

[54] http://lisp.cisco.com/lisp_over.html
[55] http://www.ipv6.mx/index.php/component/content/article/318-transicion-ipv6-cisco-lisp-vs-servicios-de-tunel
[56] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/solution_overview_c22-650815.html

Cisco sugiere el uso de LISP para interconectar "islas" de IPv6 a través de Internet IPv4.

Capítulo 3 Levantamiento de la información de la red de la Universidad Internacional del Ecuador.

3.1. Identificación de la RED de la UIDE.

La Universidad Internacional del Ecuador se compone tres sedes ubicadas en Guayaquil, Loja y Quito, un Centro de Apoyo ubicado en la Ciudad de Quito en el sector de la Eloy Alfaro, dos Clínicas Odontológicas ubicadas en el Sector del Valle de los Chillos todas estas interconectadas a través de enlaces de fibra por medio del ISP.

El presente trabajo toma en cuenta a la matriz Quito pues en esta se aplicara la solución. La figura 16 presenta la topología de la red referencial de la Universidad Internacional del Ecuador Matriz.

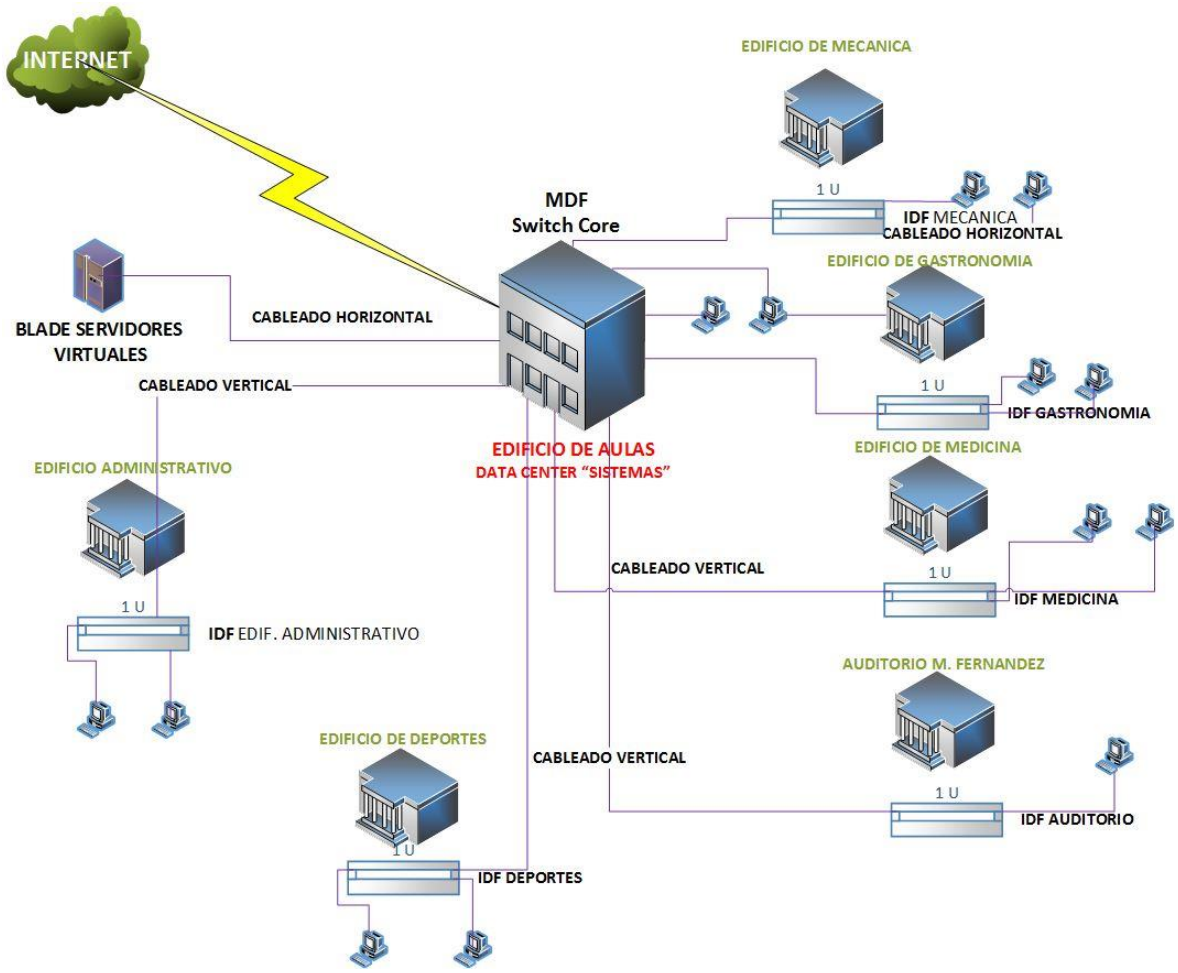


Figura 16 Topología de la UIDE. Fuente: Autor

La Sede matriz de la Universidad Internacional del Ecuador maneja un enlace de internet, servicio brindado por el ISP Telconet con una velocidad de 100 Mbps, además la UIDE cuenta con un enlace dedicado a IPV6 el cual al momento no se encuentra en uso, la comunicación entre los edificios internos (facultad de mecánica, Edificio de medicina, Deportes, Edificio administrativo, Edificio de aulas, Auditorio Marcelo Fernández y caballerizas Premium), se lo hace a través de un Backbone de fibra óptica.

El equipo activo encargado de direccionar la comunicación es un Switch Cisco 3750 utilizado como switch core, el mismo que se encuentra ubicado en el departamento de

sistemas (edificio de aulas), lugar donde funciona el Datacenter, los enlaces a cada uno de los edificios cuenta con fibra óptica a Gbps.

Cada uno de los edificios cuenta con uno o más switch dependiendo del número de usuarios por área, estas redes secundarias se comunican directamente con los usuarios, se utiliza enlaces de cable UTP en CAT 6A en el 98% ya que desde el 2013 se ha venido actualizando la categoría del cableado con fin de obtener mayor aprovechamiento del enlace.

Los enlaces mencionados en el párrafo anterior se concentran en el datacenter de sistemas así como también varios de los equipos activos de red (switch, router, etc.), al estar interconectados los equipos de cada uno de los edificios al switch core, esto permite manejar la configuración de Vlans y enrutamiento de red desde el núcleo.

El equipamiento de los swtich de la [57]UIDE en un 99% son de marca Cisco y con diferentes números de puertos de acuerdo al área de servicio, esta homogeneidad facilita en gran medida el mecanismo de transición del protocolo IPv4 a IPv6.

Otro factor a tomar en cuenta es el servicio de video conferencia el mismo que dada su importancia en la transmisión de imágenes y video a través la red IP debe tomarse en cuenta para no afectar su calidad, el laboratorio principal encargado de proporcionar este servicio se encuentra ubicado en el edificio de Administrativo.

[57] Universidad Internacional del Ecuador.

La administración de la Universidad Internacional del Ecuador tanto a nivel financiero como académico depende de diferentes servicios los mismos que son administrados por varios servidores los mismos que se encuentran detallados en la tabla 6.

Servidor.	**Detalle.**
Aplicaciones Base de datos	Servicios de BDD del sistema financiero y académico.
Desarrollo de Aplicaciones y BDD	Aplicaciones en producción y en etapa de pruebas.
Web	Administra Aplicaciones Web en área Académica.
Proxy	Para la administración del acceso al internet.
Archivos	Servidor para almacenar y compartir información.
Correo Electrónico	Servicio de correo Outlook.
Activity Directory	Servidores para el manejo de usuarios.
Telefonía	Servidor de telefonía Elastix.
CRM	Manejo de aplicaciones de promoción.
Antivirus	Sistema de protección.
Biblioteca	Manejo de bibliotecas virtuales como propias de la institución.

Tabla 6 Servidores y servicios que estos brindan a la UIDE. Fuente: Del Autor

Las aplicaciones que dispone la Universidad Internacional del Ecuador funcionan de manera adecuada utilizando la red de datos actual con el uso del protocolo IPV4 sin

embargo debido al aumento en el número de usuarios y al consumo en el ancho de banda, se busca optimizar el funcionamiento de la red con IPv6.

En este trabajo se realiza el análisis tomando en cuenta el diseño de la red IPv4 de la UIDE y la coexistencia que deberá existir al migrar a IPV6 de tal manera se permita la conexión de la red LAN de la UIDE hacia el Internet, de tal manera todas las áreas y departamentos de la matriz cuenten con acceso IPv6 por medio del Backbone de fibra óptica, así como también hacer uso del enlace dedicado a IPv6 en nuevas aplicaciones que se vienen desarrollando en la UIDE.

Con el análisis y el plan de implementación que consta en este trabajo se busca la migración total en la red de datos de la Universidad Internacional del Ecuador siendo la matriz en donde se llevara a cabo la primera etapa consecuentemente se realizara la migración en las diferentes sedes.

3.1.1. Tráfico de red.

[58]"El tráfico de red de área local se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación, y a la velocidad que se transfiere por ello la importancia del conocimiento sobre la "Teoría de la información" y sus diferentes elementos para poder evaluar en formas más eficiente y eficaz el tráfico en la red".

[58] http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/869/2145

[59]"El análisis de tráfico de red permite contar con información detallada y precisa del consumo de recursos de red, monitorear y controlar el rendimiento de las aplicaciones, El análisis del tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas al bus. Dichas sondas, con su interfaz Ethernet funcionando en modo promiscuo, capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutaran, de forma continua, aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma.

Lo que se busca con el análisis de red es identificar y clasificar las aplicaciones que se encuentran corriendo sobre la red, y el uso de ancho de banda de tráfico entrante y saliente, actualmente existen varias herramientas que nos ayudan en el análisis y monitores de la red la finalidad es observar las características que se mencionan a continuación:

- Descubrimiento y análisis de tráfico. Identifica y clasifica las aplicaciones que se encuentran corriendo sobre la red.
- Eficiencia de la red. Identifica el porcentaje de tráfico de la red dedicada a la retransmisión de paquetes. Además, determina la porción de tráfico y consumo de ancho de banda correspondiente a aplicaciones recreativas, aplicaciones críticas de negocio y tráfico no crítico.

[59] http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/869/2145

- Utilización de ancho de banda. Examina la utilización del enlace para determinar la variabilidad en el uso de enlace y entender los requerimientos de capacidad del ancho de banda.
- Control de múltiples instalaciones. Permite administrar y controlar redes remotas, obtener reportes desde múltiples consolas sobre el estado de la red, además de permitirnos monitorear redes de manera simultánea desde una consola.
- Control de información. Permite visualizar y almacenar datos de la red para mejorar reportes y tendencias, analizar el tráfico de la red proyectados los datos en el tiempo también permite generar reportes con el fin de justificar las necesidades de actualizaciones de la red".

La herramienta utilizada en la Universidad Internacional del Ecuador para realizar el análisis del tráfico de red es TracertPlus/Ethernet por medio de la cual se puede controlar y administrar la red local como se puede observar en la figura 17.

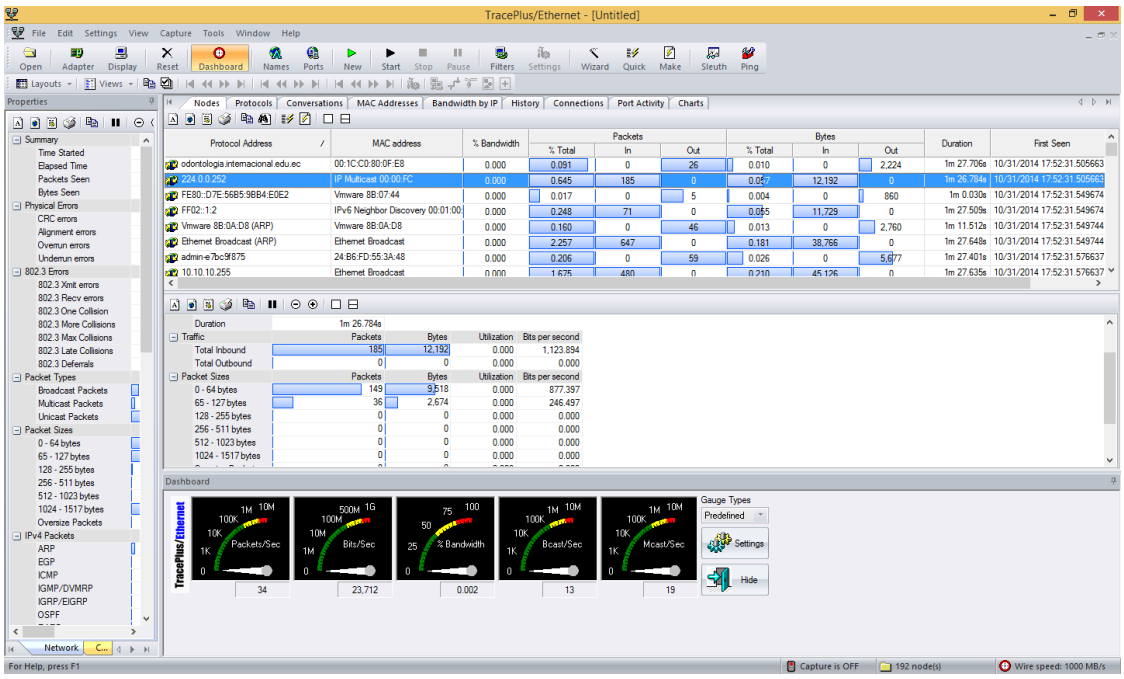


Figura 17 Interfaz de TracePlus. Fuente: Datos de la UIDE.

Con el uso de la herramienta TracetPlus se genera un informe que detalla el tráfico que genera cada host en la red, en el informe se observan varios parámetros entre ellos la transferencia de datos, los protocolos utilizados, paquetes enviados y recibidos, el comportamiento del protocolo IP.

Entre las varias herramientas existes para el análisis del tráfico de red la UIDE hace uso de TracePlus por la ventaja que ofrece sugiriendo acciones para la mejora en el rendimiento de la conexión local. Los datos obtenidos brindan una visión clara para establecer permisos de accesos, limitar el intercambio de datos y solucionar errores que afecten a la red.

Los parámetros analizados en la red de la Sede matriz de la Universidad Internacional del Ecuador son:

- Análisis de paquetes Bits/Segundo.

- Análisis del porcentaje de Ancho de Banda.
- Análisis de los protocolos principales.

El monitoreo de la red se lo realiza desde un host en el departamento de sistemas (Área de redes e infraestructura), este equipo se conecta a un switch secundario ubicado en el datacenter y a la vez este se conecta al switch core de tal manera se pueda analizar todo el tráfico de la red LAN.

3.1.2. Distribución del cableado.

Por medio del análisis de la red se determinara la situación de la red así como el protocolo IPV4 que funciona bajo la red, la intención es poder observar y medir las variables que tienen peso en la migración a IPv6.

La matriz de la Universidad Internacional del Ecuador se encuentra ubicada en Quito Sector Collacoto, (Av. Simón Bolívar y Jorge Fernández), a su vez está compuesta de varios edificios los mismos que se detallan en la tabla 7:

Código	Edificio (Nombre)
001	Edificio de Aulas.
002	Edificio Administrativo.
003	Edificio Facultad de Mecánica.
004	Edificio Facultad de Gastronomía.
005	Edificio facultad de Biología
006	Edificio de Deportes.
007	Edificio de Hípica.

008	Auditorio Marcelo Fernández.

Tabla 7 Edificios de la matriz de la UIDE. Fuente: Autor

La interconexión desde cada edificio al switch core se la realiza a través de varios Switch Marca cisco los mismos que se ubican en diversos racks de cada uno de los edificios, con respecto al cableado este es interno de tal manera exista separación con el cableado eléctrico.

3.1.2.1. Cableado horizontal.

El cableado horizontal de cada una de las áreas se extiende desde los IDF´s (servicios de distribución intermedia), hacia cada uno de los host en las distintas áreas.

Los IDF´s dependen del servicio de distribución principal, estos se encuentran ubicados en cada uno de los edificios en ciertos casos los edificios pueden manejar varios IDF´s dependiendo del número de usuarios a los que este da servicio, en cada bastidor de los IDF se encuentran uno o varios switch marca cisco en su mayoría son de 48 puertos los mismos que manejan la transmisión de voz y datos.

Dentro de cada bastidor se encuentran los componentes de los IDF que son.

- Racks Abiertos.
- Gabinetes.
- Pach panel.
- Ups.

La tabla 8 muestra la distribución de los bastidores y rack en cada uno de los edificios.

N°	***Tipo de rack***	***Edificio.***
1	Rack Abierto	Edificio de aulas subsuelo
2	Rack Abierto	Edificio de aulas Planta baja.
3	Rack Abierto	Edificio de aulas primer piso.
4	Rack Cerrado	Edificio de aulas primer piso laboratorio 1
5	Rack Cerrado	Edificio de aulas primer piso laboratorio 2
6	Rack Cerrado	Edificio de aulas primer piso laboratorio 3
7	Rack Cerrado	Edificio de aulas primer piso laboratorio 4
8	Rack Cerrado	Edificio de aulas primer piso laboratorio 5
9	Rack Abierto	Edificio de aula segundo piso.
10	Rack Abierto	Edificio Administrativo subsuelo.
11	Rack Abierto	Edificio Administrativo Biblioteca.
12	Rack Abierto	Edificio Administrativo Primer piso.
13	Rack Cerrado	Edificio de deportes primer piso.
14	Rack Cerrado	Edificio de deportes segundo piso.
15	Rack Cerrado	Edificio caballerizas Premium.
16	Rack Abierto	Edificio de medicina.
17	Rack Cerrado	Edificio de Gastronomía.
18	Rack Cerrado	Edificio de Mecánica Planta baja.
19	Rack Cerrado	Edificio de Mecánica laboratorios.

Tabla 8 Distribución de bastidores y tipo rack de la UIDE. Fuente: El autor

3.1.2.1.1. Cable UTP

En la tabla 9 se presentan las características del cable UTP utilizado en el cableado horizontal.

Detalles Técnicos

	LSZH
Capacitancia Mutua	5.6 nF/100 m máximo
Impedancia de Entrada	100Ω ± 15% (1-62.5 MHz) / ± 22% (62.5-200 MHz) / ± 25% (200-500 MHz)
Resistencia CC Conductor	66.58 Ω/Km máximo
Voltaje	300 V CA/CC
Diferencia de Retardo	45 nseg máximo
Retardo de Propagación	536 nseg/100 m máximo @ 500 MHz
Velocidad Nominal de Propagación	72%
Temperatura de Operación	-20° C a +60° C
Temperatura de Almacenamiento	-20° C a +80° C
Radio de Curvatura	4 x Diámetro del cable ≈ 1.14" (28.8 mm)

Embalaje	Carrete de Madera de 305 m	18.33 Kg/305 m	
Materiales	Conductores	23 AWG, Unifilar, 0.554 mm Ø	
	Aislación	Polietileno 0.243 mm (1.04 mm Ø nominal)	
	Chaqueta	LSZH 0.64 mm (7.20 mm Ø nominal) RoHS	
Certificaciones	Seguridad	**Listado UL** según: UL444 IEC 60332-1	
	Desempeño	**Verificado ETL** Especificaciones de Canal según ANSI/TIA/EIA-568-C	

Tabla 9 Características de cable categoría 6A. Fuente: http://www.ds3comunicaciones.com/AMP/1859218-X_.pdf

3.1.2.2. Cableado Vertical.

El cableado vertical encargado de la interconexión desde los IDF´s hacia el MDF (servicio de distribución principal). Es el encargado del transporte de los datos desde el switch core hacia los Switch de cada edificio.

El MDF se encuentra en el data center de sistemas ubicado en el edificio de aulas primero piso esta área se encuentra bajo temperatura y humedad contralada por un sistema de climatización autónomo, el sistema eléctrico también es controlado mediante un sistema autónomo de ups.

El canal de transmisión para la interconexión entre el MDF y cada uno de los IDF es a través de fibra óptica el acceso a la fibra para su mantenimiento de lo hace directamente sobre los Racks.

Tras el análisis al que se ha sometido el cableado estructurado de la UIDE este tiene los siguientes beneficios:

- Confiabilidad. La red de datos de la UIDE se ha venido actualizando desde hace ya algún tiempo en varios nodos lo que hace que sea una red confiable capaz de cumplir con los requisitos para este proyecto.
- Capacidad de crecimiento. La topología bajo la cual ha sido diseñada la red permite seguir creciendo en los nodos que ha si lo requieran o creación de nuevos si es el caso.
- Fácil administración. La ubicación de los equipos permite el fácil control de cambios o detección de errores en la red de tal manera la corrección de estos problemas se lo haga en el menor tiempo posible.
- Seguridad. Al acceso al MDF e IDF´s se rige bajo normas de seguridad establecidas en los procesos del departamento de sistemas lo cual da un manejo único y controlado a las personas indicadas e identificadas lo que genera un alto grado de seguridad en el manejo del cableado.

Con estos datos extraídos del análisis de la red de datos de la UIDE se puede establecer que el proceso de migración a IPV6 es soportado por la red sin que se pueda presentar algún inconveniente de tipo físico.

3.2. Levantamiento y obtención del Diagrama Lógico.

Dentro del diagrama lógico de la UIDE se detallan los equipos de red y la interconexión entre ellos en este punto se contemplan los servidores y los servicios que estos brindan pues estos también pueden afectar de alguna forma los patrones de tráfico, uso de ancho de banda y seguridad así tenemos:

- Routers.
- Switch´s.
- Firewalls.
- Servidores.
- Access point.
- Estaciones de trabajo.

3.2.1. Diseño de la topología de red.

Una red informática está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente). Con respecto a la parte lógica se maneja un gran concepto sin embargo se lo analiza como el modo como se comunican los host a través del medio para el envío de datos.

[60]"Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

[60] http://www.angelfire.com/cantina/oronaweb/topologia.htm

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad".

En la red de datos de la matriz de la Universidad internacional del Ecuador se maneja una topología en estrella extendida, a esta se conectan las estrellas individuales de cada edificio el enlace es punto a punto esta topología la podemos observar en la figura 18.

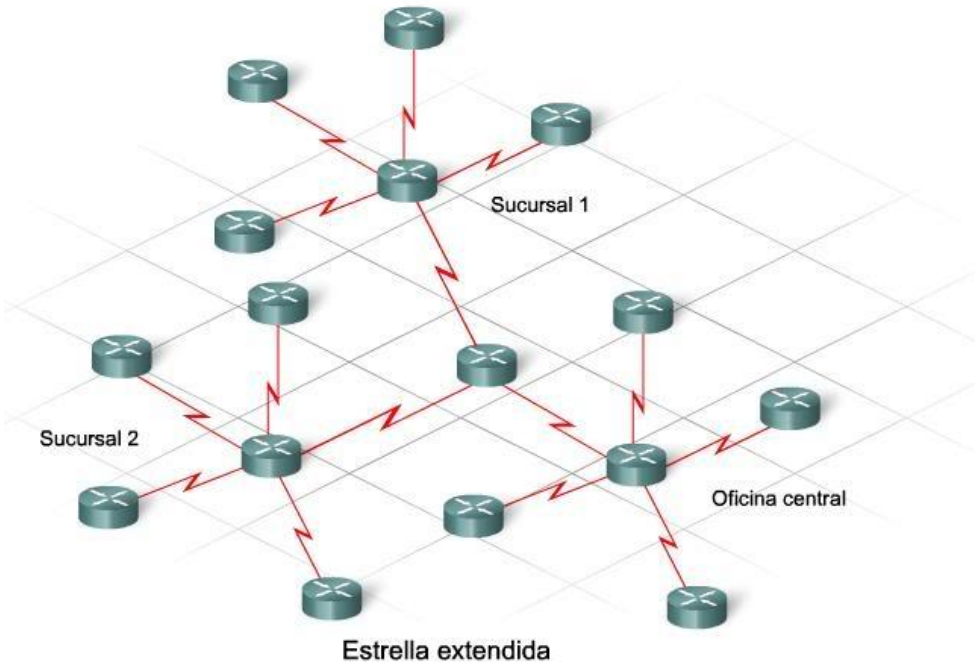


Figura 18 Estrella extendida. Fuente:
http://topologias4conalep.blogspot.com/p/topologia-en-estrella-y-estrella.html

[61]"Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de éste.

Dada su transmisión, una red en estrella tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un switch. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

Esta topología tiene varias ventajas como son:

- Tiene los medios para prevenir problemas.
- Si una PC se desconecta o el cable sufre algún daño solo queda fuera de la red esa PC.
- Fácil de agregar, reconfigurar arquitectura host.
- Fácil de prevenir daños o conflictos.
- Permite que todos los nodos se comuniquen entre sí de manera conveniente".

La red y la topología en la UIDE ha sido simulada en el software Cisco Packet Tracert para mantener una visualización del funcionamiento de la red, así también manejar la una configuración básica de los equipos.

Para mayor información del diseño de la red ver el Anexo C.

[61] http://topologias4conalep.blogspot.com/p/topologia-en-estrella-y-estrella.html

3.2.2. Diseño de Vlans

Para la administración de la red en la UIDE se ha creado varias Vlan´s, cada una destinada a brindar cierto servicio además de otros beneficios que se deja a consideración:

- Uso eficiente del ancho de banda.
- Separar los accesos a la información de áreas.
- Facilidad en la administración de la red.
- Seguridad en el acceso a los dominios.

Cada Vlan tiene como objetivo separar los servicios o a su vez controlar los accesos entre dependencias, en la tabla diez se da a conocer las Vlan que maneja la UIDE.

# VLAN	NOMBRE
1	VLAN1
2	ADMINISTRATIVA 1
3	TELEFONIA CISCO
4	LABORATORIOS
5	ADMINISTRATIVA 2
6	WIRELESS
7	TELEFONIA ELASTIX
9	ACADEMICO
34	SEGURIDAD

Tabla 10. Vlans de la UIDE. Fuente Autor

3.2.2.1. Reglas de conectividad de VLANS

Para el acceso o negación del mismo entre Vlans se han creado varias reglas de conexión "ACL" esto depende de la información que manejan los diversos departamentos o a su vez si existe algún recurso de uso común entre áreas.

Los accesos de cada Vlan las muestra la tabla 11.

# y Nombre de VLAN	Acceso
1. VLAN1	Acceso único
2. ADMINISTRATIVA 1	5-4-9
3. TELEFONIA CISCO	Acceso único
4. LABORATORIOS	9
5. ADMINISTRATIVA 2	2-4-9
6. WIRELESS	Acceso único
7. TELEFONIA ELASTIX	Acceso único
9. ACADEMICO	2-9
34. SEGURIDAD	ACCESO UNICO

Tabla 11. Access list. Fuente: Autor.

El manejo de Access list lo realiza el Área de Redes e infraestructura, el diseño maneja dos Vlans encargadas del área administrativa esto no quiere decir que todos los host pueden acceder de una Vlan a otra esto depende de la necesidad que presenten los usuarios de acuerdo a ello se sigue en proceso de aprobación luego de esto se niega o permite el acceso.

Con respecto a los laboratorios estos se encuentran en una sola Vlan lo que permite que estos dispongan de la información concerniente sin ninguna restricción, sin embargo al igual que en las Vlans de la parte administrativa se da acceso a otras de acuerdo a la necesidad y aprobación.

3.2.3. Distribuciones de direcciones IP.

Una dirección IP representa la dirección de cada computadora en la red, para poderla identificar y enviarle la dirección que esta requiera, las direcciones IPs en una empresa se calcula de acuerdo al número de Host y el porcentaje de crecimiento de la red.

La UIDE cuenta con varias direcciones IPs públicas, sin embargo la disponibilidad de estas se ha ido limitando debido al aumento en servicios que necesitan acceso desde la web, internamente se maneja las IPs por medio de NAT con el fin de distribuir en la intranet los servicios y manejar el crecimiento de usuarios.

Estas direcciones IP que se maneja en la UIDE son de tipo C en la tabla doce se puede observar un cuadro comparativo con el tipo de dirección IP y el número de Host que esta soporta.

Clase	Dirección	# de host
A	10.0.0.0/8	16777214
B	172.16.0.0/16	65534
C	192.168.0.0/24	254

Tabla 12 Tipo de direcciones IP. Fuente: el Autor

En la tabla trece se realizan la proyección de crecimiento por cada nodo que compone la red de datos de la UIDE

Switch	# de host	% de crecimiento 25%	Total
Edificio Caballerizas premiun	24	6	30
Edificio de Deportes	24	6	30
Edificio Administrativo SB	48	12	60

Edificio Administrativo PB	48	12	60
Edificio Administrativo 1P	48	12	60
Edificio Administrativo 1P	24	6	30
Biblioteca	24	6	30
Edificio de Aulas SB1	48	12	60
Edificio de Aulas PB1	48	12	60
Edificio de Aulas PB2	48	12	60
Edificio de Aulas 1P1	48	12	60
Edificio de Aulas 1P2	48	12	60
Edificio de Aulas Lab1	24	6	30
Edificio de Aulas Lab2	24	6	30
Edificio de Aulas Lab3	24	6	30
Edificio de Aulas Lab4	24	6	30
Auditorio	8	2	10
Edificio de Medicina	24	6	30
Edificio de Gastronomia	24	6	30
Edificio de Mecanica	48	12	60
Edificio de Mecanica Laboratorios	48	12	60
Total			910

Tabla 13 Proyección de crecimiento de la red de la UIDE. Fuente. Datos de la UIDE

La tabla trece brinda los datos necesarios proyectados para el cálculo de direcciones IP evitando el desperdicio de IP´s o el sobredimensionamiento de la red

Las IPs internas que maneja la red de datos se indica en la tabla 14 donde se detalla la vlan y el rango de direcciones que esta dispone.

# VLAN	NOMBRE	Dirección IP	# de Host
1	VLAN1	10.1.1.0/24	254
2	ADMINISTRATIVA 1	10.10.10.0/24	254
3	TELEFONIA CISCO	192.168.3.0/24	254
4	LABORATORIOS	10.10.11.0/24	254
5	ADMINISTRATIVA 2	10.10.15.0/24	254
6	WIRELESS CISCO	10.10.16.0/24	254
7	TELEFONIA ELASTIX	10.10.20.0/23	510
9	ACADEMICO	10.10.12.0/24	254
34	SEGURIDAD	10.10.34.0/24	254

Tabla 14. Direcciones IP. En cada VLAN. Fuente: Autor.

3.2.4. Elaboración de tablas de enrutamiento.

Los saltos en la configuración de la red de la UIDE son estáticos por lo que cualquier cambio o adición en las tablas de enrutamiento se lo debe realizar manualmente por el administrador.

La tabla de enrutamiento se las detalla a continuación:

Dirección IP Destino	Interfaz de Salida	Dirección IP del Salto
172.17.0.0/24	Serial 0/1/0	200.93.0.0/30

Tabla 15 Tabla de enrutamiento en Firewall. Fuente: Datos de la UIDE

3.2.5. Servicios.

La universidad Internacional del Ecuador brinda servicios a nivel académico como son portales para el estudiante, portal para el docente, consulta de notas, record académico, plataforma virtual, bibliotecas virtuales a nivel administrativo la aplicación principal maneja el sistema financiero.

Estos servicios están distribuidos para que según sea el caso se pueda acceder desde la intranet o fuera de ella. Todas las aplicaciones se encuentran en los servidores virtuales que la UIDE posee en su Blade ubicados en el datacenter de sistemas.

A continuación se detalla los servicios que se ofrece la UIDE:

- Ambientes virtuales.

  La UIDE tiene a disposición de la comunidad universitaria varios ambientes virtuales manejados desde la plataforma disponible en los siguientes campos:

- Modalidad presencial.
- Modalidad a distancia.
- Modalidad virtual (Moodle, blackboard).

- Consultas.

  Los estudiantes pueden realizar varios tipos de consultas dentro del sistema académico:

  - Calificaciones.
  - Proformas.
  - Horario de clases.
  - Consulta de Créditos.
  - Pagos pendientes.
  - Evaluación al docente.
  - Registro académico.

- Productos.

  Dentro de los productos la UIDE maneja el campus agreement de Microsoft lo que posibilita el uso del estudiante a herramientas que constan dentro de este paquete como son: Office, Visio, FrontPage, Project, visual studio, etc.

- Sistema académico.

  El sistema académico de la Universidad se encarga de la gestión de datos de uso académico del estudiante donde los docentes registran las calificaciones y el estudiante hace las consultas sobre las mismas.

- Sistema financiero.

  El sistema financiero maneja los pagos que realiza el estudiante en sus responsabilidades económicas para con la Universidad como son: pagos de matrículas, pagos en gastos de dirección de tesis, multas, derechos de exámenes, etc.

  Además de lo mencionado anteriormente el sistema financiero se encarga del manejo de los gastos administrativos que mantiene la UIDE.

3.3. Levantamiento del Diagrama Físico.

El marco de distribución principal "MDF" por sus siglas (Main Distribution Frame) en ingles está ubicado en el edificio de Aulas primer piso, la topología como se analizó anteriormente es una estrella extendida, la figura 19 muestra el diagrama físico de la Matriz de la UIDE.

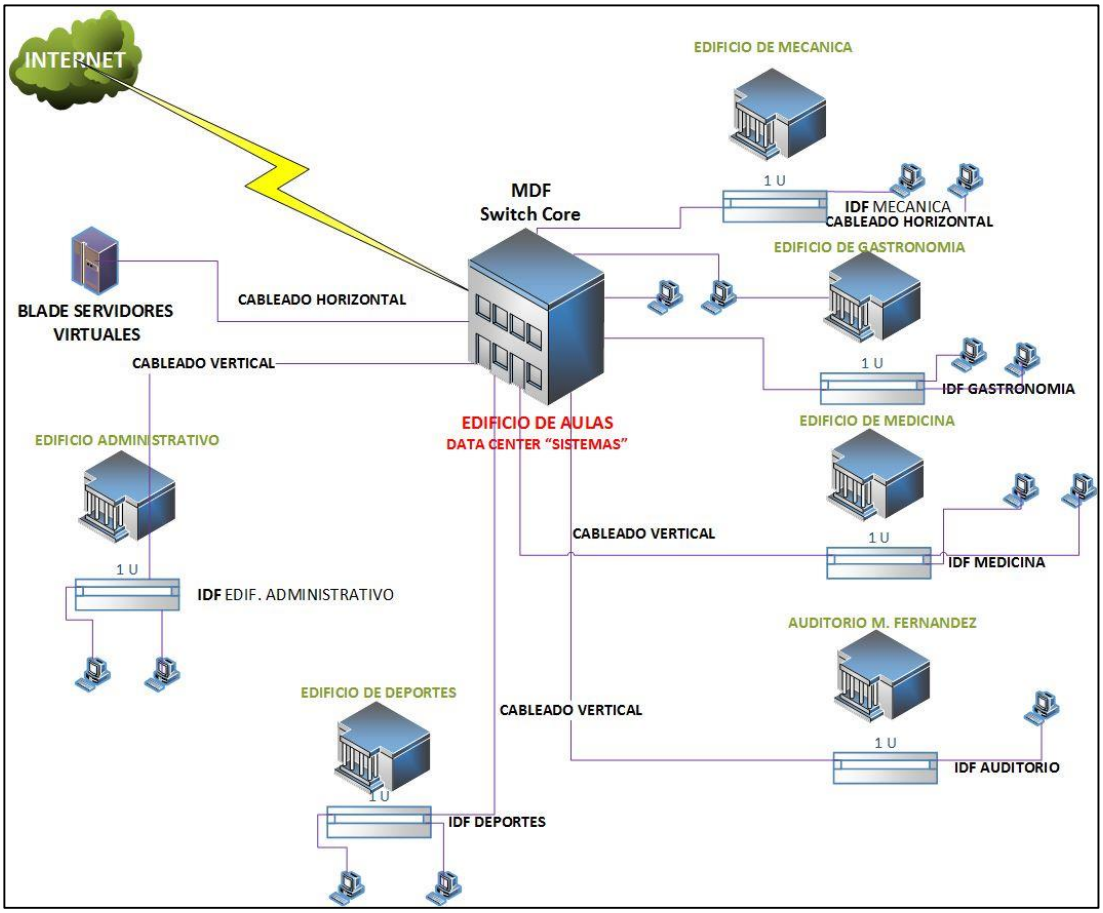


Figura 19 Diagrama Físico. Fuente: El Autor

En la gráfica 19 se observa la ubicación del MDF y la distribución de cada IDF en cada los edificios de la matriz de la UIDE, en estos edificios se distribuyen varias estaciones de trabajo, estas están conectadas a la red de manera física es decir que en cada sitio de trabajo existen puntos de red que se conectan a los swtich ubicados en los diferentes bastidores de los edificios, del punto de red a las tarjetas de red de cada equipo se realiza la conexión a través de un patch cord de categoría 6 y 6A, esta conexión provee de los diferentes servicios a los usuarios dependiendo los perfiles que estos manejen.

La parte activa de la red de los IDF´s es manejada por varios switch cisco entre los modelos (2950, 2960, 3560), estos están ubicados en los bastidores de cada edificio la

conexión switch core es a través de fibra óptica que está ubicado en el Data center (MDF).

La protección y seguridad de la red interna contra ataques o intrusos se lo hace por medio de un firewall "ASA" que esta enlazado al switch core, desde el Firewall se realiza la conexión al Router de telconet que permite la conexión externa.

3.3.1. Características de los Equipos de Red.

Las características principales de la parte activa de Red se detallan a continuación:

Los servidores de la UIDE son virtuales los mismos que están alojados en un chasis IBM con las siguientes características. Tabla 16.

Chasis Blade para servidores Virtuales	
Características	**Descripción**
Marca	Chasis IBM BladeCenter-H Midplane
Modelo	8852HC1

Tabla 16 Características de Chasis IBM. Fuente: Datos de la UIDE.

El chasis IBM se compone de cuatro servidores que cumplen las siguientes características físicas ver tabla 17.

Cantidad	Características	Descripción
	Marca	IBM BladeCenter HS22
	Modelo	HS22 (Type 7870)
2	Procesador	Intel Xeon processor MP (3.07 GHz Processor Cores 6)
9	Memoria	DDR III SDRAM (84G)
2	Disco Duro	Storage
	Sistema Operativo	esxi 5.5

Tabla 17 Características de los servidores. Fuente: Datos de la UIDE

Las aplicaciones instaladas en los servidores las presenta la tabla 18.

Servidor	Servicios
Web	Páginas Web
Proxy	Dns, bloqueo de paginas
Antivirus	Filtrado de correo, protección Anti spam
desarrollo	SQL server, Power Builder, Visual punto net
Biblioteca	Aplicación Web, ficheros
Aplicaciones	C##, SQL, Power Builder
Base de Datos	SQL server
Correo Electrónico	Micrsoft Exchange

Tabla 18 Aplicaciones de los servidores. Fuente: Datos de la UIDE

Los equipos de cómputo que dispone la UIDE tanto para el uso de estudiantes en laboratorios, como para el uso del área administrativa presentan las características que se puede visualizar en la tabla 19.

Características	Descripción
Procesador	Intel Core i5
Memoria	4GB
Velocidad	3.20 GHZ
Disco Duro	500 GB
Sistema Operativo	Windows 7-8
Tarjeta de red	10/100/1000 Mbps

Tabla 19 Características de CPU del Área administrativa y laboratorios. Fuente: datos de la UIDE

Las características del equipo Firewall Cisco ASA 5540 se las presenta en la tabla 20.

Características	Descripción
tipo de dispositivo	el aparato de seguridad
Instalado módulos qty (max)	0 (1)
Ram instalada (max)	gb 1
De memoria flash instalado (max)	64 mb flash
tecnología de conectividad	con conexión de cable
los datos de protocolo de enlace	Ethernet, fast ethernet, gigabit ethernet
La red/protocolo de transporte	ipsec

el rendimiento	El rendimiento de firewall: mbps 650& brvbar; el rendimiento de vpn: mbps 325& brvbar; velocidad de conexión: las conexiones 25000 por segundo
de la capacidad	Períodos de sesiones simultáneos: 400000& brvbar; ipsec vpn pares: 5000& brvbar; ssl vpn de sus compañeros: 2& brvbar; interfaces virtual (vlans): 200
Características	Protección de firewall, vpn apoyo, el equilibrio de carga, soporte de vlan, de alta disponibilidad
el algoritmo de cifrado	Des, triple des, aes
Ranuras de expansión total (libre)	1 (1) x ranura de expansión& brvbar; memoria 1
Interfaces	1 x red - ethernet 10base-t/100base-tx - rj-45& brvbar; 1 x - la gestión de la consola - rj-45& brvbar; x 2 hi - velocidad usb - 4 pin usb tipo a& brvbar; 1 x - gestión auxiliar - rj-45& brvbar; 4 x red - ethernet 10base-t/100base-tx/1000base-t rj-45 -
cumplimiento de normas	Ce, certificado fcc clase a, cispr 22 clase un, la norma en 60950, la norma en 61000-3- 2,1950 ul, vcci clase una ite, iec 60950, la norma en 61000-3- 3, csa 22.2 no. 950, en55022 clase a, ts001 aca, como/nzs 3260, fcc parte 15
dispositivo de energía	Fuente de alimentación - interna
voltaje necesario	Ca 120/230 v (50/60 hz)
de energía siempre	190 vatios
min de temperatura de funcionamiento	0& deg; c
max temperatura de funcionamiento	40& deg; c
rango de humedad de funcionamiento	- 5 95%

Tabla 20 Características del Equipo Firewall ASA 5540. Fuente: Datos de la UIDE

El Router principal es un cisco 7604 el mismo que presenta las siguientes características (tabla 21).

GENERAL	
Device Type	Router - with Cisco 7600 Series Route Switch Processor 720 with PFC-3C
Enclosure Type	Desktop - modular - 5U
Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Performance	IPv4 routing : 400 Mbps
	IPv6 routing : 200 Mbps
	Switching capacity : 720 Gbps
Capacity	IPv4 routes : 256000

	IPv6 routes : 128000
	NetFlow entries : 128000
	ACL rules : 128000
Network / Transport Protocol	TCP/IP, ICMP/IP
Routing Protocol	OSPF, RIP, BGP-4, IS-IS, IGMP, PIM-SM, PIM-DM
Features	Layer 3 switching, Layer 2 switching, dynamic IP address assignment , DHCP support, MPLS support, VLAN support, IGMP snooping, traffic shaping, DoS attack prevention, Access Control List (ACL) support, Quality of Service (QoS)
Compliant Standards	IEEE 802.1x , NEBS level 3, FCC Class A certified, CISPR 22 Class A, EN 60950, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, AS/NZ 3548 Class A, CSA C22.2 No. 60950-00, ICES-003 Class A
Processor	PowerPC 1.2 GHz
RAM	2 GB (installed) / 6 GB (max)
EXPANSION / CONNECTIVITY	
Interfaces	1 x 10Base-T/100Base-TX/1000Base-T - RJ-45
	Management : 1 x console - RJ-45
	2 x SFP (mini-GBIC)
Expansion Slots	4 (total) / 3 (free) x expansion slot
	3 (total) / 2 (free) x CompactFlash Card - type II
Installed Modules Qty (Max)	1 (installed) / 4 (max)

Tabla 21 Caracteristicas de Router cisco 7604. Fuente:

http://www.hardware.com/us/products/cisco/7604-RSP720C-P

El switch Core encargado de la administración de la red de datos de la UIDE es un Cisco 3950 las características están disponibles en la tabla 22.

Product Name	Part Number	Description

Cisco Catalyst 3750G-24TS	WS-C3750G-24TS-S	• 24 10/100/1000 ports
		• 32-Gbps, high-speed stacking bus
		• Innovative stacking technology
		• 1 RU stackable multilayer switch
		• Delivers enterprise-class intelligent services to the network edge
		• SMI installed
		• SMI provides basic RIP and static routing, upgradable to full
		dynamic IP routing
Standards		● IEEE 802.1s
		● IEEE 802.1w
		● IEEE 802.1x
		● IEEE 802.3ad
		● IEEE 802.3af
		● IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX,
		and 1000BASE-T ports
		● IEEE 802.1D Spanning Tree Protocol
		● IEEE 802.1p CoS Prioritization
		● IEEE 802.1Q VLAN
		● IEEE 802.3 10BASE-T specification
		● IEEE 802.3u 100BASE-TX specification
		● IEEE 802.3ab 1000BASE-T specification
		● IEEE 802.3z 1000BASE-X specification
Software		Cisco IOS IP Base

Tabla 22 características del Switch Core. Fuente: http://www.andovercg.com/datasheets/cisco-faq_c3750_Public1.pdf

Los switch que se encargan de la interconexión entre el MDF e IDF son cisco de la serie 2960 las características son presentadas en la tabla 23.

Modelo	Cisco Catalyst 2960G-48TC - conmutador - 20 puertos
	Tipo de dispositivo Conmutador
	Factor de forma Externo - 1U
	Dimensiones (Ancho x Profundidad x Altura) 44.5 cm x 32.8 cm x 4.4 cm
	Peso 4.5 kg

Memoria	Memoria RAM 64 MB
	Memoria Flash 32 MB
Numero de puertos	Cantidad de puertos 20 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia	Velocidad de transferencia de datos 1 Gbps
comunicación	Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet
	Puertos auxiliares de red 4x10/100/1000Base-T/SFP (mini-GBIC)(señal ascendente)
	Protocolo de gestión remota SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c
	Modo comunicación Semidúplex, dúplex pleno
	Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, snooping IGMP
Estándares	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE

Tabla 23 Caracteristicas de Switch 2960. Fuente: http://www.electronisys.cl/index.php?route=product/product&product_id=485

Con respecto a la telefonía IP que se maneja en la sede Matriz de la UIDE los equipos que se dispone son los que se presentan en las tablas siguientes de acuerdo a la marca y modelo como indica la tabla 24.

Terminal Yealink T20P:	Pantalla de 2 lineas x 15 caracteres LCD
	Salida para auriculares (RJ9)
	2 puertos LAN, PoE
	Soporte VLAN y QoS
	2 puertos LAN 10/100 con Switch.
	Soporta módulo de expansión con botones BLF
	Chipset TI TITAN y procesador de voz Texas Instruments
	Voz HD: Codec HD con altavoz y auricular de banda ancha
	Alimentación: PoE estándar según norma IEEE 802.3af o fuente de alimentación opcional

Funciones de telefonía	Manos libres
	Llamada en espera, desvío, transferencia, rechazo de llamada
	Identificación de llamante (Caller ID), Lista de llamadas, No Molestar (DND), Rellamada, Flash.
	Conferencia a 3, marcaciones rápidas, ajuste de volumen, selección de timbre personalizado.
	Multi idioma, con soporte para castellano.
	Respuesta automática (auto answer).
	Soporta teclas Busy Lamp Field (BLF) y Shared Bridged Line Appearance (BLA)
Características SIP	SIP 2.0(RFC3261) protocol, NAT transversal: modo STUN
	Marcación In-band DTMF y out-of band RFC2833 DTMF
	Modo Proxy y modo SIP peer-to-peer.
	Codecs HD: G722
	Codecs VoIP estándar: G.711, G.723.1, G.726, G.729A/B
Características de integración y seguridad	Agenda empresarial descargable (XML, LDAP, hasta 200 items) y politonos para timbre. Customización XML de la pantalla.
	Soporta SRTP/TLS/HTTPS, encriptación AES.
	Comunicaciones seguras activando SRTP (RFC3711) en la configuración
	Soporte de Transport Layer Security (TLS)
	Soporte en la configuración de VLAN (802.1 pq), QoS
	Gestión de la autentificación usando MD5/MD5-sess
	Bloqueo del terminal para protección de la privacidad personal.

Tabla 24 Características de teléfono IP Yealink T20P. Fuente: Datos de la UIDE

Características del terminal Yealink T21P	Pantalla de 2 lineas x 15 caracteres LCD
	Manos libres
	Salida para auriculares (RJ9)
	2 puertos LAN, PoE
	Soporte VLAN y QoS
	2 puertos LAN 10/100 con Switch.
	Permite montaje mural
	Soporta módulo de expansión con botones BLF
	Chipset TI TITAN y procesador de voz Texas Instruments
	Voz HD: Codec HD con altavoz y auricular de banda ancha
	Alimentación: PoE estándar según norma IEEE 802.3af ó fuente de alimentación incluida
Características de Voz	Codecs HD: G722
	Codecs VoIP estándar: G.711, G.723.1, G.726, G.729A/B

	Altavoz manos libres full duplex
Funciones de telefonía	Llamada en espera, desvío, transferencia, rechazo de llamada
	Identificación de llamante (Caller ID), Lista de llamadas, No Molestar (DND), Rellamada, Flash
	Conferencia a 3, marcaciones rápidas, ajuste de volumen, selección de timbre personalizado
	Multi idioma, con soporte para castellano
	Botón de silenciar (Mute) y manos libres
	Respuesta automática (auto answer)
	Soporta teclas Busy Lamp Field (BLF) y Shared Bridged Line Appearance (BLA)
Características SIP	SIP 2.0(RFC3261) protocol, NAT transversal: modo STUN
	Marcación In-band DTMF y out-of band RFC2833 DTMF
	Modo Proxy y modo SIP peer-to-peer
Características de integración y seguridad	Agenda empresarial descargable (XML, LDAP, hasta 200 items) y politonos para timbre. Customización XML de la pantalla.
	Acceso a configuración por HTTP y/o HTTPS
	Soporta SRTP/TLS/HTTPS, encriptación AES.
	Comunicaciones seguras activando SRTP (RFC3711) en la configuración
	Soporte de Transport Layer Security (TLS)
	Soporte en la configuración de VLAN (802.1 pq), QoS
	Gestión de la autentificación usando MD5/MD5-sess
	Configuración segura via cifrado AES
	Bloqueo del terminal para protección de la privacidad personal.
	Modos de configuración para Administrador y usuario.

Tabla 25 Caracteristicas de Telefono IP Yealink T21P. Fuente: http://www.yealink.com/sp/product_info.aspx?ProductsCateID=650&CateId=622&BaseInfoCateId=650&Cate_Id=650&parentcateid=622

Especificaciones	Características del Teléfono
	>6 cuentas VoIP, línea directa, llamada de emergencia
	>Llamada en espera, transferencia de llamada, Desvío de llamadas
	>Retener.silenciar, flash, respuesta automática,remarcar
	>Lista de no deseados, historial de llamadas (100 entradas)
	>Ajuste de volumen, selección de tono de timbrado
	>Esquema de tono, registro de sistema
	>Multi-idioma (más de 20)
	>Compatible hasta con 6 módulos de expansión
Integración del sistema IP PBX	>Plan de marcación, marcar ahora
	>SMS, buzón de voz, MWI

	>BLF/BLA, intercomunicador, localizador
	>Detención de llamada, captura de llamada
	>Tono de timbrado distintivo
Códecs y funciones de voz	>Códec de banda ancha: G.722
	>Códec de banda angosta: G.711, G.723.1, G.726, G.729AB
	>VAD, CNG, AEC, PLC, AJB, AGC
	>Altavoz con AEC
Funciones de red	>SIP v1 (RFC2543), v2 (RFC3261)
	>NAT transversal: Modo STUN
	>DTMF: En banda, RFC2833, SIP Info
	>Modo de puente/router
	>Cliente TFTP/DHCP/PPPoE
	>Servidor Telnet/HTTP/HTTPS
Administración	>Auto configuración vía FTP/TFTP/HTTP/PnP
	>Configuración: navegador/teléfono/auto configuración
	>Llamada IP directa sin proxy SIP
	>Marcar número vía servidor SIP
	>Marcar URL vía servidor SIP
Seguridad	>HTTPS (servidor/cliente)
	>SRTP (RFC3711)
	>Seguridad de la capa de transporte (TLS)
	>Bloqueo del teléfono para protección personal
	>Modo de configuración admin/usuario
Características físicas	>TI TITAN chipset
	>Pantalla LCD de 320x160 con 4 escalas de gris
	>48 teclas, incluyendo 16 teclas programables
	>1 puerto RJ9 (4P4C) para microteléfono
	>1 puerto RJ9 (4P4C) para auriculares
	>2 puertos Ethernet RJ45 10/100M

Tabla 26 Características de teléfono IP Yealink T28P. Fuente: http://www.yealink.com/sp/product_info.aspx?ProductsCateID=650&CateId=622&BaseInfoCateId=650&Cate_Id=650&parentcateid=622

CAPITULO 4. Diseño del plan de migración a IPV6 y la coexistencia con IPV4 de la red de datos de la Universidad Internacional del Ecuador.

4.1. Metodología de la migración

Este trabajo busca diseñar un plan de migración a IPV6 y a su vez que mantenga la coexistencia de IPv4 de tal manera no se afecte a la red de datos y mucho menos a los servicios que son vitales para el funcionamientos de las diversas actividades de la UIDE, teniendo en cuenta estos factores y los análisis de los diversos campos que se abarcaron en capítulos anteriores, se decide que el mecanismo de transición Dual Stack cumple con los necesidades que demanda este proceso.

El mecanismo Dual Stack como se había mencionado en su análisis brinda la posibilidad de equipar tanto a host como equipos de la parte activa con una pila para cada protocolo de tal manera se pueda enviar y recibir paquetes IPv4 e IPv6.

Además de la posibilidad que se ha buscado en los diversos mecanismos de transición de poder realizar una migración gradual, esto nos la ofrece Dual Stack, con esta ventaja la configuración se la realizara por nodos, esto permite realizar pruebas de funcionamiento de las aplicaciones que serán transportadas por la red para finalmente y de acuerdo a la situación del entorno lograr una transición completa a IPV6, la figura 20 consta del esquema de Dual Stack.

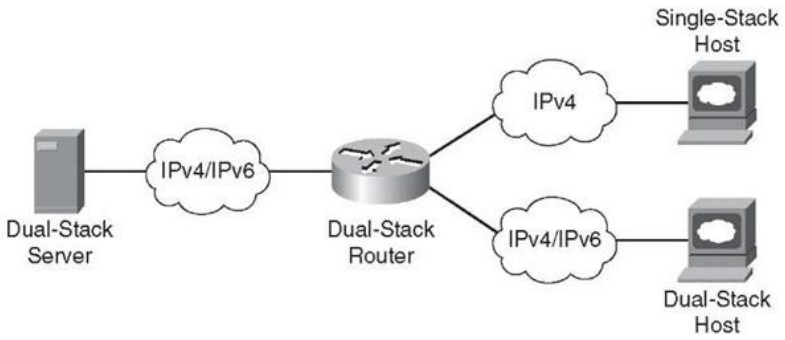


Figura 20 Esquema del mecanismo de transicion Dual Stack. Fuente: http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-1/

4.2. Conexión a internet.

La Universidad internacional del Ecuador maneja un enlace de datos a través de IPv4, además posee un enlace dedicado a IPV6 el mismo que al momento no se encuentra en uso debido a la no utilización de este protocolo en la red, estos enlaces son adquiridos a Telconet.

[62]"TELCONET es una empresa con operaciones en Ecuador con una trayectoria de más de 18 años en Soluciones de Conectividad, Internet, Centro de Datos y Servicios Gerencia dos. Con una sólida plataforma de infraestructura de Fibra Óptica de un altísimo nivel de capilaridad que le ha permitido desarrollar negocios junto con el resto de sus filiales que pertenecen al Grupo Empresarial así como con sus asociados de Negocios.

[62] http://www.telconet.net/telconet/telconet

Los servicios que dispone son:

- Internet dedicado.
- Transito al Backbone de datos.
- Transmisión de datos.
- Internet 2.
- Centro de datos.
- Cloud pública.
- Comunicaciones unificadas.
- Seguridad lógica.

Telconet es la única red en el país para manejo de IPv6 e Internet 2. La Red Académica Avanzada del Ecuador (Red CEDIA) opera sobre la Red Nacional NGN de TELCONET, uniendo las principales universidades, escuelas politécnicas, organizaciones de ciencia y tecnología del país, con plataformas de fibra óptica cuyas capacidades exclusivas para esta red van en el orden de 1 Gbps.

- Su implementación de basa en:
- Definición del modelo 6VPE.
- Habilitación de Routers.
- Creación de un esquema de direccionamiento.
- Laboratorios y pruebas.
- Liberación del producto.”

Las universidades que soportan el protocolo Ipv6 en Ecuador se muestran en la tabla 27.

PROVINCIA	Universidad
PICHINCHA	USFQ
	PUCE
	FUNDACYT
	EPN
	UTE
	UIDE
	ESPE
	UTN
	UCE
IMBABURA	PUCE
CHIMBORAZO	ESPOCH
GUAYAS	UCSG
	ESPOL
	UNEMI
LOJA	UTPL
AZUAY	UPS
SANTO DOMINGO DE LOS TSACHILAS	PUCE

Tabla 27. Universidades que soportan IPv6. Fuente: http://www.telconet.net/servicios/internet2

4.3. Protocolos de Enrutamiento para el plan de migración.

OSPF, ha sido pensado para el entorno de Internet y su pila de protocolos TCP/IP, como un protocolo de routing interno, es decir, que distribuye información entre routers que pertenecen al mismo Sistema Autónomo.

El fundamento principal en el cual se basa un protocolo de estado de enlace es en la existencia de un mapa de la red el cual es poseído por todos los nodos y que regularmente es actualizado.

Para llevar a cabo este propósito la red debe de ser capaz de entre otros objetivos de:

- Almacenar en cada nodo el mapa de la red.

- Ante cualquier cambio en la estructura de la red actuar rápidamente, con seguridad sin crear bucles y teniendo en cuenta posibles particiones o uniones de la red.

Las principales características son:

- Respuesta rápida y sin bucles ante cambios.

La algoritmia SPF sobre la que se basa OSPF permite con la tecnología actual que existe en los nodos un tiempo de respuesta en cuanto tiempo de computación para el cálculo del mapa local de la red mucho más rápido que dicho calculo en el protocolo RIP. Además como todos los nodos de la red calculan el mapa de manera idéntica y poseen el mismo mapa se genera sin bucles ni nodos que se encuentren contando en infinito; principal problema sufrido por los protocolos basados en la algoritmia de vector distancia como RIP.

- Seguridad ante los cambios.

Para que el algoritmo de routing funcione adecuadamente debe existir una copia idéntica de la topología de la red en cada nodo de esta. Existen diversos fallos que pueden ocurrir en la red como fallos de los protocolos de sincronización o inundación, errores de memoria, introducción de información errónea. El protocolo OSPF especifica que todos los intercambios entre routers deben ser autentificados. El OSPF permite una variedad de esquemas de autentificación y también permite seleccionar un esquema para un área diferente al esquena de otra

área. La idea detrás de la autentificación es garantizar que sólo los routers confiables difundan información de routing.

- Soporte de múltiples métricas.

  La tecnología actual hace que sea posible soportar varias métricas en paralelo, Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cuál es el mejor. Esta elección se realizara en base a los requisitos que existan en la comunicación. Diferentes métricas utilizadas pueden ser:

  - Mayor rendimiento
  - Menor retardo
  - Menor coste
  - Mayor fiabilidad

  La posibilidad de utilizar varias métricas para el cálculo de una ruta, implica que OSPF provea de un mecanismo para que una vez elegida una métrica en un paquete para realizar su routing esta sea la misma siempre para ese paquete, esta característica dota a OSPF de un routing de servicio de tipo en base a la métrica.

- Balanceado de carga en múltiples caminos.

  OSPF permite el balanceado de carga entre los nodos que exista más de un camino. Para realizar este balanceo aplica:

- Una versión de SPF con una modificación que impide la creación de bucles parciales.
- Un algoritmo que permite calcular la cantidad de tráfico que debe ser enviado por cada camino.

- Escalabilidad en el crecimiento de rutas externas.

El continuo crecimiento de Internet es debido a que cada vez son más los sistemas autónomos que se conectan entre sí a través de routers externos. Además de tener en cuenta la posibilidad de acceder al exterior del sistema autónomo a través de un determinado router externo u otro se debe tener en cuenta que se tiene varios proveedores de servicios y es más versátil elegir en cada momento el router exterior y servicio requerido que establecer una ruta y servicio por defecto cuando se trata de routing externo como se tenía hasta ahora. OSPF soluciona este problema permitiendo tener en la base de datos del mapa local los denominados "Gateway link state records".Estos registros nos permiten almacenar el valor de las métricas calculadas y hacen más fácil el cálculo de la ruta óptima para el exterior. Por cada entrada externa existirá una nueva entrada de tipo "Gateway link state records" en la base de datos, es decir, la base de datos crecerá linealmente con el número de entradas externas tal como ocurre con los protocolos de vector distancia, pero el coste del cálculo de las rutas crecerá en función de N*log*N para OSPF y no en función de N^2 como ocurre en los protocolos de vector distancia.

4.3.1. Configuración del protocolo OSPF en Ipv6

Las configuraciones que se muestran se las ha realizado en el paquete de simulación Packet Tracert.

1. Asignación del nombre al router.
2. Configuración de enrutamiento de los paquetes Ipv6.
3. Configuración de IPv6 en la interfast FastEthernet del Router.
4. Verificación de las configuraciones.

Los comandos de configuración de los pasos anteriores en packet tracer se los puede visualizar en la tabla 28.

Router>ena
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname REnlace
REnlace(config)#end
REnlace#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
REnlace#
REnlace>ena
REnlace#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
REnlace(config)#ipv6 unicast-routing
REnlace(config)#do sh interface
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
Hardware is CN Gigabit Ethernet, address is 0004.9a6a.1601 (bia 0004.9a6a.1601)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,

Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
REnlace(config)#int GigabitEthernet 0/0
REnlace(config-if)#ipv6 enable
REnlace(config-if)#ipv6 address 2001:1:a:1::1/64
REnlace(config-if)#do wr
Building configuration...
[OK]
REnlace(config-if)#end
REnlace#
%SYS-5-CONFIG_I: Configured from console by console
REnlace#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
REnlace(config)#int gigabitethernet 0/0
REnlace(config-if)#ipv6 ospf 1 area 0
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
REnlace(config-if)#

Tabla 28 Comando de configuración de Router con datos de IPV6 y de ospf

Una vez ejecutados los comandos de configuración se obtendrá la configuración del router habilitado IPV6 y ospf en la interface designada como lo muestra la figura 21.

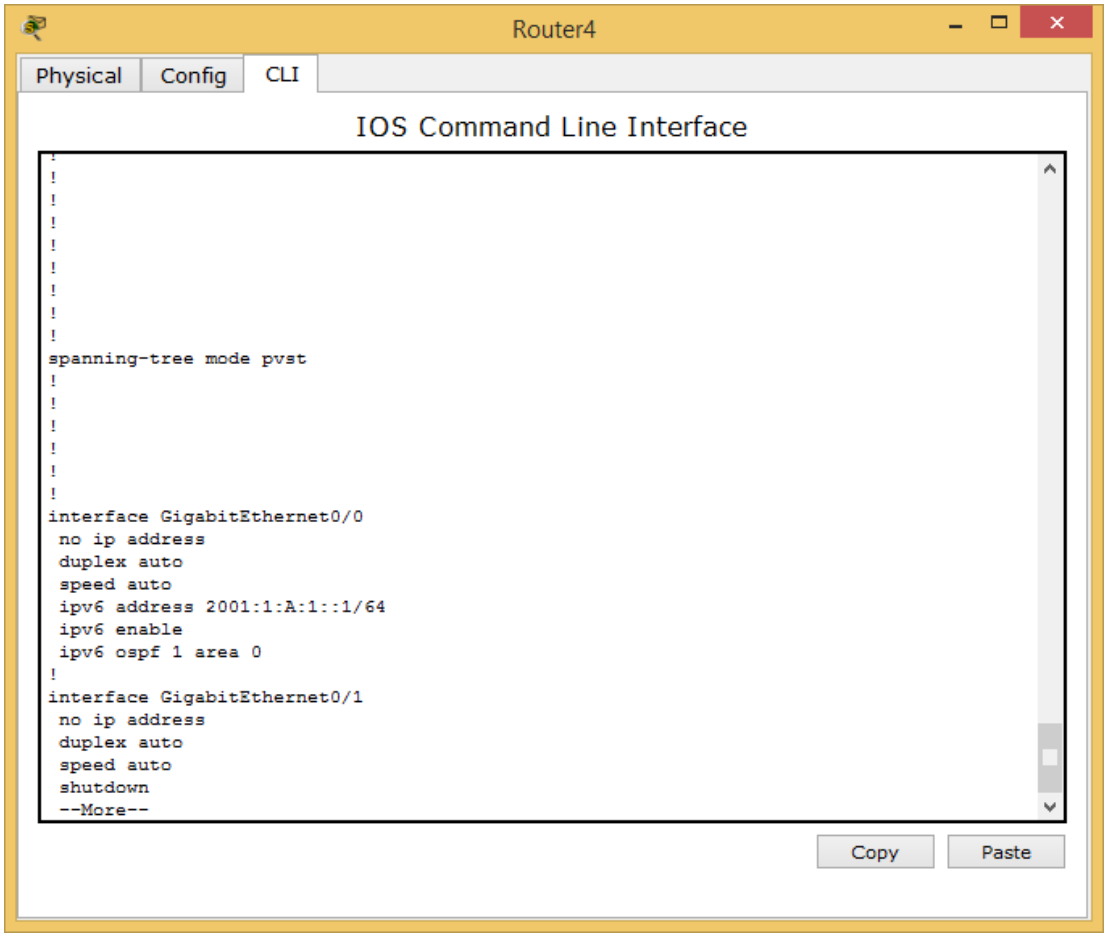


Figura 21 Configuración de IPv6 y ospf en Router 2911 en packet tracer. Fuente: El autor

4.3.2. Configuración del protocolo RIP en IPv6

1. Habilitar Rip en el router.
2. Habilitar Rip en la interfast del router.
3. Verificar las configuraciones.

La configuración del protocolo RIP en IPv6 lo muestra la tabla 29.

REnlace#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
REnlace(config)#ipv6 router rip process1

REnlace(config-rtr)#interface gigabiteth 0/0
REnlace(config-if)#ipv6 rip process1 enable
REnlace(config-if)#do wr
Building configuration...
[OK]

Tabla 29 Configuración del protocolo RIP en IPv6 en router 2911. Fuente: El autor

Una vez aplicados los comandos de configuración de los protocolos IPv6 en la Interface GigabitEthernet se obtendrá los resultados que muestra la figura 22.

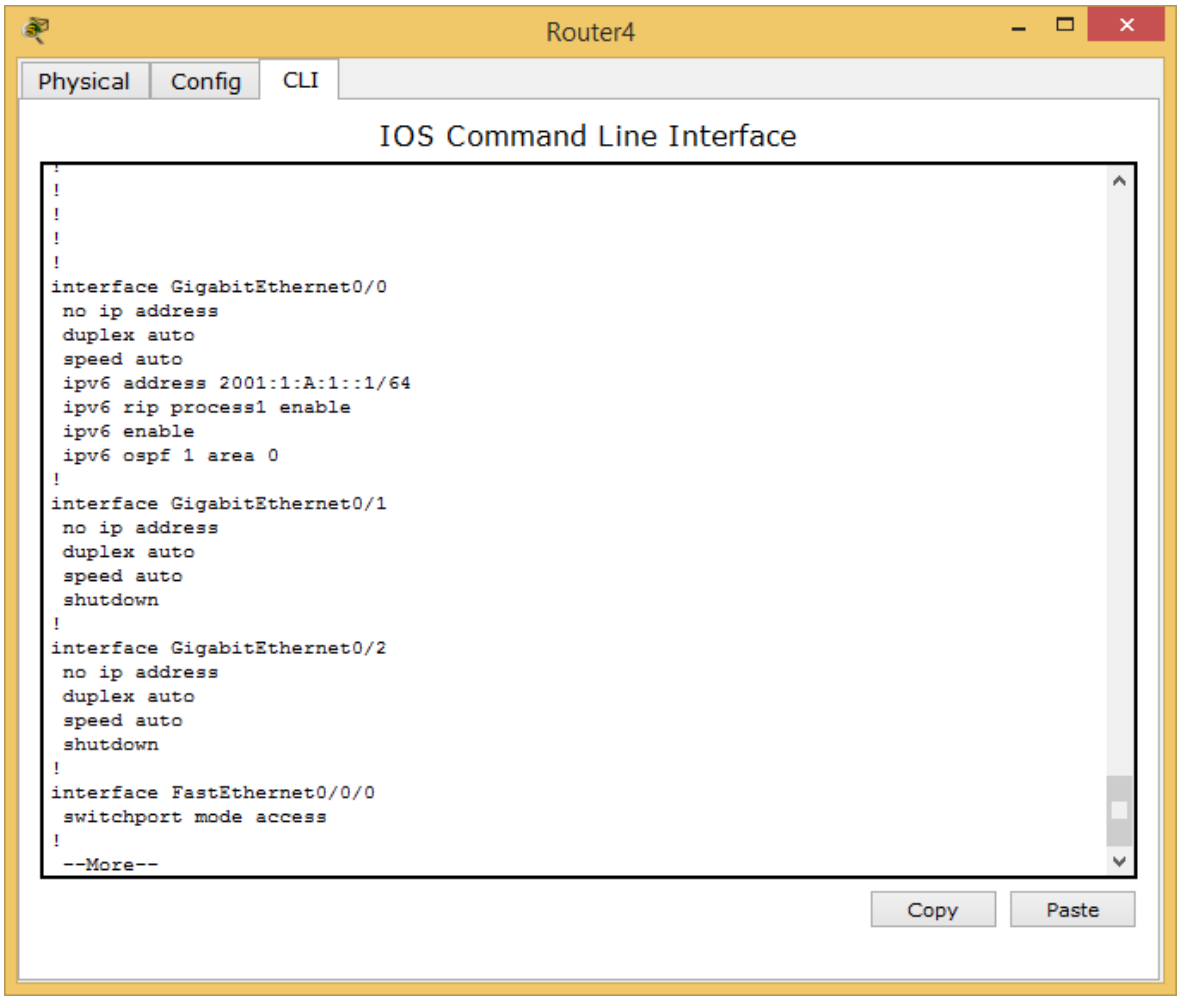


Figura 22 Configuración del Protocolo RIP en un Router. Fuente: el Autor.

4.3.3. Configuración de las rutas estáticas en ipv6

1. Habilitar rutas estáticas dentro del router con el Gateway necesario para la red.

2. Verificar la lista de rutas estáticas. (show ipv6 route static)

La configuración de las rutas estáticas en IPv6 se las visualiza en la figura 23.

```
Router2# configure terminal
Router2(config)# ipv6 route <prefijo_IPv6>/<longitud_del_prefijo> <interfaz_o_gateway>

nota: en caso de querer usar un gateway por defecto:
prefijo_IPv6/longitud_del_prefijo= :: /0
```

Figura 23 Configuración de rutas estáticas. Fuente: http://repositorio.cedia.org.ec/bitstream/123456789/44/2/cedia%20ipv6%20curso.pdf.

4.4. Escenarios de transición a IPV6.

Para realizar una transición al protocolo Ipv6 hay que tomar en cuenta las aplicaciones y servicios con que cuenta la UIDE de tal manera estas no se sean afectadas, es por esto que la transición se debe ser realizada tomando en cuenta con la coexistencia de los dos protocolos IPV4-IPV6, para lo cual es necesario visualizar los diferentes escenarios para la migración del protocolo.

4.4.1. Primer escenario.

El primer escenario consiste en mantener el protocolo Ipv4 hacia la red externa y manejar Ipv6 en la red interna de la matriz, lo propuesto permite manejar el protocolo IPv6 por vía DHCP en todos los equipos de la red hasta el Firewall que es manejado por un equipo cisco ASA, en este equipo se establece la configuración

del mecanismo de transición Dual Stack, mismo que permite la comunicación de la red local de IPv6 a Ipv4.

El diagrama al que hace referencia el primer escenario se lo puede visualizar en la figura 24.

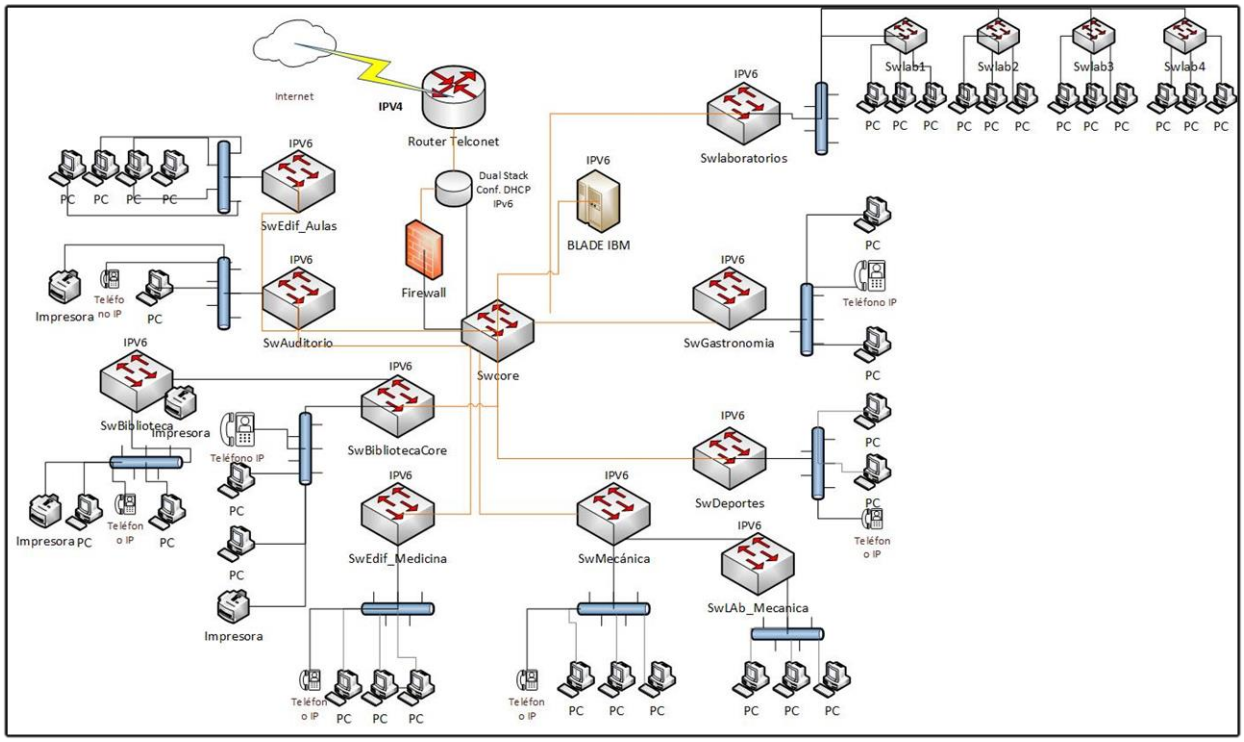


Figura 24 Esquema primer escenario. Fuente. El Autor.

4.4.1.1. Configuración del primer escenario

La configuración del primer escenario se la ha probado en la herramienta de simulación Packet tracert con las siguientes líneas de comandos.

Rfirewall>enable
Rfirewall# configure terminal
Rfirewall(config)#interface s0/1/0 ingreso
Rfirewall(config-if)#ipv6 enable
Rfirewall(config-if)#ip address 200.93.221.230 255.255.255.252

Rfirewall(config-if)#ipv6 address 2800:68:10::2/64
Rfirewall(confi-ifg)#exit
Rfirewall>enable
Rfirewall# configure terminal
Rfirewall(config)#interface GigabitEthernet0/0
Rfirewall(config-if)#ipv6 enable
Rfirewall(config-if)#ip address 172.17.2.1 255.255.255.0
Rfirewall(config-if)#ipv6 address 2800:68:10:1::1/64 ingreso dirección IPv6
Rfirewall(config-if)#exit
Para configuración de las rutas en el firewall es la siguiente:
Rfirewall>enable
Rfirewall# configure terminal
Rfirewall# ip route 172.0.0.0 255.255.255.252 serial0/1/0
Rfirewall# ip route 200.0.0.0 255.255.255.252 serial0/1/0
Rfirewall# ipv6 route 2800:68:10:1::/64 serial0/1/0
Rfirewall# ipv6 route 2800:68:10::1/64 serial0/1/0
Rfirewall(config-if)#exit

Tabla 30. Configuración de Firewall primer escenario. Fuente: el Autor

4.4.2. Segundo Escenario.

Para este el segundo escenario se asume que el enlace externo va a manejar una salida a través del protocolo IPv6, esto implica que tanto a nivel externo como interno ya está activo y funcional el protocolo IPv6, para este escenario se toma en cuenta la configuración del primer escenario en cuanto a la activación de DHCP en la parte interna de la red y en este caso el firewall estará configurado con un direccionamiento estático IPV6.

Las configuraciones en el router de entrada se encargan TELCONET, por lo que no se tiene acceso a las mismas.

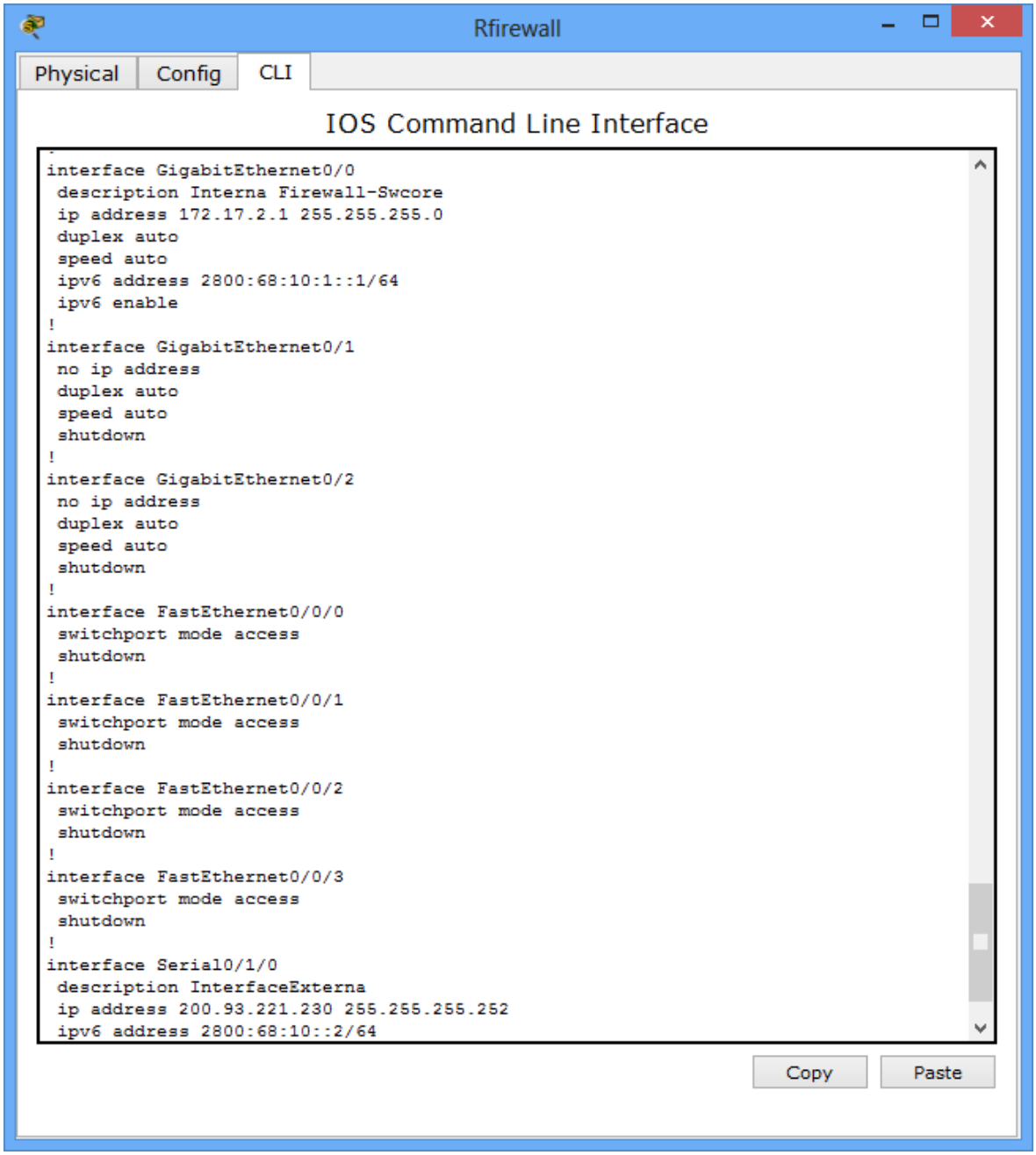


Figura 25 Configuración de equipos para el escenario 1. Fuente: El Autor

4.4.2.1. Configuración del segundo escenario

La configuración del segundo escenario se detalla a continuación con las siguientes características en cada línea de comando, basado en el esquema de la figura 26.

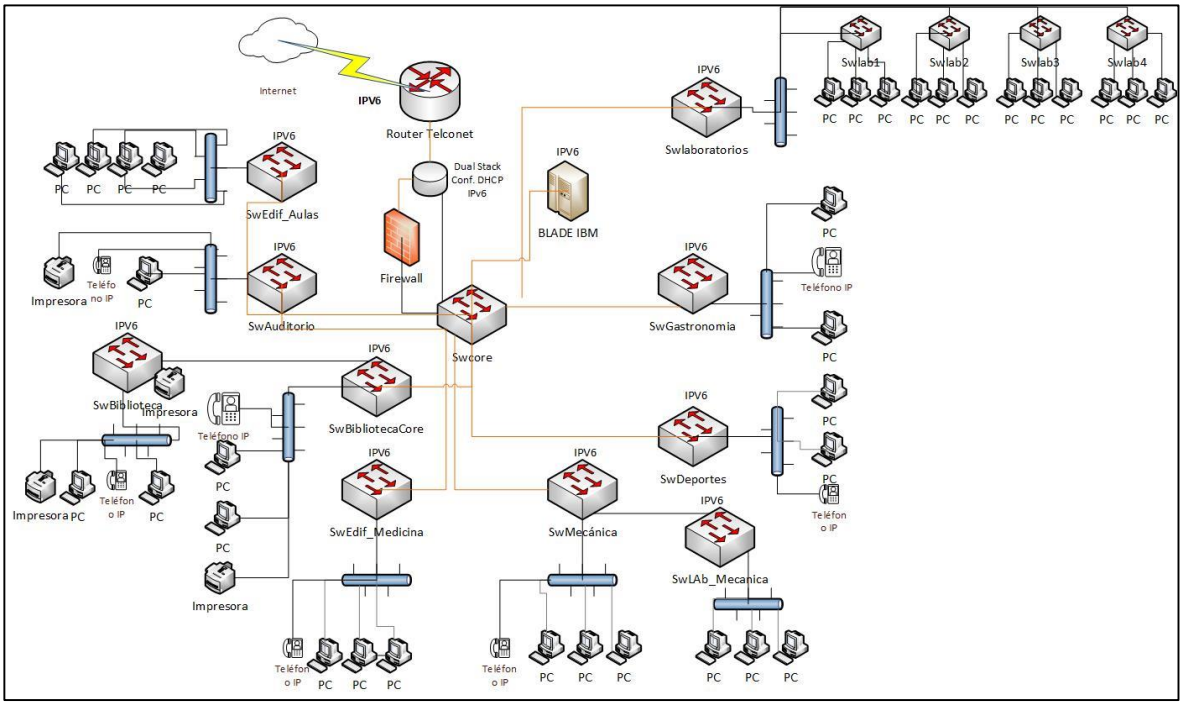


Figura 26 Esquema segundo escenario. Fuente: El Autor.

Comandos de configuración del segundo escenario.

Rfirewall>enable
Rfirewall# configure terminal
Rfirewall(config)#interface s0/1/0 ingreso
Rfirewall(config-if)#ipv6 enable
Rfirewall(config-if)#ipv6 address 2800:68:10::2/64
Rfirewall(confi-ifg)#exit
Rfirewall>enable
Rfirewall# configure terminal
Rfirewall(config)#interface GigabitEthernet0/0
Rfirewall(config-if)#ipv6 enable
Rfirewall(config-if)#ipv6 address 2800:68:10:1::1/64 ingreso dirección IPv6
Rfirewall(config-if)#exit
Para configuración de las rutas en el firewall es la siguiente:
Rfirewall>enable
Rfirewall# configure terminal
Rfirewall# ipv6 route 2800:68:10:1::/64 serial0/1/0
Rfirewall# ipv6 route 2800:68:10::1/64 serial0/1/0
Rfirewall(config-if)#exit

Tabla 31 Configuración de equipos para el segundo escenario. Fuente: El autor

4.5. Diseño del diagrama lógico

4.5.1. Diseño de la topología de red IPv6.

Como se había señalado en este trabajo el 99% de los equipos de la Universidad Internacional del Ecuador son de marca Cisco y en su gran mayoría estos soportan IPV6, al buscar la coexistencia entre los protocolos IPv4 – Ipv6 la topología de red se mantiene el análisis se lo realiza a través del simulador Packet Tracer donde se observara el comportamiento de la red y las configuraciones en cada equipo, para posteriormente realizar su implementación real.

4.5.2. Diseño de Vlan en IPV6

En la red, operan de forma simultanea IPv4 e IPv6, ambos protocolos son desplegados completamente y los protocolos de enrutamiento deben llevar los prefijos al protocolo correspondiente, de manera transparente, las configuraciones que se aplican en IPv6 son las mismas del protocolo IPv4 por lo tanto no existe inconveniente en las Vlans y es fácilmente soportado tanto los datos y voz.

4.5.2.1. Configuración de Vlans en IPV6

swcore#vlan database
swcore(vlan)#vlan 2 name Adminstrativa
swcore(vlan)#exit
swcore#vlan database
swcore(vlan)#vlan 4 name laboratorios
swcore(vlan)#exit
swcore#vlan database
swcore(vlan)#vlan 5 name Adminstrativa2
swcore(vlan)#exit
swcore#vlan database
swcore(vlan)#vlan 6 name Wireless
swcore(vlan)#exit

swcore#vlan database
swcore(vlan)#vlan 7 name Telefonia
swcore(vlan)#exit
swcore#vlan database
swcore(vlan)#vlan 34 name Seguridad
swcore(vlan)#exit

Tabla 32 Configuración de Vlan´s. Fuente: El Autor.

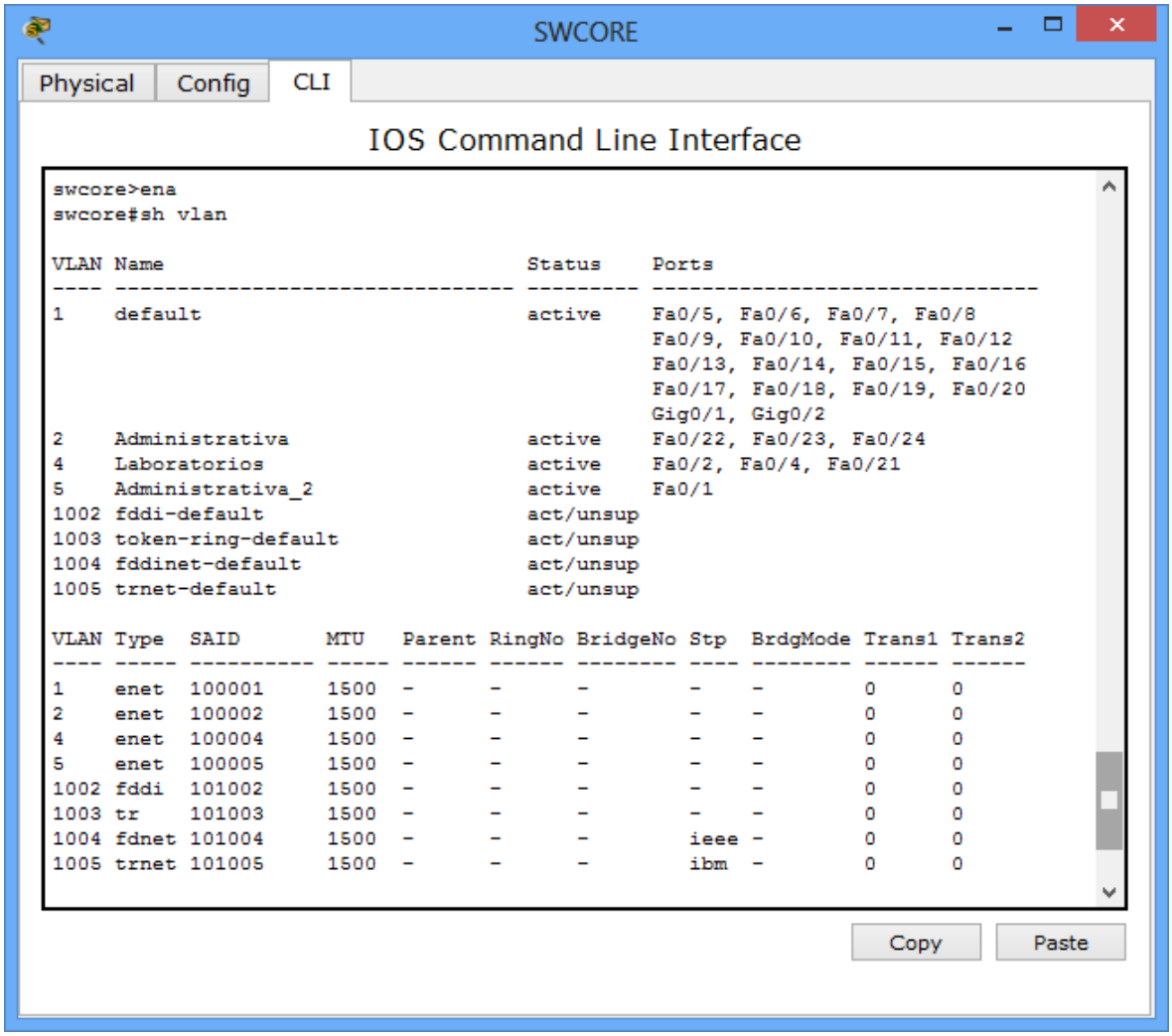


Figura 27 Vlan´s en packet tracer. Fuente: El autor

Configuración de las interfaces para vlan´s

Router>ena
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shut
Router(config-if)#interface fastEthernet 0/0)
Router(config-subif)#encapsulation dot1Q
Router(config-subif)#ipv6 address 2800:68:200::1/64

Tabla 33 Configuración de las interfaces para vlan´s Fuente: El Autor

4.5.3. Reglas de conectividad entre Vlans en IPV6

Las reglas de conectividad ACL´s de mantendrán con las mismas características que describieron en el capítulo tres de tal manera se mantenga el acceso entre las áreas que actualmente se comunican entre sí.

- Sintaxis de configuración de ACLS en Ipv6.

  ipv6 access-list <NAME> [permit|deny] <src-prefix[*]> | any | host <hostip> ... <dest-prefix[*]> | any | host <hostip> ... [log | log-input]

- Ejemplo

Bloquear el tráfico HTTP y HTTPS para que no llegue al **Servidor3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

4.5.4. Direccionamiento Ipv6 en la red de datos en la Sede Matriz de la UIDE

En IPv6 se tiene: parte de red y parte de interface.

Cada una de las universidades tienen una red /48, es decir tiene 64bits - 48bits = 16 bits disponibles para las subredes, para poder realizar éste proceso se debe considerar éstas dos reglas:

- Las subredes más pequeñas serán /64 y serán para departamentos, donde se asume que internamente no se realizará otra subred dentro de ella.
- Se deberá sumarizar redes en lo posible.

Tomando en cuenta que la subred más pequeña será /64, en cada subred puede existir 2^64 hosts (18446744073709551616 direcciones).

Esta cifra podría indicar que hay un desperdicio de direcciones, por las técnicas usadas en IPv4, sin embargo las direcciones disponibles en IPv6 son demasiadas y la cifra mencionada anteriormente es insignificante comparado con ello.

Tomando en cuenta estos aspectos, todas las interfaces serán /64, es decir de los 128 bits totales de cada dirección, los primeros 64 representarán la red, y los siguientes 64 representarán la interface, conocido en IPv4 como la porción de host. Para sumarizar, se tiene del bit 48 al 63, es decir con estos bits se puede tener 2^16 (65536) subredes, lo cual es suficiente para la red de la Universidad.

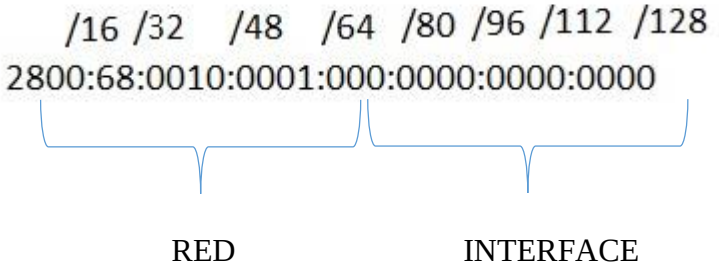


Figura 28 Distribución de una dirección IPV6. Fuente: El Autor

La figura 28 y sus características son definidos de la siguiente manera.

- Los primeros 32 bits definen la red de CEDIA -> 2800:68 Los siguientes 16 bits definen la red de la UIDE ➔:10:
- Los siguientes 16 bits definen a cada una de las redes de la UIDE :1:
- Los últimos 64 bits son los que definen a un host específico.

La arquitectura de la red de la UIDE es en forma de estrella, el direccionamiento IPv6 se lo realizará, aplicando lo siguiente:

- cada dependencia recibe una /56
- cada subred dentro de cada facultad recibe una /64
- las interfaces reciben una /64.

Para la distribución de IPv6 se toma en cuenta las recomendaciones de las RFC 3177 y RFC 3531 de tal manera se pueda planificar sin inconvenientes este proceso.

En primera instancia se tiene:

- 2800:68: RED CEDIA
- 2800:68:0010 RED UIDE Matriz.

Por lo tanto quedan disponibles para interfaces, de los bits 64 al 128, para subredes finales, entonces solo se tiene 16 bits para la creación de las mismas

De acuerdo al análisis de host con los que cuenta la UIDE y la proyección de crecimiento se toma en cuenta los datos de la siguiente tabla con el número total de direcciones.

Prefijo IPV6	Descripción
2800:0068:0010:0000:ffff:ffff:ffff:ffc0/128	Representa una subred con una sola dirección IPV6
2800:68:0010:1::/64	El prefijo de red 2800:68:0010:1::/64 puede manejar 2^{64} nodos. Esta es la longitud por defecto de un prefijo para una subred.
2800:68:0010::/48	El prefijo de red 2800:68:0010::/48 puede manejar 2^{16} prefijos de red de 64 bit. Esta es la longitud por defecto de un prefijo para un sitio.

Tabla 34 Direcciones IPv6 Disponibles. Fuente:
http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Para la configuración de los host se ha establecido por medio de DHCP caso contrario sucede en los equipos de la parte activa de la red donde la asignación de direcciones IP de lo realiza manualmente de tal manera se pueda llevar una configuración y administración controlada.

4.5.4.1. Distribución de direcciones IPV6 para las Vlans

La distribución de direcciones IPv6 para cada Vlan y de acuerdo al esquema que se maneja en la red de datos actual se la puede observar en la tabla a continuación.

Nombre de la Subred	*Descripción*	*Dirección de Red*	*Prefijo*
	Interfaces	2800:68:10::	56
Vlan1	Vlan Default	2800:68:100::	56
Vlan2	Vlan Administrativa	2800:68:200::	56

Vlan4	Vlan Laboratorios	2800:68:400::	56
Vlan5	Vlan Administrativa2	2800:68:500::	56
Vlan6	Vlan Wireless	2800:68:600::	56
Vlan7	Vlan Telefonía	2800:68:700::	56
Vlan34	Vlan Seguridad	2800:68:900::	56

Tabla 35 Distribución de IP´s en cada dependencia. Fuente: El Autor.

La tabla 36 muestra la tabla de direcciones IPV6, Gateway para cada Vlan, así como las direcciones útiles para cada subred.

Nombre de la subred	Descripción	Dirección de subred	Prefijo	Gateway	Subredes	Rango	Núm Hosts
VLAN 1	Vlan Default	2800:68:0010:100::	64	2800:68:0010:100::1	255/64	2800:68:10:100:0:0:0:1 - 2800:68:10:100:ffff:ffff:ffff:fffe	2^{64}
VLAN 2	Vlan Administrativa	2800:68:0010:200::	64	2800:68:0010:200::1	255/64	2800:68:10:200:0:0:0:1 - 2800:68:10:200:ffff:ffff:ffff:fffe	2^{64}
VLAN 4	Vlan Laboratorios	2800:68:0010:400::	64	2800:68:0010:400::1	255/64	2800:68:10:400:0:0:0:1 - 2800:68:10:400:ffff:ffff:ffff:fffe	2^{64}
VLAN 5	Vlan Administrativa2	2800:68:0010:500::	64	2800:68:0010:500::1	255/64	2800:68:10:500:0:0:0:1 - 2800:68:10:500:ffff:ffff:ffff:fffe	2^{64}
VLAN 6	Vlan Wireless	2800:68:0010:600::	64	2800:68:0010:600::1	255/64	2800:68:10:600:0:0:0:1 - 2800:68:10:600:ffff:ffff:ffff:fffe	2^{64}
VLAN 7	Vlan Telefonía	2800:68:0010:700::	64	2800:68:0010:700::1	255/64	2800:68:10:700:0:0:0:1 - 2800:68:10:700:ffff:ffff:ffff:fffe	2^{64}
VLAN 34	Vlan Seguridad	2800:68:0010:900::	64	2800:68:0010:900::1	255/64	2800:68:10:900:0:0:0:1 - 2800:68:10:900:ffff:ffff:ffff:fffe	2^{64}

Tabla 36 Distribución de vlan - Gateway. Fuente: El Autor

4.5.5. Servicios sobre IPv6

La Universidad Internacional del Ecuador dispone de varios servicios de los que depende el desarrollo de las diversas actividades que en esta se realizan, como se ha venido señalando a lo largo de este trabajo, la importancia de los sistemas tanto

financiero como académico es vital para cualquier implementación que se realice a nivel de infraestructura o configuración.

Además están los servicios comunes para el desarrollo de cualquier empresa como son correo electrónico, telefonía, etc. Estos servicios tiene soporte IPV6 puesto que en un mayor porcentaje están instalados sobre plataformas Windows y Linux lo que ofrece facilidades para su implementación y soporte en el caso de ser necesario, en estos casos la parte a modificar son los archivos de configuración.

4.6. Diseño del diagrama Físico.

4.6.1. Evaluación del diagrama físico.

La red de datos de la UIDE ha venido desarrollando bajo una topología estrella mixta, esto ha permitido el crecimiento de la red en varios segmentos sin presentar algún problema y siguiendo las normas y estándares tanto a nivel de seguridad como en la calidad manejados en el establecimiento.

Adicional a este punto el análisis abarca la ubicación tanto del MDF como la distribución de cada IDF concluyendo que estos además de contar con lugares aptos para su fácil manejo cuentan con una centralización exacta para la distribución y comunicación entre equipos de red activa, por lo cual esto no varía en el diseño del diagrama físico.

- Hardware

En la tabla 37 se detallan los equipos que dispone la UIDE y su compatibilidad con el protocolo IPV6, dentro de esta constan tantos servidores, Pc´s (de uso

administrativo, académico o estudiantil), equipos de la parte activa de la red (firewall, router, Switch) y teléfonos IP, los cuales cumplen con los requisitos necesarios para soportar el nuevo protocolo.

Equipo de red	Marca/Modelo	Soporta Ipv6	Acción a realizar
Servidores	IBM BladeCenter-H Midplane	SI	Verificar que el S.O tenga las actualizaciones necesarias.
PC´s		Si	Actualizar los equipos.
Firewall	Cisco ASA 5540	Si	Actualización del SO.
Router	Cisco 7604	ñSI	Actualización del SO.
Switch	Cisco 3750	SI	Actualización del SO.
	Cisco 2950		
	Cisco 2960		
Teléfonos	Yealink	SI	Actualización de firmware
	Elastix		

Tabla 37 Detalle de Equipos. Fuente: Datos de la UIDE

- Software

Los sistemas operativos que maneja la UIDE soportan IPV6, en su mayoría son sistemas Windows de última generación y en los sistemas operativos Linux en el peor de los casos se activa el módulo IPV6 para su funcionamiento, la tabla diecisiete presenta los sistemas operativos que la UIDE maneja.

Servidor	S.O instalado	Soporta Ipv6	Observación
Aplicaciones	Windows server 2008 R2	Si	
Bases de Datos			
Correo electrónico			
Antivirus			

CRM			
Proxi			
Archivos			
Aplicaciones WEB			
Biblioteca WEB	Centos 6.2	Si	En el caso de ser necesario se habilitara el módulo de IPV6
Telefonía			
Help Desk			
Moodle			

Tabla 38 Sistemas Operativos de los servidores. Fuente: Datos de la UIDE

Con respecto a los Pc´s con los que cuenta la UIDE tanto para las actividades de la parte administrativa como para el uso de los estudiantes, todos los equipos soportan en protocolo IPV6 como lo muestra la tabla 38.

Usuarios	**S.O. Instalado**	**Soporta IPV6**	**Observaciones**
Administrativos	Win 7 y Win 8	Si	
Laboratorios	Windows 8	Si	

Tabla 39 Sistema Operativo en PC´s de la UIDE. Fuente: Datos de la UIDE

4.7 Consideraciones para el Plan de implementación

4.7.1 Consideraciones.

Para la implantación de del plan de coexistencia, se han desarrollado tanto técnicas como análisis de procesos para la transición entre las dos versiones, la idea fundamental que se maneja es mantener la base funcional de la red de tal manera exista coexistencia entre los dos protocolos y la transición sea gradual al protocolo IPV6.

A lo largo de este trabajo se han analizado técnicas de transición con características específicas que se apliquen de manera individual o con otras técnicas de migración lo cual se puede acomodar a las diferentes necesidades de las empresas.

Para la implementación se aplica un método que permite la interoperabilidad lo cual brinda un gran nivel de seguridad en el funcionamiento de la red y la migración al protocolo Ipv6 este es un factor que se toma en cuenta debido al periodo de tiempo que estos protocolos deban coexistir en la red de la UIDE.

Para la primera fase de implementación del nuevo protocolo se toma en cuenta la disponibilidad que debe existir para las varias aplicaciones que maneja tanto la parte administrativa como académica, por lo tanto no se maneja nodos que trabajen únicamente con el protocolo IPv6, tras esto todos los nodos manejan el método Dual Stack.

4.7.2. Perspectiva general de la metodología.

La descripción de la metodología PETI (planeación estratégica de tecnologías de la información), está compuesta de cuatro fases las mismas que se detallan a continuación:

Fase 1: Situación Actual.[63]

[63] http://www.cisco.com/web/ES/about/press/2012/2012-05-30-internet-sera-cuatro-veces-mas-grande-en-2016--informe-vini-de-cisco.html

"El Informe Cisco VNI prevé que el tráfico IP global supere la barrera del Zettabyte y que haya 19.000 millones de dispositivos conectados, casi 2,5 conexiones por cada persona del planeta".

El tráfico IP global se multiplicará por cuatro entre 2011 y 2016 hasta alcanzar 1,3 Zettabytes, lo que supone una tasa de crecimiento interanual del 29 por ciento en este período. En España, el incremento es aún más acusado: el tráfico IP se multiplicará por 13 entre 2011 y 2016 hasta los 3,8 Exabytes anuales o 320 Petabytes mensuales (tasa de crecimiento interanual del 67 por ciento).

Así se desprende de la última edición del informe anual Cisco Visual Networking Index (VNI) 2011-2016, que analiza el crecimiento y evolución del Protocolo IP a escala global. El informe de este año cubre el período 2011-2016, y desvela el incremento de tráfico IP que previsiblemente viajará por redes públicas y privadas, incluyendo Internet, redes IP gestionadas y el tráfico móvil generado por los consumidores y usuarios empresariales. Este año Cisco también ha realizado un estudio complementario Cisco VNI Service Adoption Forecast, que ofrece el ratio de crecimiento previsto en servicios destinados al mercado residencial, segmento móvil de consumo y entorno empresarial tanto a escala global como regional.

El informe Cisco VNI (Visual Networking Index) 2011-2016 destaca distintos factores como los principales responsables de la evolución del tráfico IP:

1. El creciente número de dispositivos conectados. La proliferación de tablets, teléfonos móviles y otros dispositivos y conexiones máquina a máquina (M2M) está incrementando la demanda de conectividad. En 2016 habrá cerca

de 18.900 millones de dispositivos conectados a la Red a escala mundial, casi 2,5 conexiones por cada persona del planeta (frente a los 10.300 millones de dispositivos conectados en 2011). En España habrá 258 millones de dispositivos conectados en 2016 (5,1 conexiones por habitante), desde un total de 135 millones contabilizados en 2011 (2,8 conexiones per cápita).

2. Más usuarios de Internet. En 2016 habrá 3.400 millones de usuarios de Internet, aproximadamente el 45 por ciento de la población mundial prevista (7.500 millones de personas según la estimación de Naciones Unidas). En 2011 el número global de internautas era de 2.000 millones (aproximadamente el 28 por ciento de una población total de 7.100 millones). En España habrá 37 millones de usuarios de Internet de líneas fijas (excluyendo las conexiones sólo móviles, que sumarán otros 6,6 millones) en 2016, desde los 31 millones contabilizados en 2011.

3. Mayor velocidad de la banda ancha. Se prevé que la velocidad media de banda ancha fija se multiplique casi por cuatro, desde los 9 Mbps de 2011 hasta los 34 Mbps en 2016. En España, la velocidad media de banda ancha se multiplicará por cuatro entre 2011 y 2016, desde los 10,2 Mbps hasta los 40 Mbps. Entre 2010 y 2011 la velocidad media de banda ancha creció en España un 57 por ciento, desde los 6,5 Mbps hasta los 10,2 Mbps.

4. Más vídeo: Para el año 2016, 1,2 millones de minutos de vídeo el equivalente a 833 días o más de dos años cruzarán Internet cada segundo.

5. Crecimiento Wi-Fi. Para 2016, más de la mitad del tráfico mundial de Internet procederá de conexiones Wi-Fi.[64]

"según datos del MINTEL (ministerio de Telecomunicaciones) y el INEC (Instituto Nacional de Estadísticas y censos) se ha determinado que en Ecuador existe una aplicación total de Internet que representa el 36,77% es decir alrededor de 5,5 millones de usuarios a nivel nacional.

De acuerdo a los datos se ha podido determinar que el acceso al internet ha aumentado 7 veces más en relación al año 2006, debido a que 25 de cada 100 hogares ecuatorianos cuentan con una computadora de escritorio y 10 poseen un equipo portátil"[65]

Se analizan los siguientes puntos que determinan la situación de la red de datos de la UIDE.

- La UIDE es una institución educativa que maneja altos estándares de calidad y ha venido creciendo bajo estos, tanto a nivel de infraestructura como de servicios por lo que es vital el desarrollo del plan de migración al protocolo IPV6 con el fin de avanzar a la par de la tecnología de Internet además de actualizar la red de datos de la institución y hacer uso del canal dedicado a IPV6 que la UIDE dispone.

- A lo largo de este trabajo se ha señalado varios aspectos fundamentales acerca de las condiciones de la red de la UIDE, (Capitulo tres), donde se determina que la infraestructura de red de la UIDE se ha diseñado basada en el protocolo

[64] http://www.cisco.com/web/ES/about/press/2012/2012-05-30-internet-sera-cuatro-veces-mas-grande-en-2016--informe-vini-de-cisco.html
[65] ANDES (2012), 5.5 millones de personas tienen acceso a internet en Ecuador, obtenida el 13 de Agosto de 2012, de http://andes.info.ec/2009-2011.php/?p=141153

IPV4, al momento esta red da servicio y soporte a las aplicaciones que se maneja tanto a nivel académico como administrativo dentro de la Universidad, sin embargo el crecimiento e innovación de aplicaciones que se están manejando en la actualidad hace que se presenten desempeños no óptimos sobre los servicios.

4.7.3. Fase 2: Modelo de Negocios/organización.

Lo ideal en una estrategia de migración se basa en la configuración del Gateway ya que este es encargado de brindar la comunicación necesaria para las aplicaciones por ende permite que la institución continúe con sus actividades cotidianas, esto va a permitir que se vaya levantando la nueva infraestructura de red en los diferentes nodos, además se deben ir realizando los cambios necesarios en la configuración de las aplicaciones que así lo necesiten para su funcionamiento.

La configuración del Gateway en la actualidad no es un tema de mayor controversia puesto que las nuevas generaciones de dispositivos ofrecen la posibilidad de operar en ambientes mixtos IPV4/IPV6, esta opción permite realizar una migración controlada además de realizar las pruebas necesarias.

[66]"Según Stonesoft, muchas compañías han sufrido engaños sobre la complejidad que rodea la seguridad de IPv6. Así, la compañía está en disposición de ayudar tanto a las empresas privadas como a las públicas a implementar IPv6 de una forma segura y rentable.

[66]http://www.mintic.gov.co/portal/604/w3-article-5866.html

Basándose en su experiencia en despliegues IPv6 a gran escala, Stonesoft comparte los siguientes consejos sobre seguridad IPv6:

1. Moderniza tu red existente: rehacer tu red IPv4 implica limpiarla, deshacerse de lo inservible y actualizarla hasta hacerla nueva. Limpia y elimina las características desfasadas y desactualizadas. La actualización debe consistir en asegurar cada aspecto de la red que pueda estar efectivamente sin clasificar hasta el siguiente nivel, y que quede, de hecho, felizmente activo a lo largo de ese nivel.
2. Planea una introducción gradual: sigue el ejemplo de la seguridad de las Administraciones Públicas, que han estado trabajando con IPv6 durante más de media década, hasta la fecha. La completa implementación está planeada en tres fases, a lo largo de un lapso de tiempo de otros seis años.
3. No es necesario que avances tan despacio como el Gobierno, pero es cierto que si introduce gradualmente IPv6 te dará tiempo de sobra para asegurarse de que el protocolo funcionará con el estado actual de la técnica de la infraestructura IPv4. Además, tienes otra ventaja, y es que logrará mantener bajo control su presupuesto.
4. Decántate por la doble /pila/apilado: opta por el modo de doble apilado en su implementación IPv6. El doble apilado trae aparejados una serie importante de beneficios, si bien puede requerir actualizaciones del router para alcanzar las demandas necesarias de memoria y potencia y soportar el funcionamiento simultáneo de IPv4 e IPv6.

5. Ten cuidado de sus túneles: la publicación "Directrices para un seguro despliegue del protocolo IPv6", del Instituto Nacional americano de Estándares y Tecnología, sugiere contemplar y considerar los túneles de la misma forma que se trataría un link externo: con extremo cuidado. Esta investigación recomienda inspeccionar cada fragmento de tráfico de túnel antes de permitir tanto la salida como la entrada del sistema.

6. Ten en cuenta a los maliciosos: Los usuarios maliciosos ya se están infiltrando en el protocolo IPv6 más rápidamente de lo que lo han hecho en otros avances. No olvides las advertencias sobre los peligros de los anuncios de los routers y los ataques de "hombre en el medio".

7. Modernízate y adopta un firewall certificado: se cuidadoso con los anuncios relativos a la compatibilidad con IPv6. Sin una verificación externa, es probable que el proveedor haya simplemente adosado un generador de tráfico en su producto y diga que funciona. Debes centrar tu atención en los productos que hayan sido objeto de certificación por terceras partes, pues pueden usar las pruebas prácticas usando los métodos de evaluación públicamente aceptados para asegurarse de que usted sabe exactamente lo que su firewall puede manejar.

8. Requiera autenticación: la autenticación es más crítica y, afortunadamente, más fácil que nunca hasta ahora. Stonesoft recomienda considerar el uso de un proxy HTTP/HTTPS para que los usuarios accedan a Internet. Una vez que establezcas autenticación requerida para incluso acceder on-line, habrás reducido la amenaza de terceros no deseados entrando en su red sin aprobación.

9. Desempolva los libros: conoce la sintaxis IPv6. Esta es muy similar a la usada por IPv4, pero cuenta con notables diferencias en su fundación. Si conoces la sintaxis le será mucho más fácil decidir rápidamente cómo manejar una brecha de seguridad o implementar las medidas necesarias. Dado que IPv6 ha estado técnicamente presente desde hace más de una década, no hay precisamente falta de información sobre la materia por parte de los gigantes tecnológicos, e incluso cuenta con una guía de 188 páginas del Gobierno norteamericano.

10. Pulsa el botón "off": apagar las capacidades IPv6 cuando no se están usando puede sonar a obviedad, pero a lo mejor no es tan sencillo como tú piensas. Esto es porque un número determinado de programas ya han sido configurados para trabajar con IPv6, y otros tantos ya tienen el protocolo de encendido de forma automática por defecto. Comprueba una, dos y tres veces tu entorno para asegurarte de que IPv6 sólo está disponible cuando realmente está siendo usado. En este sentido, instalar un mecanismo con la capacidad de deshabilitar IPv6 en un sentido amplio puede ser una gran inversión.

11. Saber "cómo matar": incluso con amplías partes de su red con el protocolo IPv6 deshabilitado, puedes aún afrontar la amenaza de visitantes IPv6 no deseados. Si ese es el caso, deberías saber cómo eliminarlos antes de que puedan infectar a otros asociados a tu red. Es justo entonces cuando conocer la sintaxis IPv6 puede ser un salvavidas, particularmente a la hora de implantar firewalls efectivos y filtros de tráfico. De hecho, puedes crear filtros que permitan el acceso a lo que usted quiera, mantener alejado lo que no."[67]

http://www.mintic.gov.co/portal/604/w3-article-5866.html

4.7.4. Fase 3: Modelo de tecnologías de la Información.

La aplicación de esta fase depende de las características tanto del software como del hardware que forma parte de la infraestructura de la UIDE, para ello se tomó como base el análisis que se realiza en el capítulo tres, una vez realizado este proceso se determinara con precisión si los nodos soportan la versión del protocolo IPV6 y en caso que se requiera actualizaciones a nivel físico o de software poder solventarlo a tiempo y no causar problemas de estabilidad en los servicios.

A continuación se listan los sistemas operativos que soportan IPV6.

[68]"IPv6 está soportado por los principales sistemas operativos de la actualidad:

- Microsoft Windows 7, Vista, Windows Server 2008, Windows Server 2003, Windows XP (Service Pack 2 o superior), Windows CE (4.1 o superior), Red Hat Linux (7 o superior), Debian, SUSE Linux (10.x o superior), Fedora, Ubuntu, FreeBSD (4 o superior), HP-UX, Apple MAC OS, Sun Solaris (8 o superior), Tru64 UNIX, Symbian (7 o superior).

Los sistemas operativos de los principales fabricantes de plataformas de red están listos para IPv6:

- Cisco, Juniper, Huawei, etc.

Los tres primeros sistemas operativos empleados en teléfonos móviles soportan IPv6:

[68] http://www.cu.ipv6tf.org/soipv6.htm

- Linux, Symbian y Windows Mobile.

Plataformas de desarrollo con soporte IPv6 para Windows:

- JAVA SDK, .NET 1.1 o superior, Visual Studio 2003 o superior.

Programas de certificación que incluyen IPv6:

- Apple Bonjour Conformance test 1.2.3
- Microsoft's Premium "Certified for Windows Vista/7"."

Dentro de la UIDE se maneja aplicaciones de uso común que soportan el protocolo IPV6 estos son:

- Winamp desde la versión 5.34
- Mozilla Firefox desde la versión 2.0
- Mozilla Thunderbird desde la versión 2.0.0.4
- Internet explorer desde la versión 4.0.1
- Microsoft Outlook desde la versión 2003
- Vlc media player desde la versión 0.8.6
- Windows media player desde la versión 9.0

4.7.5. Fase 4: Modelo de la planeación.

4.7.5.1. Escenarios de migración

[69]"Existen dos posibles para una estrategia de migración suave y controlada. Las empresas pueden mover los clientes hacia IPv6 mientras mantienen sus servidores en IPv4 o pueden migrar los servidores a IPv6 y dejar a sus clientes en un ambiente IPv4. Mover el cliente a IPv6 requiere que todos los clientes sean capaces de agregarse a la red vía caminos IPv6 permitidos.

Muchas empresas encontrarán más fácil comenzar a migrar servidores (aplicaciones) antes que los dispositivos cliente, esto simplemente porque los servidores están completamente bajo el control de las empresas mientras que los dispositivos clientes a menudo no lo están.

Al migrar servidores, el dispositivo Gateway se encuentra entre los servidores y los clientes, y debe agregarse una red capaz de soportar IPv6. El resultado es que la red tendrá IPv4 sobre el lado del cliente del dispositivo y ambos protocolos IPv4 e IPv6 detrás de él.

Una vez que la red IPv6 es establecida, los servidores pueden moverse de la red IPv4. Dado que los dispositivos cliente en un futuro estarán basados en IPv6, es imperativo que las empresas se aseguren que su infraestructura y aplicaciones también sean capaces de soportar IPv6."

4.7.5.2. Prioridades de la Implementación.

[69] http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106-enterprisenotreadyipv6

Las prioridades de una implementación de este tipo está basada en la inversión que debe hacer la institución y va de acuerdo al uso de la tecnología de punta que esta debe utilizar, al ser parte de la comunidad educativa donde la calidad está dada por la tecnología ya sea en equipos, infraestructura o protocolos de comunicación, es por esto que en este trabajo se analiza los temas importantes para una migración correcta y controlada.

4.7.5.2.1. Seguridad.

Debido al crecimiento constante de la población universitaria y penetración de internet existente en el campus de la UIDE es importante el tema de la seguridad en la red, tanto en el proceso de migración como en el funcionamiento de IPV6 como tal, por lo tanto los niveles de seguridad deben ser incrementados ya sea utilizando métodos ya conocidos como son la encriptación de datos.

"IPv6 incluye explícitamente la posibilidad de utilizar el modelo de seguridad IPsec (Internet Protocol Security) que proporciona autenticidad, integridad y confidencialidad a las comunicaciones de extremo a extremo.

IPsec es un conjunto de protocolos abiertos que tienen como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6), y de ese modo, a todos los protocolos de capas superiores.

En IPv4 la implementación de IPsec se define en una especificación diferente a la del propio protocolo IPv4, por lo que la inclusión del protocolo se hace con mecanismos definidos fuera del mismo, mientras que en IPv6 la propia arquitectura "extensible" del protocolo permite implementar IPsec de forma natural. Es importante reseñar que

IPv6 habilita la posibilidad de usar IPsec, y no los mecanismos de cifrado y autenticación propios de IPsec.

IPsec tiene dos modos de funcionamiento que proporcionan distintos niveles de seguridad:

- Modo Transporte: se cifra y/o autentica la carga útil, o payload, pero las cabeceras no se tienen en cuenta. Tiene como ventaja que se puede utilizar de extremo a extremo pero, por contra, la información de las cabeceras, como la dirección IP de origen y destino, es visible.
- Modo Túnel: una plataforma, o pasarela, encapsula el paquete original en otro paquete. Con ello se cifra y/o autentica el paquete original completo, pero se necesita de una plataforma que realice el túnel.

Además, IPsec tiene dos modos o protocolos de transferencia, que a su vez pueden funcionar en modo túnel o transporte:

- AH (Authentication Header): proporciona autenticación, integridad y un servicio de anti-repetición opcional.
- ESP (Encapsulating Security Payload): además de las ventajas anteriores proporciona confidencialidad."[70]

[71]"Tanto IPv4 e IPv6 tienen diferentes preocupaciones de seguridad, IPv6 no debe considerarse mejor que su predecesor desde una perspectiva de seguridad. Sin embargo

[70] cert_inf_seguridad_implantacion_ipv6
[71] http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/338-como-proteger-el-cambio-a-redes-ipv6

se toma en cuenta estos consejos para proteger la implementación de los riesgos de seguridad inherentes a las implementaciones de IPv6.

1. Reconocer los riesgos de las configuraciones de doble pila.

En una configuración de doble pila, un dispositivo admite simultáneamente IPv4 e IPv6. Las reglas de los firewalls y otros controles de seguridad que detienen el tráfico no deseado en IPv4, es improbable que sean eficaces para detener tráfico IPv6, por lo que las organizaciones suelen necesitar tecnologías de seguridad paralelas para afrontar esta nueva situación. Sin estas tecnologías, IPv6 está en alto riesgo de ser utilizado para comprometer o abusar de un dispositivo, creando posibles riesgos de seguridad que podrían no ser detenidos o detectados.

2. Deshabilitar y bloquear IPv6 en lo que no se necesita.

Una práctica de seguridad general es desactivar todos los protocolos de red innecesarios. Sin embargo, incluso si una institución tiene una política contra el uso de IPv6, puede encontrar que algunos dispositivos están habilitados para el uso de IPv6 de todos modos. El nuevo hardware a menudo viene con IPv6 habilitado automáticamente por omisión. Y dada la creciente popularidad de traer su propio dispositivo al trabajo, es probable que algunos de éstos tendrán IPv6 habilitado. Deshabilite IPv6 en dispositivos de propiedad del gobierno cuando no es necesario y bloquee todo el tráfico IPv6 no deseado en las redes inalámbricas y huésped.

3. Limite las formas permitidas de Túneles IPv6.

El tunneling encapsula los paquetes IPv6 dentro de paquetes IPv4. Cada forma permitida de túneles IPv6 presenta un vector de ataque adicional y puede ocultar el tráfico del examen de seguridad. Configure el firewall para permitir sólo las formas de túneles IPv6 que el departamento de TI autoriza y bloquee el resto. Además, acomode todos los túneles de IPv6 de manera que sus contenidos internos sean examinados por firewalls, sistemas de detección de intrusiones de software anti-malware, y otros controles de seguridad de red.

4. Compensar la pérdida de la traducción de direcciones de red.

La traducción de direcciones de red (NAT) es una tecnología de red IPv4 de uso común que, como efecto secundario de su función, proporciona una capa de protección frente a los dispositivos habilitados para IPv4 mediante la ocultación de ellos del contacto directo con las redes externas. Por desgracia, ya que no hay contrapartida de NAT en dispositivos IPv6, los que fueron protegidos previamente por NAT podrían ahora estar directamente expuestos a los ataques.

Esto es particularmente cierto en las redes domésticas, donde no hay otros controles de seguridad perimetral en el lugar. Para mitigar esto, asegúrese de que cualquier dispositivo que ejecuta IPv6 esté protegido por un firewall en el host o en la red, que bloquee de tráfico entrante no deseado.

5. Verifique las capacidades de IPv6 de herramientas de seguridad y administración.

Muchos host y redes de seguridad existentes y las herramientas de administración podrían no proveer soporte completo para IPv6. Si permite el uso de IPv6 en su red, asegúrese de que cada herramienta se puede manejar adecuadamente la actividad en IPv6. Por ejemplo, ¿el software de log es capaz de llevar registro de direcciones IPv6 o sólo de IPv4?, ¿las herramientas de gestión de seguridad de la red son capaces de agrupar múltiples direcciones IPv6 asignadas a un mismo dispositivo?

Evalúe sus herramientas para asegurarse de que funcionan correctamente antes de implementar IPv6."

4.7.6. Plan de implementación de IPV6

La migración a IPV6 es un proceso que genera un cierto grado de incertidumbre tanto en su ejecución como en la importancia de la migración y a esto se une el factor económico puesto que la migración representa un gasto muy importante para cualquier institución sea educativa o cualquier otro servicio que brinde, desde el punto de vista económico la migración a IPV6 no genera un retorno a la inversión, además, si la empresa no maneja publicaciones a través del servicio de internet la migración no provee beneficios, la migración al protocolo IPv6 implica a demás entrenamiento, actualización de la infraestructura o reemplazo en alguno de los casos ya que son necesarios equipos con mayores capacidades de hardware, la inversión también debe abarcar adecuaciones de software.

[72]"Desde un punto técnico hay que hacer las siguientes consideraciones:

- Cambio de paradigma tecnológico (codificación diferente, configuración diferente, notación diferente).
- Cambio de tecnologías a aquellas que soporten IPv6.
- Cambios en los esquemas de ruteo.
- Tablas enormes en los esquemas de ruteo.
- Interoperabilidad entre IPv4 e IPv6 (que sí está definido en el protocolo).
- Cambios en las aplicaciones.
- Cambios en los protocolos base (ARP, ICMP, IGMP).
- Mayor cantidad de ancho de banda (el encabezado de IPv6 es casi el doble de grande que el de IPv4).

La posibilidad del uso de NAT, el mismo que permite el poder salir con una sola dirección al mundo ha postergado la necesidad de direcciones IPv4".

Con el análisis anterior y al ser la UIDE una institución de calidad y en constante adaptación a los cambios tecnológicos con el fin de brindar a la población Universitaria servicios de punta, por estas razones cabe señalar las características a las que se debe apegar la migración al protocolo IPv6 en la UIDE.

[72] http://www.magazcitum.com.mx/?p=568

El primer paso para la migración es establecer un cronograma el cual permita establecer las actividades y los tiempos que tomara la ejecución de cada proceso para esto se utilizara herramientas que se ajusten a lo requerido.

Para el plan de implementación se toman en cuenta los siguientes criterios:

1. Capacitación.

En la actualidad en el Ecuador las personas de sistemas y redes, no tienen un vasto conocimiento de IUPv6, ni existe la experiencia de trabajar con dos protocolos de red simultáneamente, por lo que la capacitación del personal en el protocolo IPv6 es el punto de partida para la implementación.

IPv6 ha heredado varias similitudes de Ipv4, sin embargo en este protocolo también se han introducido características y diferencias que no permiten la implementación si el personal no está debidamente capacitado. Por esto la recomendación como primer paso es capacitar a los administradores de las plataformas de TI.

Tener al personal debidamente capacitado permite que la implementación sea segura y cumpla con los tiempos dispuestos en el cronograma, también va a permitir la reducción de los costos al permitir.

2. Planificación.

En la etapa de planificación, se deben establecer los distintos planes y configuraciones que deberán tener los distintos componentes de software y de hardware que participarán en la implementación de IPv6.

a. Nivel de Adopción.

Lo primero a definir es que redes y servicios van a participar en la implementación a IPv6, y en qué plazos o etapas.

En la etapa de Levantamiento, puede establecerse que hay equipamiento o servicios en los que no es posible implementar IPv6. Esto, puede impactar en la decisión de no adoptar IPv6 en toda la red de la institución y dejar ciertos servicios sólo en IPv4, hasta que se produzca una renovación ya sea del equipamiento o de la versión del software.

Además, suele suceder que la renovación, en particular de software, no es una decisión sólo del área TI de la institución, si no que del área que utiliza el software, ya sea por motivos financieros, de aplicaciones o personalizaciones desarrolladas en torno al software u otros.

El Nivel de Adopción, es entonces, una decisión estratégica, en que se pueden ver involucradas varias áreas de la institución, en particular, las que operan o utilizan servicios y las que son responsables por su renovación.

b. Plan de Direccionamiento.

La adopción de IPv6 da la oportunidad de re direccionar completamente la red y solucionar los problemas ocasionados por los crecimientos inorgánicos de las instituciones.

c. Plan de Seguridad

El plan de seguridad debe seguir las recomendaciones de los documentos [RFC 4890] y [RFC 4942].

Por lo general, las redes IPv4 e IPv6 tienden a ser similares, por lo que la gran mayoría de los criterios de seguridad utilizados en IPv4 siguen siendo válidos en IPv6. Los clásicos ataques en IPv4 tienen su símil en IPv6. Adicionalmente, han aparecidos nuevos ataques por cambios en el protocolo y sobretodo riesgos introducidos por los mecanismos de transición.

La principal consideración a tomar en términos de seguridad es que, al contrario de IPv4, todos los equipos, incluyendo los de usuarios finales tendrán direcciones públicas por lo que pueden ser accedidos desde el exterior en una configuración por defecto. Si bien esto no quiere decir que sufrirán más ataques, sí requieren un cuidado especial. Es por esto que el uso de firewalls tanto corporativos como los de los terminales se hace crítico.

3. Plan de asignación de direcciones.

Para la migración del protocolo IPV6 se establece una dirección IPv6 base que conferirá en este caso TELCONET que es el ISP de la UIDE, con esto se establecerá la configuración de la red, es necesario también identificar los nodos y dispositivos que manejaran una dirección IPV6.

Los nodos que se manejan en la UIDE son los siguientes:

- Router
- Firewall
- Switch Core
- Switch´s secundarios (de cada edificio y piso).

4. Herramientas de Monitoreo y Log

Las herramientas de monitoreo y de análisis o correlación de logs, que actualmente se utilizan en la UIDE en el análisis se considera que estas capacidades deben mantenerse para el tráfico IPv6, si es necesario la actualización de una o varias de las herramientas se considera aplicaciones de software libre existentes que dan resultados exitosos en el monitoreo de la redes y servidores en IPv6 estos pueden ser:

- Nagios.
- Zabbix.
- Cacti.
- Zenoss.
- Munin.

5. Seleccionar un protocolo de enrutamiento adecuado para IPV6 y establecer políticas de enrutamiento.

En el capítulo tres se hace el análisis de las ventajas y desventajas del uso de cada protocolo tras lo cual el que cumple con las características necesarias en este proceso es el protocolo OSFP de la misma manera las rutas son estáticas.

6. Implementación de un mecanismo de transición.

El mecanismo de transición a implementarse es Dual Stack por los beneficios que brinda a la transición el análisis se lo detalla en el capítulo tres.

7. Habilitar el protocolo IPV6 en los clientes.

La asignación de las IP´s del protocolo IPv6 se lo realizara por medio de DHCP, para lo que se debe trabajar con un proceso y en un cronograma establecido:

a. Habilitar la configuración DHCPv6 en el router Pincipal.
b. Asignar tiempos en los que se habilite el protocolo DHCPv6 en cada departamento y realizar las pruebas de funcionamiento.
c. De acuerdo al cronograma establecido habilitar el protocolo DHCPv6 a cada una de las máquinas de los usuarios.

4.7.7 Costos de la implementación.

En todo proyecto de TI, los costos son un tema fundamental en el análisis previo a la implementación, más aun si el área en la que se realizara el cambio, actualización o implementación afecte directamente a la infraestructura ya que los elementos que están conjugados llegan a valores económicos muy altos en especial al tratarse de equipos de la parte activa de la red.

En el caso de la UIDE esta cuenta con equipos que se han venido actualizando previamente para la migración al protocolo IPV6 y manejando la posibilidad de coexistencia con el protocolo actual IPV4.

En el análisis desarrollado se toma en cuenta los siguientes factores que actúan de manera directa en la implementación:

- Hardware.
- Software.
- Recurso Humano.
- Capacitación.

4.7.7.1 Hardware.

El hardware de la UIDE se ha analizado a lo largo de este trabajo de lo que se ha concluido que estos soportan sin ningún inconveniente el protocolo IPV6, además de la actualización que se ha venido realizando en varios Switch Cisco 2950 al modelo cisco 2960XR con lo cual se garantiza la migración a IPv6. La siguiente tabla muestra los equipos actuales que componen la parte activa de red.

Por los motivos descritos no es necesaria la compra de nuevos equipos siendo el único trabajo que se realizara, la actualización del IOS si es el caso en los equipos 2950, dejando la configuración como paso siguiente.

EQUIPO	MODELO	AREA
SWITCH	Cisco 2950	Laboratorio 1
SWITCH	Cisco 2950	Laboratorio 3

SWITCH	Cisco 2950	Laboratorio 4
SWITCH	Cisco 2950	Deportes
SWITCH	Cisco 2960	Gastronomia
SWITCH	Cisco 3560	Biblioteca core
SWITCH	Cisco 3950	Edificio Administrativo
SWITCH	Cisco 3560	Biblioteca
SWITCH	Cisco 3560	Residencias
SWITCH	Cisco 2950	Ed. Aulas Piso 2
SWITCH	Cisco 2950	Datacenter
SWITCH	Cisco 2950	Ed. Aulas PB
SWITCH	Cisco 2950	Ed. Aulas Subsuelo 1
SWITCH	Cisco 2950	Mecanica
SWITCH	Cisco 2960	Caballerizas
SWITCH	Cisco 2960	Marketing
SWITCH	Cisco 2960	Medicina
SWITCH	Cisco 2960	Datacenter sistemas
SWITCH	Cisco 2960	Datacenter
SWITCH	Cisco 2960	Caballerizas
SWITCH	cisco SG500 48 PoE	Planta baja edificio de aulas
SWITCH	cisco SG300 8 Puertos	Auditorio Marcelo Fernandez
SWITCH	cisco SG300 28 PoE	Primer Piso
SWITCH	cisco SG300 28 PoE	segundo piso
SWITCH	cisco SG300-10	Garita 1

Tabla 40 Tabla de equipos de la UIDE. Fuente: El Autor

4.7.7.2 Software.

Con respecto al software los servidores de la UIDE en mayor parte disponen de sistemas operativos de Microsoft Windows Server 2008 R2 y 2012 en servidores y Windows 7 y 8 en clientes, todos soportan IPV6, para estos sistemas operativos el licenciamiento se lo hace a través del campus agreement el mismo que se lo renueva todos los años bajo el presupuesto académico por lo que no se debe realizar adquisición alguna en temas de licenciamiento.

Por otro parte para contadas aplicaciones se hace uso de sistemas operativos bajo Linux, sistemas que soportan IPV6 sin tener costos adicionales.

4.7.7.3 Recurso Humano.

Dentro del recurso humano no se toma en cuenta la mano de obra ya que la migración la realizara el personal del área de redes e infraestructura de la UIDE el mismo que está capacitado para llevar a cabo el plan de migración, sin embargo que se contratara un paquete de horas de soporte técnico con la empresa Shekinan la misma que tiene la experiencia necesaria para despejar dudas que se generen en el tiempo de implementación.

Cantidad en horas	Descripción	Costo por hora	Costo Total
40	Horas de soporte	$50	$2000

Tabla 41 Paquete de horas de soporte. Fuente: Shekinan

4.7.7.4 Capacitación.

El proceso de migración debe ir de la mano tanto en la ejecución de pruebas asa como en capacitaciones que se realice al personal técnico y a los usuarios.

Cantidad en horas	Descripción	Costo por hora	Total
Pruebas de funcionamiento	100	$40	$4000
Capacitación de personal técnico en el manejo de IPV6	40	$50	$2000
Capacitación para los usuarios en el uso de IPV6 “Aplicaciones”	20	$50	$1000
Costo Total			$7000

Tabla 42 Costos de capacitaciones. Fuente: Shekinan

4.7.7.5. Costo Final.

En el costo final se asigna un 30% para gastos adicionales o variaciones que exista en los ítems considerados anteriormente, dentro de posibles gastos están aplicaciones que no dependen de la UIDE directamente de la UIDE sin embargo la afectación del servicio que estas proveen es directo a las actividades de la Universidad. Las aplicaciones o servicios que son dados por empresas proveedoras son: Sistema de copiado e impresoras y Bibliotecas virtuales.

El detalle de inversión es el siguiente:

Detalle.	Valor
Hardware	$0,0
Software	$0,0
Recurso Humano	$2000
Capacitación	$7000
Imprevistos (30%)	$2700
Total.	$11700

Tabla 43 Valores totales a invertir. Fuente: El Autor.

4.7.8. Impacto de la implementación de IPV6

La implementación de IPv6 al igual que IPv4 actúa sobre la capa de red sin que existan cambios en las capas subsiguientes.

Dentro de la implementación se considera los siguientes puntos con el fin de reducir el impacto durante este proceso.

- Manejar un presupuesto ya definido con el fin de que no existan costos inflados que ponga en riesgo la implementación.
- La migración se la debe realizar de manera gradual.
- Los equipos que no soporten IPv6 deben ser actualizados de tal manera cumplan los requisitos necesarios para el buen funcionamiento de la implementación.
- La coexistencia debe ser la prioridad en la implementación de IPv6.

4.7.9. Riesgos del proyecto.

Para la implementación se toma en cuenta los siguientes factores como posibles riesgos que pueden afectar este proceso como son:

- Perdida de información.
- Daños físicos en los equipos.
- Incompatibilidad de hardware.
- Inestabilidad de las aplicaciones.
- Problemas de funcionamiento del S.O.
- Incompatibilidad de Aplicaciones.
- Falta de compromiso del personal técnico.
- Fallas de instalación y conexión de los equipos de red.
- Insuficiencia en la capacitación del personal técnico.

4.7.10. Riesgos de no implementar IPv6.

Si la institución se queda atrasada en la adopción de IPv6 puede tener problemas para utilizar determinados recursos en Internet ya que se espera que con el tiempo las aplicaciones en Internet pasarán a funcionar únicamente (o mejor) en IPv6. Si cualquiera de estas aplicaciones se vuelven importantes para el desarrollo de la UIDE, los competidores que ya está conectado con IPv6 tendrán una ventaja competitiva importante.

Otro punto a considerar es la pérdida de oportunidades para la institución en el desarrollo de aplicaciones innovadoras basadas en IPv6.

También existe el riesgo que la implementación de IPv6 falle, es decir, que se agoten las direcciones IPv4 antes que IPv6 esté bien difundido. Si esto sucede, los costos de implementación de nuevas redes conectadas a Internet pueden aumentar. El uso de NAT también aumentará, encareciendo la administración de la red y aumentando los costos en la creación de aplicaciones extremo a extremo.

Conclusiones.

Con el estudio del estado del arte se establecen los diversos pilares teóricos bajo los cuales trabajan los protocolos de internet al momento existentes, de igual manera el estudio permite concluir cual es la tendencia de uso debido a las nuevas necesidades existentes en el uso de la WEB, esto permite generar futuras investigaciones en las redes de comunicación.

El análisis que se ha realizado en este trabajo, ayuda a aclaras las diferencias existentes entre IPV4 e IPV6, siendo la característica más importante de IPV6 la cantidad de combinaciones posibles en lo que respecta a direcciones que ofrece este protocolo, esto ayuda a la UIDE al ampliar el espectro de objetos que pueden conectarse a la red, solventando los inconvenientes de IPV4 en relación al aumento continuo de dispositivos en la red.

Para el desarrollo de este trabajo se analizó varios aspectos sobre la red actual de la Universidad Internacional del Ecuador detectando factores en hardware, software y económicos que permiten a la UIDE ejecutar el plan de migración a IPV6 manteniendo siempre la coexistencia con IPV4, de este estudio se ha podido establecer los puntos críticos que deben ser tomados en cuenta en la migración de tal manera que no va a existir riesgo en los servicios necesarios para operación de la institución.

La red de datos de la Universidad Internacional del Ecuador al momento opera bajo el protocolo IPV4, la versión IPV6 operara sobre esta red, los dos protocolos tienen una funcionalidad similar, y al usar el mismo medio de trasmisión no se existirá

inconvenientes pues los principios son semejantes y los datos que en mayor parte se enviaran al usuario final están manejan los protocolos HTTP, DNS, FTP.

Tras el análisis de los diversos métodos de migración existentes se acoge para el desarrollo de este trabajo el recomendado por la IETF para un plan que se desarrollara por faces en cada nodo existente y tomando en cuenta el diseño de la red de datos de la UIDE, este método se basan en el uso de dos pilas de protocolo “Dual stack”, que trabajara transmitiendo paquetes IPV6 sobre la infraestructura IPV4.

El método de migración dual stack al ejecutar las dos pilas de protocolos de manera simultánea en cada nodo de la red, permite la navegación web con soporte para IPv6 o IPv4 sin que exista conflicto alguno.

La capacidad de autoconfiguración va a permitir a la UIDE que la información del prefijo necesaria para la configuración de nuevos equipos en la red sea propagada desde los equipos de la parte activa de la red sin necesidad de realizar este proceso manualmente.

Los procesos de migración diseñados en este plan se los concibió de forma sencilla de tal manera que existan la menor cantidad de problemas en las aplicaciones, equipos y usuarios de cada nodo en la red una vez que se ejecute la migración.

Con la migración a IPV6 la red de datos mejorar su calidad con respecto a rapidez, seguridad y fiabilidad tanto en las aplicaciones que al momento son de uso cotidiano en las labores de la UIDE así como en nuevas aplicaciones que requieran mayor proceso de datos en tiempo real. El proceso de transición a pesar de largo, complejo y

un costo elevado es necesario para las nuevas normas de calidad exigidas en los procesos internos de la Institución.

Tras el análisis de los fundamentos teóricos de los cuales depende tanto el protocolo IPV4 – IP6 y su coexistencia se ha podido desarrollar el plan de migración de IPV4 to IPV6 dentro de la matriz de la Universidad Internacional del Ecuador lo que beneficia a los tanto a estudiantes como docentes cuyo número ha ido en aumento considerablemente y el servicio tanto de internet y de aplicaciones se podría ver amenazado por las limitaciones de IPV4.

Recomendaciones.

Es importante dentro del análisis identificar los servicios que son de prioridad y trabajaran bajo ipv6 de tal manera se pueda configurar tanto los equipos de la parte activa de la red así como también los servidores.

El desarrollo del plan de migración debe considerar un diseño de la red IPV6 donde la configuración sea simple y exista la documentación necesaria de tal manera esta red que contenga como protocolo único IPV6 pase a la activación en el momento que sea necesario.

Es necesario tener claro cómo se encuentra la estructura de red de IPv4 pues sobre esta se distribuirá IPV6 de esta manera se aproveche al máximo este factor al realizar el direccionamiento.

Es recomendable que el proceso de migración se continúe en las sedes de tal manera se puedan realizar las configuraciones del caso en servidores y equipos de red para poder proporcionar los servicios a toda la UIDE con la misma calidad que dispone el protocolo IPV6.

La mayor parte de los sistemas de uso general de la UIDE cuenta con soporte IPv6, sin embargo se debe establecer como prioridad que los administradores de red conozcan las implicaciones de seguridad que maneja IPV6, esto previo a la ejecución del plan de migración de tal manera se evite impactos negativos en la redes.

Bibliografía.

http://10conceptos.com/concepto-de-ipv6/
http://www-2.dc.uba.ar/materias/tc/downloads/apuntes/ipv4.pdf
http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html
http://ciclodeinformatica.blogspot.com/2013/04/protocolo-ipv4-caracteristicas-y.html
http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html
http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4
http://los9mm.over-blog.es/article-29399073.html
http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4.
http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4
http://los9mm.over-blog.es/article-29399073.html
http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4
https://www.freebsd.org/doc/es/books/handbook/network-ipv6.html
http://www.elmundo.es/imasd/ipv6/queesipv6.html
http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6
http://www.ramonmillan.com/tutoriales/ipv6_parte1.php
http://technet.microsoft.com/es-es/library/cc784659(v=ws.10).aspx
http://tools.ietf.org/html/rfc4443
http://technet.microsoft.com/es-es/library/cc776494(WS.10).aspx
http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html
http://www.franciscosepulveda.eu
http://entendiendo-redes-ae.blogspot.com/2010/07/aspectos-basicos-de-ospfv3.html
http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6
http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf
http://www.rau.edu.uy/ipv6/queesipv6.htm
http://msdn.microsoft.com/es-es/library/cc758763(v=ws.10).aspx
http://alejandromartinezclase.wordpress.com/ipv6-caracteristicas-ventajas-y-desventajas/
http://www.networkworld.es/archive/de-ipv4-a-ipv6-asegurando-la-coexistencia
http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-47/index.html
http://www.tlalpan.uvmnet.edu/oiid/download/T%C3%BAneles%20en%20IPv6%20gesti%C3%B3n%20PO%20TI.pdf
http://ipv4to6.blogspot.com/p/tunelizacion-ipv6.html
http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf
http://msdn.microsoft.com/es-es/library/cc736336%28v=ws.10%29.aspx
http://msdn.microsoft.com/es-es/library/cc736336%28v=ws.10%29.aspx
http://www.tlalpan.uvmnet.edu/oiid/download/T%C3%BAneles%20en%20IPv6%20gesti%C3%B3n%20PO%20TI.pdf
http://repositorio.utn.edu.ec/bitstream/123456789/619/3/CAPITULO3.pdf
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html
http://lisp.cisco.com/lisp_over.html
http://www.ipv6.mx/index.php/component/content/article/318-transicion-ipv6-cisco-lisp-vs-servicios-de-tunel

http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/869/2145
http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/869/2145
http://www.angelfire.com/cantina/oronaweb/topologia.htm
http://www.yealink.com/sp/product_info.aspx?ProductsCateID=650&CateId=622&BaseInfoCateId=650&Cate_Id=650&parentcateid=622
http://www.telconet.net/telconet/telconet
http://www.mintic.gov.co/portal/604/w3-article-5866.html
http://www.cu.ipv6tf.org/soipv6.htm
http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106-enterprisenotreadyipv6
http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/338-como-proteger-el-cambio-a-redes-ipv6

Glosario de palabras

A

ACL
Access control list 51
ARP
Address Resolution Protocol o, en español, Protocolo de resolución de direcciones 29, 163

B

BootP
Bootstrap Protocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente 28
Broadcast
s una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores 15

C

CEDIA
Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado 5
CIDR
Enrutamiento entre dominios sin clases 18, 48

D

DNS
Sistema de nombres de dominio 42

G

gateway
Puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación 25

I

IANA
Internet Assigned Numbers Authority 1
ICANN
Corporación de Internet para los Nombres y Números Asignados 25
ICMPv6
Protocolo de Mensajes de Control de Internet Version 6 39
IDF
Servicios de distribución intermedia 100
IETF
Internet Engineering Task Force (IETF) (en español Grupo de Trabajo de Ingeniería de Internet). 27
interwork
Union de Redes diferentes a cualquier nivel 23
IPSec
Abreviatura de Internet Protocol security 34
IPv4

Internet Protocol version 4 1
IPV6
Internet Protocol version 6 1
ISP
Internet Service Provider 29

M

MDF
Main Distribution Frame 4

N

NAT
Network Address Translation - Traducción de Dirección de Red 27, 106

O

OSI
Open System Interconnection 8
OSPFv3
Open Shortest Path First (El camino más corto primero) 54

R

RFC
Request for Comments. (Solitud de comentarios) 1
RIR
Regional Internet registry 3

S

SSH
Secure SHell, en español 28
SSL
Secure Sockets Layer 28

T

TCP/IP
Protocolo de Control de Transmisión/Protocolo de Internet 10

U

UDP
User Datagram Protocol 10
UTP
Unshielded Twister Pair, o par trenzado sin apantallar 90

V

Vlan
Red de área local virtual 5

Anexos

Anexos

Anexo A

Características de los dispositivos.

Las versiones de los dispositivos intermedios son importantes para el desarrollo del proyecto puesto que es necesario conocer si las configuraciones necesarias para IPV6 sera soportado por el IOS.

Las versiones las podemos observar con el comando show versión.

Switch 3750.

La Versión del switch Core las muestra la figura 29.

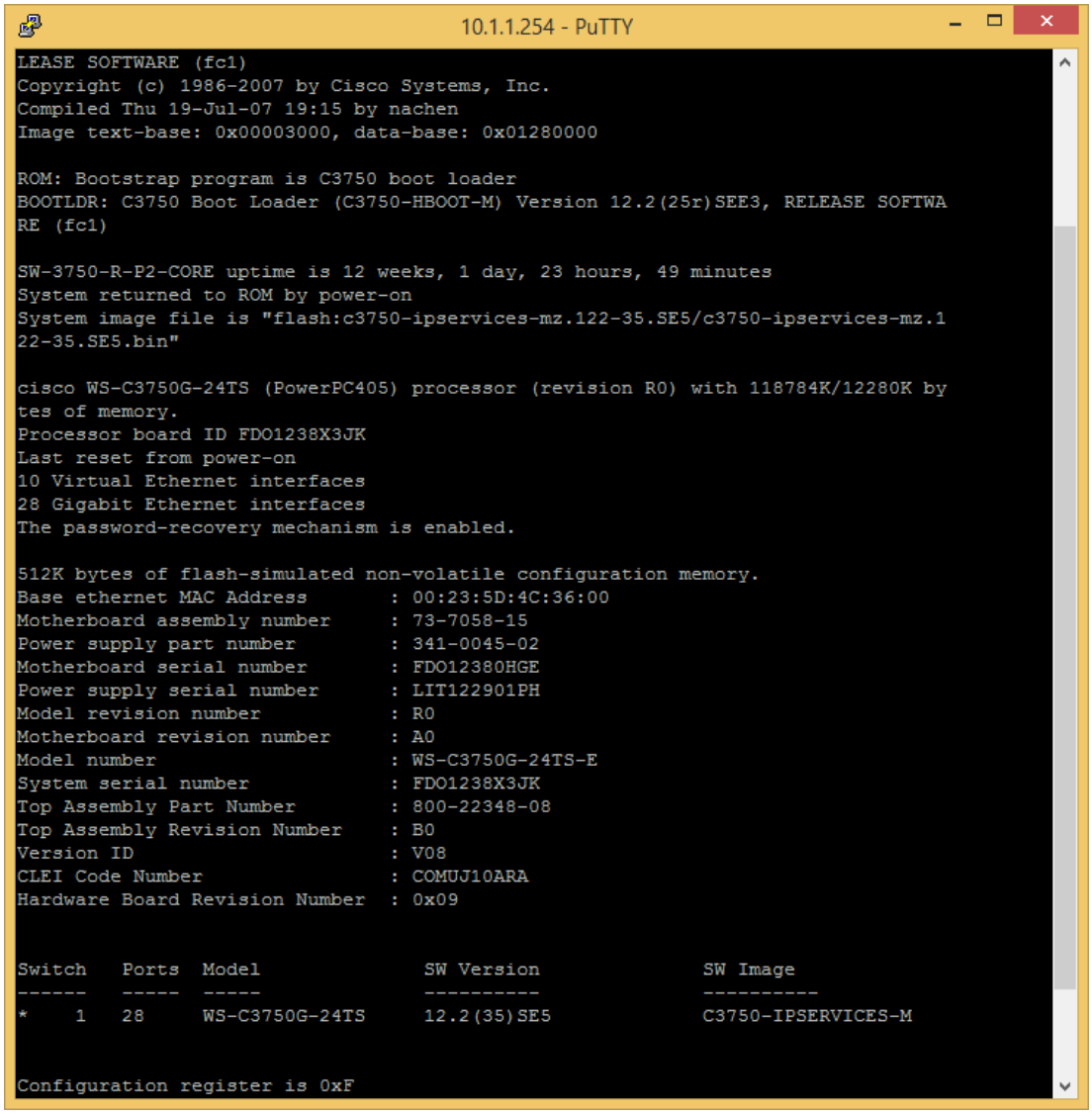


Figura 29 Versión de Switch 3750. Fuente: Datos de la UIDE.

Switch 2960-X.

La versión del switch 2960-X la presenta la figura 30 y 31.

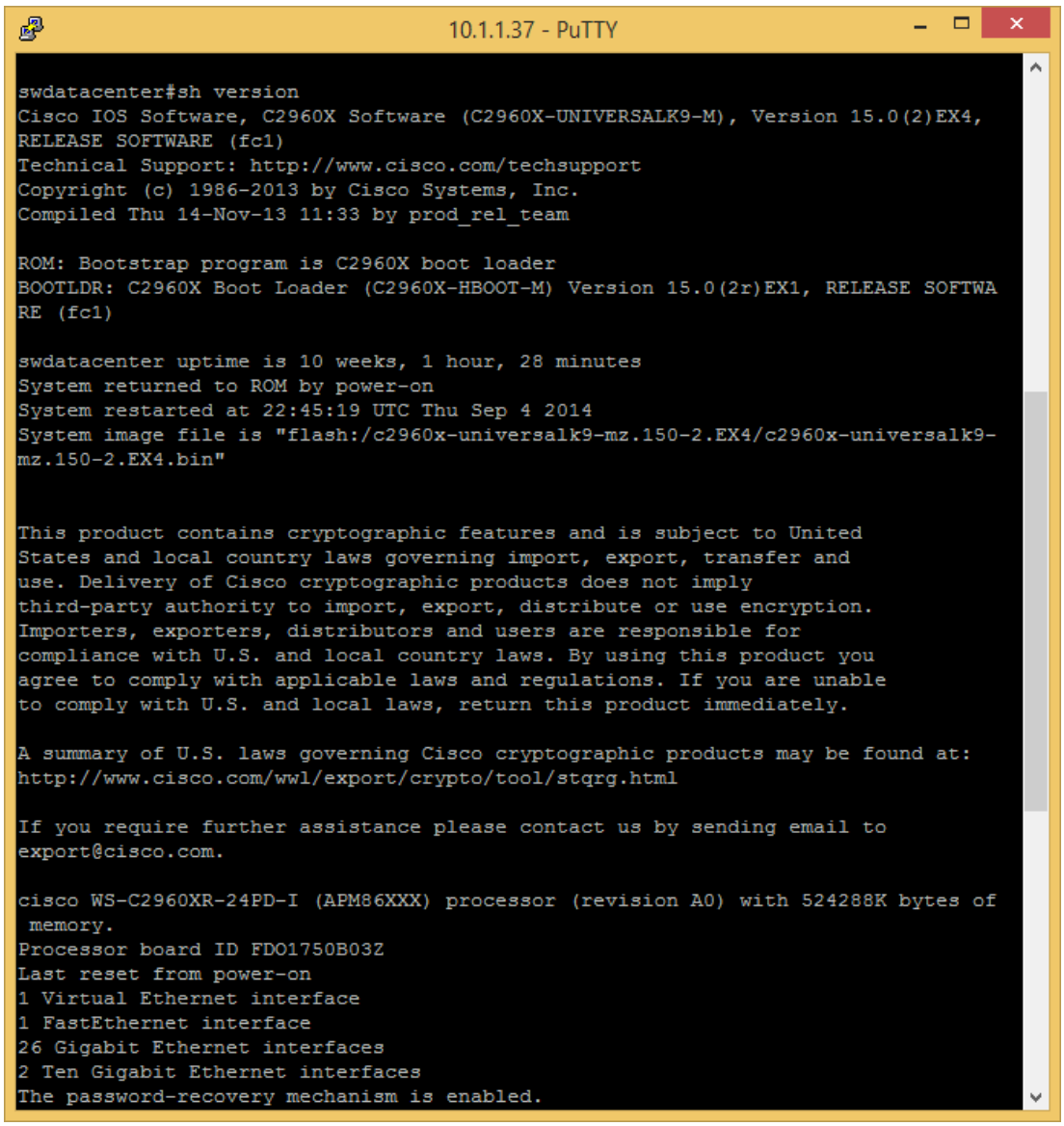


Figura 30 Versión de IOS de switch cisco 2960-X. Fuente: Datos de la UIDE.

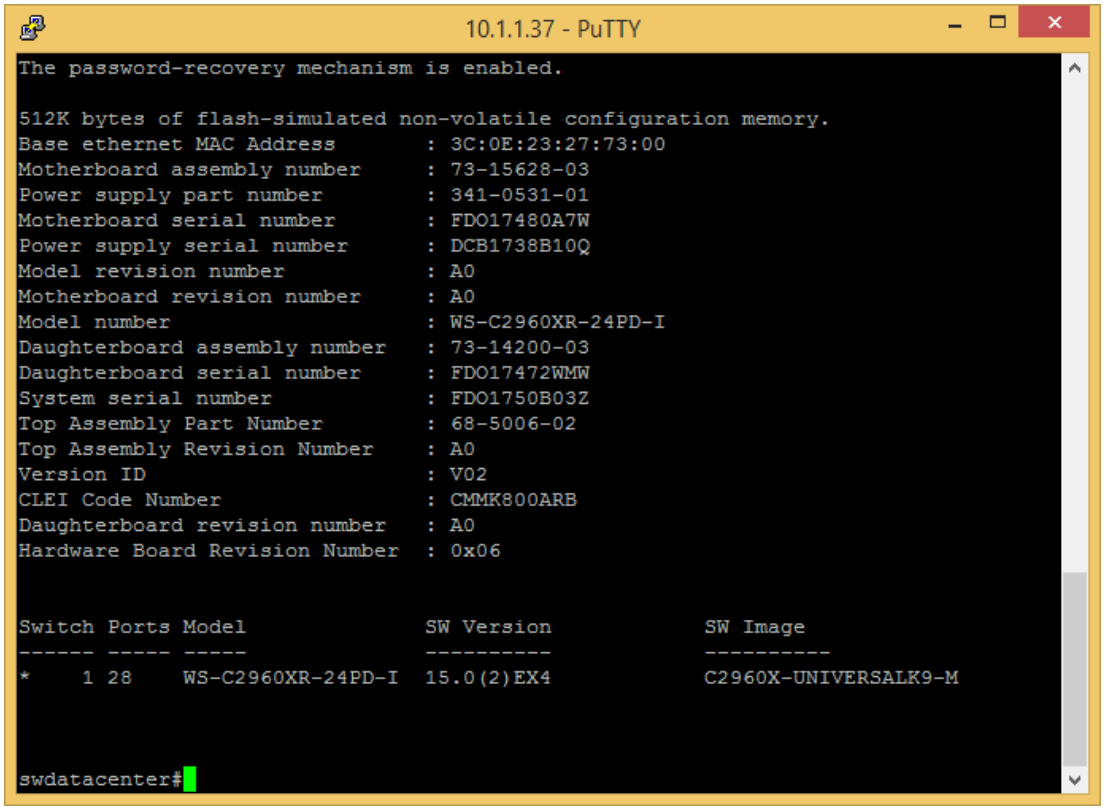


Figura 31 Versión de IOS de switch cisco 2960-X. Fuente: Datos de la UIDE.

Switch 3560.

La versión del IOS del switch 3560 se lo visualiza en la figura 32 y 33.

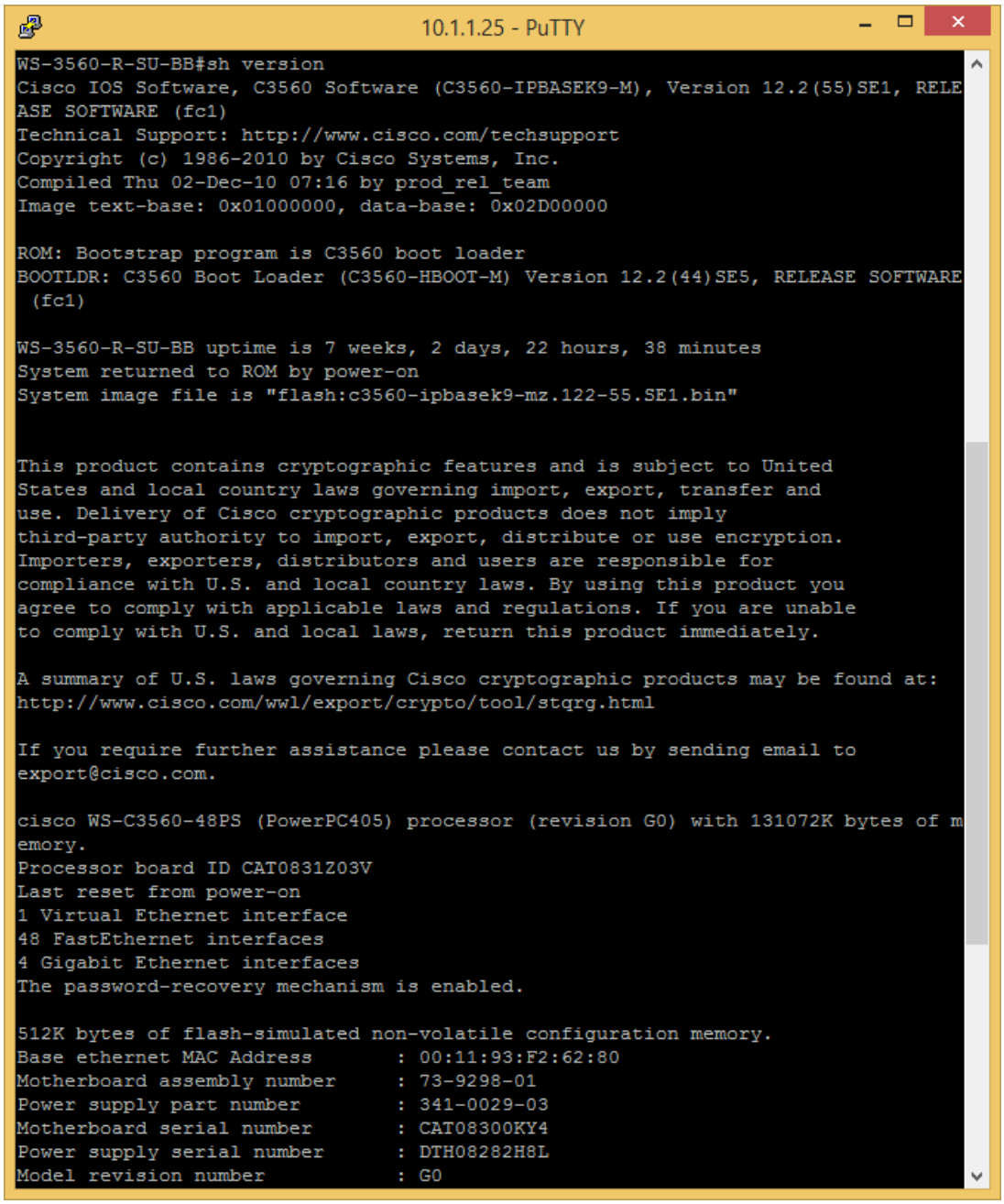


Figura 32 Versión de IOS de switch cisco 3560 Fuente: Datos de la UIDE.

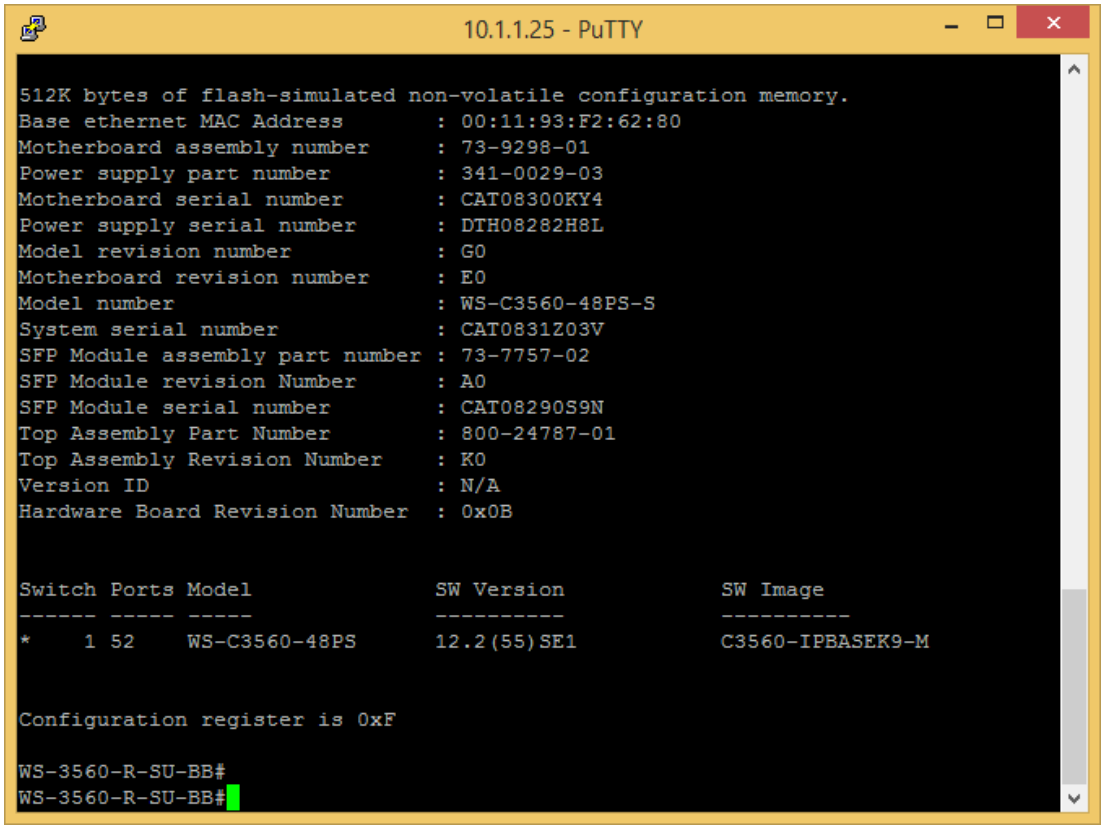


Figura 33 Versión de IOS de switch cisco 3560 Fuente: Datos de la UIDE.

Switch 2960-s

Versión de IOS de switch cisco 2960-S (figura 34 y 35).

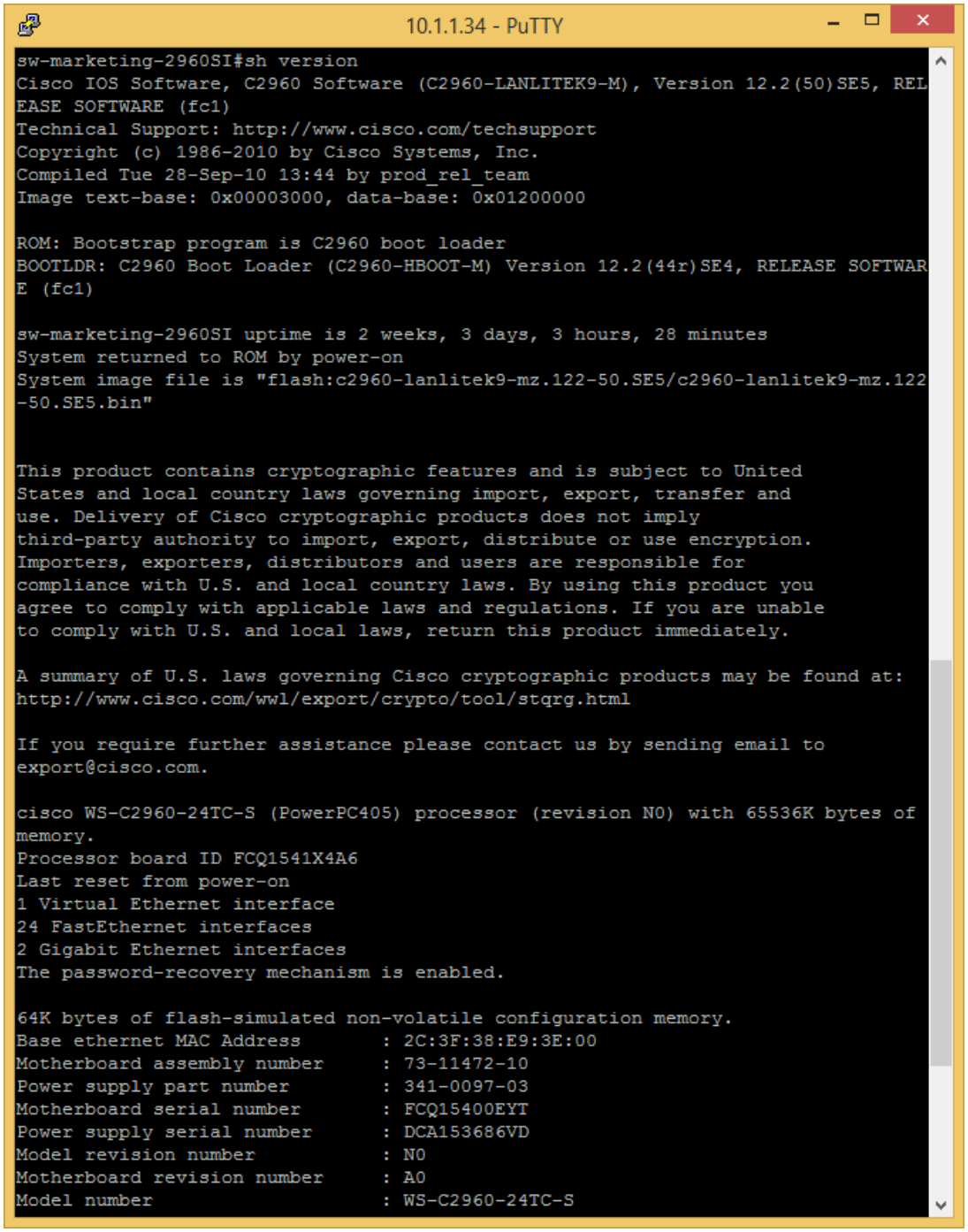


Figura 34 Versión de IOS de switch cisco 2960-S Fuente: Datos de la UIDE.

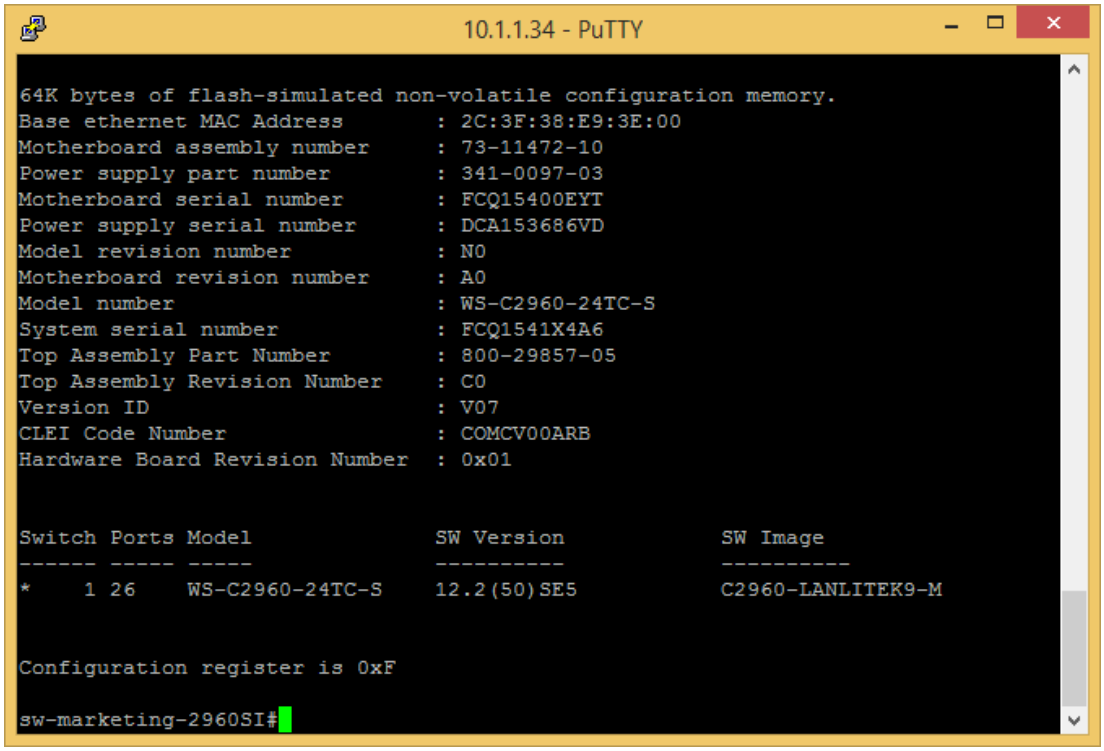


Figura 35 Versión de IOS de switch cisco 2960-S Fuente: Datos de la UIDE.

Switch 2960

La figura 36 y 37 muestran la versión del IOS del switch 2960

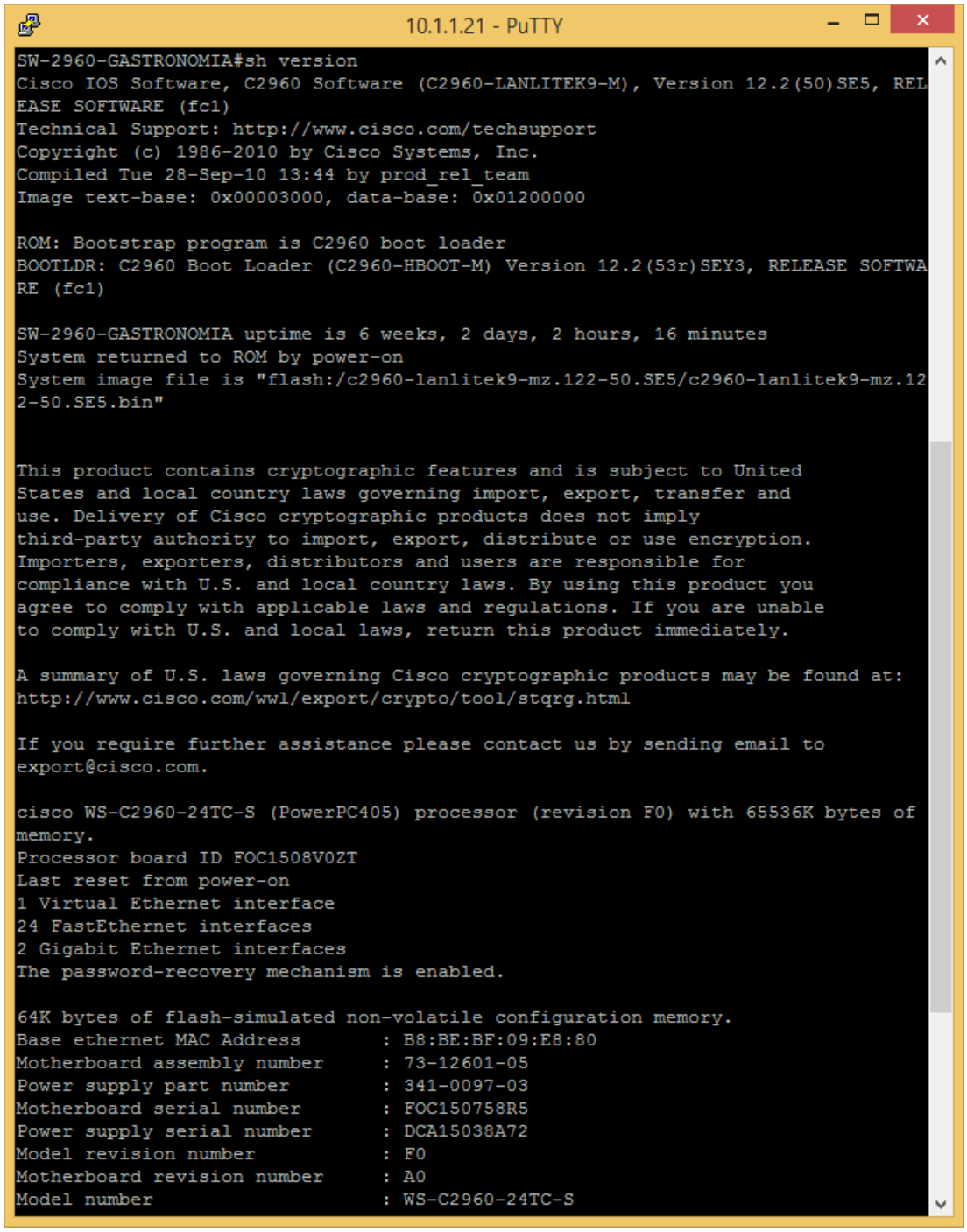


Figura 36 Versión de IOS de switch cisco 2960 Fuente: Datos de la UIDE.

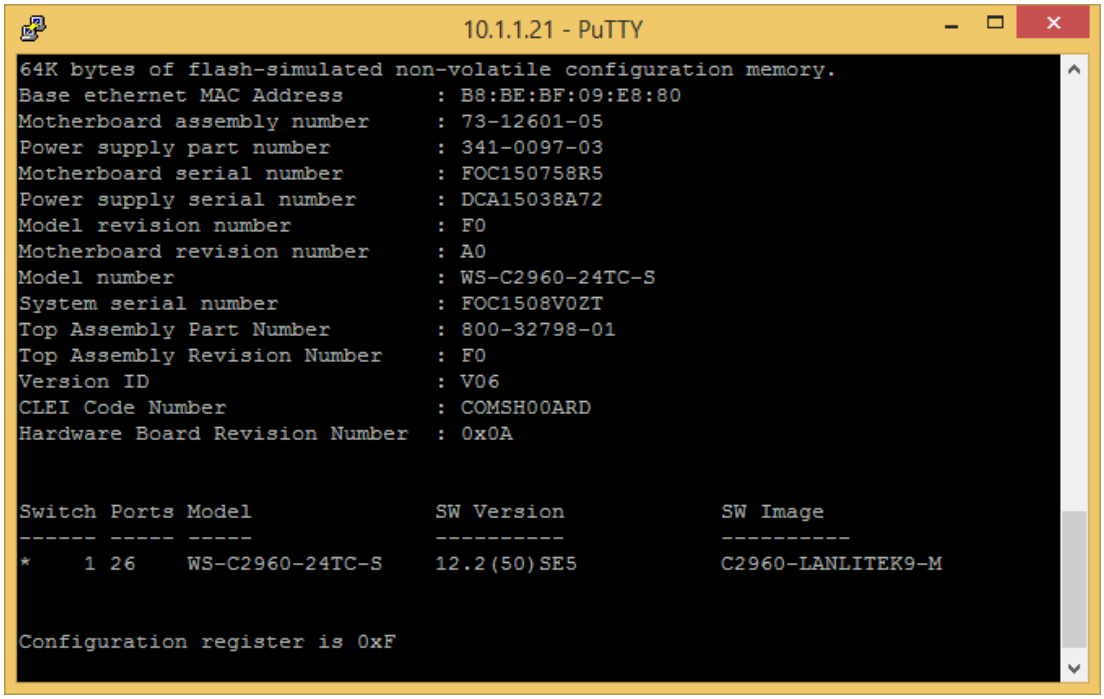


Figura 37 Versión de IOS de switch cisco 2960 Fuente: Datos de la UIDE.

Anexo B
Características de las RFC
Características de las RFC 791

INTERNET PROTOCOL

(Protocolo Internet)

DARPA INTERNET PROGRAM

ESPECIFICACION del PROTOCOLO

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. A un sistema de este tipo se le conoce como "catenet" [1]. El protocolo internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

Interfaces

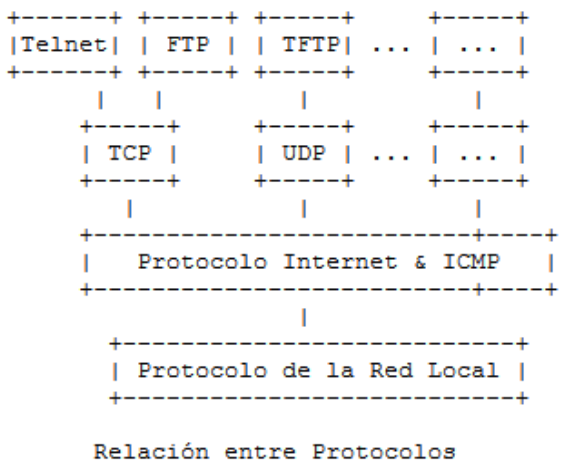
Este protocolo es utilizado por protocolos host-a-host en un entorno internet. Este protocolo utiliza a su vez protocolos de red locales para llevar el datagrama internet a la próxima pasarela ("gateway") o host de destino.

Por ejemplo, un módulo TCP llamaría al módulo internet para tomar un segmento TCP (incluyendo la cabecera TCP y los datos de usuario) como la parte de datos de un datagrama internet. El módulo TCP suministraría las direcciones y otros parámetros

de la cabecera internet al módulo internet como argumentos de la llamada. El módulo internet crearía entonces un datagrama internet y utilizaría la interfaz de la red local para transmitir el datagrama internet.

Relación con Otros Protocolos

El siguiente diagrama ilustra el lugar del protocolo internet en la jerarquía de protocolos:



Relación entre Protocolos

El protocolo Internet interactúa por un lado con los protocolos host-a-host de alto nivel y por otro con el protocolo de la red local. En este contexto una "red local" puede ser una pequeña red en un edificio o una gran red como ARPANET.

Modelo de Operación

El modelo de operación para transmitir un datagrama de una aplicación a otra se ilustra en el siguiente escenario:

Suponemos que esta transmisión involucra a una pasarela intermedia.

La aplicación remitente prepara sus datos y llama a su módulo internet local para enviar esos datos como un datagrama y pasa la dirección de destino y otros parámetros como argumentos de la llamada.

El módulo internet prepara una cabecera de datagrama y adjunta los datos a él. El módulo internet determina una dirección de la red de área local para esta dirección internet, que en este caso es la dirección de una pasarela.

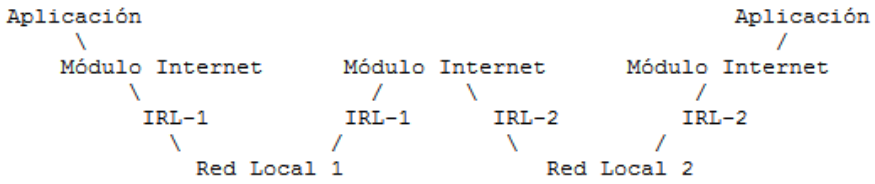
Envía este datagrama y la dirección de red local a la interfaz de red local.
La interfaz de red local crea una cabecera de red local, le adjunta l datagrama y entonces envía el resultado a través de la red local.

El datagrama llega a un host pasarela encapsulado en la cabecera de red local, la interfaz de red local desprende esta cabecera y dirige el datagrama hacia el módulo internet. El módulo internet determina a partir de la dirección internet que el datagrama debe ser reenviado a otro host en una segunda red. El módulo internet determina una dirección de red local para el host de destino. Llama a la interfaz de red local de esa red para enviar el datagrama.

Esta interfaz de red local crea una cabecera de red local y le adjunta el datagrama enviando el resultado al host de destino.

En este host de destino la interfaz de red local le quita al datagrama la cabecera de red local y se lo pasa al módulo internet.

El módulo internet determina que el datagrama va dirigido a una aplicación en este host. Pasa los datos a la aplicación en respuesta a una llamada al sistema, pasando la dirección de origen y otros parámetros como resultado de la llamada.



Trayectoria de la transmisión

Descripción de Funciones

La función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas. Esto se consigue pasando los datagramas desde un módulo internet a otro hasta que se alcanza el destino. Los módulos internet residen en hosts y pasarelas en el sistema internet. Los datagramas son encaminados desde un módulo internet a otro a través de redes individuales basándose en la interpretación de una dirección internet. Por eso, un importante mecanismo del protocolo internet es la dirección internet.

En el enrutamiento de mensajes desde un módulo internet a otro, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad se proporciona un mecanismo de fragmentación en el protocolo internet.

Direccionamiento

Se establece una distinción entre nombres, direcciones y rutas [4].

Un nombre indica que buscamos. Una dirección indica dónde está. Una ruta indica cómo llegar allí. El protocolo internet maneja principalmente direcciones. Es tarea de los protocolos de mayor nivel es decir, protocolos host-a-host o entre aplicaciones) hacer corresponder nombres con direcciones. El módulo internet hace corresponder direcciones de internet con direcciones de red local.

Es tarea de los procedimientos de menor nivel (es decir, redes locales o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de una longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección local (llamada el campo "resto"). Hay 3 formatos o clases de direcciones internet: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local.

Características de RFC 3024

Grupo de Trabajo de la Red de G. Montenegro, editor

Petición de Comentarios: 3024 Sun Microsystems, Inc

Obsoletes: 2344 Enero 2001

Categoría: Normas pista

Reverse Tunneling for Mobile IP, revisado

Condición de este Memo

Este documento especifica un protocolo de normas de Internet para la Comunidad de Internet, y solicita debate y sugerencias para Mejoras. Por favor refiérase a la edición actual del Internet Normas Oficiales de Protocolo "(STD 1) para la normalización de estado. Y la situación de este protocolo. La distribución de este memo es ilimitada.

Resumen

Mobile Protocolo de Internet (IP) utiliza un túnel de la casa a agente El nodo móvil del cuidado de la dirección, pero raramente en el reverso Dirección. Por lo general, un nodo móvil envía sus paquetes a través de un router En la red exterior, y asume que es independiente de enrutamiento Dirección de origen. Cuando esta suposición no es cierto, es conveniente Para establecer una correcta topologically invertir túnel de la atención de - Hacer frente a la casa el agente.

En este documento se propone extensiones compatibles hacia atrás-a Mobile IP Apoyo a topologically correcto invertir túneles. Este documento hace No tratar de resolver los problemas planteados por los cortafuegos situados entre Agente de la casa móvil y el nodo de la atención de la dirección.

Sección 1,3 de la especificación Mobile IP [1] se enumeran las siguientes Hipótesis:

Se supone que los datagramas IP unicast se remiten basada en la Dirección de destino en la cabecera de datagrama (es decir, no por fuente Dirección).

Debido a preocupaciones de seguridad (por ejemplo, los ataques IP spoofing), y De conformidad con el RFC 2267 [8] y [3] CERT a la consola de esta Efecto, routers que romper esta hipótesis son cada vez más Común.

En presencia de tales routers, el origen y el destino de la propiedad intelectual En la dirección de un paquete debe ser topologically correcta. Los comunicados Cumple con este túnel, ya que sus puntos finales (agente de la dirección y el hogar Cuidado-de dirección) estén debidamente asignadas las direcciones de sus respectivas Lugares. Por otra parte, la dirección IP origen de un paquete Transmitido por el nodo móvil no corresponde a la red Prefijo de donde emana.

Este documento analiza topologically correcto invertir túneles. Mobile IP hace dictar el uso de los túneles de invertir en el contexto de Datagrama de enrutamiento multicast móviles y routers. Sin embargo, la fuente Dirección IP está ajustado en el nodo móvil de la casa de dirección, de modo que estos túneles Topologically no son correctos.

Aviso de que hay muchos usos para invertir independientemente de los túneles Topológico su corrección:

- Mobile routers: invertir los túneles de obviar la necesidad de recursivo Tuneladora [1].

- Multicast: invertir los túneles que un nodo móvil fuera de casa (1) a unirse a grupos de multidifusión en su red doméstica, y (2) Transmitir los paquetes de multidifusión tales que emanan de su casa Red [1].
- El TTL de los paquetes enviados por el nodo móvil (por ejemplo, cuando El envío de paquetes a otros hosts en su red propia) pueden ser tan Baja, que podría terminar antes de llegar a su destino.

Características de las RFC 3531

Esta recomendación propone un método para administrar la asignación de bits de una dirección IPv6 bloque o rango. Cuando una organización tiene que hacer una dirección para su plan de subredes o cuando un proveedor de acceso a Internet tiene que hacer una planificación de direcciones para sus clientes, este método permite a la organización aplazar la decisión final sobre el número de bits a la partición en el espacio de direcciones que tienen.

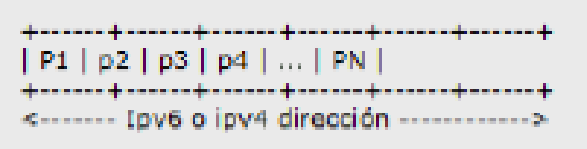
Este sistema es aplicable a cualquier esquema de direccionamiento de bits utilizando bits con particiones en el espacio, pero su primer uso es para IPv6, la RFC 3531 se ha desarrollado desde abril del 2003.

Las direcciones IPv6 tienen una estructura flexible para abordar las cesiones. Esto permite a los proveedores de servicios de Internet, diseñadores de red y otros asignar rangos de direcciones a las organizaciones y redes basadas en diferentes criterios, como el tamaño de las redes **B.2.1 Esquema**

Se define las partes de la dirección IP como p1, p2, p3,... PN en fin, de modo que una dirección IP se compone de estas partes contiguas.

Las fronteras entre cada parte están basadas en el prefijo asignado por el próximo nivel de autoridad. La parte p1 es la parte izquierda, probablemente asignada a un registro, la parte p2 puede ser asignada a un gran servicio de Internet proveedor o de un registro nacional. La parte p3 puede ser asignada a un gran cliente o un proveedor menor, etc.

Cada parte puede ser de diferente longitud.



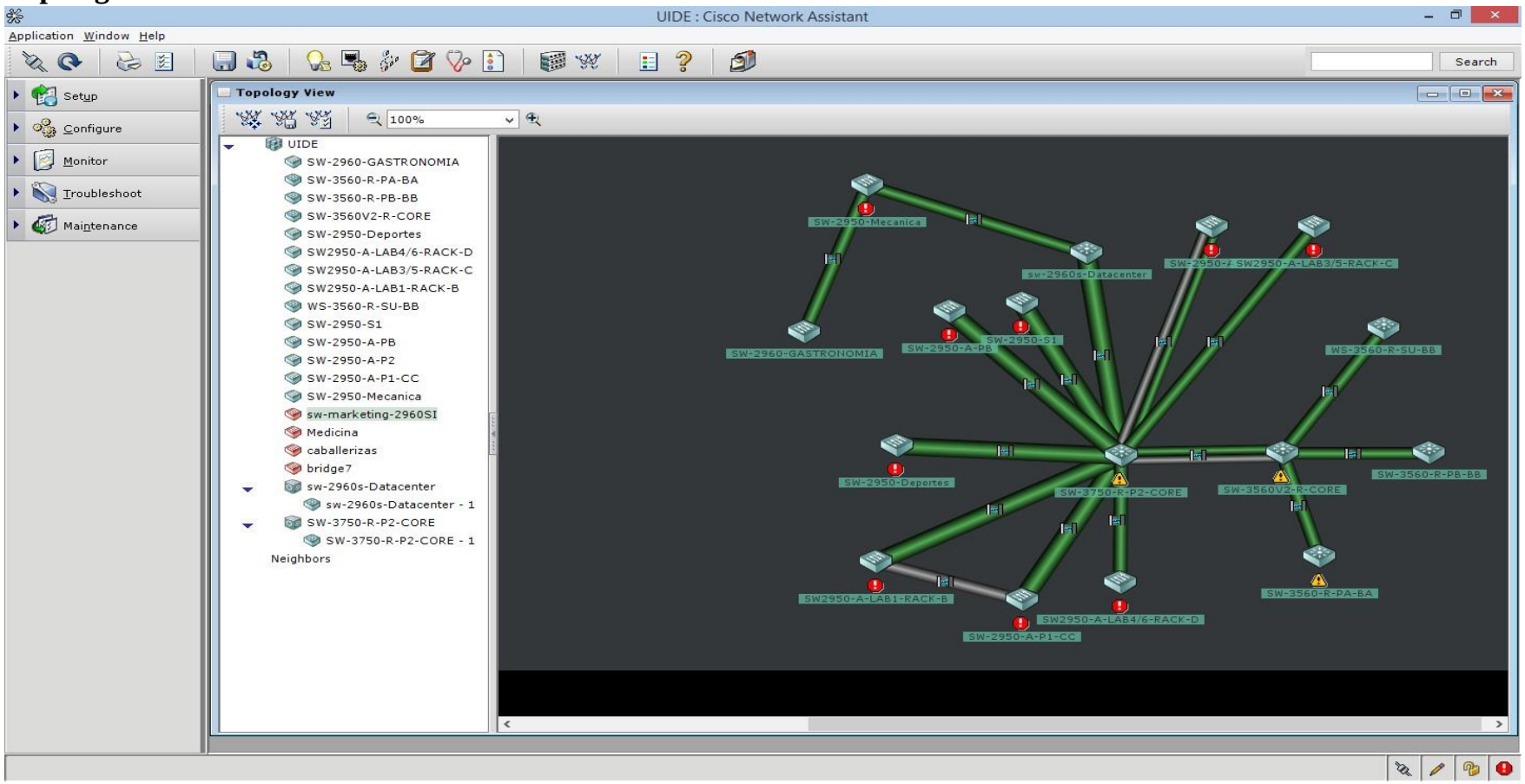
El algoritmo de asignación de direcciones es el siguiente:

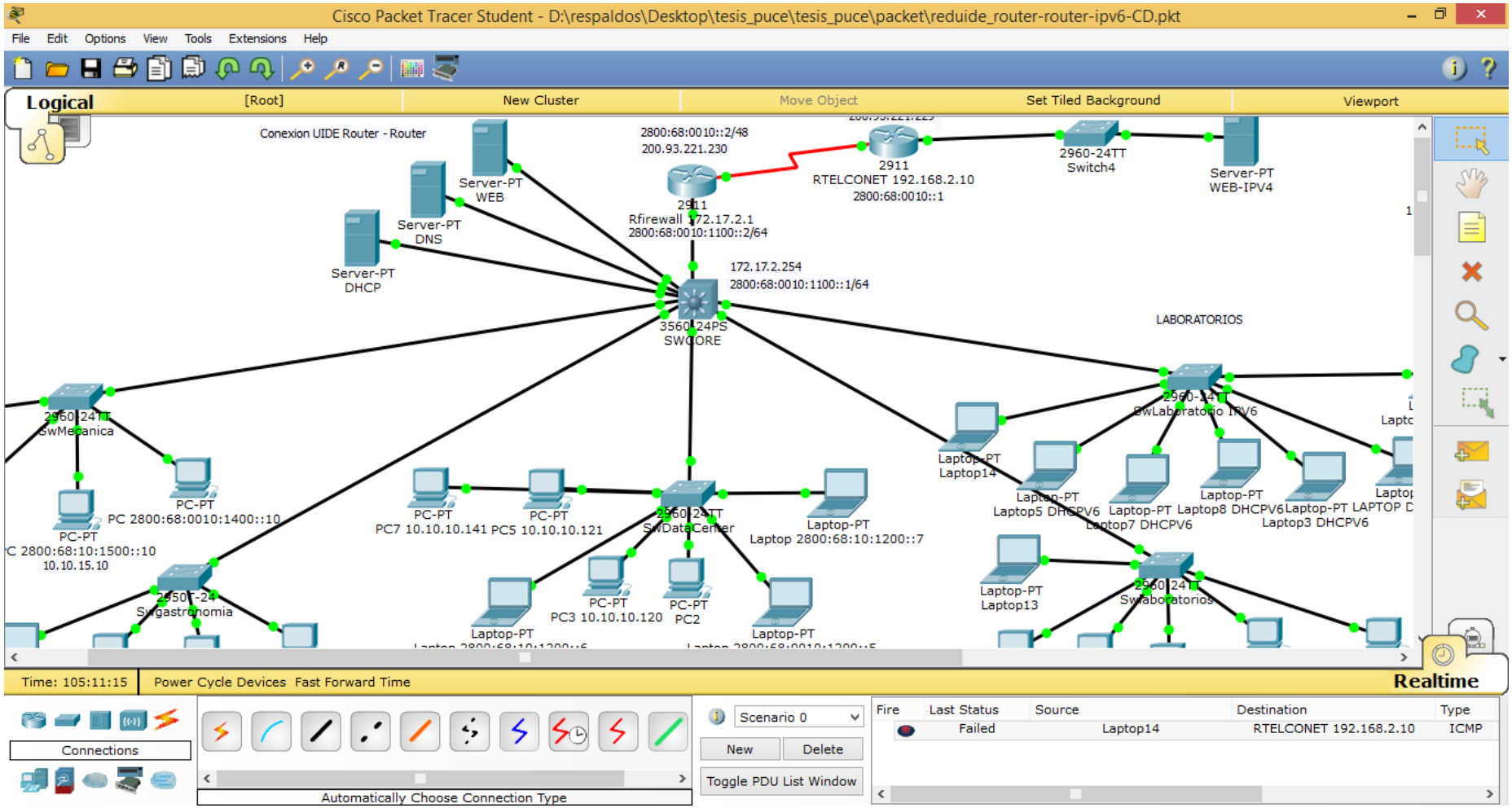
- Para la parte izquierda (p1), asignar direcciones utilizando los bits de la izquierda primero.
- Por la parte derecha (pN), asignar direcciones utilizando los bits de la derecha primero.
- Para todas las otras partes (en el centro), previamente establecer un límite arbitrario (prefijo) y luego asignar direcciones utilizando el centro de bits de la primera parte que se les asigne.

Este algoritmo crece en bits asignados de tal manera que se mantiene sin asignar los bits cerca de la frontera de las partes. Esto significa, que el prefijo entre dos partes puede cambiarse hacia adelante o hacia atrás.

Anexo C.

Topología vista de Cisco network




Cisco Packet Tracer Student - D:\respaldos\Desktop\tesis_puce\tesis_puce\packet\reduide_router-router-ipv6-CD.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Conexion UIDE Router - Router
Server-PT WEB
Server-PT DNS
Server-PT DHCP
2800:68:0010::2/48
200.93.221.230
2911
Rfirewall 172.17.2.1
2800:68:0010:1100::2/64
2911
RTELCONET 192.168.2.10
2800:68:0010::1
2960-24TT Switch4
Server-PT WEB-IPV4
172.17.2.254
2800:68:0010:1100::1/64
3560-24PS SWCORE
LABORATORIOS
2960-24TT SwMecanica
PC-PT
PC 2800:68:0010:1400::10
PC-PT
C 2800:68:10:1500::10
10.10.15.10
PC-PT PC7 10.10.10.141
PC-PT PC5 10.10.10.121
2960-24TT SwDataCenter
Laptop-PT Laptop 2800:68:10:1200::7
PC-PT PC3 10.10.10.120
PC-PT PC2
Laptop-PT
Laptop-PT Laptop14
Laptop-PT Laptop5 DHCPV6
Laptop-PT Laptop7 DHCPV6
Laptop-PT Laptop8 DHCPV6
Laptop-PT Laptop3 DHCPV6
Laptop-PT Laptop13
Time: 105:11:15
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Failed
Laptop14
RTELCONET 192.168.2.10
ICMP

Anexo C.

Cronograma de actividades para la migración

Nombre de tarea	Duración	Comienzo	Fin
Plan de implementación para la migración hacia IPV6 con coexistencia de IPV4			
Capacitación del personal técnico			
Capacitación sobre IPV6	7 días	lun 02/03/15	mar 10/03/15
Adopción de una dirección IPV6			
Verificar con telconet que este activo el enlace disponible	1 día	mié 11/03/15	mié 11/03/15
Asignación de direcciones IPV6			
identificar los nodos principales en la red de la UIDE	4 días	jue 12/03/15	mar 17/03/15
Elaboración de las tablas y direcciones IPv6	8 días	mié 18/03/15	vie 27/03/15
Actualización y pruebas de los nodos para que funcionen con Ipv4/Ipv6			
Descargar actualizaciones de IOS de ser necesario en los equipos de red	5 días	lun 30/03/15	vie 03/04/15
actualización y pruebas de funcionamiento del firewall	2 días	lun 06/04/15	mar 07/04/15
actualización y pruebas de funcionamiento del SwCore	2 días	mié 08/04/15	jue 09/04/15
actualización y pruebas de funcionamiento del Swicth de acceso	2 días	vie 10/04/15	lun 13/04/15
Actualización y pruebas de funcionamiento de teléfonos IP.	2 días	mar 14/04/15	mié 15/04/15
Actualización y pruebas de funcionamiento de Access Point.	2 días	jue 16/04/15	vie 17/04/15
Selección de un protocolo de enrutamiento.			
Selección de un protocolo con las mejores características.	5 días	sáb 18/04/15	jue 23/04/15
Implementación del mecanismo de transición			
implementación del mecanismo Dual Stack	5 días	vie 24/04/15	jue 30/04/15
Pruebas de funcionamiento.	7 días	vie 01/05/15	lun 11/05/15

Habilitar los servicios IPV6 necesarios para la operabilidad.			
configuraciones de los servidores:			
Servidor Web.	4 días	jue 14/05/15	mar 19/05/15
Servidor Proxi.	4 días	mié 20/05/15	lun 25/05/15
Servidor Archivos.	4 días	mar 26/05/15	vie 29/05/15
Servidor Antivirus.	4 días	lun 01/06/15	jue 04/06/15
Servidor de desarrollo.	4 días	vie 05/06/15	mié 10/06/15
Servidor Biblioteca.	4 días	jue 11/06/15	mar 16/06/15
Servidor de Aplicaciones.	4 días	mié 17/06/15	lun 22/06/15
Servidor de base de datos.	4 días	mar 23/06/15	vie 26/06/15
Servidor de correo electrónico.	4 días	lun 29/06/15	jue 02/07/15
Habilitar Ipv6 en los equipos de los usuarios.			
Habilitar DHCP en el router principal	3 días	mar 30/06/15	jue 02/07/15
Configuración y pruebas de funcionamiento en cada pc.	8 días	vie 03/07/15	mar 14/07/15
Capacitación para los usuarios de red.			
Elaboración de cronograma de capacitaciones.	5 días	mié 15/07/15	mar 21/07/15
Capacitación área de sistemas	1 día?	mié 22/07/15	mié 22/07/15
Capacitación área administrativa	1 día	jue 23/07/15	jue 23/07/15
Capacitación DTC.	1 día	vie 24/07/15	vie 24/07/15
Capacitación a estudiantes.	1 día	lun 27/07/15	lun 27/07/15
Capacitación a sistemas.	1 día	mar 28/07/15	mar 28/07/15